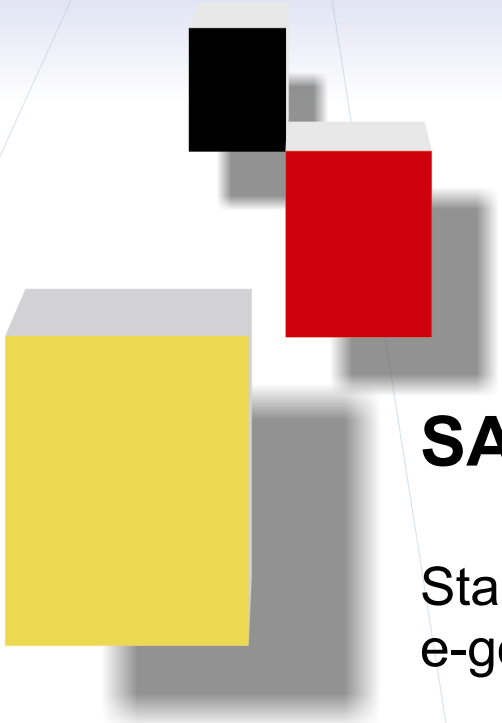
Bundesministerium
des Innern



SAGA

Standards and Architectures for e-government Applications

Version 2.0

Koordinierungs- und Beratungsstelle der Bundesregierung für Informationstechnik in der Bundesverwaltung im Bundesministerium des Innern

KBSt

KBSt Publication Series
ISSN 0179-7263
Volume 59
December 2003

KBSt Publication Series
Volume 59
ISSN 0179 - 7263

This volume was prepared by the KBSt unit at the Federal Ministry of the Interior in co-operation with the German Federal Office for Information Security (BSI) and]init[AG.

Editor:]init[AG, Berlin

Contact:

Federal Ministry of the Interior
Unit IT2 (KBSt)
11014 Berlin, Germany

E-mail: IT2@bmi.bund.de
Telephone: +49 1888 681-0
Fax: +49 1888 681-2782

Homepage and download of the digital version: http://www.kbst.bund.de/saga

SAGA

Standards and Architectures for e-government Applications
Version 2.0

December 2003

Published by the

Federal Ministry of the Interior

Word of thanks

The Co-ordinating and Advisory Agency of the Federal Government for Information Technology in the Federal Administration (KBSt) and the authors would like to thank all the members of the SAGA expert circle for their support during the preparation of this SAGA version.

We would also like to extend our thanks to all the participants in the SAGA forum whose committed comments constituted a valuable contribution towards updating the document.

Introduction:

This document presents standards, processes, methods and products of state-of-the-art IT development for e-government applications in concise form. Due to the nature of this subject, experts in this sector use many abbreviations and, mostly English, acronyms. Some of these names are protected by copyright and/or registered trademarks or products of certain manufacturers or standardisation organizations at a national and international level.

In the interest of a simple structure, copyright and source references of this kind were generally omitted. **The use of a "name" or acronym in this document does not mean that they are free from copyrights or intellectual property rights of third parties.**

Furthermore, neither the editor, authors or experts consulted can accept any responsibility for the technical functioning, compatibility or completeness of the standards discussed. This version 2.0 was published in December 2003. Please send any comments, amendments or corrections to: Bundesministerium des Innern, Referat IT2 (KBSt). These comments, amendments or corrections can also be published on the forum at: http://www.kbst.bund.de/saga.

Some of the standards discussed are inseparably linked to licensed products. Our recommendation should be understood to be of a purely technical nature. Whether and at which conditions (single/group license) a product can be economically used must be checked from case to case.

Version numbers are stated when they are relevant in the specific context discussed. Failure to state a version number does, however, not imply conformity. If no version numbers of standards are stated, the version which is most stable from a market point of view should be used, even though this is not necessarily the latest version.

The authors permit the further use of this document – even in part – on condition that it is cited as the source.

Contents

0 Revision history and status

This document, version 2.0, is a released publication of SAGA (Standards and Architectures for e-government Applications) and is binding.

0.1 Amendments to version 1.1

This document is based on the first released publication of SAGA in its version 1.1. Besides parallel monitoring of standard development trends, existing sections were amended, new sections were added and the document was given a new structure.

a. Explanation of the relationship between SAGA and other e-government documents (refer to section 1.5, page 17)
b. Introduction of an extended classification of standards with white list, grey list and black list (refer to section 2.2 "Classification and life cycles of standards", page 23)
c. Introduction of templates for a SAGA conformity declaration (refer to section 2.3.2 "Conformity declaration", page 27 and Appendix C "Templates for a SAGA conformity declaration", page 163)
d. Application of the RM-ODP[1] architecture model to German e-government; with the resultant new chapters as follows:
    i. Chapter 4 "Enterprise viewpoint: fundamentals of e-government" page 37 and following
    ii. Chapter 5 "Information viewpoint: schema repository" page 51 and following
    iii. Chapter 6 "Computational viewpoint: reference software architecture" page 53 and following
    iv. Chapter 7 "Engineering viewpoint: reference infrastructure" page 65 and following
e. Re-structuring of SAGA according to the RM-ODP model; especially former section 5.3 "Technical and specialized processes and data models" was distributed to the enterprise viewpoint (section 3.2, page 32), the information viewpoint (section 3.3, page 33) and the technology viewpoint (sections 8.1 and 8.2 page 71) and following.
f. The call center is no longer treated as an independent basic component. The results of a survey suggested a potential volume of one to six million calls per annum. In view of the financial and manpower requirements, a call center scenario with a high degree of automation is aimed at. A knowledge-based online information system as part of a portal could, for example, answer questions from Internet users and serve as a tool for information offices of public agencies.

[1] Refer to chapter 3 "Architecture model for e-government applications", page 31

g. A more detailed description of basic components of the BundOnline 2005 and the inclusion of infrastructure components and "one for all" services (refer to Appendix A "Basic modules of the BundOnline initiative", page 111). Business cases rather than the basic components themselves were classified. When a particular scenario applies to an e-government application, the use of this basic component can, for example, become mandatory in such a case.
h. Example of an online service which uses multiple basic components in Appendix B on page 159
i. An alphabetic list of all classified standards in Appendix E on page 171 instead of the overview at the beginning (sorted according to classification) and at the end (sorted according to subjects) of SAGA 1.1

Furthermore, SAGA 1.1 was the subject of intense discussion with experts from the federal and federal-state governments, municipal administrations, representatives of the business community and in the public SAGA forum. Numerous suggestions and critical comments were included in this update of the document.

0.2 Future issues

The following issues will be further scrutinised and dealt with in more detail:

a. Stronger consideration of the requirements of federal states and municipalities
b. Rules and procedures for SAGA conformity tests
c. Technical and specialized process and data models
d. Integration of first practical experience with the application of SAGA
e. New access channels, such as digital TV, game consoles, etc.

In addition to the SAGA document, the Co-ordinating and Advisory Agency of the Federal Government for Information Technology in the Federal Administration (KBSt) will offer additional information, links and tools on its website[2].

[2] Refer to http://www.kbst.bund.de/saga

1 Introduction

1.1 Background

With the Standards and Architectures for e-government Applications (SAGA), the federal government is making another important contribution towards modern and service-orientated administration.

In September 2000, Chancellor Gerhard Schröder launched the BundOnline 2005 e-government initiative with which the federal administration is pledging to provide its more than 400 Internet-enabled services online by the year 2005. User-friendly access to the administration's Internet services is to be offered to citizens and the business community. In order to control and co-ordinate the e-government initiative, the BundOnline 2005 project group was set up at the Federal Ministry of the Interior.

The project group drafted the implementation plan and updates it in annual reports to the federal cabinet. Besides the de-centralised portfolio of services to be implemented by the different public agencies, the implementation plan also defines central basic components and applications which are developed according to the "one for all" principle. In future, all these e-government applications are to be able to communicate smoothly with each other. This calls for interoperability of the BundOnline 2005 components on the basis of common architectures and standards.

The Co-ordinating and Advisory Agency of the Federal Government for Information Technology in the Federal Administration (KBSt) has formulated these standards. With participation by experts from industry and other specialists from federal, federal-state and municipal administrations, the agency first identified and evaluated existing standards. This stock-taking and evaluation then formed the basis for the first version of Standards and Architectures for e-government Applications (SAGA). The SAGA authors have since continuously updated the SAGA document in cooperation with the BundOnline 2005 project group and the expert group.

1.2 Readers of this document

SAGA is primarily designed for decision-makers in the fields of organization and information technology (e-government teams) in German administrations. The document is a guideline that serves as an orientation aid when it comes to developing concepts for technical architectures and general technical concepts for individual IT applications.

Application developers should feel free to seek further detail solutions whenever the standards presented herein are not sufficient for the implementation of technical requirements.

The federal government also sees its initiative as a contribution towards the development of e-government in Germany. The experience gathered here, as well as the basic components developed within the scope of the BundOnline 2005 project, are

designed to support all users in making their way through public agencies and to promote nation-wide e-government offers.

1.3 Purpose and structure of this document

1.3.1 Basic principles

Modern e-government calls for interoperable information and communication systems which (ideally) interact smoothly. Simple and clear-cut standards and specifications help to achieve interoperability of information and communication systems. SAGA identifies the necessary standards, formats and specifications, it sets forth conformity rules and updates these in line with technological progress.

E-government applications are developed in accordance with the following basic principles:

a. E-government applications primarily use the browser as front-end, unless the services to be implemented cannot be reasonably handled via a browser.
b. They do without active contents in order to avoid forcing users to reduce the browser's security settings and thus making damage by unsafe websites possible, or at least use only signed and quality-secured applications of the type contemplated in section 8.5 on page 78.
c. E-government applications do not store any program parts or data on the users' computers beyond the users' control.

1.3.2 Target

SAGA pursues the following aims:

a. To ensure ongoing flows of information between citizens, the federal government and its partners (interoperability)
b. To establish comparable procedures for the provision of services and for the definition of data models; federal-state governments and communal administrations have the opportunity to make use of the development results of the BundOnline 2005 initiative (re-usability)
c. To provide specifications in the form of publicly accessible documentation (openness)
d. To consider developments on the market and in the field of standardisation (cost and risk reduction)
e. To ensure the applicability of solutions against the background of changing requirements in terms of volume and transaction frequencies (scalability).

1.3.3 Tasks

SAGA is a full-scale standardisation approach for the BundOnline 2005 initiative that focuses on four development directions (tasks) as follows:

a. The definition of technical normative references, standards and architectures
b. Process modelling
c. Data modelling
d. The development of basic components

The definition of technical normative references, standards and architectures

The technical standards and architectures cover all the levels and components relevant for e-government (refer to chapter 3). They are the basis for interoperability and compatibility during the development of e-government applications and the basic components of the BundOnline 2005 initiative.

Process modelling

Process modelling means the methodical description of the e-government processes as a whole or in partial steps (refer to section 3.2, page 32), in order to:

a. Achieve a similar and comparable design and layout of the different applications
b. Ensure a high degree of re-usability of processes and systems.

Data modelling

Data modelling means the methodologically standardised description of the data communicated within the scope of e-government processes (applications) as a whole or in part (refer to section 3.3, page 33), in order to:

a. Ensure the interoperability of different – even future – applications
b. Ensure a high degree of re-usability of processes and systems.

The development of basic components

Basic components are selected, specified and implemented by BundOnline 2005 on the basis of frequently used, general process models. Five basic components and two infrastructure components have entered the implementation phase (refer to Appendix A, page 111).

1.3.4 Scope

SAGA is a standardisation project with an integrated approach that explains all the aspects necessary to achieve the aforementioned objectives. Standards or architectures not mentioned:

a. are not specific for e-government or e-commerce applications,
b. refer to a detail level other than that of the standards dealt with here in SAGA
c. are included in or referenced by the aforementioned standards
d. are too new or too controversial and are hence unlikely to become a standard in the new future

e. are not desired because they are in conflict with standards or architectures already introduced or because they restrict interoperability.

Furthermore, SAGA considers only those areas which have a major influence on the aforementioned objectives rather than all the elements of a technical architecture.

1.3.5 Structure of this document

After the introduction, chapter 2 addresses issues related to the binding nature of SAGA and to the SAGA conformity of e-government applications. Chapter 3 describes the architecture model for e-government applications. This model was also adopted for the description of the German e-government approach. Accordingly, the following chapters 4 to 9 present viewpoints of e-government in its totality.

Chapter 4 "Enterprise viewpoint: fundamentals of e-government" documents goals of German e-government, actors, roles, frames of reference, guidelines and forms of interaction (enterprise viewpoint). Chapter 5 "Information viewpoint: schema repository" deals with the work on the development of uniform and standardised data model (information viewpoint). Chapter 6 introduces a reference software architecture as a basis for developing architectures for concrete e-government applications (computational viewpoint). Chapter 7 "Engineering viewpoint: reference infrastructure" addresses the requirements for e-government computer centers and the integration of basic modules into an existing infrastructure (engineering viewpoint). Chapters 8 and 9 define the SAGA standards for the IT architecture and for ensuring data security and integrity (technology viewpoint).

Appendix A offers a detailed description of the basic modules of the BundOnline 2005 initiative. Functionalities, classified business cases (application scenarios), roadmaps and interfaces of basic components and infrastructure components are presented. What's more, the most important "one for all" services are introduced, together with information concerning the competence centers which support the development of e-government applications. Appendix B gives an example of an online service which uses multiple basic components. Appendix C contains a template for preparing a SAGA conformity declaration. Appendix D contains the references, Appendix E providing an alphabetic list of the standards referred to in chapters 8 and 9. Appendix F finally presents a list of abbreviations used in SAGA.

1.4 Services to be covered

The document defines three target groups for the federal administration's services (refer to the selection shown in Figure 1-1).

a. Government to Citizens (G2C): services which the federal government offers its citizens directly
b. Government to Business (G2B): services which the federal government offers to companies

c. Government to Government (G2G): federal government services for public agencies.

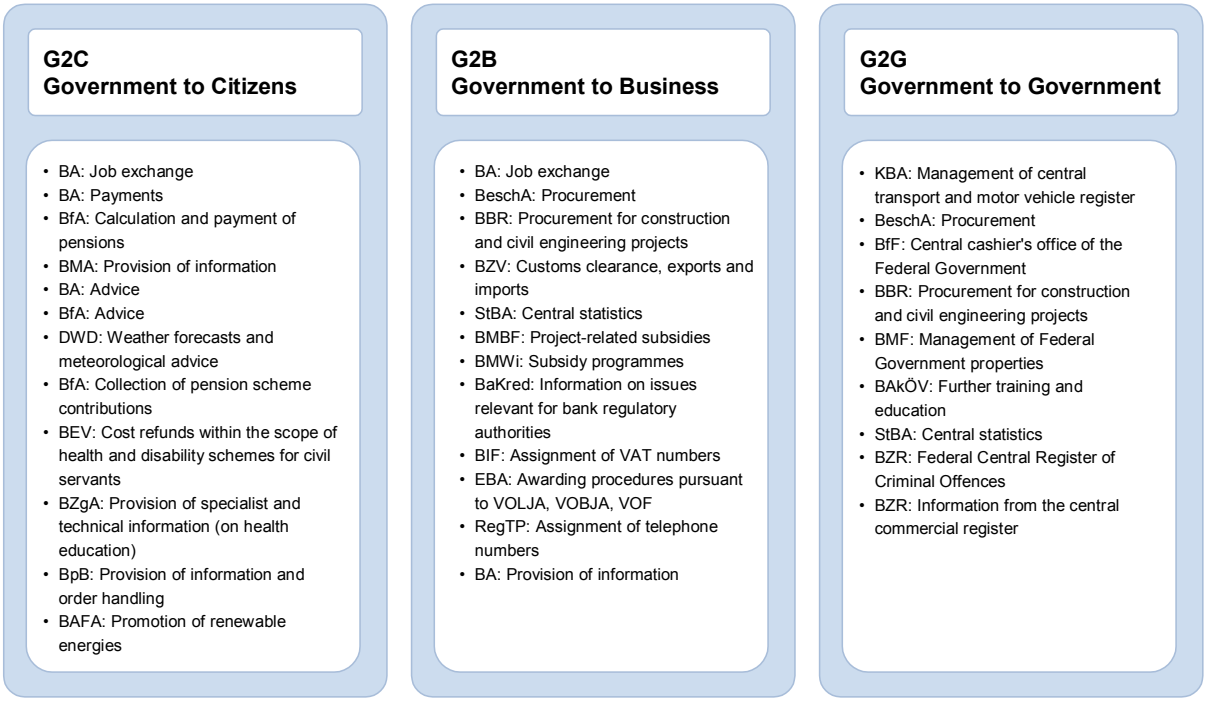


Figure 1-1: Selected services of the federal government

Around 400 services of the different Federal administrations were identified. An analysis of the services along the value chain enabled the identification of eight service types[3]. 73 percent of the services used today belong to the three following types:

a. Gathering, processing and providing information
b. Processing applications and requests sent to an administration office
c. Processing subsidy and assistance applications

1.5 Relationship with other e-government documents

Trials with standards and architectures for e-government have been underway for some years in Germany and in other countries[4]. Experience from these trials and international exchange contribute towards facilitating the definition and implementation of SAGA.

SAGA is published as part of the KBSt publication series which also includes, for example, the "V-Modell", The "Migration Guide" and "DOMEA". The documents of

[3] Refer to [BOL], page 20

[4] Refer to the corresponding documentation for the UK [e-GIF], the US [GOSIP], Australia [APEC] and Europe [IDA]

these series are adjusted to each other when updates are released. This means that SAGA supersedes statements and information of older documents and that new documents consider the statements and information of the latest SAGA version. A broad-based co-ordination process accompanies any SAGA updates in order to avoid conflicts with valid documents.

E-government manual

In order to promote the BundOnline 2005 initiative and to support federal-state and municipal authorities, the e-government manual is prepared under the leadership of the German Federal Office for Information Security (BSI). This manual is designed as a reference manual and central information exchange for issues related to e-government.

The e-government manual is a modular compilation of material which covers a wider range of issues and topics than SAGA. As far as identical issues are addressed, the e-government manual does so in a more concrete manner. This is why certain modules of the e-government manual are referenced from within SAGA[5]. SAGA sets forth guidelines, whilst the e-government manual explains the implementation of these guidelines and gives practical advice.

In mid-February 2003, SAGA became part of the e-government manual. It is the module of the manual with the strongest binding effect. All the other modules are designed to ensure conformity with SAGA.

IT baseline protection manual

The manual for the preparation of IT security concepts for normal security demands (IT baseline protection manual) recommends standard security measures for typical IT systems. The aim of these IT baseline protection requirements is to achieve a security level for IT systems through a suitable application of standard security measures at organizational, manpower, infrastructural and technical levels which is reasonable and sufficient for normal protection requirements and which can serve as the basis for IT systems and application with high security requirements.

SAGA demands the application of the IT baseline protection manual in that it is defined as a mandatory standard[6].

Barrier-free information technology ordinance – BITV

The ordinance on the creation of barrier-free information technology pursuant to section 11 of the law on equal opportunities for the disabled (barrier-free information technology ordinance – BITV) which came into effect on 24 July 2002 is referenced in

[5] Refer, for example, to sections 9.1.2, 9.2 and 9.4

[6] Refer to chapter 7 and sections 9.1.2 and 9.2

SAGA and is defined as a mandatory standard with regard to the implementation of the presentation and client tiers[7].

V-Modell

The procedure model ("V-Modell") is the development standard for IT systems of the federal agencies with binding effect for the entire area of the federal administration (EStdIT). It consists of certain core elements, i.e. "procedure model", "method allocation" and "functional tool requirements", and describes the activities and products (results) to be carried out and to be generated during the software development process.

This model must be considered in strategic planning and project management efforts and in conjunction with the implementation of e-government applications.

The model was and still is being permanently improved with the involvement of all stakeholders. The latest version is V-Modell ’97. Under the working title "V-Modell 200x", a new version is currently being developed and due to be published in 2005. Harmonisation with object-orientated processes as described by the RM-ODP is planned as part of this development effort.

Migration guide

The guide is designed to offer both strategic/economic and detailed technical decision-making aids in the case of forthcoming or recently completed migration projects. The focus of this guide is the replacement of Microsoft products both with open-source software (OSS) as well as future generation of Microsoft products. Agency-specific scenarios are developed and different migration alternatives are discussed.

SAGA version 1.1 was considered for the relevant interfaces with the migration guide. SAGA updates will have no repercussions on the statements made.

DOMEA

DOMEA stands for "document management and electronic archiving" in IT-based workflows. The aim of this concept is to introduce the electronic file. Physical files are to be replaced with workflows at public agencies in the form of fully electronic, media-consistent procedures. The electronic file is subject to the same legal and functional requirements as conventional files. Since the publication of the concept in 1999, DOMEA has become an established standard for electronic workflows at federal, federal-state and municipal agencies. For suppliers, DOMEA constitutes a major source of information when it comes to identifying the demands of public administrations which, for their part, are considered when the products are developed further.

DOMEA is currently undergoing further development. Besides the organizational concept and the resultant requirements catalogue, the modular concept will include

[7] Refer to sections 4.1.5.3 and 8.5.1.1

further modules in future which will address specific issues of the organizational concept in more detail. The draft upgrades are published on the website of the Co-ordinating and Advisory Agency of the Federal Government for Information Technology in the Federal Administration (KBSt) where they can also be discussed.

The requirements catalogue of the DOMEA concept translates organizational requirements to functional requirements which are orientated towards the SAGA standards on the one hand whilst they also influence the updating process of the SAGA document on the other. DOMEA describes the relevant requirements for software products related to the area of electronic workflow management. These requirements are in some respects even more demanding than SAGA and hence do not jeopardise SAGA conformity.

1.6 The evolution process

The Federal Ministry of the Interior proposes the standards and architectures which are to be generally adopted for e-government in Germany. This proposal is based on contributions by and annotations from the SAGA forums, the evaluation by the expert commission and the final draft by the authors. The Federal Ministry of the Interior is subsequently responsible for co-ordination with the federal ministries.

The process and data models are developed on the basis of the individual e-government projects of the public agencies. Process models of a general relevance are standardised by the Federal Office of Administration (BVA) as the competence center for processes and organization. The standardisation of the data models is co-ordinated by a process which was agreed to between the Federal Ministry of the Interior and the Senator for Finance of the Federal State of Bremen (OSCI steering group)[8].

Decisions on the development of basic components are made by the Federal Ministry of the Interior after consultation with the federal ministries.

SAGA is updated at regular intervals, amended to reflect the latest developments and results, and published at: http://www.kbst.bund.de/saga and in the e-government manual at: http://www.e-government-handbuch.de.

1.6.1 Public discussion forum

A public forum at: http://foren.kbst.bund.de/saga enables Internet users to register and discuss issues related to the application and further development of SAGA. The results of the discussions are evaluated and considered in the next version of the SAGA document.

[8] Refer also to chapter 5 "Information viewpoint: schema repository", page 51

1.6.2 Expert group

The Federal Ministry of the Interior has set up an expert group with representatives from business and public agencies, and appoints its members. The expert round will be involved in the updating process at regular intervals or whenever there is reason for involvement.

1.6.3 Request for Proposals (RFP)

When problems occur that cannot be resolved in established ways, requests for proposals are sent to the authorised expert circle in order to explore possible solutions. The proposals are presented to a closed expert forum and discussed at: http://foren.kbst.bund.de/saga.

2 Binding effect and conformity of the applications

2.1 Scope of validity and binding effect of SAGA

SAGA describes the technical boundary conditions recommended for the development, communication and interaction of IT systems of federal administrations, agencies and authorities. Conformity with SAGA is a general prerequisite for all the processes and systems that provide e-government services in Germany. In the case of systems with no direct interfaces with e-government, migration is recommended on condition of a positive outcome of the cost-to-benefit analysis. The standard software[9] to be used should, whenever possible, be products or product versions that are compatible with the architecture recommended in SAGA; refer to section 2.3.1 "Definition of conformity", page 27.

The federal ministries lay down rules for the binding effect of SAGA within their areas of competence.

2.2 Classification and life cycles of standards

2.2.1 Classification in SAGA

Standards are divided into three categories. Competing standards which are not stated should not be used or only if absolutely inevitable; refer also to section 2.2.3 "Extended classification of standards".

Mandatory:

Standards are mandatory if they are tried-and-tested and represent the preferred solution. Such standards must be observed and applied with priority.
Competing standards can be mandatory parallel if they have clearly different core applications. The standard which is best suited for the given application must be adopted in such cases.

In the event that mandatory and recommended standards or standards under observation exist parallel, the latter – i.e. standards under observation – should be adopted only in justified, exceptional cases.

A standard classified as mandatory does not necessarily have to be used in every e-government application. A mandatory standard only has to be adhered to if the use of the technology or functionality related to this standard is necessary or reasonable in view of the requirements of the specific application.

[9] Software that is simply installed and configured

Recommended:

Standards are recommended if they are tried-and-tested, but if they are not mandatory and/or if they do not represent the preferred solution or if their classification as mandatory still requires further agreement. In the event that no competing mandatory standards exist besides recommended standards, deviations from the recommended standards are permitted in justified, exceptional cases only.

Competing standards can be recommended parallel if they have clearly different core applications. The standard which is best suited for the given application must be adopted in such cases.

In the event that recommended standards or standards under observation exist parallel, the latter – i.e. standards under observation – should only be adopted in justified, exceptional cases.

Under observation:

Standards are under observation if they are in line with the intended development trend, but if they have not yet achieved a mature level or if they have not yet sufficiently proven their value on the market. In the event that no competing mandatory or recommended standards exist in addition to standards under observation, such standards under observation can serve as an orientation aid.

2.2.2 Life cycles of standards

Besides the standards classified in SAGA (refer to section 2.2.1), the life cycle model introduces another three lists of standards that give an overview of new standards yet to be assessed (white list), obsolete standards already rejected (black list) and standards to be maintained in effect (grey list).

Whilst the classification of standards as "mandatory", "recommended" and "under observation" is defined and updated in the SAGA document, presentation and ongoing updating of the standards on the lists are carried out in the SAGA section of the website of the Co-ordinating and Advisory Agency of the Federal Government for Information Technology in the Federal Administration (KBSt) at: http://www.kbst.bund.de/saga-standards.

Standards can pass through different stages during their life cycle. This is illustrated in Figure 2-1 on page 25.

The transitions of a standard between the lists in the SAGA section at: http://www.kbst.bund.de/saga-standards and the classes in the SAGA document are defined as follows.

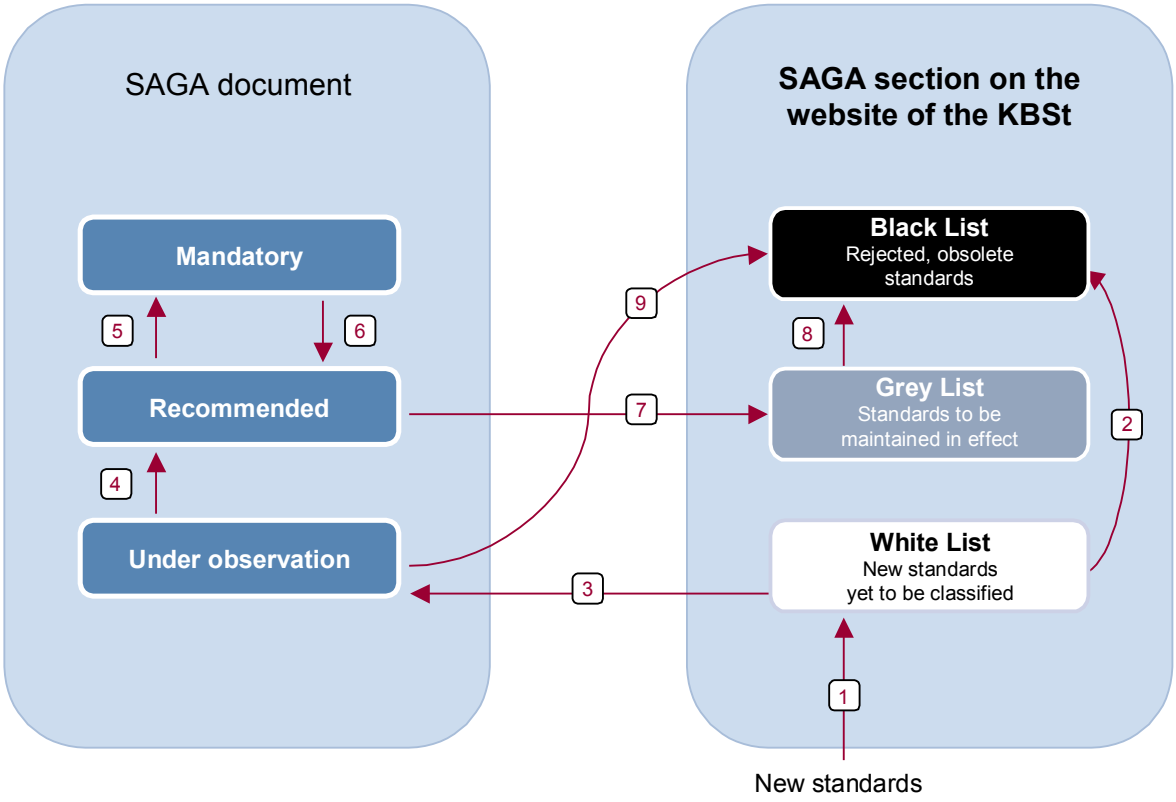


Figure 2-1: Life cycles of SAGA standards

1 New standards are proposed for classification by the SAGA team, by experts or participants of the SAGA forum (refer to section 1.6 "The evolution process", page 20). Prior to further evaluation, these standards are initially listed on a white list on the website of the Co-ordinating and Advisory Agency of the Federal Government for Information Technology in the Federal Administration. Transitions 1 and 3 can also be carried out in a single step.

2 Standards which, following evaluation, are not included in SAGA are added to the black list of rejected standards.

3 Standards with a positive test result are incorporated into the next SAGA version.

4 Coming standards with "under observation" status are classified as "recommended" in the next SAGA version.

5 Coming standards with "recommended" status are classified as "mandatory" in the next SAGA version.

6 Going standards with "mandatory" status are classified as "recommended" in the next SAGA version. Transitions 6 and 7 can also be carried out in a single step.

7 Going standards with "recommended" status are no longer contained in the next version of the SAGA document, but added to the grey list instead.

8 Obsolete standards in the grey list which are not to be maintained any longer are transferred to the black list.

9 Standards with "under observation" status which have been singled out are directly transferred to the black list.

2.2.3 Extended classification of standards

In the SAGA section on the website of the Co-ordinating and Advisory Agency of the Federal Government for Information Technology in the Federal Administration at: http://www.kbst.bund.de/saga-standards, three lists for the extended classification of standards are introduced with the publication of SAGA 2.0. No standards other than those on the grey list may be preferred to the standards classified in the SAGA document (mandatory, recommended, under observation) – however, only in the case of upgrades of existing systems in which these standards are already in use.

White list

Standards are listed on the white list if proposals for their inclusion in SAGA were submitted to the SAGA team and if these standards were not yet classified further. Standards on the white list are evaluated by the SAGA team and the expert group who may also decide that a standard is to be left on the white list if further developments are to be awaited and if a classification decision is to be made at a later stage.

Grey list

Standards are added to the grey list if they are no longer included in the current SAGA version, but if they had "recommended" or "mandatory" status in an earlier SAGA version and/or if they were widely used in the market in the past. When existing systems are upgraded, these standards are to be maintained in effect and can be used further.

Black list

Standards are added to the black list if they were examined and rejected by the SAGA team and the expert group.

2.3 SAGA conformity

2.3.1 Definition of conformity

The SAGA conformity of an e-government application[10] is evaluated on the basis of the models, procedures and standards described in SAGA:

a. Application of standardised process models
b. Consideration of standardised data models
c. Compliance with the standards and architectures described in SAGA
d. Use of existing basic components

In order to be able to make a comprehensive statement concerning the SAGA conformity of an e-government application – especially in conjunction with the implementation of complex, specialised processes – an application should first be broken down into individual components[11] before evaluating its conformity. The SAGA sub-aspects relevant for the SAGA conformity of the particular component can then be defined in a next step, so that SAGA can be reasonably and adequately considered for the given technical situation.

The standards which are relevant for ensuring SAGA conformity depend on the type of components and can vary depending on functionality, interface and application architecture.

2.3.2 Conformity declaration

As an aid for public agencies, IT service provides and manufacturers, Appendix C contains templates for a SAGA conformity declaration[12] which can be used in invitations to tender as a basis for establishing the SAGA conformity of an e-government application. An example of a complete conformity declaration will be available on the Internet at: http://www.kbst.bund.de/saga-konformitaet.

Before publishing an invitation to tender, the customer identifies the individual components of the application, discriminating between product components[13] and self-developed components. Conformity is declared for every component on the basis of the check-lists in Appendix C in the manner illustrated in Figure 2-2.

---

[10] The term "e-government application" is used as the general term for any IT system which provides e-government services of the federal government. With regard to the definition of the term "e-government service", please refer to section 4.1.2 on page 37.

[11] Components are non-trivial, self-contained, exchangeable modules of an e-government application which have a clearly defined function within the context of the architecture of the overall application and which have interfaces.

[12] Refer to page 163

[13] Software that is simply installed and configured

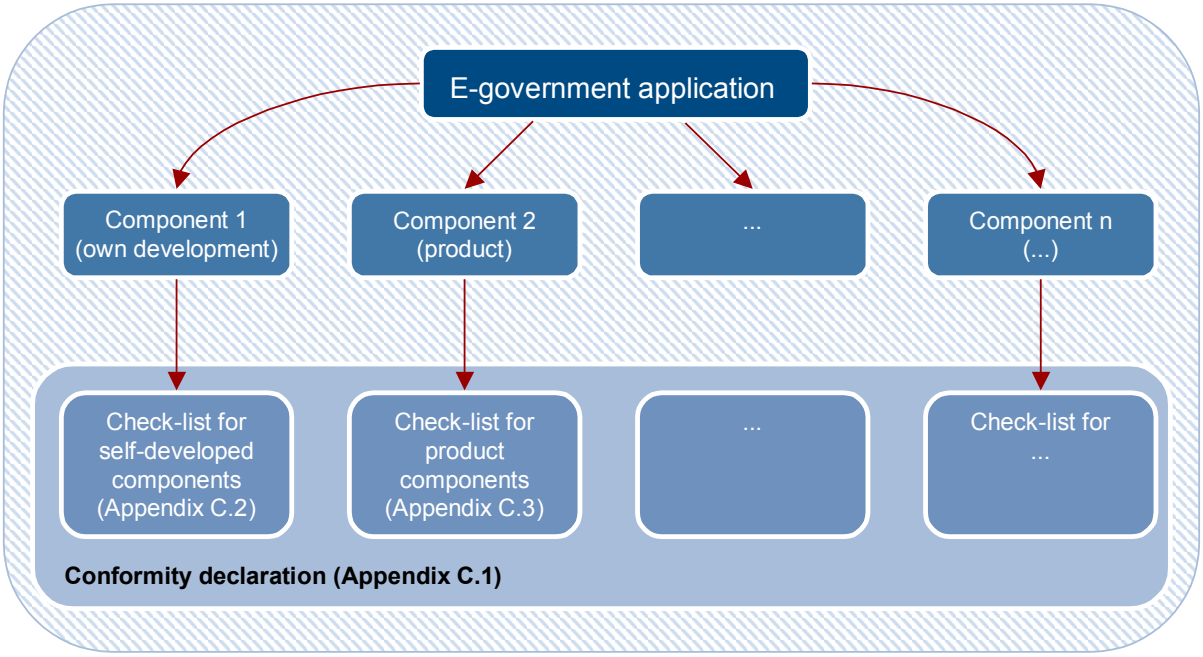


Figure 2-2: Structure of the SAGA conformity declaration and check-lists

In the SAGA conformity declaration, customers typically give an overview of the components identified for their e-government application and attach the appropriate check-list for self-developed components and product components. If suppliers are to be given more freedom with regard to the implementation of an e-government application, it can also be left to their discretion to identify components themselves and to classify these in terms of their own developments and products.

In the check-lists, the customer can already specify relevant conformity aspects for the component in question. If the customer already wishes to specify a particular standard at this stage, this can also be carried out in the check-list.

The supplier receives the conformity declaration with the completed check-lists for the components identified and states to what extent the specifications are fulfilled.

2.3.3 Conformity in the case of standards with different classification

Individual standards which are classified as mandatory do not necessarily have to be used in every e-government application. Mandatory standards must be preferred to competing standards in the selection of technologies. SAGA conformity is hence achieved by applying the particular subset of all SAGA standards which is relevant for the specific e-government application.

If mandatory or recommended SAGA standards are adopted for certain applications, standards and/or formats not listed in SAGA can be used in addition. If, for example, spreadsheet data[14] is made available in CSV format, the same data can additionally

[14] Refer to section 8.5.1.7 "File types for spreadsheets", page 82

be made available in other formats, such as Microsoft Excel, without violating SAGA conformity.

2.3.4 Responsibility for conformity

The public agency responsible for an e-government application is also responsible for ensuring conformity with SAGA. The public agencies are also responsible for examining ways to migrate special applications.

The federal ministries lay down rules for responsibility within their areas of competence.

The provision of conformity tests forms part of the future development of SAGA[15].

2.3.5 Migration for conformity

Transition phase

SAGA is subject to ongoing updating and adaptation to new requirements. It may hence happen that individual e-government applications are temporarily not in conformity with the latest SAGA version.

Migration plans should be developed for non-conforming applications on condition of a positive outcome of a cost-to-benefit analysis to this effect. This may only be the case where a major update or revision is concerned.

Measures to achieve conformity

The following measures are designed to support conformity with SAGA:

a. SAGA is included in project planning processes at an early stage.
b. Conformity with SAGA is specified and checked when projects are approved.
c. Conformity with SAGA is a mandatory criterion whenever subsidies are granted, in particular, with funds from the BundOnline 2005 initiative.
d. SAGA conformity is specified as a mandatory criterion for government contracts.

2.3.6 Non-conformity

E-government applications which are, as a whole or in part, not in conformity with SAGA are subject to the following restrictions:

a. The use of basic components can be restricted.
b. Advice and consultancy services by competence centers are limited or even impossible.
c. Interfaces with such systems cannot be supported.

[15] Refer to section 0.2 "Future issues", page 12

d. Public subsidies, in particular, from funds for the BundOnline 2005 initiative, are generally not available.
e. Integration of the system into the service portal www.bund.de may not be possible.

3 Architecture model for e-government applications

3.1 Overview

With the architecture mode, SAGA aims at the following:

a. In order to facilitate communications, a common understanding of up-to-date IT architectures, IT technologies and e-government structures is to be achieved.

b. technologies available for e-government applications are to be identified, compared, evaluated with regard to their relevance, and given a uniform and consistent structure using this model.

c. The aim is to provide uniform standards that can be used when it comes to implementing e-government projects.

The Reference Model of Open Distributed Processing (RM-ODP[16]) is the approach of choice for describing complex, distributed e-government applications. The analysis of the application is broken down into different viewpoints in order to reduce the complexity of the overall architecture. This makes the demanding system easier to understand and hence better to handle. The object-orientated paradigm is the basis of RM-ODP. Object orientation promotes clear-cut structures, re-usability and updating capability of the models, components and systems created.

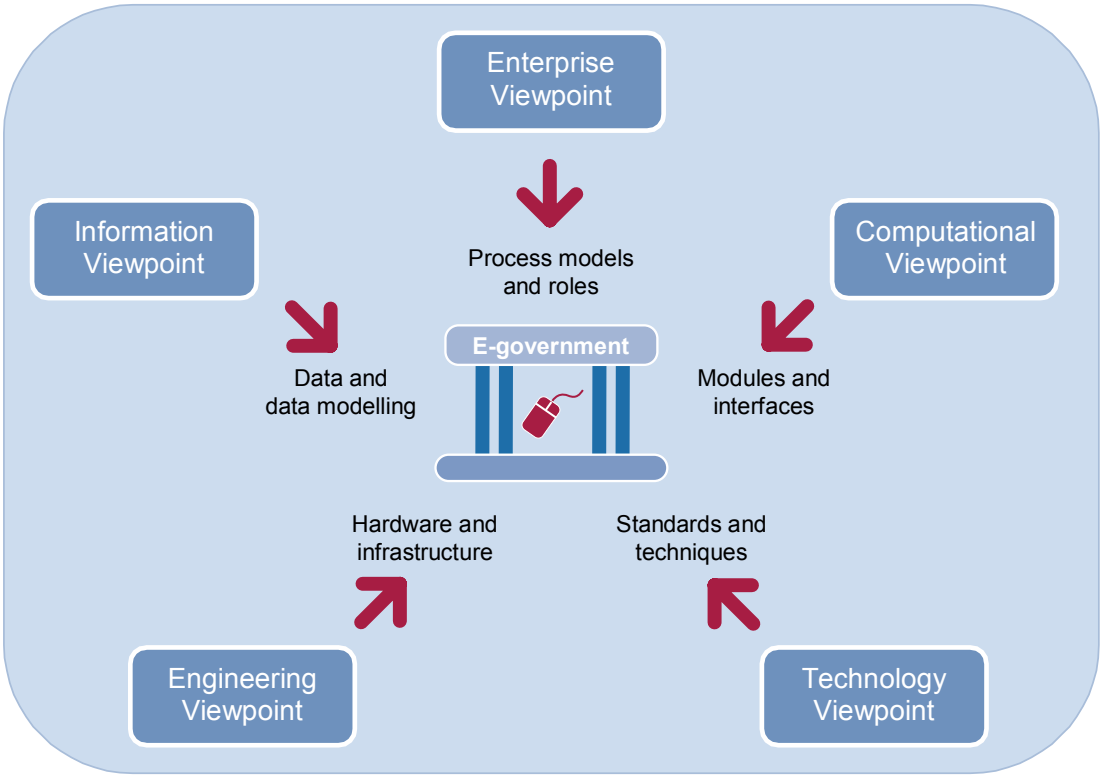


Figure 3-1: Viewpoints according to RM-ODP

[16] Reference Model of Open Distributed Processing, refer to [ISO 1996]

The RM-ODP model defines five viewpoints of a system (refer to Figure 3-1):

a. The enterprise viewpoint specifies purposes, scope, processes and policies for an application.
b. The information viewpoint describes the characteristics and semantics of the data to be processed, i.e. the data model.
c. The computational viewpoint represents the decomposition of an application into functional modules and their interaction interfaces.
d. The engineering viewpoint represents the distribution of the individual elements of the system to physical resources and their connections.
e. The technology viewpoint describes the technologies used to implement the system.

The five viewpoints can be used both to describe existing systems and to model new systems and applications. SAGA suggests, but does not demand, the use of RM-ODP to describe of e-government applications.

Furthermore, the SAGA document applies the RM-ODP model to German e-government. The result are chapters which can each be assigned to a viewpoint; refer to section 1.3.5 on page 16. This presentation of the viewpoints on the "German e-government" meta-level can be used as a basis for developing concrete models for individual e-government applications.

3.2 Enterprise viewpoint

The enterprise viewpoint for e-government applications includes two fundamental elements: the organizational structure of e-government in general as well as the organizational models of the application. This is where the overall environment for the system and its purpose are described. Furthermore, the requirements for the system, relevant constraints, executable actions and data processing policies are defined from the organization's or enterprise's point of view. This exercise includes a definition of the procedures, their rules, as well as the actors and their roles in the process.

The efficiency of information technology is strongly dependent on an integrated view. This means that first and foremost the technical application is regarded and described as a process rather than placing information technology into the foreground.

Services can and should be described in the form of technical process models. This means that all the work steps from the beginning to the end, i.e. from the inquiry by the customer (citizen, business, other public agency, etc.) to the rendering of the service, should be considered. On a first development stage, these process models should be left at a relatively abstract level.

New proposals of process definitions should always be checked with a view to

a. re-usability
b. simplicity and
c. the possibility to be described by existing process definitions.

The competence center[17] in charge of processes and organization should offer support in this respect.

Chapter 4 "Enterprise viewpoint: fundamentals of e-government" on page 37 and following describes the enterprise viewpoint of German e-government as a model which can be used as a basis for creating this viewpoint for concrete e-government applications. In section 8.1 "Process modelling" on page 71, SAGA offers descriptive tools for defining the enterprise viewpoint.

3.3 Information viewpoint

This viewpoint determines the structure and semantics of the system's information. Further items include the definition of information sources (senders) and sinks (recipients), as well as processing and transformation of information by the system. Integrity rules and invariants must be additionally described.

Section 8.2 of SAGA provides the tools needed to define the data models.

A coherent process definition calls for the use of general data definitions for major data identities (such the application) and for the data to be exchanged between processes or applications.

Data models should always be checked with a view to

a. re-usability
b. simplicity
c. the possibility to be described by existing data definitions.

The competence center[18] in charge of processes and organization should offer support in this respect.

Chapter 5 "Information viewpoint: schema repository" on page 51 corresponds to the information viewpoint of German e-government and should be considered when creating own data models. Section 8.2 "Data modelling" on page 71 classifies the technologies to be applied.

3.4 Computational viewpoint

With this viewpoint a system is broken down into logic, functional components which are suitable for distribution. The result is objects with interfaces at which they offer and/or use services.

---

[17] Refer to section A.9.4 "The workflow management, processes and organization competence center", page 156

[18] Refer to section A.9.4 "The workflow management, processes and organization competence center", page 156

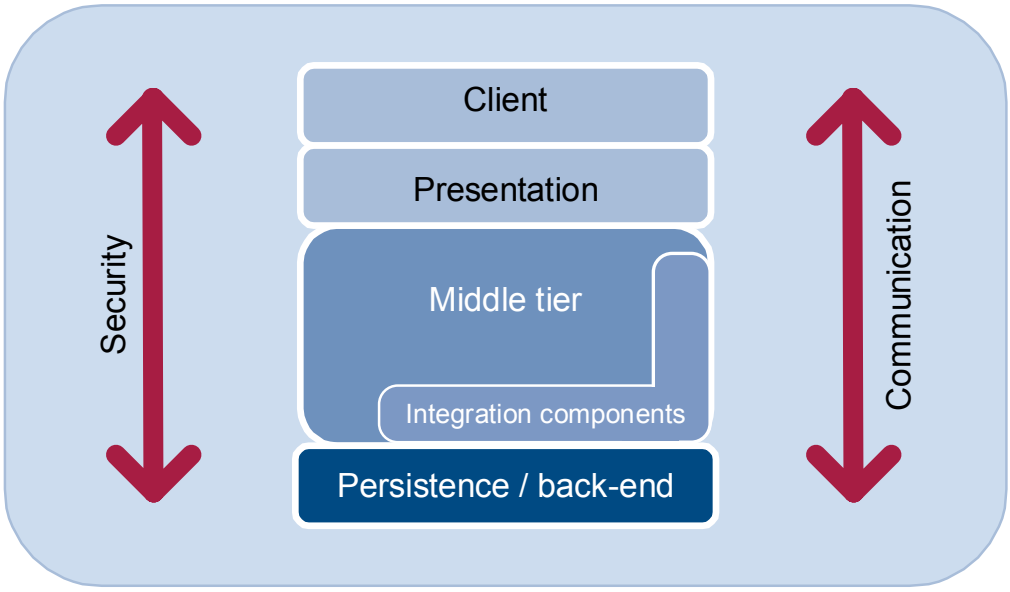


Figure 3-2: Structural view – tier model

An e-government application is generally divided into four tiers (refer to Figure 3-2):

a. The client tier represents different access channels reflecting different users, devices, transmission routes, as well as different applications in order to interact with the special applications. SAGA 2.0 refers to the following terminal devices:
   i. Web access via web browsers or special browser plug-ins
   ii. Mobile phones and personal digital assistants (PDAs)
   iii. External systems (such as ERP systems of industrial companies)

b. The presentation describes the processing of information for the client and the user's interaction with the special application. The presentation component includes all the standards for communication with the relevant terminal devices of the client tier.

c. The middle tier includes, in particular, new developments for e-government and in most cases constitutes the core of e-government-specific applications. The specific business logics of the special applications are linked together in the middle tier. The presentation of the technical components focuses on the description and discussion of standards for the middle tier and its interfaces because this is where the highest integration demand is expected within the scope of e-government solutions. The middle tier processes the data from the persistence tier.

d. The persistence tier ensures the storage of data. This is typically accomplished using databases. The back-end as a collective term represents functionalities of the operating system, specific databases as well as existing, non-SAGA-conforming special applications, legacy or ERP systems.

Within these tiers, a special application is divided into modules which interact via defined interfaces. Interaction takes place in the form of local and remote communication between the modules. The basic components defined in Appendix A provide functional modules for the implementation of e-government applications.

Safe and secure interaction between all the modules must be ensured. The protection aims are described in section 9.1.1 on page 95.

Chapter 6 "Computational viewpoint: reference software architecture" on page 53 describes a general computational viewpoint of e-government applications which can be used as a basis for creating this viewpoint for a concrete online service. In sections 8.3 to 8.7 on page 73 and following, SAGA defines standards and technologies for implementing the computational viewpoint. Chapter 9 on page 95 defines standards and models for secure interactions.

3.5 Engineering viewpoint

The engineering viewpoint describes the system support needed to permit the distribution of objects from the computational viewpoint. This includes units where objects are executed, such as computers and communication infrastructures, as well as all kinds of software platforms for distributed systems.

Chapter 7 "Engineering viewpoint: reference infrastructure" on page 65 gives a general description of the engineering viewpoint for e-government applications of federal agencies. The corresponding viewpoint of a concrete online service can be derived from this. Chapter 9 on page 95 presents several technologies to be adopted in order to support network security.

3.6 Technology viewpoint

This viewpoint describes the concrete technologies selected for implementing the system.

In chapter 8, SAGA describes the classified standards for the IT architecture. Models and standards relevant for and supporting safety and security are specified separately as general-interest issues in chapter 9 for all areas of the IT architecture.

4 Enterprise viewpoint: fundamentals of e-government

In line with the definition of the enterprise viewpoint, the general frame of reference for e-government in Germany will be described in the following as the general environment for the standardised introduction of e-government applications.

Besides this general discourse, the process level will be addressed too. Process models enabling the creation of basic modules will be developed as a frame of reference for e-government applications.

4.1 Frame of reference for e-government in Germany

4.1.1 Definition of e-government

When the term "e-government" is used, it is often not quite clear what is meant and which opportunities it offers. Many citizens regard it as just another buzzword of the computer age, whilst others consider it as the next logical step in administrative IT or as the electronic manifestation of the attempts so far made to reform the administration.

According to the BundOnline 2005 initiative, electronic government covers all decision-making and service processes in politics, government and administration as far as these processes are largely based on the use of information and communication technologies. Potential uses vary greatly in this context. They range from the modernisation of administrative processes by electronic workflow management via the provision of administrative information using portals of public agencies on the Internet right through to complex transactions and interactive electronic services for citizens on the web. The aim is to offer all services of public agencies as electronic offerings to external customers, i.e. citizens, businesses and other administrations. E-government thus represents the public sector in the emerging information society[19].

Aspects of e-democracy are not explicitly addressed in this context because the government is assumed to pursue different approaches towards its roles in relation to citizens. As far as e-government is concerned, citizens are the clients of administrations and governments. E-democracy is based on the concept of the citizen as the sovereign, representing the basis for the government to exert its power.

4.1.2 Definition of the "service" term

The term "service" must be defined in advance as a precondition for understanding certain forms of administrative action as services for the purposes of e-government. A "service" is typically rendered against payment of a fee. Within the framework of

[19] Refer also to the e-government manual (http://www.bsi.bund.de/fachthem/egov/6.htm), chapter VI 1, module: "Das E-Government-Glossar" [E-government glossary], section 1.1

the updated implementation plan of the BundOnline 2005 initiative, the term "service" was defined further for the field of e-government.

When citizens contact the government, "service" then refers to the complete performance of a process for an external user. This includes processes, obligations and burdens, such as the recognition as conscientious objector, applications for unemployment benefits or the granting of an import permit. For the purposes of the following discourse, the term "service" will hence cover any contacts between citizens or businesses on the one hand and the administration on the other[20].

4.1.3 The philosophy underlying e-government

E-government opens up new ways to reform public administrations. This concerns internal relationships within administrations on the one hand as well as external relations between administrations, citizens and business on the other[21].

4.1.3.1 Citizens' service

Citizens do not always contact administrations voluntarily. Administrative processes sometimes involve long distances and waiting time. Contacting the administration via the Internet can hence offer benefits to many citizens.

Networked computer systems will be part of the natural environment of future generations. This is also reflected by the large number of Internet users aged between 14 and 19. Increasing Internet penetration of society will also lead to an increasing demand for online services.

E-government offers a host of options for developing new forms of contact between administrations and citizens. Internet portals are a way of providing central access to the administration. A central goal of the BundOnline 2005 initiative is hence to improve citizens' service.

Even in future, every citizen must be at liberty to decide how to approach the administration. Citizens must always be offered the possibility to personally see competent officers. Consequently, administrations must offer multi-channel access with the Internet, call centers and citizen's offices as the main pillars of contact. Both the call center and the citizen's office ideally use the portal offer on the Internet and the underlying application infrastructure. The real service process itself remains independent of the access channel. E-government can hence contribute towards improving citizens' service.

---

[20] Refer also to the e-government manual (http://www.bsi.bund.de/fachthem/egov/6.htm), chapter VI 1, module: "Das E-Government-Glossar" [E-government glossary], section 1.2

[21] Refer also to the e-government manual (http://www.bsi.bund.de/fachthem/egov/6.htm), chapter I, module: "Chefsache E-Government – Leitfaden für Behördenleiter" [E-government as an executive task – a guide for heads of public administrations]

4.1.3.2 E-government as a location factor

Businesses often have more frequent contact with administrations than citizens, for example, for certification, licensing or approval processes as well as the entire service complex of the customs and tax administrations.

These obligations are in part imposed by the government, with a potentially enormous administrative effort both for administrations and for companies alike. Lengthy and complex approval procedures also result in high costs and can be made more effective for companies if state-of-the-art information and communication technologies are used. It is in the interest of both parties to streamline these exchange processes through e-government.

Public procurement also offers enormous potentials in that easier access to the tendering process can generate significantly stronger incentives for companies.

The quality of administrative services has become a factor in the global competition for attractive business locations that should no longer be underestimated. Given a high degree of rules and obligations for companies, keeping barriers as low as possible is a crucial requirement. BundOnline 2005 addresses this task on a comprehensive scale. Mass services with an enormous administrative effort, for example, in the customs sector, are energetically implemented as online processes.

4.1.4 Organizational requirements

Certain organizational requirements must be fulfilled in order to ensure the sustainable introduction of e-government. The most important of these requirements are described in the following sections.

4.1.4.1 The cross-administration approach

Countries with a federal structure are faced with the problems of a de-centralised administration structure when it comes to the implementation of e-government. The de-centralised administrative units are often largely independent of the central government. This situation is particularly striking in Germany. Whilst the federal government holds most of the legislative power, it is the federal states and municipalities that are mainly responsible for implementation.

The direct federal administration has only a few national tasks. Only those functions specifically defined in the German constitution (Articles 87-89) have an underlying administrative structure of their own, such as the Foreign Service, the Federal Armed Forces, the Federal Border Police or the Federal Revenue Administration.

Besides these functions, there are other national tasks which are typically performed by specialised administrative agencies which are responsible for the entire German territory and which have no underlying administrative structures. These include, for instance, the German Federal Office of Investigation, the Federal Statistical Office as well as the German Patent Office.

The immediate federal administration consists of:

a. Supreme federal authorities, such as the federal ministries, the Office of the Federal President and the Press and Information Office of the Federal Government
b. Superior federal authorities with central responsibility for a particular field throughout the entire Federal Republic of Germany (for example, the German Federal Cartel Office)
c. Intermediate-level federal authorities with regional responsibility (for example, the different regional finance offices)
d. Lower-level federal authorities with locally restricted activities (for example, main customs offices)

The federal government commissions external administrative bodies as independent legal personalities with regard to certain federal-state tasks related to the enforcement of laws. These legal personalities in their capacity as corporate bodies, institutions and foundations of the indirect federal administration are independently responsible for their fields of competence throughout the territory the Federal Republic of Germany and report to a ministry.

Comparable structures exist in the individual federal states. Furthermore, cities, districts and municipalities constitute the third administrative level in their capacity as territorial communities with autonomous administrations which also perform their own tasks in addition to federal and federal-state functions.

What is generally needed is co-operation, networking and co-ordination within and between administrative level. A first step that was taken at federal level was the implementation of the Berlin-Bonn Information Network (IVBB) which is an intranet for supreme federal authorities. By upgrading this network in future to the Federal Administration Information Network (IVBV), it will connect all the federal authorities to a secure, closed network – an enormous challenge both technically and in terms of organization[22].

As far as administrative procedures are concerned, insular and go-it-alone solutions must be avoided when new applications are introduced. New solutions must be co-ordinated between the different levels in order to achieve maximum service depth and width on the largest national scale possible and in order to ensure the compatibility of administrative levels.

In order to enable the nation-wide approach, the Conference of Minister-Presidents adopted on 26 June 2003 a joint strategy for integrated e-government under the title DeutschlandOnline[23]. In their joint strategy paper, the federal and federal-state gov-

[22] Refer also to the e-government manual (http://www.bsi.bund.de/fachthem/egov/6.htm), chapter V C, module: "Netzplattform für E-Government" [Network platform for e-government]

[23] Refer to http://www.deutschland-online.de/

ernments as well as municipal administrations agreed to create an integrated e-government landscape in Germany.

Administrative services are to be provided on a multi-level basis, portals are to be networked and joint infrastructures and standards developed. At the same time, e-government co-ordination is to be improved and the transfer of solutions is to be speeded up. This avoids parallel development, saves costs and integrates, modernises and optimises administrative processes.

4.1.4.2 Process optimisation

The successful introduction and implementation of e-governments calls for preparatory restructuring activities on a process level. Existing rules, processes and structures must be adapted and improved because electronic forms of rendering services would otherwise stumble into the same fundamental problems which are also encountered in conventional workflows not based on information technology.

Existing administrative processes are partly the result of historical developments and have become extremely complex during the course of years as a result of many small changes. The following measures are hence recommended before special and technical applications are implemented.

a. Simplification of processes and procedures
b. Deregulation
c. Shortening of process chains
d. Reducing interfaces
e. Avoiding iteration
f. Reducing cycle and dead times[24]

First steps have already been taken within the framework of the red tap reduction model[25]. This initiative is determined to achieve the fastest possible simplification of processes and statutory provisions concerning frequently used services involving multiple administrative levels, such as passport and motor vehicle related services.

4.1.4.3 Qualification of personnel

The use and updating of standards means a continuous exchange of information and training process. Training people in the use of a PC costs more than the PCs themselves, but also yields a more sustainable effect. Public service staff were found to be highly motivated to support e-government. This important asset must be exploited and increased in the interest of implementing e-government.

---

[24] Refer also to the e-government manual (http://www.bsi.bund.de/fachthem/egov/6.htm), chapter III, module: "Phase 3 – Analyse" [Phase 3 – analysis]

[25] Refer to http://www.staat-modern.de/

Focal issues include intensive staff training as well as increasing the attractiveness of jobs in public administrations for IT experts. Activities of this kind are organized via the Federal Ministry of the Interior and/or the BundOnline 2005 project group.

4.1.4.4 Involvement of users

The use of e-government is strongly dependent on customer acceptance of the services offered. Full utilisation of the savings potential of e-government is contingent upon the online services provided being accepted and used by potential users.

Expectations among citizens, companies and public agencies as the specific target groups need to be identified on an ongoing basis.

The service portfolio and the service rendering process must be adapted to these expectations.

4.1.5 Legal frame of reference

Legal guidelines must be considered in addition to the organizational frame of reference. The most important of these requirements are described in the following sections. A detailed description of the legal adjustments carried out is available from the federal government's e-government manual[26] and the updated implementation plan of the BundOnline 2005 initiative[27].

4.1.5.1 Electronic signatures

Modern e-government requires that legal foundations be adapted on a timely basis in order to avoid media inconsistency and to enable efficient, paper-less administrative work.

Legal adjustments

The legally binding nature of electronic communications is a crucial success factor for the implementation of e-government. What is hence needed is a digital solution for a signature with legally binding effect, i.e. the electronic signature. The legal adjustments necessary to enable the use of electronic signatures have been largely completed in Germany. Besides amendments to the German Signature Act to comply with European requirements, the electronic signature has also been integrated into the relevant blanket clauses in administrative and private law[28].

---

[26] Refer to the e-government manual (http://www.bsi.bund.de/fachthem/egov/6.htm), chapter II, module: "Rechtliche Rahmenbedingungen für E-Government" [Legal frame of reference for e-government]

[27] Refer to http://www.bund.de/BundOnline-2005/Umsetzungsplan-.7193.htm

[28] For information concerning the legal basis for the electronic signature, please refer to http://www.bsi.bund.de/esig/basics/legalbas/

Dissemination of the electronic signature

Both dissemination and acceptance of electronic signatures among and by citizens and businesses are dependent on several factors. The costs for the necessary equipment (smartcard, software, card reader) are still relatively high and thus represent a major obstacle to the nation-wide introduction of the electronic signature.

Furthermore, there is still a serious information backlog among the population with regard to the use and added value of electronic signatures. Furthermore, the products themselves are not yet really mature. Development-related starting problems discourage potential users. The software which must be installed to enable the use of electronic signatures often contains bugs or does not even work at all, and is very difficult to install for lay people. What's more, a standardised chip medium and mass applications which might pave the way to market penetration are not yet available.

In April 2003, government and business representatives established the Signature Alliance in order to promote the stronger dissemination of multi-function signature smartcards and to overcome the above-mentioned obstacles. This alliance is based on the idea that the increasing use of electronic signatures will benefit government and business alike because electronic signatures will be needed both for secure e-commerce and e-government applications with legally binding effect. The alliance relies on two strategies to this effect. On the one hand, the alliance partners agreed to adopt common standards. On the other hand, the attractiveness of the alliance is to be boosted for all its members using realistic business models.

First practical applications suggest that smartcards are particularly attractive for citizens if they can use them for both private and public services.

4.1.5.2 Data protection

E-government offers a host of options and rationalisation potentials in the IT sector. Ideally, data from the most varied contexts is gathered once only by a central function and is subsequently available to any de-centralised purposes and uses.

However, when electronic data is exchanged within and between public agencies, data protection requirements must be considered and implemented by way of suitable technical and organizational measures. Personal data, in particular, may not be gathered, processed or disclosed for any purpose other than the use explicitly contemplated by law.

The federal government's e-government manual includes a separate module[29] with comprehensive information concerning the issue of data-protection-compliant e-government.

[29] Refer to the e-government manual (http://www.bsi.bund.de/fachthem/egov/6.htm), chapter II, module: "Datenschutzgerechtes E-Government" [Data-protection-compliant e-government]

4.1.5.3 Barrier-freedom

More than eight million disabled people, 6.6 million of whom are severely disabled, live in Germany. People with impaired vision and physical handicaps, in particular, depend on technical aids as a precondition for using the Internet, such as large screens or a magnifying-glass function, Braille line, voice output, etc. In order to optimally enable these devices for e-government applications, a host of rules and requirements must be considered during programming, designing and editing.

On 1 May 2002, the new Law on Equal Opportunities for the Disabled (BGG) came into effect with the aim of overcoming and preventing disadvantages for disabled people, to ensure the discrimination-free participation of the disabled in social life, and to enable these people to live an autonomous, independent life.

This is also applicable to the use of the Internet. The most important criteria and references are to be found in the Ordinance on the Creation of Barrier-free Information Technology pursuant to section 11 of the Law on Equal Opportunities for the Disabled (Barrier-free Information Technology Ordinance – BITV) which came into effect on 24 July 2002.

This ordinance specifies the Web Content Accessibility Guideline 1.0 (WCAG 1) from 1999 as the technical standard.

The Barrier-free Information Technology Ordinance is binding upon public agencies of the federal administration[30] and applies to:

a. Internet presences and offers
b. Intranet presences and offers which are available to the general public
c. IT-based graphic user interfaces which are available to the general public

4.2 Frame of reference for e-government applications

4.2.1 Interactions in e-government

4.2.1.1 Interaction levels

E-government services can be generally broken down according to interaction levels, i.e. information, communication and transaction[31].

Information primarily covers the provision of information for the people, for businesses and other elements of society. Users on this level merely act as recipients of information. This area is the most developed one, and almost all public institutions are on the Internet with an extensive web presence.

---

[30] Refer to the e-government manual (http://www.bsi.bund.de/fachthem/egov/6.htm), chapter IV, module: "Barrierefreies E-Government" [Barrier-free e-government]

[31] Refer to [Lucke et al. 2000], page 3

Many of these information systems are supplemented by **communication** solutions with dialogue and participation offerings which enable the exchange of news, messages and information. This offer ranges from simpler solutions, such as e-mail or web-based discussion forums, right through to more complex applications, such as video conference systems for telecooperation. In this respect too, the development of German administrations can be described as well advanced.

Transaction applications represent the highest interaction level. This sector covers the real rendering of services by public administrations. These applications include, for example, the electronic receipt and processing of applications or orders as well as the provision of forms which can be filled in and immediately sent to the correct recipient directly on the computer. Electronic payment or tendering systems also belong to this category.

A few transaction services are already completely implemented. The electronic signature is an important element that ensures the authenticity and confidentiality of the data exchanged between the different parties. The electronic exchange of documents with legally binding effect still involves technical and organizational challenges for public administrations and a satisfactory solution has yet to be found here. Another adverse factor is the sparse dissemination of the electronic signature in all parts of society.

Pioneering work is still necessary with regard to the handling of transactions. The following discussion will hence focus on transaction services and the related organizational and technical challenges.

4.2.1.2 Interaction relations

Besides the classification in terms of interaction levels, the different partners involved in e-government can also be distinguished[32].

a. Government to citizen (G2C)

   This situation refers to the electronic interaction between citizens and administrations. This area also covers non-profit and non-governmental organizations.

b. Government to business (G2B)

   This term covers electronic relations between administrations and business.

c. Government to government (G2G)

   This application covers the vast field of electronic relations between different public agencies and institutions of the public administration sector.

Services are hence rendered to citizens, business and other administrations. The focus in this case is on the G2C and G2B interaction relations. Relations between public agencies (G2G) are handled within the framework of the relevant transaction services between administrations and citizens and/or business. Communications

[32] Refer to [Lucke et al. 2000], page 3

within a public agency (government-to-employee, G2E) are not explicitly addressed in this context.

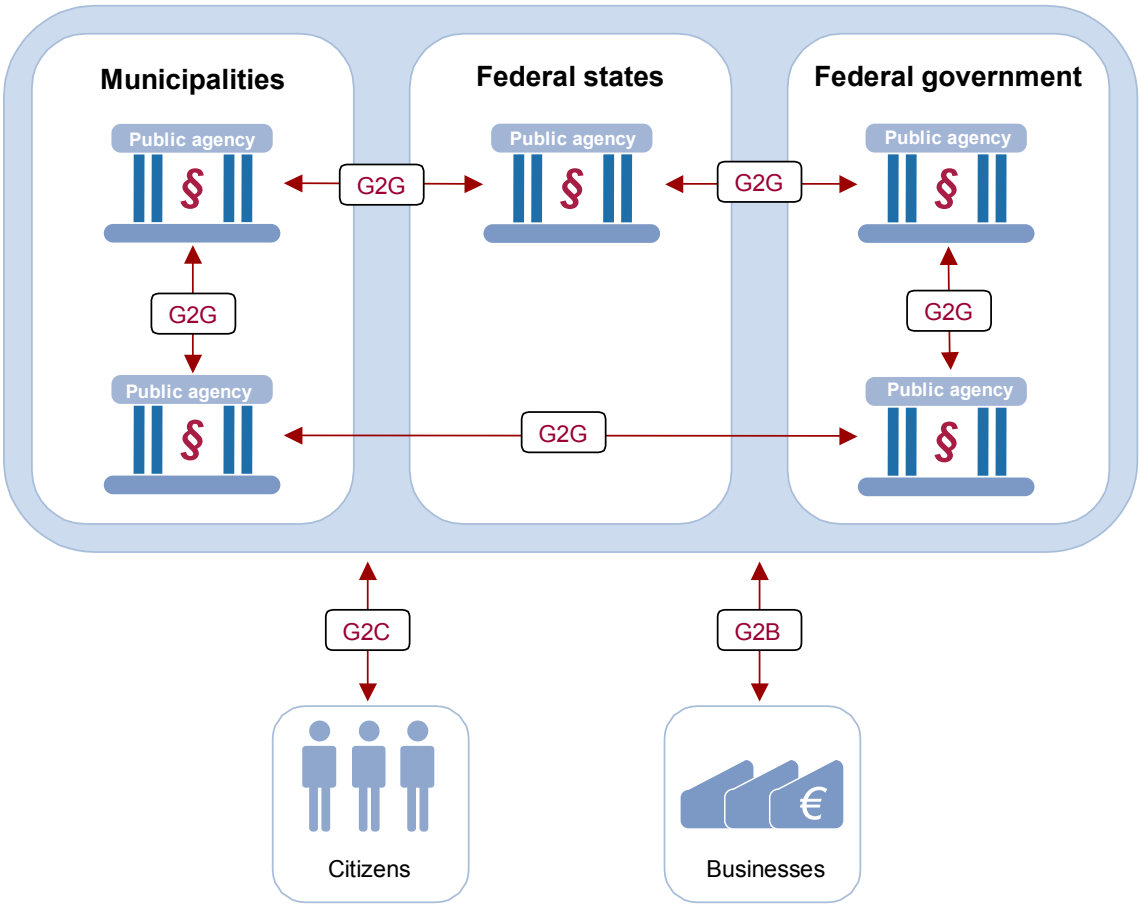


Figure 4-1: Overview of e-government interactions

4.2.2 Transactions in e-government

As already mentioned, public administration services not only cover the field of pure services, but also rights and obligations. A functional classification of administrations is necessary as a precondition for standardising the different types of administrative activity – and hence the possible transactions. Generally valid types of transactional services can be identified on this basis.

4.2.2.1 Transactional service types

The German administration can be divided into service and intervention functions based on responsibilities and legal forms. Different services types can be identified and classified as service-type and intervention-type services on the basis of the different categories of functional administrative branches.

Services are demanded, i.e. initiated, by citizens or businesses from the administration. Services include:

a. applications for public payments
b. granting of subsidies
a. subsidy and promotion measures
b. approval and licensing procedures

Intervention is a case where the administration intervenes in the citizen's legal sphere, encroaching on the citizen's freedom or property and/or imposing obligations upon the citizen. In this case, certain measures are initiated by the administration. Cases of intervention are:

a. administrative fines
b. criminal prosecution
c. legal proceedings
d. collection of taxes
e. collection of customs duties
f. registration obligations

Public procurement represents another service type where the government acts as the customer. Contracts for goods and services are subject to defined administrative procedures.

4.2.2.2 Sub-steps, actions and roles of transaction services

The individual transaction types can be broken down further into individual sub-steps. Sub-steps consist of one or more actions in which different actors are involved. Examples of sub-steps, actions and roles related to the service area are discussed in the following. This methodological approach can then be used as a basis for developing similar models for any other transaction type.

As a precondition for applying for a service, citizens must first be given the opportunity to obtain detailed information. The information step is followed by the submission of the application. The application is passed on to the public agency and from there to the officer in charge. Other organizational units or public agencies may have to be asked for comments or information. As already mentioned, processes may have to be optimised or reformed in this field. The examination of the case is followed by a decision. This decision, again, may have to be sent to other departments or officers for information.

Finally the decision is communicated to the applicant. If the decision corresponds to the applicant's request, the case is closed and funds are disbursed, if applicable. In this case, permanent control of the application of funds must be possible. The procedure ends with archiving as the last sub-step.

If the applicant does not agree to the decision, remedies in law are available in the form of a protest or legal proceedings, for example.

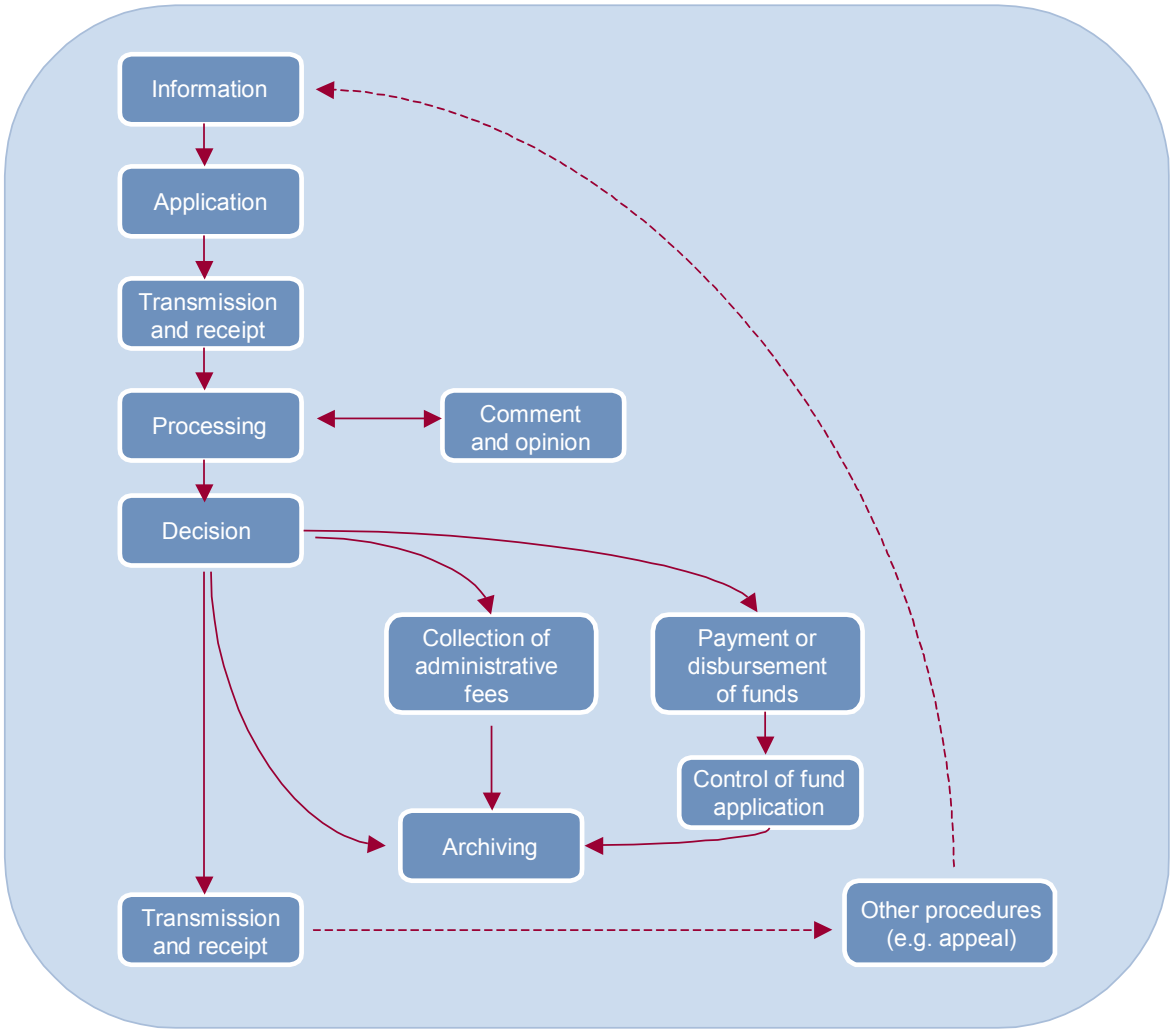


Figure 4-2: Sub-steps of transaction services

This means that for the services sector those sub-steps can be defined for which Figures 4-2 and 4-3 show the interactions and contain further explanations.

Every sub-step involves different actions and roles which are attributed to different actors. The "application" sub-step, for example, includes the actions of submitting, transmitting and receiving the application. The applicant's role is typically performed by a citizen or company. At the public agency, the post office – ideally a virtual one – receives the application and passes it on to the officer in charge. The officer who receives the application also confirms its receipt.

In analogy to this procedure, the other sub-steps include further actions and roles which are summarised in the list below.

Not every service type defined in section 4.2.2.1 must necessarily include all the sub-steps. Depending on the particular process, sub-steps can be carried out repeatedly during the life of a case.

Sub-steps	Actions	Roles
Information	Providing information Requesting information	Interested citizen Editor
Application	Submission of application Transmission of application Receipt of application	Applicant Post office Officer
Processing	Examination of the case Request for information Providing information	Officer Superior Applicant Post office Further officers
Comment and opinion	Information evaluation	Officer Superior Further officers
Decision	Writing the decision Service of the decision	Officer Superior Applicant Post office
Collection of administrative fees	Collection of fees	Payer Cashier's office
Payment or disbursement of funds	Payment	Payee Cashier's office
Control of funds application	Examination of the case Request for information Providing information	Officer Superior Payee Post office Further officers
Archiving	Archiving	Officer Records management unit
Reference to other procedures	Data transmission	Applicant Officer Other public agencies and officers

Figure 4-3: Sub-steps, actions and roles of transaction services

4.2.3 Modules for the implementation of electronic procedures

The analysis of service types explained above and the related identification of sub-steps, actions and rules can be used as a basis for identifying functional modules

which – given the required configuration possibilities – can be used ´to implement different procedures using information technology. The potential applications of these modules are dependent upon the quality of the process analysis and the chosen software architecture[33].

The following types of basic modules can be defined in conjunction with the above-described procedure.

a. User interface

   The analysis of the different roles leads to the need to develop certain basic modules which enable functions for access to the e-government application. This includes a uniform user interface which is easily remembered, as user and role management functions as well as functions for authenticating users in the system.

b. Action modules

   The actions identified are implemented in the form of application modules, with priorities being defined, for example, on the basis of their potential frequency of use in the implementation of the business logic. De-centralised and central modules can be distinguished here.

c. Integration and infrastructure modules

   The definition of basic modules leads to the development of software or network-based components which standardise communication between the basic modules.

The basic modules identified within the framework of the BundOnline 2005 initiative are described in more detail in Appendix A on page 111. The development of special applications based on re-usable software components, such as BundOnline basic modules, is outlined in chapter 6 "Computational viewpoint: reference software architecture" on page 53.

[33] Refer to chapter 6 "Computational viewpoint: reference software architecture", page 53

5 Information viewpoint: schema repository

The definitions of standards for IT architecture and data security contained in chapters 8 and 9 are necessary but not sufficient preconditions for achieving interoperability between the e-government applications of the federal administration. The technologies defined do not yet ensure uniform data grammar, semantics and layout. However, interoperable applications require exactly this common semantics for the data exchanged between these systems. It is not until commonly used schemas and identical definitions of elementary data types are used that the necessary preconditions are created.

E-government actors and their communication relations are very diverse, so that the process of agreeing to the related schemas becomes correspondingly complex. First schemas have already been agreed to and defined within the framework of the reconciliation and development of applications which use one or more of the interaction relations discussed in section 4.2.1.2.

Although this means that the work already done here could in part be used in other projects too, an established communication platform which would open up this potential is not yet available.

On behalf of the Co-operation Committee for Automatic Data Processing for the Federal-government, Federal-state Government and Municipal Administration Sector (KoopA ADV), the Bremen Senator for Finance has set up a steering group which co-ordinates and accompanies all projects related to the OSCI transport issue. The corresponding repository is currently in the process of being implemented.

The Bremen-based steering unit also acts as a contact partner and competence centre for standardising schema contents for projects by federal government, federal-state governments and municipal administrations, such as "xMeld" as the standard for data and transaction schemas for registration applications.

The Co-ordinating and Advisory Agency of the Federal Government for Information Technology in the Federal Administration (KBSt) initially acts as the lead agency for the establishment and administration of the federal government's XML schemas. This includes, in particular, responsibility for defining the elementary schemas of the federal administration, i.e. the so-called core components. In co-ordination with the Bremen-based steering group, the establishment of a multi-level repository is planned, especially within the framework of the DeutschlandOnline initiative.

This repository provides the relevant XML schemas and supplements these with registration data:

a. Source
    i. Authors
    ii. Contact partners
b. Documentation
c. Version management

d. Information concerning the status of the co-ordination process
e. Quality information, such as
    i. Scope
    ii. Binding effect

The federal government's central XML information point is currently being set up on the website of the Co-ordinating and Advisory Agency of the Federal Government for Information Technology in the Federal Administration (KBSt) at: http://www.kbst.bund.de/xml-technologie. The development of the joint platform with the steering group in Bremen can also be traced there. The XML information point will offer the following functions.

a. Provision of information
b. Communication platform for the exchange of experience between developers and users of XML schemas
c. Publication of and reference to methods, guidelines and directives for the use of the schemas
d. A catalogue of XML projects by the federal administration, including information concerning project contents and contact partners
e. A collection of core components
f. Establishment and provision of repositories
    i. UDDI service for the federal administration
    ii. Schema repository
    iii. References to other directories
g. Hub for exchanging with international bodies and institutions, for example, within the framework of schema standardisation work for European administration processes.

6 Computational viewpoint: reference software architecture

This chapter explains the architecture decisions made within the framework of SAGA and describes the resultant architecture models for the individual special application. For this purpose, some general preconditions and requirements for a software architecture for e-government applications are introduced first. Further sections explain the basic architecture decisions and apply these in the form of a reference architecture to a typical, albeit idealised, special application. This reference software architecture in the sense of the computational viewpoint according to the RM-ODP model[34] describes the technical structure of e-government applications. The section ends by presenting conclusions for the technology viewpoint from the software architecture.

The decision for Java and J2EE as the basic technologies is based on chapter 8 "Technology viewpoint (part I): standards for the IT architecture", because these technologies are mandatory[35]. It is, however, also possible to apply the reference software architecture to other technologies too.

6.1 Requirements and preconditions

The computational viewpoint in SAGA was introduced in order to offer technical assistance when drafting e-government applications, taking into consideration the goals[36] defined in SAGA as well as the philosophy and requirements described within the scope of the discussion of the enterprise viewpoint in chapter 4 with special emphasis being placed on re-usability and interoperability. One central aspect in this context is the integration of special and technical applications into existing and future e-government architectures and infrastructures, especially with a view to the derived basic modules.

6.1.1 Administration-specific preconditions and frames of reference

Design decisions for the establishment of a software architecture for e-government applications must consider certain requirements and frames of reference the most important of which will be outlined below.

6.1.1.1 Administration-wide services

As already discussed in detail in chapter 4[37], Germany features a very heterogeneous landscape of public agencies. This heterogeneity is in part due to Germany's

---

[34] Refer to chapter 3 "Architecture model for e-government applications", section 3.4 "Computational viewpoint", page 33

[35] Refer to section 8.3.1 "Application architecture with middleware", page 73

[36] Refer to section 1.3.2 "Target", page 14

[37] Refer to section 4.1.4.1 "The cross-administration approach", page 39

federal structure and the resultant, different administrative levels. Furthermore, responsibilities and requirements for the individual administrative branches vary from one administrative level to anther.

As a consequence of the de-centralised administrative structure, the individual administrative areas often implement their particular applications independently. The rendering of online services without media inconsistency is a central goal of e-government. Insular solutions make this almost impossible or lead to high costs when it comes to linking them together, especially in cases where multiple public agencies are involved in the rendering of a service.

6.1.1.2 Process optimisation

Besides avoiding insular solutions and parallel development work, the reorganization of process chains is also recommended. The goal being – as explained in chapter 4[38] – to simplify complex administrative procedures.

Simplifying processes in special procedures enables substantial cost savings when it comes to implementing special applications. Furthermore, error-susceptibility as well as updating and upgrading costs can be reduced significantly.

For example, the points where the qualified digital signature is absolutely necessary and where the use of an advanced signature is sufficient should be identified. Any amendments to the applicable laws must be considered in the form of the appropriate updates in such a case.

The e-government-manual, for example, offers comprehensive support with regard to process optimisation tasks[39].

6.1.1.3 Data protection requirements

Another central aspect in design decisions is to ensure adherence to data protection requirements. Despite all the advantages resulting from the central, non-redundant storage of data, measures must be taken to ensure adherence to all applicable laws when storing and processing personal data.

The software architecture must hence include certain security systems in order to ward off manipulation of data and attacks by hackers.

For further information related to the issue of data-protection-compliant e-government, please refer to the e-government manual[40].

---

[38] Refer to section 4.1.4.2 "Process optimisation", page 41

[39] Refer to the e-government manual (http://www.bsi.bund.de/fachthem/egov/6.htm), chapter V D, module: "eStrategie, Prozessanalyse and -gestaltung" [e-strategy, process analysis and design]

[40] Refer to the e-government manual (http://www.bsi.bund.de/fachthem/egov/6.htm), chapter II, module: "Datenschutzgerechtes E-Government" [Data-protection-compliant e-government]

6.1.1.4 Further frames of reference

Besides the preconditions and frames of reference already identified and described, further conditions exist which influence the architecture decisions to be made and the software architecture selected. These conditions are addressed in documents which are listed in section 1.5 "Relationship with other e-government documents" on page 17 with the scope of such documents on the one hand and that of SAGA being clearly distinguished in these documents.

6.1.2 Interoperability and reusability

As already described, it is particularly the media-consistent implementation of transaction services which involves special organizational and financial requirements for the individual public agencies. What is often needed is agency-spanning co-operation by linking together existing special applications and using cost-intensive software components, such as a payment platform or modules for supporting electronic signatures.

Reusability of software components and interoperability of the individual applications and components are indispensable preconditions for taking up these challenges.

The use of standardised and reusable processes within the framework of a uniform and standardised software architecture in e-government can help reduce costs in the long term. This standardised approach leads to uniform interfaces when it comes to drafting and implementing software projects, so that the special applications can meet the SAGA requirements and aims.

For this purpose, basic modules were identified in a first step in chapter 4[41]. These basic modules must be integrated into a software architecture as a precondition for their use in conjunction with the implementation of special applications. The software architecture cannot be of a random nature, instead it must satisfy certain requirements and criteria in order to achieve the goals set.

6.1.3 Further basic requirements for a software architecture

Besides the concrete aims of the development of a special applications which can, for example, be concluded from specific technical requirements, any system to be developed must also fulfil a number of general requirements. These general aims and/or basic requirements for a special application must be considered in the design decisions to be made within the framework of the software architecture.

a. Security
   Confidentiality, authenticity and reproducibility as well as compliance with the Federal Data Protection Act and the relevant security-related chapters of the e-government manual must be ensured in the use of e-government applications.

[41] Refer to section 4.2.3 "Modules for the implementation of electronic procedures", page 49

b. Reusability
   Reusability of an e-government application or of one of its components is one of the central requirements which is to be achieved by adhering to and using SAGA. Redundant development of applications for similar or identical services is thereby avoided, so that cost savings can be achieved in the long term. Furthermore, the use of tried-and-tested modules enhances the quality of the entire system.

c. Flexibility
   Adjustment to new frames of reference as well as upgrades are easily possible and/or at a reasonable cost.

   E-government applications must be designed in such a manner that modifications of or amendments to an application – resulting, for example, from changes in legislation, process optimisation or use by other public agencies – can be carried out in an effective manner and at a reasonable cost.

d. Openness
   In order to enable simple integration of existing or new systems, the system in use must include well-defined and well-documented interfaces.

   Many public agencies already operate cost-intensive legacy systems. The communication protocols defined in SAGA should hence enable smooth integration, especially with a view to legacy systems. The openness of an e-government application is one of the crucial factors for its successful use.

e. Scalability

   Distribution of an e-government application or its individual components must be possible without any problems. This is the only way to ensure the ongoing use of an application in an efficient and performant manner as use increases. Especially in the case of an e-government application which is centrally operated, the number of public agencies using it is not definite, so that its future, cost-effective scalability must be ensured when the number of public agencies and users increases.

f. Performance
   A short response time of an application is vitally important in order to ensure its widespread acceptance among citizens and businesses. Complex transactions often require processing large amounts of data. The successful use of an application is contingent upon the user-friendly and performant provision of data.

g. Availability
   Access to e-government applications must be permanently ensured. A permanently available application signals reliability and trustworthiness, so that citizens and businesses become more and more willing to use the application and to supply the – typically confidential – data necessary for the transaction represented by the application.

h. Error tolerance
   The system must be capable of handling unforeseen and invalid system states. Errors or unforeseeable events may not lead to a crash or uncontrolled system behaviour which the user is unable to understand.

Very much like availability, error tolerance is an important parameter for the trustworthiness of an application. Faultless, transparent operation of an application is a vital prerequisite for the user's trust in complex transactions.

i. Updating capability
   Operation and updating of e-government systems should be as simple and easy as possible. External experts who were not involved in the development of the system must be capable of ensuring efficient system maintenance and updating even without longer familiarisation time.

This enumeration approximately reflects the priorities of the individual requirements under technical software aspects. The concrete weighting of the individual aspects depends on factors which must be identified and evaluated when developing the concept for the particular special application. In the case of applications with very high access rates, for example, availability is probably more important, whilst security issues are likely to be a higher priority in conjunction with complex approval and licensing procedures.

6.2 Architecture decisions

The software architecture outlined here involves several fundamental design decisions. These are the mandatory use of object-orientated software development paradigms and a component-based software development approach on this basis.

Component-based software development

In the context of this reference software architecture, software components are defined in exactly the same manner discussed in section 2.3.1 on page 27.

Component-based software development enables the compiling of software from existing components and their reuse. This system is expected to yield several positive effects, such as:

a. faster development and provision of the application
b. lower costs
c. higher quality
d. less complex structure
e. flexible application systems and modern system architectures

However, the use of component-based software development not only has positive consequences. Development costs and requirements are initially higher, additional training costs may be incurred, and design errors can lead to an unwanted dependence on components which adversely affects the system architecture. Although the advantages are likely to be felt rather in the medium and long term whilst negative effects cannot be ruled out in the short term, the e-government sector is nevertheless perfectly suited for the use of software components due to project cycle times and the high share of similar and comparable applications. In order to develop robust,

reusable components, clear-cut functional definitions of the components are necessary in order to generate maximum benefits by reducing parallel development efforts.

Separation of presentation and business logic

Separating presentation and business logic offers a technical solution for the optimum support of multiple presentation channels, such as different browser types or mobile devices, such as personal digital assistants (PDAs). Besides this aspect, the separation of presentation and business logic significantly enhances the quality of code structure, thereby substantially improving updating and trouble-shooting capabilities, flexibility, reusability and reproducibility whilst at the same time lowering costs in the medium term. Furthermore, such a separation enables the potential distribution of an application to several servers, with one server being responsible for the presentation tier and another one for the business logic. This has a positive impact on operation with regard to security, upgrading capability and scalability aspects. Special attention should be paid here to communication because a less-than-optimum distribution adversely affects performance.

Separation of business and data logic

The separation of business and data logic leads to applications which are independent of the database type[42]. At the same time, functionality is not directly dependent on the database via abstraction and performance, for example, by caching.

Four-tier architecture

The implementation of the above-stated aspects leads to a multi-layer architecture with four tiers. The implementation of a special application in tiers with the inclusion of components calls for a clear-cut assignment of components to a specific tier. This facilitates the classification of components and implies formal definitions of their functionalities.

The individual tiers of the multi-tier architecture are the client tier, the presentation tier, the middle tier and the persistence tier / back-end.

a. The **client tier** is where users and application software interact. The data processed by the presentation tier as well as the user interface are visualised.
b. The **presentation tier** is responsible for presenting the application data (for example, as a website).
c. The **middle tier**, also called the application tier, accommodates the most important components for implementing the application logic irrespective of their presentation. This is where the program sequence is controlled. The data from the persistence tier is processed accordingly and passed on to the presentation tier where user entries are validated or authorisation is granted, for example. An optional part of this tier integrates central components, legacy or ERP systems,

[42] In the sense of relational database vs. object-orientated database

when necessary. External services can be given access via application interfaces to the application without having to use the presentation tier.

d. The **persistence tier** is responsible for the storage of data objects. It abstracts from the database. The **back-end** as a collective term represents functionalities of the operating system, specific databases as well as existing, non-SAGA-conforming special applications, legacy or ERP systems.

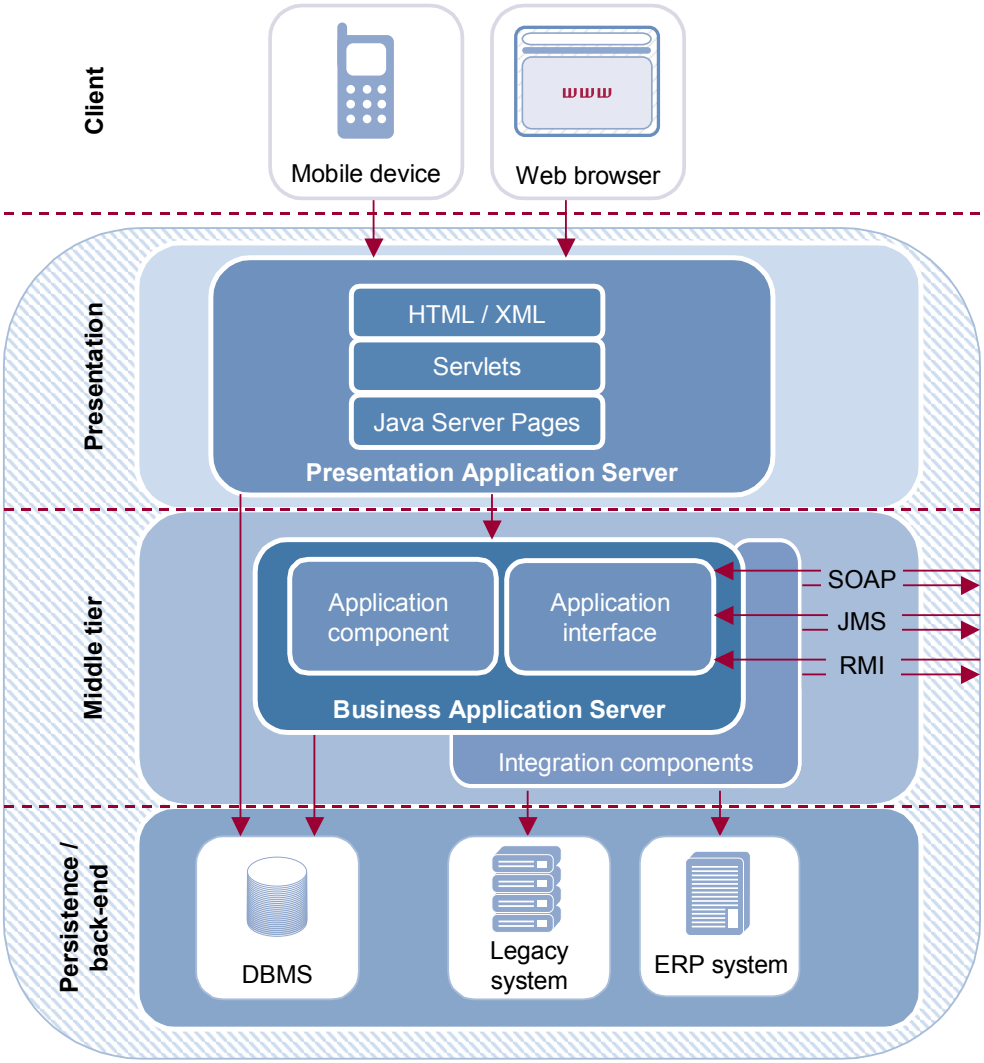


Figure 6-1: Example of a four-tier architecture for e-government applications

Figure 6-1 is a graphic illustration of the structure. It shows the structure of the presentation tier which consists of a presentation application server for presentation purposes and the related individual components, such as Servlet Engine. The business application server in the middle tier forms the backbone of the application and, via application interfaces, enables other applications to use the special application as a service.

The middle tier can be omitted in the case of simple applications which are neither transaction-based nor use special integrative functionalities. However, for the pur-

poses of the following discussion of an idealised, typical special application, this case will not be addressed in more detail.

Java and J2EE

The multi-tier architecture is preferably implemented using the Java programming language as outlined in section 8.3.1 "Application architecture with middleware" on the technology viewpoint on page 73. The decision in favour of Java is based on its platform-independence, optimum support of object-orientated software techniques, stability of the execution environment and the large number of free and commercially available APIs. One may conclude that the use of Java ensures optimum support of a multi-tier architecture.

The focus on a middle tier and the use of Java logically suggest the use of J2EE. The result is a detailed technical paradigm for software production and the basis of an application framework.

An application framework defines the standard behaviour and the structure of all applications using a group of abstract[43] and concrete[44] classes which are tuned to each other. New applications are created by deriving concrete classes from the abstract framework classes and adding independent, application-specific classes. Similar objectives are pursued with regard to the purposes of application frameworks and components. Application frameworks should also lead to the reusability of program components. This is, however, achieved by inheritance on class level. However, productivity and quality gains during the development of interactive application systems are also faced with certain disadvantages, such as a high degree of complexity and inflexible structures which can lead to unforeseen problems during application development. However, the component approach makes the attractive application framework concept for the reuse of software structures flexible and hence constitutes a perfect supplement.

Weak connections between distributed components

Tiers and components are connected to a harmonious overall system within the multi-tier architecture by standardised, identical interfaces. This is a necessary precondition for joining applications from any components together. Furthermore, a weak connection of distributed components should be preferred.

Communication between components via method calls or web services

HTTP-based network protocols are used for communication between components of the client and presentation tiers. The components of the application tier communicate via method calls or interfaces which are determined by a component framework. In

[43] Abstract classes define interfaces only which are then filled by concrete methods of a sub-class.

[44] Complete, fully implemented classes featuring a particular functionality.

the case of communication with distributed components or with components which, in view of their specific application, are available as central components only, communication proceeds via web services even on the middle tier.

XML-based data interfaces

Data interfaces with external systems must be generally implemented via XML and the related schema definitions[45].

6.3 Reference architecture for e-government applications

The architecture features described in the preceding chapter are discussed in more detail and applied on the basis of a reference architecture for an idealised, typical special application. As explained in the section on architecture decisions, this special application is configured as a component-based system according to the four-tier model.

6.3.1 Basic functionalities of the components used

One feature which all the components of an application have in common is that they can avail themselves of the general services of an infrastructure, such as support of test methods, logging and monitoring. These services ensure certain given infrastructure interfaces of the components. For information concerning the implementation of this basic functionalities, please refer to: http://www.kbst.bund.de/saga-tools.

Support of test methods

Guidelines orientated towards issues of process organization exist in addition to recommendations for software structures. The important step of debugging and testing an application is, for example, often separated from the real development step and sometimes even neglected. Test scenarios should be considered and firmly integrated into the development process as early as during the performance specifications phase.

Logging

Uniform procedures for handling system information are recommended in order to facilitate the operation of an application. Standardised log components and formats must be in place for this purpose. The size of a log file should not grow infinitely, but must also cover a certain reasonable period of time. This calls for a log file management mechanism which can be based on file size parameters or time aspects. Under normal working conditions, no information other than errors should be recorded in the log file. In order to enable the recording of data which is, for example, needed for analysis purposes, a mechanism must be in place which enables log levels as well as

[45] Refer to chapter 5 "Information viewpoint: schema repository", page 51

activation and deactivation of log messages from certain levels. Log levels are used to classify events with regard to their relevance within the framework of the application / component function. To this effect, the cases in which log levels are to be applied should be clearly identified during the software architecture design phase.

Monitoring

Monitoring for the purposes of this section refers to the monitoring of individual system resources during ongoing operations with a view to their status or performance, for example. The monitoring service is designed as a tool for system operators helping them to identify the current system status. This requires a definition of operating conditions and states and the implementation of suitable mechanisms at the application end in order to provide system status information.

Configuration management

This term in this context refers to the system and/or system resource configuration. Whenever possible, the same mechanism should be adopted for all the components, enabling central configuration of all the components. It should be possible to configure important system parameters even during the system runtime. Application solutions are in most cases based on static configurations which are saved in so-called property files. Re-configuration, for example, of the log level, often requires restarting the application. This should be avoided.

Error treatment

If a component fails and consequently stops working with an error, it must be possible to trace the error throughout the entire processing path. This means that the log of an error situation must show the origin of the error. This information is usually available from the normal stacktrace of an application. Furthermore, the log should contain as much additional information as possible, so that a problem can be quickly identified and remedied. In the case of web applications, for example, a tried-and-tested approach is to state the complete request (including the URL) which caused an error.

Security

Components giving access to critical or sensitive data or executing write transactions on such data must fulfil the security requirements discussed in chapter 9 "Technology viewpoint (part II): standards for data security" on page 95 and following.

6.3.2 Structure of a typical special application

On the basis of the existing infrastructure of a public agency, special applications must be implemented which can be easily integrated into this infrastructure on the one hand whilst also being able to cooperate with existing applications on the other. This cooperation not only includes communication, but first and foremost strives for technical identity in much the same manner as it is aimed at in SAGA in order to

minimise installation, maintenance/updating and implementation costs. When a special application to be implemented is drafted, the components to be newly developed and areas in which existing components can be reused are selected from the point of view of the components concept. In this sense, the basic components mentioned in Appendix A "Basic modules of the BundOnline initiative" on page 111 and following should checked first and foremost with regard to their suitability.

The special application in question implements a transactional e-government service and is thereby based on the focal orientation outlined in the enterprise viewpoint in section 4.2.1.1 "Interaction levels" on page 44.

Typical communications take place between the client tier, the web browser as the thin client as favoured herein, and the presentation tier. Certain components of the presentation tier convert the data – which can, for example, exist in XML format – to HTML format as needed by the web browser.

The real application logic is implemented on the middle tier. The tasks of a web application include, for example, validating user entries and comparing these to the related data stocks and processing and transmitting the data to the presentation tier.

The middle tier is also where communication and logic integration of basic components take place, such as e-payment and data security as well as "one for all" (OFA) services. The services of the special application are offered to external applications via application interfaces. In line with the business cases mentioned in section A.1.3 on page 113 and following, the e-payment basic component implements payment transactions. The condition for use of the basic component requires that it be operated centrally by the Federal Finance Office. The special application hence communicates via web services on an SOAP basis[46]. The "data security" basic component is operated in a de-centralised manner and, in line with the business cases, covers the security aspects related to the exchange of documents and e-mail communications.

Besides the use of SOAP, communications with distributed components also use Remote Method Invocation (RMI)[47] or a message service[48]. The components of the persistence tier implement database access and caching strategies.

In reality, a special application will always have to be fitted with integration solutions because it must communicate with an existing data system. These integration components as shown in Figure 6-2 "Reference software architecture" are directly located on the middle tier. For this purpose, the components to be developed will offer ways to communicate with other systems, such as SAP solutions.

---

[46] Refer to page 88

[47] Refer to page 88

[48] Refer to page 74

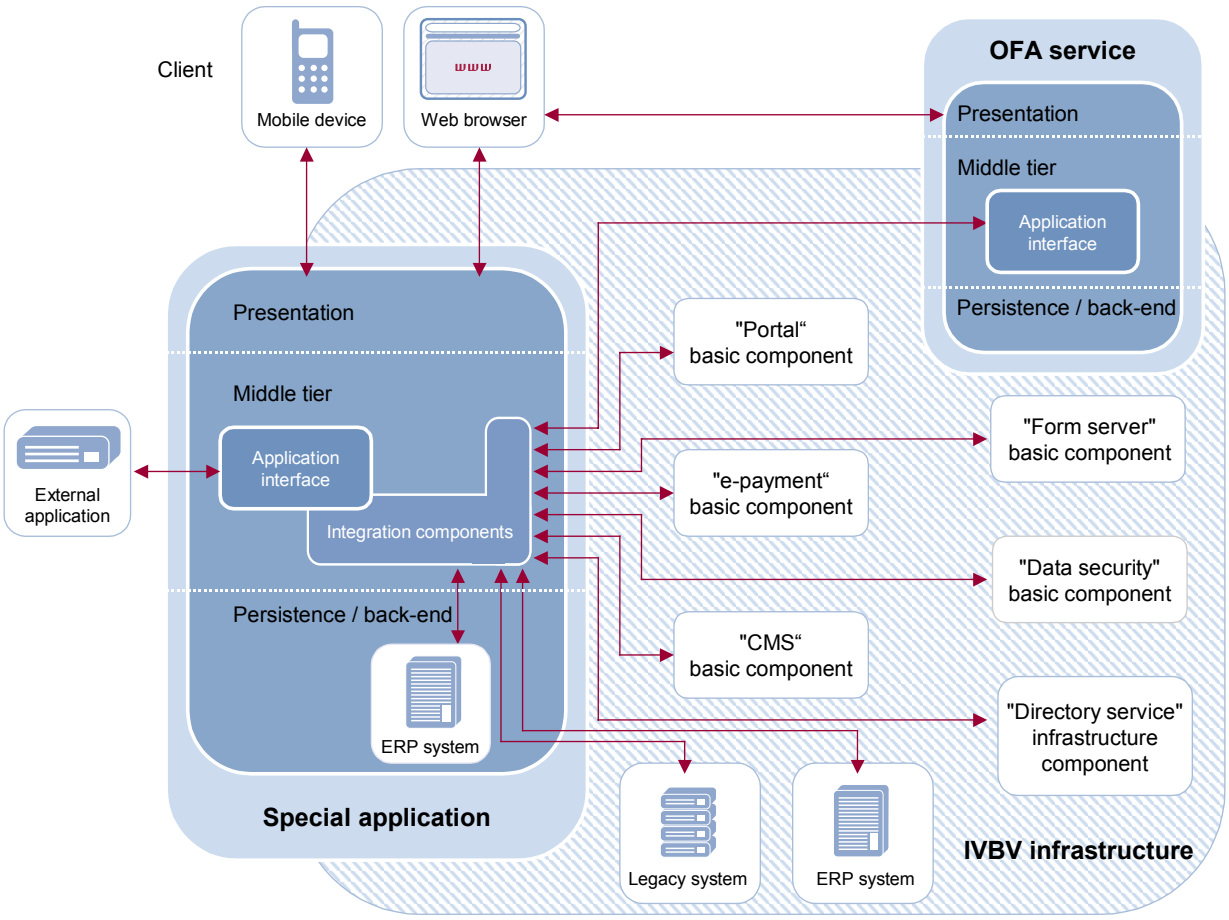


Figure 6-2: Reference software architecture

The implementation of a real special application chiefly involves the implementation of identified components and their communication with the above-mentioned basic functionalities. The requirements for the software quality components are high in terms of clear functional definition, robustness and documentation in light of the intended reusability. The final step is to assemble the components to an executable application. This effort can draw on existing frameworks on the one hand and the configuration management which is supported by all the modules on the other.

6.4 Conclusions from the software architecture

The preconditions and architecture decisions discussed in this chapter have all kinds of consequences for the following chapters dealing with the engineering and technology viewpoints.

The underlying architecture decisions are partly documented as mandatory standards in the corresponding sections. This includes, for example, the specification of J2EE in section 8.3.1 "Application architecture with middleware".

7 Engineering viewpoint: reference infrastructure

The selection of the appropriate infrastructure is a central success factor when it comes to planning, designing and operating e-government applications. A stable and secure IT infrastructure is the basic precondition for the reliable operation of e-government applications with high reliability. Today's data protection, data security, efficiency and availability requirements for e-government set high standards for operators of applications and infrastructures.

The reference infrastructure for e-government applications is modelled on the basis of the engineering viewpoint according to RM-ODP[49] and describes the encapsulation of system units and their connections. Although the standards and technologies of the reference infrastructure described do not form part of an engineering viewpoint in a stricter sense, they were nevertheless included in order to make the presentation as realistic as possible. The following explanations can be broken down according to the top-down approach to an engineering viewpoint of a single special application.

The recommendations by the German Federal Office for Information Security (BSI) on the security of e-government applications[50] and the BSI's IT Baseline Protection Manual[51] deserve special consideration in this context. If a lower protection demand is identified for special applications, less demanding security requirements can be applied to a given infrastructure than those considered in the following reference.

Not every public agency requires its own, complete e-government infrastructure. Smaller institutions may well use the computer centers of external IT service providers or higher-level public agencies.

7.1 Design of an e-government infrastructure

The introduction of a reference infrastructure in SAGA serves the aim of defining the infrastructural preconditions necessary for the operation of e-government applications and the required system architecture. The following goals are to be achieved by defining parameters or a reference infrastructure in the sense of an operating environment.

a. Physical protection of systems
b. Maximum availability of systems
c. Increasing the security of systems and system components through classification on the basis of their protection demand

---

[49] Refer to chapter 3 "Architecture model for e-government applications", section 3.5 "Engineering viewpoint", page 35

[50] Refer to the e-government manual at: http://www.e-government-handbuch.de/

[51] Refer to http://www.it-grundschutzhandbuch.de/

d. Classification of systems and system components according to separate security zones
e. Scalability of systems and infrastructures
f. Simple service, efficient maintenance and updating of complex e-government applications and system components by operating personnel

Figure 7-1 shows a general overall view of a distributed e-government application with the user, network and infrastructure areas.

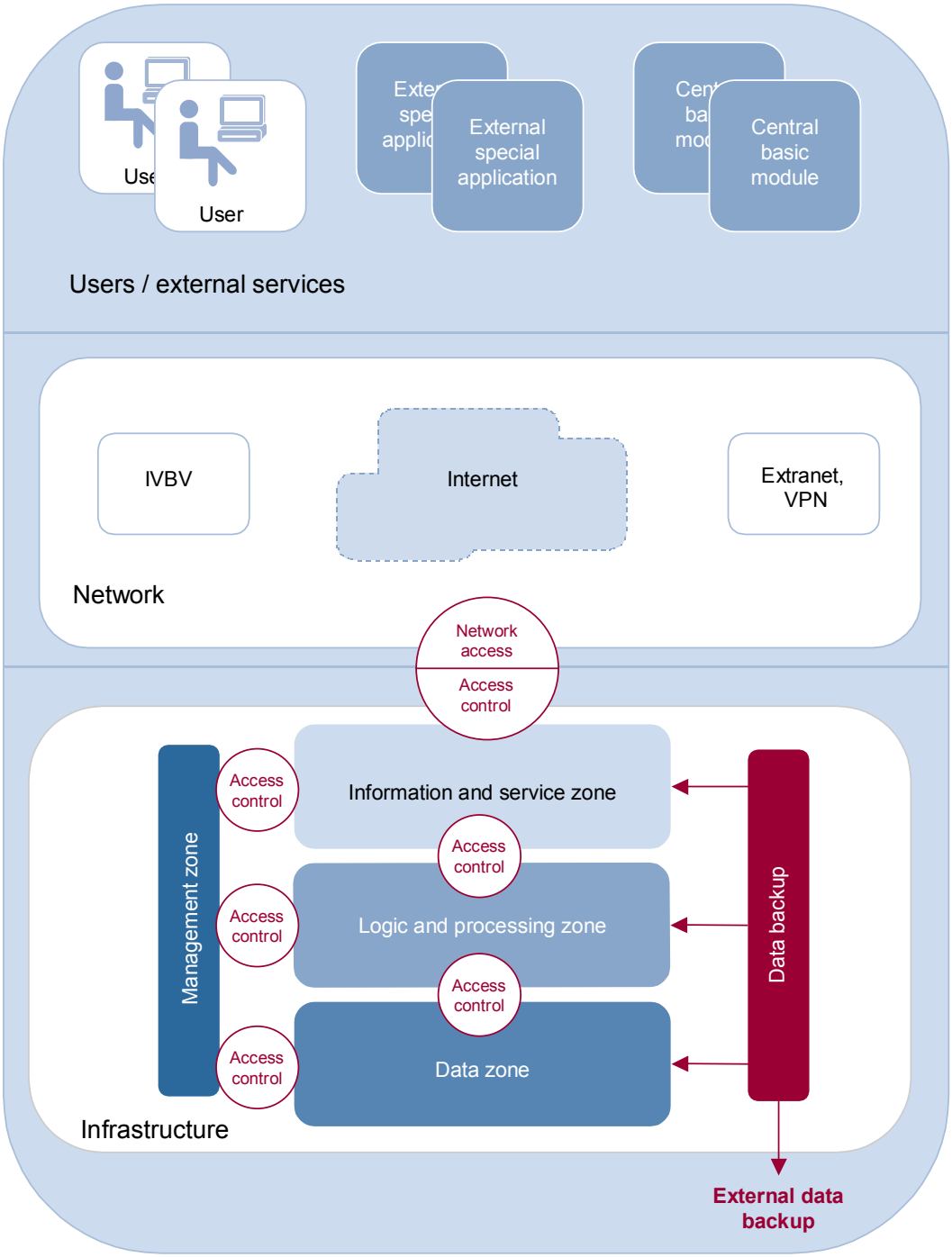


Figure 7-1: Engineering viewpoint of an e-government application

Both the network and the user areas are typically beyond the control of the operator of an e-government application and hence do not form a focal point of interest in this discussion. The infrastructure area, in contrast, is controlled by the operator and must feature a suitable architecture and system structure in order to meet the operational requirements for e-government applications.

The requirements for a computer centre and its IT infrastructure are described below.

7.1.1 Physical infrastructure

The protection of systems against external influences, the elements and unauthorised access requires the provision of suitable space. Computer centres designed to host e-government applications should hence at least feature the following properties.

a. Fire-resistant, structurally enclosed security space protected against radio interference
b. Access control, including personal authentication
c. Fire-extinguishing system with non-corrosive and non-toxic extinguishing agents
d. Redundant power supply, including uninterruptible power supply
e. Redundant air conditioning system
f. Data backup media in a fire-resistant vault outside the computer centre

7.1.2 Zone concept and communication relations

The systems inside the computer centre are located in different zones which are defined on the basis of the relevant safety and security requirements for the services and data of the respective zones. In order to ensure that the zone concept covers the general protection requirements of e-government applications, the four zones described below should at least be implemented within a computer centre's infrastructure. Operation of complex e-government applications may require further zones. The zones should be strictly physically separated. This means:

a. Any network component (router, switch, hub, etc.) can only be used as an interface between one zone and another, so that any network component only passes on data concerning or originating from the two zones directly connected to it. This prevents any mixing up of data streams in the case of a fault or deliberate attack.
b. A server system can host the systems of a single zone only. This means that distributed applications must run on server systems in different zones.
c. A server system with e-government applications requiring communication connections to several zones must include a corresponding number of physically and logically separated network connections (for example, multiple network cards). This system thereby rules out a transition from one zone to another.

Information and services zone

The information and services zone covers that part of the network which is located between the Internet and the other zones of the network. This zone contains servers which can be accessed by external networks or which, for their part, use the services of external networks. Further information zones should be set up if systems with different security levels are to be operated.

Communication between systems of the information and services zone on the one hand and systems of the logic and processing zone on the other should be protected by encrypted communication channels.

Logic and processing zone

The systems of this zone process data from the data zone and make such data available to users via systems of the information and services zone. Direct communication between external networks – such as the Internet – and the logic and processing zone is not permitted.

Data zone

The data zone contains all the systems where data is stored and made available for longer periods of time. Access to this zone is permitted from the processing zone and the management zone only. Direct access from external networks is not permitted under any circumstances. Furthermore, no other zones except the management zone may be actively accessed from within this zone.

Management zone

The management zone contains all the systems which are needed for administrative purposes or for monitoring systems in the other zones. Furthermore, this zone can also contain central user administration or authentication services. Access from the management zone to other zones and vice versa is hence permitted.

Access from within external networks to the management zone is not permitted under any circumstances.

Data backup

Every zone should include its own data backup components. Data of the information zones should be backed up via protected communication channels.

7.1.3 Network access and access control

Access control systems control the separation of the individual zones within the computer centre as well as access by and to external networks. Different technologies can be used for these purposes.

The interface between the information and services zone and external networks is the most security-critical point and is hence protected by a combination of multiple

security mechanisms. Separation into different network segments and address areas is implemented here on the network protocol level. Internal network addresses are masked in TCP/IP-based networks on the basis of the Network Address Translation (NAT) protocol, and are hence not published in external networks.

Furthermore, filter mechanisms are in place to ensure that access from external networks is restricted to defined services in the information and services zone. The filter rules are typically implemented on firewalls or firewall routers which examine the information in the headers of the incoming data packages on the basis of package filters and reject unauthorised access attempts.

Furthermore, application gateways can be used which fully isolate communications, validate data streams on the application level and, when necessary, implement a protocol-conforming re-generation of requests.

The communication relations between the internal zones are also subject to access control systems. In order to adequately control access to the sensitive areas of the logic and processing zone as well as the data zone, firewalls should be used because of their comprehensive filter options. These firewalls work on the basis of dynamic package filters (stateful inspection) and are capable of monitoring not just individual packages but even communication streams involving multiple packages. Dynamic package filters enable the validation of network connections not just on the basis of invariable rules but additionally even on the basis of historical communication relations.

Thanks to simple and flexible administration, VLAN technology is the system of choice for controlling access to the systems in the management zone. For this purpose, all the systems requiring access to a service in the management zone are combined to form a virtual network segment (VLAN). In order to prevent unwanted communication between the individual zones via the VLANs of the management zone, all the systems are fitted with a second network interface which may not be used for any purposes other than administration and which is fitted with a package filter.

Using VLAN technology for connecting any zones other than the management zones is not recommended for security reasons.

7.2 Network, users and external services

The network level is the link between the systems of the computer centre infrastructure and external services as well as users of e-government applications. This level covers both the Internet, the Federal Administration Information Network (IVBV) as well as further VPN-based networks or extranets. Intranets also form part of the network level. Although a clear consolidation trend has been observed in recent years in the field of network technologies, a host of different technologies are still in use. However, abstraction on higher protocol or application levels can make the system

interoperable, so that SAGA does not give concrete technology recommendations for the network level.

From the point of view of the engineering viewpoint to an e-government application, however, secure and performant communication with the Internet, IVBV or extranets has an important role to play in order to ensure reliable access to users and external services. When e-government applications are designed, the necessary bandwidths must hence be made available on the basis of an assessment of the anticipated network communication, and the access control mechanisms described in section 7.1.3 must be implemented.

The BundOnline 2005 initiative offers several external services in the form of basic and infrastructure components both on the Internet and via the IVBV. For additional information concerning the IVBV infrastructure component, please refer to Appendix A "Basic modules of the BundOnline initiative", section A.6, page 139.

Further services, such as the e-payment basic component, can be accessed via web service interfaces on the Internet. For this purpose, the basic component provides the web service interfaces necessary on the server end on the one hand as well as a reference implementation for calling the web services by the relevant e-government application on the other. Communication with external special applications of other public agencies or businesses proceed in a similar manner; middleware communication interfaces may be used for these purposes too.

De-centralised basic modules, in contrast, such as "data security" basic components, are implemented within the computer centre infrastructure of the individual public agencies. The rules already described in section 7.1 should be followed in this case too.

8 Technology viewpoint (part I): standards for the IT architecture

In this chapter, technical standards are assigned to the individual elements of the architecture model introduced in chapter 3. Furthermore, this chapter also provides brief descriptions of these technical standards. If no version numbers of standards are stated, the version which is most stable from a market point of view should be used, even though this is not necessarily the latest version.

8.1 Process modelling

Mandatory: Role models and flow charts

Role models and flow charts can be used to define simple processes. All the roles and systems related to a process must be identified, and the process steps must be described in the form of flow charts. Flow charts should in a broader sense be orientated towards DIN 66001: "Informationsverarbeitung, Sinnbilder und ihre Anwendung" [Information processing, symbols and their use].

Recommended: Unified Modeling Language (UML)

The Unified Modeling Language (UML)[52] should be used for object-orientated modelling for the preparation and documentation of large projects. Use cases are a particularly tried-and-tested way of creating and co-ordinating transparent specifications. UML is, however, a complex application that requires skills and, when necessary, the use of special tools. On the other hand, however, XML data structures or Java program parts can be directly generated from the appropriate specifications.

8.2 Data modelling

8.2.1 Modelling tools

Mandatory: Entity Relationship Diagrams

Functional data models for the development of coarse technical concepts are to be presented in the form of Entity Relationship Diagrams.

Mandatory: XML Schema Definition (XSD) v1.0

The data specification is to be implemented as an XML schema (refer to the following section 8.2.2).

[52] Refer to http://www.omg.org/

Under observation: Unified Modeling Language (UML)

The Unified Modeling Language (UML)[53] can be used for object-orientated modelling for preparing and documenting large projects. XML schemas can be directly generated from the corresponding specifications.

8.2.2 Data description

Mandatory: Extensible Markup Language (XML)

XML (Extensible Markup Language)[54] is to serve as the universal and primary standard for the exchange of data between all the information systems relevant for administrative purposes.

New systems to be installed should be capable of exchanging data using XML. Existing systems do not necessarily have to be XML-enabled.

If necessary, it is also possible to use middleware which interprets incoming XML information and transforms or converts such information to the data format required by legacy and/or external systems. This process can take place in either direction. The performance and execution of a transaction can be monitored by workflow and transaction mechanisms.

Mandatory: XML Schema Definition (XSD) v1.0

XML schemas according to World Wide Web Consortium (W3C)[55] are to be generated using the XML Schema Definition (XSD) for the structured description of data.

8.2.3 Data transformation

Recommended: Extensible Stylesheet Language Transformation (XSLT) v1.0

If applications use different XML schemas, conversion from one format to another can become necessary for data interchanging purposes. This format conversion is carried out via the XSLT[56] language defined by W3C as part of XSL (Extensible Stylesheet Language).

---

[53] Refer to http://www.omg.org/

[54] Refer to http://www.w3.org/XML

[55] Refer to http://www.w3.org/XML/Schema

[56] Refer to http://www.w3.org/TR/xslt

8.2.4 Character sets

The standards defined in section 8.5 "Presentation"[57] are applicable to the character sets to be used for exchanging data. The character set of individual parts of XML schemas can be further restricted in this context.

8.3 Application architecture

This section defines programming languages as well as technologies for implementing the application architecture. The first part defines standards for the middleware tier of the e-government architecture module with special emphasis on the aspect of application integration. This is followed by an extension of the standards to cover applications without middleware, so that the middleware standards can also be used for simpler applications.

The specifications and recommendations are based on the design principles that were laid down in the implementation plan of the BundOnline2005 initiative, i.e. operating-system neutrality, interoperability and portability.

Middleware services – such as replication, distributed transaction management, personalisation, internationalisation, messaging, etc. – are referenced in the current version to a limited extent.

Deviations from the technologies to be preferred (i.e. mandatory, recommended technologies) are acceptable in justified cases, for example, in the case of significant economic advantages.

8.3.1 Application architecture with middleware

Mandatory: Java 2 Platform, Enterprise Edition (J2EE) v1.4

The development and integration of the following applications (integrated applications) on the middle tier, i.e.

a. basic components,
b. applications which directly integrate basic components or libraries provided for this purpose, and
c. applications designed, as a whole or in part (components), for re-use (porting)

require the use of Java 2 Platform, Enterprise Edition (J2EE)[58] technologies. J2EE is a specification which defines several programming interfaces and a development process. J2EE in its entirety constitutes an architecture that considers and supports major aspects of business-critical applications. J2EE already offers important function modules which can be used to develop applications. Versions 1.4 and higher include,

---

[57] Refer to section 8.5.1.4 "Character sets", page 80

[58] Refer to http://java.sun.com/j2ee/

as so-called core libraries, even standard application programming interfaces (APIs) and technologies which were still classified individually in SAGA 1.1, i.e. Java Authentication and Authorization Service (JAAS), Java API for XML Parsing (JAXP) and Java Naming and Directory Interface (JNDI). All the core libraries should be given preference over alternative technologies.

Compared to J2SE, J2EE offers as so-called optional libraries several APIs and technologies, including, for example, the following: Java Message Service (JMS) 1.1, J2EE Connector Architecture 1.5, Java Transaction API (JTA) 1.0, JavaMail API 1.3, Java API for XML Registries (JAXR) 1.0, Java Management Extensions (JMX) 1.2, Enterprise JavaBeans (EJB) 2.1, Web Services 1.1, Java Server Pages (JSP) 2.0 and Servlet API 2.4. In the following, the use of the JMS and J2EE Connector Architecture communication technologies will be classified as mandatory. The Java EJB and Servlet-API middleware technologies form the basis for application server applications.

Thanks to the Java Community Process[59], more and more application-near modules will increase the diversity of J2EE in the near future. New modules are defined via so-called Java Specification Requests (JSR).

Mandatory: Java 2 Platform, Standard Edition (J2SE) v1.4

If an application does not require the full J2EE functionality either initially or on a permanent basis, J2EE technologies should be used individually as an alternative solution. The basis for this is the Java 2 Platform, Standard Edition (J2SE)[60]. The individual technologies should be used in accordance with J2EE Specification 1.4 in order to create a compatible migration path to J2EE.

Mandatory: Java Database Connectivity (JDBC) v3.0

JDBC should be used for access to databases.

Mandatory: Java Message Service (JMS) v1.1, J2EE Connector Architecture v1.5

Either the Java Message Service (JMS)[61] or the J2EE Connector Architecture should be used to integrate external systems.

Under observation: Microsoft Windows .NET Framework

.NET Framework is a middleware technology which was developed by Microsoft. The system architecture of .NET includes a runtime environment for different program-

[59] Refer to http://www.jcp.org/

[60] Refer to http://java.sun.com/j2se/

[61] Refer to http://java.sun.com/products/jms/

ming languages and a development environment. It supports major web standards (including SOAP, WSDL, UDDI, XML).

Core components of the .NET middleware were standardised by international organizations. Projects are currently underway which aim to implement core components of the .NET middleware on non-Windows operating systems.

The .NET architecture does not yet fulfil the portability requirements on an operating-system-independent basis. It is expected that Microsoft will develop the .NET technology to an open standard whilst also ensuring conformity with the standards contemplated in SAGA in this context.

8.3.2 Application architecture without middleware

In addition to the standards discussed in the previous section, the following technology is also available for simple e-government applications without middleware.

Recommended: PHP: Hypertext Preprocessor (PHP) v4.x

PHP[62] (recursive acronym for "PHP: Hypertext Preprocessor") can be used for applications without an integration requirement, i.e. non-distributed stand-alone applications which do not communicate with one of the basic components, legacy systems or other special e-government applications). PHP is developed as an open-source project by the Apache Software Foundation and represents a script language embedded in HTML for developing web applications.

8.4 Client

The client is a software on a terminal device which makes use of a service offered by the middle tier. The client tier includes both the classical user site with all the options state-of-the-art technology has to offer in order to interact with public administrations, with access to information possible via different media. In Germany, the following media are currently the most popular, so that optimum conditions for the widespread use of e-government applications will exist if the information on offer is tailored to these devices:

a. Computers (PCs, laptops)
b. Mobile phones / personal digital assistants (PDAs)
c. External systems (such as ERP systems by industrial companies)

Standardisation efforts for game consoles and, in particular, for digital interactive TV have not yet resulted in uniform recommendations. The so-called "thin client" seems to be the most promising device in terms of public acceptance. Thin clients come with very low-profile hardware and software and require the server to provide as much functionality as possible.

---

[62] Refer to http://www.php.net/

8.4.1 Web-based / computer-based access to information

Two different clients are generally available on computers in order to access or receive information, i.e. web browsers and specific client applications (such as Java Clients – also Applets) which, for example, enable direct access to Internet-based services, e-mail clients and to the operating system, depending on privilege levels. Whenever active contents are used, no client technologies other than those permitted in SAGA may be used. The use of Active-X-Controls is generally not permitted. When active contents are used, a parallel offer without active contents should also be available, if possible (refer also to section 1.3.1).

8.4.1.1 Web browsers

In order to enable a wide-spread use the of e-government applications on offer, web browsers should be used as the front-end device which must be capable of processing and presenting the presentation-tier formats (refer to section 8.5). The following browser-based client technologies are permitted in this context:

a. The use of cookies is permitted on condition that
   i. these are not persistent and
   ii. websites of a domain do not include contents of other domains which set

   The recommendations for the HTTP protocol according to section 8.6.3 must be taken into consideration in this context.
b. The use of Javascript is permitted on condition that a server certificate and an SSL connection (refer to section 9.3.1) are used in order to enable the client to identify this as authentic and integer. Section 8.5.1.5 must be taken into consideration when Javascript is used.
c. The use of Java Applets is permitted if these are signed by the server and can hence be identified by the client as authentic and integer. Manufacturers of Java Applets must subject their product to quality assurance, preferably by an independent software company, or must at least warrant the required quality in the form of a self-declaration. Further information on this subject can be found on the web at: http://www.kbst.bund.de/saga-applets.
d. A positive list of supported plug-ins is kept and published on the web at: http://www.kbst.bund.de/saga-plugins.
e. Configuration examples are prepared for usual browser types and made publicly available by the BSI on the Internet.
f. The confidentiality of form data must be ensured by the use of SSL-encrypted channels and the pertinent server certificates.
g. The statutory instrument (ordinance) on barrier-freedom remains fully applicable to the use of permitted client technologies.

8.4.1.2 Client applications with direct access to Internet-based services

The web browser is the standard client for applications with direct access to web servers. Client applications can be used if the functionality of a web browser must be reasonably seen to be inadequate, for example, in cases of complex business transactions with direct file system access or use of legacy software. These applications are installed on the client and must be updated as required by technical progress. Updates can be made available on CD-ROM or as signed applications for downloading from a website. The use of Java applications is recommended for this purpose (advantage: platform independence).

Client applications must meet with the following requirements:

a. Any personal and security-critical data is stored in encrypted form on the local data medium.
b. Secure data transmission to the server is supported, for example, in accordance with the OSCI transport specifications. No protocols other than those defined in section 8.6.1.2 are permitted for any other client/server communications.
c. The formats documented in SAGA for exchanging user data with other applications should be supported.
d. A manufacturer-independent software firm assures the quality of the application.
e. The application is supplied along with a software certificate which is verified during the course of the installation.
f. Besides an option to download the application from the Internet, distribution on CD-ROM is also offered.
g. The statutory instrument (ordinance) on barrier-freedom must be taken into consideration.

8.4.1.3 E-mail client

The E-mail clients used to receive, send and process e-mails must at least ensure technical support of the following two e-mail standards:

a. SMTP: for receiving and sending e-mails
b. MIME: as the e-mail format description

Note that the communication of these clients is standardised with regard to communication with public administrations only and/or restricted to the above. With regard to the use of external mail servers not connected to federal institutions, the client is not subject to any restriction whatsoever in terms of the standards and protocols used.

In exceptional cases, it may be necessary to offer electronic mailboxes. The standards described in section 5.6.3 must be used.

8.4.2 Access to information via mobile phone / PDA

Protocols which are served at the server end (refer to section 8.5.2) are currently necessary in order to use the offer of the presentation tier. Applications on terminal devices of this kind are not yet very common in Germany.

8.4.3 Access to information via external systems

Communications and interaction between external and internal systems are to be handled via a subset of the standards which are defined for communications and interaction between internal systems. In this respect, XML via SOAL is considered as being equivalent to RMI for server-to-server communications[63].

8.5 Presentation

The presentation element provides the client tier with information. Depending on the given application, different formats must be made available. These are listed in the following sections. The use of open interchange formats which offer a sufficient number of functions and which are available on different platforms is generally required.

It is permitted to offer the information in addition – or, if so agreed to by all the parties involved, even as an alternative – to the mandatory and recommended formats using formats not considered within the scope of SAGA.

8.5.1 Information processing – computer / web

8.5.1.1 Presentation for the disabled

Mandatory: Barrier-free information technology ordinance (BITV)

In order to make the Internet as an information medium accessible to disabled people too, the avoidance of barriers for people with disabilities is requested. In order to ensure this kind of barrier-free presentation, the requirements of the "Ordinance on the creation of barrier-free information technology pursuant to the law on equal opportunities for the disabled (barrier-free information technology ordinance – BITV)"[64] should be adhered to. This statutory instrument implements section 11 of the "Behindertengleichstellungsgesetz" (Equal Opportunities for Individuals with Disabilities Act) and, in particular, considers the Web Content Accessibility Guidelines[65] of W3C in version 1.0. Concerning the barrier freedom issue, refer also to section 4.1.5.3 on page 44.

---

[63] Refer to sections 8.2 "Data modelling", 8.3 "Application architecture", 8.6 "Communication" and 8.7 "Connection to the back-end"

[64] Refer to http://www.bmi.bund.de/Annex/de_22681/BITV.pdf

[65] Refer to http://www.w3.org/TR/WCAG10

8.5.1.2 Interchange formats for hypertext

Mandatory: Hypertext Markup Language (HTML) v3.2

The HTML v3.2[66] format must be supported in order to ensure support of older browser generations.

Recommended: Hypertext Markup Language (HTML) v4.01

The browsers which are already widely used today support the successor format of HTML v3.2. W3C recommends on the one hand that authors use HTML v4.01[67], and that browsers which support HTML v4.01 are downward-compatible on the other. HTML v4.01 is also required for the technical implementation of barrier-free access according to the Web Content Accessibility Guidelines Version 1.0.

Notwithstanding this, it may, however, occur that certain browsers do not fully support HTML v4.01. This is why functional compatibility with HTML v.3.2 must be ensured. This means that a) information can be presented completely and b) functions can be used completely, but that certain design and layout restrictions for the presentation on the HTML page cannot be avoided.

Under observation: Extensible Hypertext Markup Language (XHTML) v1.0

XHTML v1.0[68] formulates HTML v4.01 as an XML application. XHTML v1.0 is to be used when new browser generations are developed and launched. Applications should ensure functional compatibility with HTML v.3.2.

8.5.1.3 Style sheets

Style sheets can be used in order to ensure a uniform presentation of the information offered with different browser types. Style sheets are format templates for data of all kinds which describe how markups are to be presented in SGML-conforming languages. Depending on the given application, one or both of the following style sheets established by W3C can be used:

Recommended: Cascading Style Sheets Language Level 2 (CSS2)

Cascading Style Sheets Language Level 2 (CSS2)[69] should be used to design HTML pages.

---

[66] Refer to http://www.w3.org/TR/REC-html32

[67] Refer to http://www.w3.org/TR/html401/

[68] Refer to http://www.w3.org/TR/xhtml1/

[69] Refer to http://www.w3.org/TR/REC-CSS2/

Recommended: Extensible Stylesheet Language (XSL) v1.0

The Extensible Stylesheet Language (XSL)[70], version 1.0, should be used to transform and present XML documents in HTML files.

8.5.1.4 Character sets

Mandatory: ISO 10646-1:2000 / Unicode v3.0 UTF-8

In order to provide enough characters for the different characters, numbers and symbols used world-wide, the character set used for documents in the HTML format should be ISO 10646-1:2000/Unicode v3.0 in the UTF-8 encoding version[71].

Recommended: ISO 10646-1:2000 / Unicode v3.0 UTF-16

UTF-16 encoding [72] should be used for documents in Greek or other non-west European languages.

Recommended: ISO 8859-1

The ISO 8859-1 character set is still in use and can continue to be used in future.

Recommended: ISO 8859-15

Encoding according to ISO 8859-15 is still in use, and continues to be permitted within this framework.

8.5.1.5 Static and dynamic, passive and active contents

Static contents are (HTML) files which are generated by a web server not during runtime but which are typically imported from and supplied by the file system. **Dynamic contents** are HTML files which are generated and sent on the server during runtime – for example, in response to database queries.

Passive contents are HTML files which do not contain any program code or computer programs or which reload during the runtime. **Active contents** are computer programs which are contained on websites (e.g. JavaScript) or which are automatically reloaded when a page is viewed (e.g. Java Applets, ActiveX Controls or flash animations) and which are executed on the client (by the browser or by the operating system). When active contents are used, the restrictions described in section 8.4 must be taken into consideration.

[70] Refer to http://www.w3.org/TR/xsl/

[71] This specification is available at: http://www.unicode.org/.

[72] This specification is available at: http://www.unicode.org/.

Mandatory: Hypertext Markup Language (HTML)

If information is to be provided, HTML pages should be used on the basis of the hypertext interchange formats defined in section 8.5.1.2. The support of active contents and plug-ins may only be taken for granted to the extent defined in section 8.1.

Mandatory: ECMA-262 – ECMAScript Language Specification

n as far as Javascript is used within HTML pages according to section 8.4.1.1, this must comply with the ECMA -262 specification[73].

Recommended: Servlets and Java Server Pages (JSP) or Extensible Stylesheet Language (XSL)

Servlets and JSP[74] or Servlets and XSL[75] should be used for the server-based, dynamic generation of HTML pages.

8.5.1.6 File types and type identification for text documents

Different file types must be used for text documents, depending on the given application:

Mandatory: Text (.txt)

Simple text documents that can be edited are exchanged in the widely used (.txt) format in order to ensure general readability. The character set to be used is described in the ISO 8859-1 standard and includes ASCII characters and umlauted vowels.

Mandatory: Hypertext Markup Language (HTML)

Hypertext documents will be used in the HTML format as (.html) files (refer to section 8.5.1.2).

Mandatory: Portable Document Format (PDF) v1.3

Text documents not to be edited should be made available in Adobe's Portable Document Format as (.pdf) files. PDF version 1.3 is used by the Acrobat software[76] version 4 and higher.

---

[73] Refer to http://www.ecma-international.org/

[74] Refer to http://java.sun.com/products/jsp/

[75] Refer to http://www.w3.org/TR/xsl/

[76] Refer to http://www.adobe.de/products/acrobat/readstep2.html

Recommended: Extensible Markup Language (XML)

XML[77] can also be used to describe documents and offers more design and layout options than HTML.

Under observation: Portable Document Format (PDF) v1.4

In order to support forms and barrier-free text documents, it is also possible to use version 1.4 of Portable Document Format from Adobe as (.pdf) which is not yet very widely used. PDF version 1.4 is supported by Acrobat software version 5 and higher. If this format is used for forms, the recommendations of the "Sicherer Internet-Auftritt" [Secure Internet Presence] module of the e-government manual must be considered with regard to active contents (refer to section 8.5.1.5).

Mandatory: Multipurpose Internet Mail Extensions (MIME)

The Multipurpose Internet Mail Extensions (MIME) format must be used for the standardised definition of the format of a file or any part thereof. It enables the e-mail client or the web browser to identify the file type without any doubt; refer to RFC 2045 to RFC 2049.

8.5.1.7 File types for spreadsheets

Different data interchange formats for spreadsheets are to be used, depending on document variability requirements.

Mandatory: Comma Separated Value (CSV)

Delimited, comma-separated spreadsheets must be stored and exchanged as (.csv) files.

Mandatory: Portable Document Format (PDF) v1.3

Analogous to section 8.5.1.6.

Under observation: Portable Document Format (PDF) v1.4

Analogous to section 8.5.1.6.

8.5.1.8 File types for presentations

Presentations should be exchanged in different formats, depending on document variability requirements.

[77] For detailed specifications, please refer to: http://www.w3.org/TR/2000/REC-xml-20001006.

Mandatory: Hypertext Markup Language (HTML)

Presentations that can be edited should be exchanged as hypertext documents in the HTML format as (.html) files (refer to section 8.5.1.2 "Interchange formats for hypertext").

Mandatory: Portable Document Format (PDF) v1.3

Analogous to section 8.5.1.6.

Under observation: Portable Document Format (PDF) v1.4

Analogous to section 8.5.1.6.

8.5.1.9 Interchange formats for graphics

Mandatory: Graphics Interchange Format (GIF)

In view of its wide-spread use, the Graphics Interchange Format (.gif) should be used for interchanging graphics and diagrams, with (.gif) graphics files being compressed with a colour depth of 256 colours (8 bits per pixel).

Mandatory: Joint Photographic Experts Group (JPEG)

The Joint Photographic Experts Group (.jpg) format must be used for interchanging photographs. This format supports changes in the compression factor and the definition of the density, so that a compromise between file size, quality and use is facilitated. 16.7 million colours (24-bit colour information) are supported.

Recommended: Portable Network Graphics (PNG)

The Portable Network Graphics[78] (.png) graphics format should be used whenever this is possible. The (.png) is license-free. It supports 16 million colours, transparency, loss-free compression, incremental display of graphics (beginning with the coarse structure until the file is completely transmitted) and the identification of damaged files.

(.png) will become mandatory instead of (.gif) as soon as new browsers of the fifth generation have been fully established.

Recommended: Tagged Image File Format (TIFF)

The Tagged Image File Format (.tif) should be used for graphic information that does not permit any loss of information. (.tif) is a file format for bitmaps, with different formatting options enabling applications to process or to ignore part of the image.

[78] Refer to http://www.w3.org/TR/REC-png

Recommended: Enhanced Compressed Wavelet (ECW)

The Enhanced Compressed Wavelet (.ecw) bitmap format should be used whenever maximum compression is required.

8.5.1.10 Interchange formats for geographical information (grid data, vector data)

The provision of geographical information via the Internet ("geo-data kiosk") and its cartographic presentation (WebGIS) on the Internet is becoming increasingly popular. The presentation of geographical information in the form of thematic maps via Internet portals can be carried out via grid data or as vector graphics at the presentation level. A vector graphic describes an image as a sequence of geometrical objects. These objects (e.g. line, circle, spline, overlay) have the following properties: position, colour and arrangement.

Recommended: Geography Markup Language (GML)

GML (Geography Markup Language) is a markup language for the transport and storage of geographical information that considers geographical and non-geographical properties. GML was defined by the Open GIS Consortium (OGC)[79]. GML does not contain any information concerning the presentation on the screen or in a map. The geometries are represented by simple features which were also defined by the OGC.

Since version 2.0, the specification has been based on XML Schema Definition (XSD) rather than on document type definitions (DTD).

8.5.1.11 Interchange formats for audio and video files

Mandatory: MPEG-1 Layer 3 (MP3)

The customary (.mp3) format should be used for interchanging audio sequences, with (.mp3) meaning MPEG-1 Layer 3 (MPEG = Motion Picture Experts Group). (.mp3) is a method that enables extremely high compression rates for audio data with maximum quality[80]. A suitable plug-in enables a browser to "play" such files.

Mandatory: Quicktime (.qt, .mov)

The customary Quicktime format[81] should be used to interchange video sequences. A suitable plug-in enables a browser to "play" such files.

---

[79] Refer to http://www.opengis.org/

[80] For further information concerning (.mp3), please refer to: http://www.iis.fraunhofer.de/.

[81] Refer to http://quicktime.apple.com/

Under observation: Windows Media Video (.wmv)

The quality of the Windows Media Video (WMV) format is better than that of the Quicktime format. However, players for different operating systems are not yet available for the WMV format to the same extent as in the case of Quicktime. The exclusive use of WMV is only possible in the case of homogenous target groups whose operating systems are known and supported by players for the WMV format used.

8.5.1.12 Interchange formats for audio and video streaming

In contrast to "normal" audio and video sequences, audio and video streaming offers a format that enables playing even during transmission. This enables live transmission of videos, whereas "normal" audio and video files must be completely transmitted first before they can be started. This area is occasionally characterised by a slightly confusing mix of suppliers, products, container and content formats. Since SAGA does not intend to recommend products, recommendations will be given for the container format only.

One important requirement in this context means that the recommendations should be compatible – to the maximum extent possible – with the customary streaming servers and client products. Due to the fact that this area has been a field of strong competition for several years, the different products are currently highly compatible in terms of the formats supported.

Mandatory: Hypertext Transfer Protocol (HTTP) v1.1

In order to reach as many citizens as possible, the server product selected should in any case enable the transport of streaming data via HTTP.

Mandatory: Quicktime (.qt, .mov)

In order to achieve the maximum possible degree of compatibility of the streaming signal with commonly used browsers, audio and video clients, as well as plug-ins, the use of the Quicktime format[82] is recommended because this is currently supported by all customary products.

Under observation: Ogg

Ogg[83] is a manufacturer-independent container format for streaming audio (Ogg Vorbis) and video (Ogg Theora, Ogg Tarkin) which is currently being developed under Open Source. Leading streaming server manufacturers have already announced that they will support this format in the near future. This format is expected to become increasingly popular in the near future.

---

[82] Refer to http://quicktime.apple.com/

[83] Refer to http://www.ogg.org/

Under observation: Windows Media Video (.wmv)

The quality of the Windows Media Video (WMV) format is better than that of the Quicktime format. However, players and streaming servers for different operating systems are not yet available for the WMV format to the same extent as in the case of Quicktime. The exclusive use of WMV is only possible in the case of homogenous target groups whose operating systems are known and supported by players for the WMV format used.

8.5.1.13 Animation

Mandatory: Animated GIF

Animation means moving features in graphics displayed on a site. Animated GIF, a variant of the GIF graphic format, should be the preferred product in this case. With this format, several individual GIF images are stored in a file, with the possibility to define their sequence, display time and number of repetitions.

8.5.1.14 Data compression

Compression systems should be used in order to enable the exchange of large files and minimise network load.

Mandatory: ZIP v2.0

Compressed data should be exchanged as (.zip) files in the internationally common ZIP format, version 2.0.

Recommended: GZIP v4.3

An alternative is the GZIP format, version 4.3, with (.gz) files as specified in RFC 1952[84].

8.5.2 Information processing – mobile phone / PDA

In the event that an information offer for mobile phones and PDAs is to be developed, preference should be given to the SMS system because this is widely accepted by citizens. The presentation of websites for mobile communications is not yet widely used in Germany.

Mandatory: Short Message Services (SMS)

Short Message Services are to be implemented on the basis of the specifications issued by the SMS Forum[85]. The SMS Forum is an international forum of all major IT companies.

---

[84] Refer to http://www.ietf.org/rfc/rfc1952.txt

Under observation: Wireless Markup Language (WML) v1.x

The Wireless Markup Language[86] was defined for use in narrow-band environments, in particular, for wireless communications, and is the markup language belonging to the WAP. All wireless communications providers in Germany support WML v1.x.

The highly successful i-mode service of the Japanese telecommunications company NTT DoCoMo was recently launched in Germany under a license for mobile phones. Pursuant to the license agreement, terminal devices are supplied in Germany with dual-browser systems which support both the proprietary iHTML format and the WML v1.x format that is commonly used in Europe, so that WML v1.x meets with the SAGA requirements.

Under observation: Wireless Application Protocol (WAP) v1.x

The Wireless Application Protocol (WAP)[87] v1.x is a specification for the development of applications that use wireless communication networks. Its main application is mobile communications.

Under observation: Extensible Hypertext Markup Language (XHTML) Basic

XHTML Basic[88] is a standard for presenting HTML pages converted to XML for applications which do not support the full presentation functionality of HTML (such as mobile phone or PDAs). Subsets of HTML Basic are currently under definition for different terminal devices.

Like WML v1.0, WML v2.0 is once again based on XML. It is, however, a subset of the XHTML Mobile Profile Specification which, on its part, is a subset of XHTML Basic.

8.5.3 Information processing – external systems

Refer to sections 8.2 "Data modelling", 8.3 "Application architecture", 8.6 "Communication" and 8.7 "Connection to the back-end". However, only a subset of the standards mentioned in the middleware area is relevant for communication with external systems. XML and web service technology are at the heart of communications with external systems. Existing interfaces that are based on OSI technology will be gradually migrated.

---

[85] Refer to http://www.smsforum.net/

[86] Refer to http://www.wapforum.org/what/technical.htm

[87] Refer to http://www.wapforum.org/

[88] Refer to http://www.w3.org/TR/xhtml-basic/

8.6 Communication

Within the "communication" element, a distinction is made between application, middleware and network protocols as well as directory services.

8.6.1 Middleware protocols

In the case of middleware protocols, a distinction is made between server applications that communicate within an administration (refer to section 8.6.1.1) and client applications outside the administration which communicate with an administration server (refer to section 8.6.1.2).

8.6.1.1 Server-to-server communication within the administration

Mandatory: Remote Method Invocation (RMI)

Remote Method Invocation (RMI)[89] is particularly suitable for communication between applications or application components which are based on a J2EE architecture. Via RMI, an object on a Java Virtual Machine (VM) can invoke methods of an object that runs on another Java VM.

Mandatory: Simple Object Access Protocol (SOAP) v1.1

SOAP[90] can be used for communication between applications or application components which are based on a J2EE architecture if the requirements to the protocol extent permit this. SOAP is particularly suitable for communication between servers not based on J2EE. SOAP can be used to exchange structured data as XML objects between applications or application components via an Internet protocol (e.g. via HTTP).

Mandatory: Web Services Description Language (WSDL) v1.1

The Web Services Description Language (WSDL) should be used for service definition purposes. WSDL is a standardised language[91] that describes web services in such a manner that they can be used by other applications without a need to know further implementation details or to use the same programming language.

Mandatory: XML Schema Definition (XSD) v1.0

The data elements to be transmitted are to be specified via XML Schema[92].

---

[89] Refer to http://java.sun.com/rmi/

[90] Refer to http://www.w3.org/TR/SOAP/

[91] Refer to http://www.w3.org/TR/wsdl

[92] Refer to http://www.w3.org/XML/Schema

Recommended:	Java Remote Method Invocation over Internet Inter-ORB Protocol (RMI-IIOP)

RMI-IIOP is an integral part of J2EE. J2EE applications or application components can communicate via RMI-IIOP with CORBA components if the suitable Object Request Brokers are available on the pertinent application servers.

8.6.1.2 Client-to-server communication

Web services are to be used for access by client applications via the Internet to service applications offered by administrations.

By providing a web service layer for an existing server application, it enables client systems to invoke the functions of the applications via the Hypertext Transfer Protocol (HTTP). A web service is a software component which uses SOAP in order to communicate with other components via the HTTP standard protocol. XML is used for the message content itself. XML was already described in section 8.2 "Data modelling" as a universal and primary standard for exchanging data between all the information systems relevant for administrative purposes.

The Web Service Interoperability Organization defines profiles of existing standards in order to facilitate the compilation of the required standards. The profile to be applied is WS-I-Basic and includes XML Schema v1.0, SOAP v1.1, WSDL v1.1, and UDDI v1.0.

Mandatory:	Simple Object Access Protocol (SOAP) v1.1

SOAP[93] can be used to exchange structured data as XML objects between applications via an Internet protocol (e.g. via HTTP).

Mandatory:	Web Services Description Language (WSDL) v1.1

The Web Services Description Language (WSDL) should be used for service definition purposes. WSDL is a standardised language[94] that describes web services in such a manner that they can be used by other applications without a need to know further implementation details or to use the same programming language.

Mandatory:	XML Schema Definition (XSD) v1.0

The data elements to be transmitted are to be specified via XML Schema[95].

[93] Refer to http://www.w3.org/TR/SOAP/

[94] Refer to http://www.w3.org/TR/wsdl

[95] Refer to http://www.w3.org/XML/Schema

Under observation: Universal Description, Discovery and Integration (UDDI) v1.0

The UDDI (Universal Description, Discovery and Integration) project, in its latest version 2.0[96], is an XML-based technology initiative that is being pursued by companies from all industries that targets the publishing, structured management and offering to users of web services. UDDI is based on standards issued by W3C and the Internet Engineering Task Force (IETF), such as XML, HTTP, DNS and SOAP.

8.6.2 Network protocols

Mandatory: Internet Protocol (IP) v4

The IT environment of the federal administration currently uses IP v4 (RFC 0791, RFC 1700) in conjunction with TCP (Transmission Control Protocol, RFC 793) and UDP (User Datagram Protocol, RFC 768).

Under observation: Internet Protocol (IP) v6

IP v6 is the next version of the IP protocol which is not yet very widely used. One of the changes compared to the current version 4 is the extension of the IP address to 128 bits in order to permit addressing of multi-embedded and mobile IP-based systems in future.

IP v6 includes IPsec (IP-Security Protocol) which is chiefly used in the VPN (Virtual Private Network) area and which can also be used independent of IP v6. For further information on this subject, please refer to the website of the "Sicherheit im Internet" [Security on the Internet] action group[97] or of the German Federal Office for Information Security[98].

When new system components are to be introduced, these new components should support both IP v4 and IP v6 in order to enable future migration.

Mandatory: Domain Name Services (DNS)

Domain Name Services (DNS, RFC 1034, RFC 1035, RFC 1591) have been a standard Internet feature since the mid-1980s. DNS refers to a hierarchical name server service at central points of the Internet. This is where a server name entered is converted to the pertinent IP address.

---

[96] Refer to http://www.uddi.org/

[97] Refer to http://www.sicherheit-im-internet.de/

[98] Refer to http://www.bsi.de/

8.6.3 Application protocols

Section 6.4.2 deals with the integration of security-related infrastructure components (such as directory services for certificates, revocation lists, etc).

Mandatory: File Transfer Protocol (FTP)

The File Transfer Protocol (FTP, RFC 959, RFC 1123, RFC 2228, RFC 2640) is considered the standard file transfer protocol. FTP is one of the oldest Internet services. FTP enables the shared use of files, offers users standardised user interfaces for different file system types, and transfers data in an efficient and reliable manner. FTP is typically somewhat faster than HTTP when larger files are to be downloaded.

Mandatory: Hypertext Transfer Protocol (HTTP) v1.1

HTTP v1.1 (RFC 2616) is to be used for communication between client and web server. However, web servers should also support HTTP v1.0 (RFC 1945) in addition to version 1.1. The HTTP State Management Mechanism (RFC 2965) standard is to be adopted in conjunction with HTTP Session Management and cookies.

Mandatory: Simple Mail Transfer Protocol (SMTP) / Multipurpose Internet Mail Extensions (MIME)

E-mail protocols in conformity with the SMTP/MIME specifications for exchanging messages (RFC 821, RFC 822, RFC 2045, RFC 2046, RFC 2047, RFC 2048, RFC 2049) are required for e-mail transport. E-mail attachments should correspond to the file formats defined in section 8.5.

Mandatory: Post Office Protocol (POP) 3 / Internet Message Access Protocol (IMAP)

In exceptional cases, it may be necessary to offer electronic mailboxes. POP3 or IMAP should be used as commonly used standards to this effect.

8.6.4 Directory services

Mandatory: Lightweighted Directory Access Protocol (LDAP) v3

LDAP v3 (RFC 2251) is an X.500-based Internet protocol which is optimised with regard to hierarchically structured information and which is used for directory service access.

Under observation: Universal Description, Discovery and Integration (UDDI) v1.0

The UDDI[99] project is an XML-based technology initiative that is pursued by companies from all industries that targets the publishing, structured management and offer-

[99] Refer to http://www.uddi.org/

ing to users of web services. UDDI is based on standards issued by W3C and IETF, such as XML, HTTP, DNS and SOAP.

Under observation: Directory Services Markup Language (DSML) v2

DSML[100] is a definition in XML which enables access to directory services. It enables the handling of several directories at the same time.

8.7 Connection to the back-end

The German administration uses several legacy systems which are very likely to remain in use even in the future (such as ERP, mainframe transaction processing, database systems and other legacy applications). Depending on the operating modes supported, these legacy systems can be divided into three categories as follows:

a. Secure-transaction processing by end users via existing dialogue systems
b. Asynchronous data batch processing (bulk data processing)
c. Program-to-program communication on the basis of proprietary protocols

Two options are generally available for integrating legacy systems:

a. Direct integration via so-called "legacy interfaces"
b. Integration via a separate integration layer, with modular encapsulation of real access to the legacy systems

Detailed solution concepts must be evaluated and compared with a view to the aims to be achieved, the available time and budget, as well as the functions to be supported during the integration of the legacy system.

The following sections discuss different solution concepts which proved to be suitable with the three above-mentioned operating modes.

8.7.1 Dialogue systems

The integration of legacy systems of this kind into e-government solutions of the German administration is possible with or without an integration layer.

a. With an integration layer

   New user interfaces are developed for presentation in the browser. Processing of the legacy data will then take place in a separate integration layer.

b. Without an integration layer

   A suitable product migrates the existing dialogues to user interfaces which can then be executed in a browser.

[100] Refer to http://www.oasis-open.org/

8.7.2 Batch processing

Many large communication systems process their data by batch processes, in particular, when large amounts of data are to be processed. The data is supplied on data volumes or transmitted by file transfer.

Recommended:	Extensible Markup Language (XML)

With this mode, data transmission via XML documents is to be supported in future; refer to section 8.2 "Data modelling". This opens up new options and increases the flexibility of interfaces.

8.7.3 Program-to-program communication

Certain interfaces are widely used by federal administrations. These interfaces are to be applied and modernised.

Recommended:	Extensible Markup Language (XML)

Information interchange via XML documents has become the established procedure when it comes to adapting processing interfaces which are still based on proprietary protocols to advanced technologies. Today, many manufacturers offer the interfaces necessary for converting data to XML formats, so that development requirements are reduced and the development of a separate connector functionality may no longer be necessary.

Recommended:	Java Message Service (JMS) v1.1, J2EE Connector Architecture v1.5

In order to ensure smooth integration into the J2EE platform, it is recommended that the Java Message Service or the J2EE Connector Architecture be used for integration.

Recommended:	Web services

Web services are the medium of choice for data transmission[101].

[101] Refer to http://www.w3.org/TR/ws-arch/

9 Technology viewpoint (part II): standards for data security

Ensuring data security is one major aspect for the successful implementation of services within the scope of the BundOnline 2005 project. Data security represents and supports the trusted and secure interaction between citizens, public authorities and business.

The e-government architecture model (refer to chapter 3) identifies data security as an omnipresent component which can be supported – as demanded or required – by suitable processes, methods and data formats in every element and every pillar of the kit. Technical means must be used in such a manner that trust is created among those who communicate with each other, that baseline protection is ensured and that classic protection aims are fulfilled.

As the relevance of security measures has increased enormously in recent years due to the growing use of the Internet, standardisation efforts have also increased in this area. The result is a host of security standards, directives and recommendations.

This chapter introduces the relevant security standards and recommendations for e-government services.

9.1 Aims and principles of data security

The data security standards presented here help determine whether a particular service requires protection. Only if a need for protection is identified will it be necessary to take protective measures.

9.1.1 Protection aims

Protection aims define the security interests of communication partners in a general form:

a. *Confidentiality* – protection against disclosure to unauthorised parties:

   no data is made available or disclosed to unauthorised individuals, entities or processes.

b. *Integrity* – protection against manipulation:

   unauthorised modification or destruction of data is not possible.

c. *Authenticity* – protection against faked identity/origin:

   measures are taken to ensure that an entity or resource (such as an individual, process, system, document, information) actually is what he, she or it claims to be.

d. *Availability* – protection against failure of IT systems*:*

   the properties of an entity and/or resource can be accessed and/or used when this is attempted by an authorised entity.

Information encryption (cryptography) is an important tool for securing confidentiality, integrity and authenticity.

A high degree of availability is achieved through multiplicity, distribution and error tolerance.

9.1.2 Protection requirements

The protection requirements must be identified for each and every IT application. These requirements are a function of the potential damage caused by impairment of the IT application in question.

The IT Baseline Protection Manual[102] (section 2.2 Determining the protection demand) explains the procedure of determining the protection demand. The e-government-manual[103] (module: Phase plan for e-government – phase 3 "Analysis"[104]) breaks these requirements down into four categories as follows on the basis of the IT Baseline Protection Manual.

Category	Effect of damage
"None"	No particular protection is required as no impact from loss or damage is expected.
"Basic to moderate"	The impact of any loss or damage is limited.
"High"	The impact of any loss or damage may be considerable.
"Very high"	The impact of any loss or damage can attain catastrophic proportions which could threaten the very survival of the agency/company.

Figure 9-1: Protection requirement categories

A protection requirement category can be assigned to every protection aim in order to evaluate applications from a security point of view. The e-government manual (module: e-government phase plan – phase 3 "Analysis") gives examples of how to identify protection requirements.

One aspect to be particularly considered when determining protection requirements is whether personal data are processed in order to ensure that data protection laws are adhered to. SAGA does not explain any data protection measures. The e-govern-

[102] Refer to http://www.it-grundschutzhandbuch.de/

[103] Refer to http://www.e-government-handbuch.de/

[104] Refer to the e-government manual (http://www.bsi.bund.de/fachthem/egov/6.htm), chapter III, module: "Phase 3 – Analyse" [Phase 3 – analysis]

ment manual (module: Data-protection-compliant e-government[105]) contains data protection information with regard to frames of reference, challenges and recommended actions.

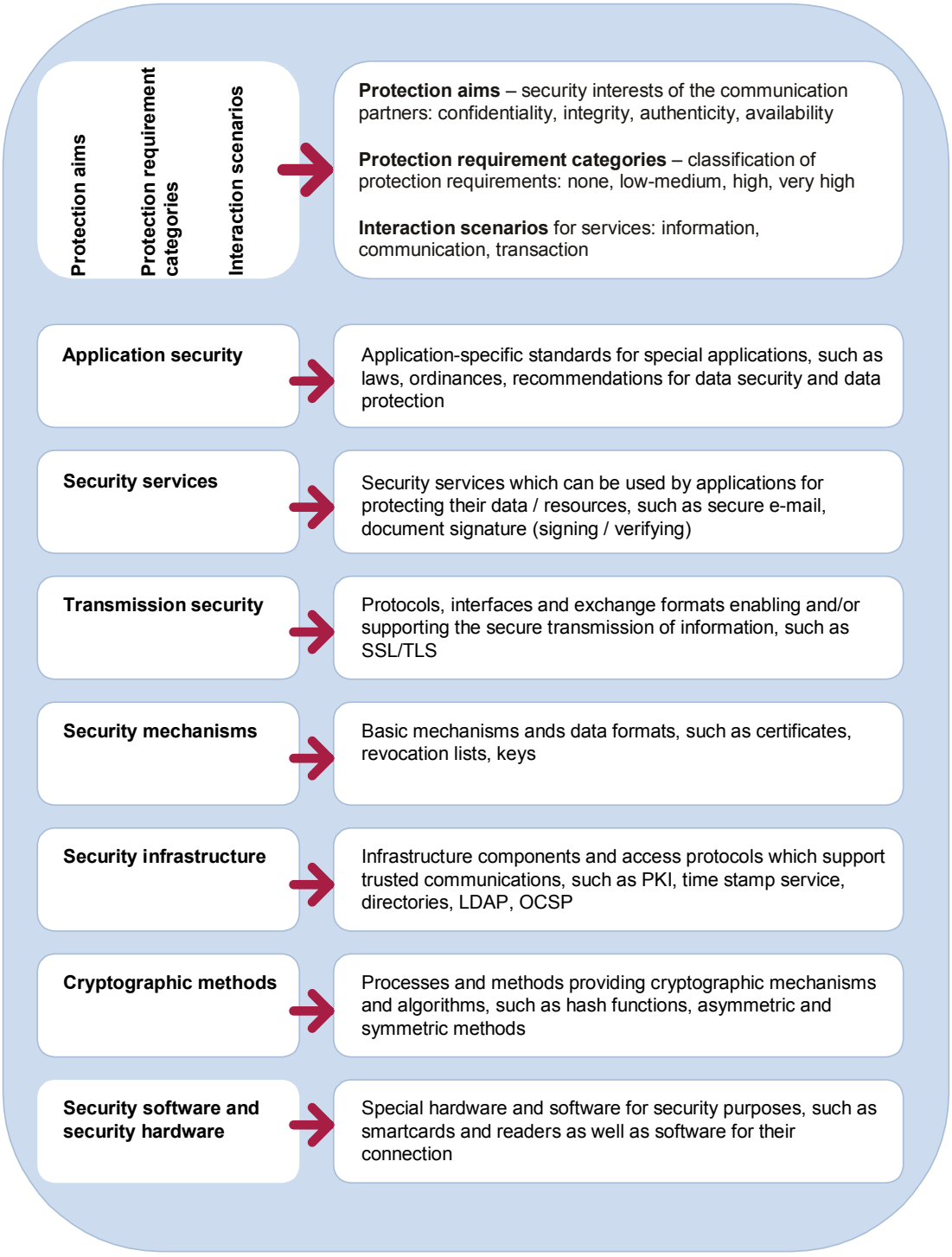


Figure 9-2: Structure model for security standards

[105] Refer to the e-government manual (http://www.bsi.bund.de/fachthem/egov/6.htm), chapter II, module: "Datenschutzgerechtes E-Government" [Data-protection-compliant e-government]

9.1.3 Structure model for data security

In order to make security standards easier to understand and apply, the e-government architecture model discussed in chapter 3 was further upgraded to a security-specific structure model (refer to Figure 9-2, page 97).

The structure model is not a tier model, instead it illustrates different specification processes in order to achieve the desired security targets. In this way, it creates an understanding of the complex nature of IT security.

A data security standard typically covers more than one structure level, so that a target classification is not carried out. However, every standard can be viewed from the point of view of the individual structure levels.

The structure model and the data security standards mentioned do not release the respective experts from their duty to carry out a thorough analysis of the application in question with a view to conformity with laws and legal protection requirements and to check and comply with the security level at all instances and in all processes of the interaction chain. An application-specific risk analysis must be carried out, protection requirements must be identified and a security concept must be developed.

Protection aims, protection requirements and applications determine the goals of security measures.

9.2 Standards for the security concept

Laws and resolutions of the federal government must be generally considered as mandatory. These laws and resolutions are supplemented by recommendations and directives for IT security.

The recommendations and guidelines by the German Federal Office for Information Security (BSI) and the Co-operation Committee for Automatic Data Processing for the Federal-government, Federal-state Government and Municipal Administration Sector (KoopA ADV) should be used to determine protection requirements. If an IT application or component is found to need protection, adherence to these recommendations and guidelines is mandatory.

Mandatory: BSI, IT baseline protection manual

The application of the BSI's IT Baseline Protection Manual (manual for the preparation of IT security concepts for normal security demands)[106] and the implementation of the standard security measures addressed therein are required. The IT Baseline Protection Manual offers a simple and convenient way to implement IT security concepts. The structure of the IT Baseline Protection Manual supports a component-orientated approach.

[106] Refer to http://www.it-grundschutzhandbuch.de/

Recommended:	Co-operation Committee for Automatic Data Processing for the Federal-government, Federal-state Government and Municipal Administration Sector (KoopA ADV), Guideline for the Introduction of the Electronic Signature and Encryption in the Administration

The Guideline for the Introduction of the Electronic Signature and Encryption in the Administration issued by the Co-operation Committee for Automatic Data Processing for the Federal-government, Federal-state Government and Municipal Administration Sector (KoopA ADV)[107] is designed to facilitate solutions to cryptographic problems for selected projects in the public administration, and is hence primarily devised as a working aid for public agencies. Typical problems and tasks are defined in the form of scenarios for which potential solutions are identified and described.

Recommended:	BSI, e-government manual

BSI's e-government manual[108] was created in order to support the BundOnline 2005 initiative. The manual contains organizational and technical recommendations concerning the use of IT in e-government applications. Security-related recommendations are one of the central features.

9.3 Standards for specific applications

In order to enable a realistic assignment of security standards, frequently encountered applications are formulated from a security point of view (refer to Figure 9-3 on page 100).

9.3.1 Secure transmission of web contents and web server authenticity

When a client communicates with the web server of a public agency, measures must be taken to ensure that communication really takes place with this server (web server authenticity). The retrieval of information, i.e. the transmission of web contents, for which integrity and/or confidentiality is required, must be accomplished in a secure manner during communication via the Internet.

Mandatory:	Secure Sockets Layer (SSL) / Transport Layer Security (TLS)

The SSL protocol is a cryptographic protocol which ensures integrity, confidentiality and authenticity on the world wide web. SSL was developed further to the TLS protocol[109].

---

[107] Refer to http://www.koopa.de/Arbeitsgruppen/Kommunikation/kommunikation.htm

[108] Refer to http://www.e-government-handbuch.de/

[109] Refer to http://www.ietf.org/rfc/rfc2246.txt

	Information	Communication	Transaction / integration
Secure transmission of web contents (integrity and confidentiality)	▸ SSL/TLS		
Web server authenticity			
Securing e-mail communications		▸ MTT version 2 ▸ ISIS-MTT	
Secured exchange of documents (authenticity, integrity and confidentiality)		▸ MTT version 2 ▸ ISIS-MTT ▸ XML signature and XML encryption	
Transactions			▸ OSCI transport v1.2
Web services			▸ WS security

Figure 9-3: Security standards for specific applications

SSL/TLS are based on TCP/IP and secure communication protocols for such applications as HTTP, FTP, IIOP, etc., in a transparent manner. SSL/TLS-secured WWW pages are addressed with https:// rather than http://.

The use of HTTP via SSL-secured connections is often referred to as HTTPS.

SSL/TLS also supports the single-ended authentication of the public agency's server in relation to the client of the communication partner in order to reassure the latter that it is really connected to the public agency's server.

SSL/TLS offers the following cryptographic mechanisms.

a. Asymmetric authentication of the communication partners (via X.509 certificates)
b. Secure exchange of session keys (via RSA encryption or Diffie-Hellman key agreement)
c. Symmetric encryption of communication contents
d. Symmetric message authentication (via MACs) and protection against reply attacks

The principles of operation of SSL/TLS are described in detail in section 5.2.2 of the Guideline for the Introduction of the Electronic Signature and Encryption in the Administration issued by the Co-operation Committee for Automatic Data Processing for

the Federal-government, Federal-state Government and Municipal Administration Sector (KoopA ADV)[110]. The combination of different methods is referred to as a "cipher suite" in SSL/TLS. An SSL/TLS cipher suite always contains four cryptographic algorithms: a signature method, a key exchange method, a symmetric encryption method as well as a hash function.

The Guideline for the Introduction of the Electronic Signature and Encryption in the Administration issued by the Co-operation Committee for Automatic Data Processing for the Federal-government, Federal-state Government and Municipal Administration Sector (KoopA ADV) gives the following recommendations.

a. A certain maximum key length should be defined for symmetric methods, i.e. presently 128 bits or 112-bit 3 DES, with simple-DES and RC2 being not recommended.
b. SHA1 should be used for the hash function.
c. RSA modulo should at least have 1024 bits.

9.3.2 Securing e-mail communications

The secure exchange of e-mails is one possible application for the "communication" interaction stage. Secure e-mail communication includes the securing of e-mails during their transmission from a sender to a recipient. This application looks at e-mails in their entirety. Section 9.3.3 "Secured document exchange" discusses the procedures for securing documents, including e-mail attachments.

Mandatory: MailTrusT (MTT) Version 2 / SPHINX / PKI-1-Verwaltung

MTT version 2

The MTT-Spezifikation[111], version 2, is a development by the German TeleTrusT e.V. This Standard covers:

a. X.509v3 certificates and X.509-CRLv2 revocation list formats
b. S/MIME-v3 document format
c. PKCS and PKIX management messages

This standard is classified as mandatory because it forms the basis both for the SPHINX project and for the administration PKI. This standard will be replaced in future by ISIS-MTT (see below).

SPHINX

The cryptographic methods used in SPHINX form part of the MTT specification. In the "SPHINX – secure e-mail" pilot trial, the end-to-end security of e-mails based on

[110] Refer to http://www.koopa.de/Arbeitsgruppen/Kommunikation/kommunikation.htm

[111] Refer to http://www.teletrust.de/glossar.asp?id=60960,1

public-key cryptography was tested on a manufacturer-spanning basis. The overall concept was developed on the basis of the MailTrusT specification (MTT version 2) and covers the underlying standards for electronic signature and encryption as well as the infrastructure measures and organizational requirements necessary for the introduction of security technology. On the basis of this concept, a security infrastructure was developed for the public agencies and organizations involved which enables the secure exchange of documents between users.

PKI-1 administration – public key infrastructure for public agencies

Drawing from the experience of the SPHINX pilot project, the BSI implemented a public key infrastructure (PKI) for the administration sector (PKI-1 administration). The root certification authority (Policy Certification Authority: PCA) of the PKI-1 administration must be used. Federal authorities, municipal administrations and other public institutions operate their own certification authorities which are certified by the PCA-1 administration. The BSI offers documentation at: http://www.bsi.de/ concerning the use of SPHINX within the context of the PKI-1 administration.

Mandatory: Industrial Signature Interoperability Specification (ISIS)-MTT

The ISIS-MTT specification[112] considers a host of applications for processes to secure electronic business (for example, file, mail, transaction and time "protection") on the basis of the basic functionalities, i.e. electronic signature, encryption and authentication.

ISIS-MTT is a delta specification which is based on existing, relevant international standards (S/MIME, PKIX, PKCS, X.509, ETSI, CEN ETSI). The specification focuses on conformity requirements which must be fulfilled by conforming PKI components and applications during the generation and processing of certain data objects, such as certificates.

The scope of the ISIS-MTT specification was determined by the merging and unification of the MailTrusT (version 2, March 1999, TeleTrusT e.V.) and ISIS (Industrial Signature Interoperability Specification: version 1.2, December 1999, T7 e.V.) specifications.

The ISIS-MTT specification chiefly consists of a kernel document which is exclusively based on the profiling (restriction of optional characteristics) of international standards and which is hence expected to ensure interoperability on an international scale. The basis of ISIS-MTT is a core specification which is mandatory for all manufacturers and suppliers and which can be supplemented by optional profiles as required. The "SigG-conforming Systems and Applications" and "Optional Enhancements to the SigG-Profile" profiles which are already available describe the current stage of qualified signatures in Germany.

[112] Refer to http://www.isis-mtt.org/

ISIS-MTT is classified as mandatory because ISIS-MTT is the successor to MTT v2, with MTT v2 being fully integrated into ISIS-MTT. As soon as ISIS-MTT is supported by suitable products (presumably before the end of 2003), ISIS-MTT will replace the MTT v2 standard.

9.3.3 Secured document exchange

The "communication" interaction stage requires the exchange of secure documents. This includes, for example, the securing of documents as e-mail attachments as well as the securing of documents for all kinds of communication paths.

The MTT v2 and ISIS-MTT standards are relevant for securing e-mail attachments, whilst XML Signature and XML Encryption as XML-specific standards are becoming increasingly relevant for the secure exchange of XML documents (for example, for forms designed for further processing).

Mandatory: MailTrusT (MTT) version 2 / SPHINX / PKI-1 administration

The MTT version-2 specification (refer to section 9.3.2 "Securing e-mail communications") also defines an interoperable data exchange format for signed and encrypted data. MTT considers, above all, the securing of binary data, so that the secured transmission of all kinds of files is possible as e-mail attachments.

MTT version 2, the SPHINX project and the administration PKI support the secure end-to-end exchange of documents. MTT v2 will be replaced in future by ISIS-MTT (refer to section 9.3.2).

Mandatory: Industrial Signature Interoperability Specification (ISIS)-MTT

ISIS-MTT (refer to section 9.3.2 "Securing e-mail communications") fully integrates MTT version 2 and will replace this standard in future.

Mandatory: XML Signature

XML Signature is a common standard of W3C and IETF (W3C, XML Signature Syntax and Processing, W3C Recommendation and IETF RFC 3275, March 2002)[113].

This standard describes digital signatures for all kinds of data (typically, however, XML) by providing an XML schema and a set of processing rules (for generating and validating the signature). The signature can cover one or more documents and different kinds of data (pictures, text, etc.).

Placement of the XML signature is possible in three ways as follows.

a. Enveloped: The signature can be embedded, i.e. the XML fragment which represents the signature is inserted into the signed document.

[113] Refer to http://www.w3.org/TR/xmldsig-core/

b. Enveloping: The signature can act as an envelope, i.e. it is applied to a document to which reference is made within the signature.
c. Detached: The signature can be independent (detached), i.e. it is kept separate from the source, either in the same or in another XML document.

One central property of XML Signature is that it is possible to sign specific parts of an XML document only rather than the entire document. Both asymmetric cryptographic algorithms and symmetric methods can be used. These must be selected depending on the protection aim.

Thanks to this flexibility, it is, for example, possible to secure the integrity of certain elements of an XML document whilst other parts can be edited. For example, a signed XML form which is sent to a user. The user can complete certain fields without violating the integrity of the document. This was not possible with conventional signatures because the complete document was always signed, so that any change or addition would have meant a violation of its integrity.

The following cryptographic algorithms are specified.

a. Hash function: SHA1
b. Encoding: base64
c. MAC: HMAC-SHA1 (symmetric keys); (HMAC RFC 2104)
d. Signature: DSA SHA1 (DSS); additionally recommended: RSA SHA1

Specialisation of the cryptographic preferences for specific communication scenarios has not yet taken place.

Recommended: XML Encryption

XML Encryption is a W3C standard, however, unlike XML Signature not yet an RFC (XML Encryption Syntax and Processing, W3C Recommendation, 10 December 2002)[114].

XML Encryption provides an XML schema and a set of processing rules (for encryption/decryption) which supports the encryption/decryption of complete documents, document parts (document elements) or element contents.

Both a symmetric or an asymmetric key can be used for encryption.

The following cryptographic algorithms are specified.

a. Block encryption: 3DES, AES
b. Key transport: RSA (RSAES-PKCS1-v1_5 algorithm, RFC 2437)
c. Key agreement: Diffie-Hellman (optional)
d. Hash function: SHA1, RIPEMD-160
e. Encoding: base64

[114] Refer to http://www.w3.org/TR/xmlenc-core/

XML Encryption is recommended in addition to XML Signature. However, this standard is not yet accepted to the same extent as XML Signature.

9.3.4 Transactions

Transactions cover the complex, specialised business cases with a multi-stage value chain between communication partners.

Mandatory: Online Service Computer Interface (OSCI)-Transport v1.2

The Online Service Computer Interface (OSCI)[115] is the result of a competition; MEDIA@Komm. OSCI covers a host of protocols which are suitable for e-government requirements and which are implemented by the OSCI steering group. The aim is to support transactions in the form of web services and their complete consummation via the Internet.

OSCI Transport 1.2 is that part of "OSCI" which is responsible for the cross-section tasks in the security area. The existence of a central intermediary which can perform added-value services without jeopardising confidentiality at the business case data level is a characteristic feature for the secure implementation of e-government processes using OSCI. As a secure transmission protocol, it enables binding online transactions (even in conformity with the German Act on Digital Signature).

OSCI Transport supports asynchronous communication via an intermediary as well as end-to-end encryption for the confidential transmission of data. OSCI Transport standardises both message contents as well as transport and security functions and is based on international standards (including, for example, XML Signature, DES, AES, RSA and X.509) for which suitable, concrete contents are developed as required.

Central design criteria for OSCI Transport, version 1.2, were the following.

a. Reference to open standards (SOAP, XML Signature, XML Encryption)
b. Technical independence, i.e. transmission using any technical communication protocol without any specific requirements regarding platforms or programming languages
c. Scalability of security levels (advanced signatures or qualified and/or accredited electronic signatures as required by the specific application).

9.3.5 Web services

The increasing importance of XML as a data exchange and specifications format even in the security area as well as the introduction of web services as integrative middleware is leading to the active standardisation of XML security standards by

[115] Refer to http://www.osci.de/

W3C and OASIS specialists. It is presently not yet possible to assess the relevance and final scope of the drafts.

Under observation: Web Services (WS) Security

WS-Security[116] is a new industry standard for secure web services. It defines upgrades of the SOAP protocol in order to provide and ensure confidentiality, integrity and the binding effect of SOAP messages for securing web services. The use of different security models and different cryptographic method must be possible.

WS-Security also enables different "security tokens", i.e. data formats which warrant specific identities or properties, such as X.509 certificates, Kerberos Tickets or encrypted keys.

WS-Security is considered to be a type of foundation document for web service security which is to be followed in future by further documents (WS-Policy, WS-Trust, WS-Privacy, WS-Secure Conversation, WS-Federation and WS-Authorization).

WS-Security is a joint development by IBM, Microsoft and Verisign and hence features strong manufacturer support. Although it is at present not yet possible to finally assess the relevance of this standard, it may well turn out to be important for the SOAP communication of future web services.

9.4 General data security standards

General security standards cover those standards which cannot be assigned to specific applications and/or interaction stages; refer to Figure 9-4.

	Information	Communication	Transaction / Integration
Integration of security infrastructure		▸ ISIS-MTT	
Integration of smartcards	▸ ISO/IEC 7816		
Key management	▸ XKMS v2		
Cryptographic algorithms for the electronic signature	▸ Publication by RegTP (hash functions: RIPEMD-160, SHA1; signature algorithms: RSA, DSA, DSA variants)		
Symmetric cryptographic algorithms	▸ Triple-DES, IDEA, AES		

Figure 9-4: General security standards

[116] Refer to http://www-106.ibm.com/developerworks/library/ws-secure/

9.4.1 Authentication

In order to ensure that authentication as a protection aim is achieved, certain e-government applications require the identification and authentication of communication partners. Different authentication mechanisms can be adopted in this context, such as user identification / password, PIN / TAN or certificates. The "Authentication in e-government"[117] module of the e-government manual addresses technical security aspects of different authentication methods.

9.4.2 Integration of security infrastructure

The security infrastructure includes directory, certification and time-stamp components which support the distribution and handling of certificates, revocation lists and time stamps both for e-mail as well as for web environments. Access to these components takes place via operational protocols.

Mandatory: Industrial Signature Interoperability Specification (ISIS)-MTT

ISIS-MTT (refer to section 9.3.2 "Securing e-mail communications") describes, in part 4 "Operational Protocols", protocols and profiles for connecting security infrastructures. These include access to directories via LDAP v3, Online Certificate Status Protocol (OCSP), FTP and HTTP as well as the Time Stamp Protocol (TSP).

9.4.3 Integration of smartcards

Integration of smartcards, smartcard readers and their driver architectures and/or complex, multi-function "Smartcard / reader bundles" is, for example, necessary in order to use qualified electronic signatures in conjunction with the client infrastructure.

The D21 initiative[118] addresses this issue through its working group 5 – "Smartcards project". The results of this project group will supplement the above-listed standards for the integration of smartcards.

Mandatory: ISO/IEC 7816

Smartcards (chip cards) must comply with the ISO/IEC 7816 standard. Components supporting the universal "Cryptographic Token Interface" (Cryptoki) must be in conformity with ISIS-MTT part 7 (Cryptographic Token Interface).

---

[117] Refer to the e-government manual (http://www.bsi.bund.de/fachthem/egov/6.htm), chapter IV B, module: "Authentisierung im E-Government" [Authentication in e-government]

[118] Refer to http://www.initiatived21.de/

9.4.4 Key management

As a precondition for applications using electronic signatures, it must be possible to assign public electronic keys (public keys) to real individuals or institutions. In order to achieve interoperability between different applications, identical data formats must be in place, and standardised mechanisms must be used to read and write data.

Recommended: XML Key Management Specification (XKMS) v2

XKMS[119] specifies protocols for the registration and distribution of public keys. The protocols were designed for interaction with XML Signature and XML Encryption and are hence used for XML-based communications, such as web services. The specification consists of two parts, i.e. the XML Key Registration Service Specification (X-KRSS) and the XML Key Information Service Specification (X-KISS).

Clients can use relatively simple XKMS queries to find and validate public keys, with relay servers accessing existing LDAP and OCSP infrastructures in order to answer these queries. This means that parallel use of different directory services is possible with just one protocol.

9.4.5 Cryptographic algorithms for the electronic signature

The security of an electronic signature is primarily dependent upon the strength of the underlying cryptographic algorithms. Concerning the "electronic signature" issue, refer also to section 4.1.5.1 on page 42.

Mandatory: Cryptographic algorithms for the electronic signature according to the Regulatory Authority for Telecommunications and Posts (RegTP)

Every year, the Regulatory Authority for Telecommunications and Posts (RegTP) publishes those cryptographic algorithms which can be considered as suitable at least for the forthcoming six years with a view to fulfilling the requirements of the German Signature Act (SigG) and the Digital Signature Ordinance (SigV)[120]. The German Federal Office for Information Security (BSI) can classify further methods as suitable.

An electronic signature for the purposes of the Act includes the following cryptographic algorithms.

a. An algorithm for hashing data (i.e. a hash function) which reduces the data to be signed to a hash value, i.e. a bit string of a constant length. This then means that the hash value rather than the data itself is signed.
b. An asymmetric signature method which consists of a signing and a verification algorithm. The signature method is dependent on a key pair which consists of a

[119] Refer to http://www.w3.org/TR/xkms2/

[120] Refer to http://www.regtp.de/tech_reg_tele/in_06-02-02-00-00_m/03/

private (i.e. secret) key for signing (generating) and the pertinent public key for verifying (checking) the signature.

c. A method for creating key pairs for the individual communication partners.

Suitable hash functions

a. RIPEMD-160
   RIPEMD-160 is a cryptographic hash function which, like SHA1, generates hash values with length of 160 bits.

b. SHA1
   SHA1 (Secure Hash Algorithm) is a cryptographic hash function which is very commonly used. SHA1 processes blocks with a length of 512 bits and generates hash values with a length of 160 bits.

Suitable signature algorithms

a. RSA
   RSA was developed by Rivest, Shamir and Adleman. The RSA method is the most important asymmetric method. It is also termed public key method. The security is based on the difficulty to factorise large natural numbers. Usual modulus lengths are 512, 1024 and 2048 bits, with 512-bit keys being no longer recommended.

b. DSA
   The Digital Signature Algorithm (DSA) is a signature method which was developed and specified in 1991 in the US Digital Signature Standard (DSS). DSA is a mere signature algorithm (with RSA, in contrast, enabling both the electronic signature and the exchange of keys). Although the US government has obtained a patent for DSS, its use is free.

c. DSA variants are based on elliptic curves (EC-DSA, EC-KDSA, EC-GDSA, Nyberg-Rueppel signatures).

The suitability and/or specific form of the algorithms to be applied can be influenced by the applicable standards; ISIS-MTT part 6, for example, specifies the cryptographic algorithms valid for ISIS-MTT.

9.4.6 Symmetric cryptographic algorithms for encryption

Cryptographic algorithms for encryption can be applied to data and/or keys in order to ensure their confidential transmission.

Symmetric methods, when applied, use the same private key for encryption and decryption. These methods usually feature very high performance.

Although the Regulatory Authority for Telecommunications and Posts (RegTP) does not specify any encryption algorithms, the algorithms specified in ISIS-MTT part 6 (Cryptographic Algorithms) are adopted in this case. The specifications in the ISIS-MTT standard prevail in cases of doubt. With regard to mode and padding of the algorithm in question, reference is made to ISIS-MTT part 6.

Mandatory: Triple Data Encryption Algorithm (Triple-DES)

Triple-DES[121], also termed 3DES, is a triple DES variant, i.e. a symmetric encryption algorithm with an effective key length of 168 bits. 3DES uses three DES keys with 56 bits each. Although this method is considered to be secure, it does not feature very high performance.

Mandatory: International Data Encryption Algorithm (IDEA)

IDEA was developed in Europe and features a key length of 128 bits.

Under observation: Advanced Encryption Standard (AES)

AES[122] is a symmetric block cipher which will replace Triple-DES as the standard and which encrypts 128-bit data blocks with key lengths of 128, 192 or 256 bits. The next ISIS-MTT version will include AES in part 6 (Cryptographic Algorithms).

[121] Refer to http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf

[122] Refer to http://csrc.nist.gov/

Appendix A Basic modules of the BundOnline initiative

The implementation of the more than 400 Internet-enabled services identified within the framework of BundOnline 2005 is supported by so-called **basic components**. Basic components centrally offer certain technical functionalities which can be used by different services and public agencies. Basic components provide technology platforms which, once developed, are widely used by the federal administration, either without any changes or in adapted configurations.

Basic components provide functionality blocks which form part of a host of services and which are integrated, as services or modules, into e-government applications. They are implemented in several stages. This means that new versions of the basic components with upgraded functionalities will become available during the course of time.

With regard to business cases classified as mandatory, the basic components must be generally used for the implementation of e-government applications. Any temporary use of alternative implementation approaches for functionality blocks implemented by basic components must be restricted to justified, exceptional cases if this helps avoid future migration costs. Appendix B gives an example on page 159 of how several basic components can be integrated into the processes of a special application.

Besides the basic components which directly perform sub-processes of e-government applications, **infrastructure components** are also made available within the framework of the BundOnline initiative. These infrastructure components support the implementation of an intranet for the entire federal administrations. Although the services are not specific to concrete e-government applications, they nevertheless have a key role to play in electronic communications between public agencies.

One for all services ("OFA services") not only support sub-processes in the way basic components do, but also perform complete services on their own. These services are of a type offered by several public agencies in an identical or similar manner.

So-called **competence centers** are set up in addition to the basic components. The main task of competence centers is to offer public agencies accompanying support when it comes to introducing the relevant basic components and adapting their business processes to the use of e-government applications.

A.1 Payment platform basic component ("e-payment")

A.1.1 Introduction

The web-based "e-payment" platform is used by special applications of the federal administration in order to generate automatic debit entries, to report the success or failure of a collection attempt and to make revenues available to the Federal Budget-

ing and Accountancy Service. The special applications can sell products or services or collect fees.

The basic component is provided centrally. Time-consuming and costly process analyses are no longer necessary at the special application end. Quantity discounts and hence better terms and conditions can be obtained from banks.

Contact partner	Mr Volker Walgenbach ePayment@bff.bund.de Bundesamt für Finanzen Friedhofstrasse 1 53225 Bonn Tel. +49 228 406-2905 Fax +49 228 406-2241
Availability of the basic component in version 2.0	Since July 2003
Web address for information concerning the basic components and contents of the versions	https://epay.bff-online.de/doku/ For login information and password, please contact the above-named contact partner, or send an e-mail to: ePayment@bff.bund.de.

A.1.2 Features

The payment platform supports the following payment methods.

a. Direct debit
b. Bank transfer
c. Credit card (version 2.0 and higher)

The following section will discuss the individual methods in more detail for the different business cases. The "Roadmap" section which follows enumerates several payment methods the implementation of which is still under examination.

The basic component solely handles the revenue end of transactions. Payments still use the conventional methods. Revenue orders received by the payment system are automatically passed on to the payment monitoring system (ZÜV) where they are represented by conventional debit posting.

Amounts of less than five euro are not collected for reasons of economic efficiency. Such amounts remain as debit entries in the payment monitoring system either until the debit amount exceeds five euro or until the debit entry is automatically eliminated at the end of a financial year. In the case of payment partner accounts or in the case of a payment falling due at the end of a year, the debit entry remains even during the following financial year. Micropayments, i.e. the process of accumulating debit entries

up to a certain amount, are not considered because the Federal Budget Code (BHO) stipulates the immediate collection of amounts.

Business processes where payment is just one of several modules must be developed from within the special applications. In line with the specific nature of such processes, the payment platform must then be integrated into the special method. The e-payment project group operates a competence center offering consultancy services and advice on all issues related to electronic payments. To this effect, experience from pilot projects is gathered and made available.

Section A.1.5 "Interfaces" on page 116 describes a reference implementation for integrating the basic component into special processes.

A.1.3 Business cases

All business cases are classified as **mandatory**. E-government applications primarily use the browser as the front-end, unless the services to be implemented cannot be reasonably handled via a browser.

Some of the following business cases include an address and solvency check. The basic component party relies on external service providers which offer online checks. The address check ensures that an address really exists. The solvency check includes, for example, a plausibility check of account number and bank code, the analysis of open invoices, the volume of invoices paid and reverse entries, if any. As a result, a customer can, for example, be granted a higher purchasing volume or allowed to pay after delivery. The special applications can configure the individual test steps and their performance from case to case.

Bank transfer prior to delivery

Prepayment by bank transfer is a secure payment method and hence particularly suitable for large-sum payments.

a. Registration of the customer with the customer's e-mail address or another unambiguous feature for service of the bill.
b. The customer fills the shopping cart and states a delivery address.
c. The special application sends the bill to the customer.
d. The special application transmits the data necessary for the debit entry either in cycles (for example, once a day) or immediately online. Once a day, the e-payment server sends the data of all the bank transfers to be expected to the payment monitoring system.
e. The customer pays the bill.
f. The payment monitoring system informs the e-payment server that the bill was paid.
g. The special application retrieves the recent payment information from the e-payment server in cycles (for example, once a day).
h. The special application ships the goods or renders the service.

Bank transfer after delivery

This form of payment is commonly used in mail order business. It is particularly suitable for the physical shipment of products or for rendering services. The suitability of this system for electronic downloads must be examined from case to case.

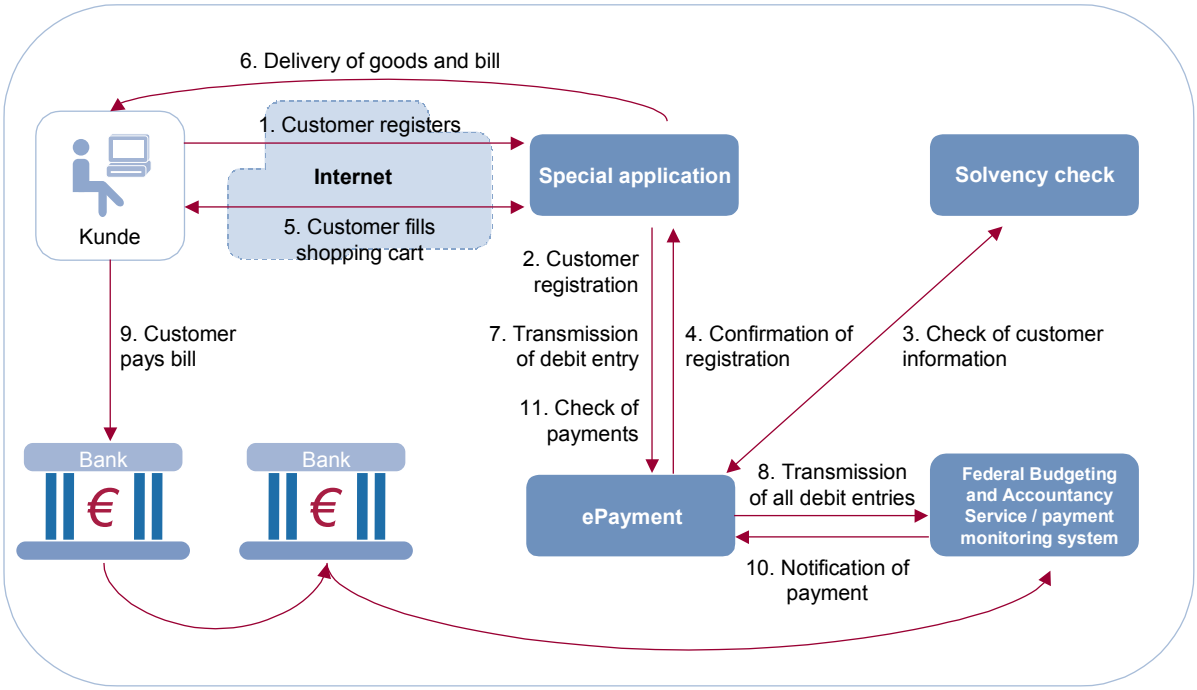


Figure A-1: Bank transfer after delivery with the e-payment basic component

1. Registration of the customer with the customer's address data for identification and e-mail address for service of the bill
2. Check of customer data
3. The customer fills the shopping cart.
4. The special application immediately ships the goods or performs the service and sends the bill to the customer.
5. The special application transmits the data necessary for the debit entry either in cycles (for example, once a day) or immediately online. Once a day, the e-payment server sends the data of all the bank transfers to be expected to the payment monitoring system.
6. The customer pays the bill.
7. The payment monitoring system informs the e-payment server that the bill has been paid.
8. The special application retrieves the recent payment information from the e-payment server in cycles (for example, once a day).

Collection by electronic direct debit

Direct debit is a very popular form of payment in Germany, with electronic direct debit being a very common form of payment on the Internet. This method is a suitable form of payment for once-off services and for goods shipped. The amount due is collected immediately. The "Repeated direct debit with cash-collect authorisation" form of payment should be adopted for repeating payment processes.

Checks are a vital precondition because users can theoretically submit incorrect account information and because payments collected can be re-debited for a period of one year. In view of the risks for the special application, this method is not suitable for larger amounts. It is left to the discretion of every special application at what level it determines the upper limits for the different solvency levels.

a. Registration of the customer with the customer's address data for identification as well as account information
b. Immediate check of the complete customer information
c. The customer fills the shopping cart.
d. (Either immediately or after receipt of payment), the special application ships the goods or performs the service and sends the bill to the customer.
e. The payment monitoring system collects the amounts due once a day or when due.
f. The payment monitoring system informs the e-payment server that the bill has been paid.
g. The special application retrieves the recent payment information from the e-payment server in cycles (for example, once a day).

Repeated direct debit with cash-collect authorisation

This method is particularly suitable when it comes to collecting fees for recurring services. This payment method is relatively secure because the customer signs a cash-collect authorisation form which can be submitted to the bank should a re-debit occur. It is left to the discretion of every special application at what level it determines the upper limits for the different solvency levels.

Since the authorisation process takes several days when used by a customer for the first time, the special application should be capable of storing a shopping cart over a longer period of time.

a. Registration of the customer in order to be able to assign the cash-collect authorisation to the customer at a later time
b. The customer fills the shopping cart.
c. If a direct debit authorisation was already issued to the special application, step f follows.
d. The customer grants the cash-collect authorisation once and sends it by post.
e. The customer's PIN is sent once by post.

f. The customer uses the PIN to confirm the payment process for the goods and services in the shopping cart.
g. (Either immediately or after receipt of payment), the special application ships the goods or performs the service and sends the bill to the customer.
h. The amount due is debited to the customer's account and credited to the federal government's account.
i. The payment monitoring system informs the e-payment server that the bill has been paid.
j. The special application retrieves the recent payment information from the e-payment server in cycles (for example, once a day).

Credit card

a. Registration of the customer; address information is not absolutely necessary with this form of payment.
b. Address verification can be carried out if goods are delivered or services rendered immediately.
c. The customer fills the shopping cart.
d. The special application checks the credit card information, including the Card Verification Code (CVC), and sends this information to the e-payment system for debiting the credit card.
e. (Either immediately or after receipt of payment), the special application ships the goods or performs the service and sends the bill to the customer.
f. The e-payment and the payment monitoring system jointly settle the bill, i.e. collect the amount due.
g. The payment monitoring system informs the e-payment server that the bill has been paid.
h. The special application retrieves the recent payment information from the e-payment server in cycles (for example, once a day).

A.1.4 Roadmap

Version 2.0 of the payment platform basic component is available for productive operation. Major upgrades are currently not planned. The pertinent competence center ensures maintenance, service and operation. Work on connecting special e-government applications to the e-payment system is currently underway. Within this framework, the basic component will be continuously developed further in order to consider and address new requirements.

A.1.5 Interfaces

The payment platform is implemented using central web services. These are so far the following services.

a. Customer data management
b. Bank search
c. Bank transfer methods
d. Direct debit payment methods
e. Credit card payment methods

The project group provides a reference implementation in Java which enables integration of the basic component into a local special application / e-shop. The implementation includes all the necessary SOAP interfaces, including serialisers and deserialisers. Open-source libraries were used for implementation throughout. Integration into commercial shop systems, such as Intershop Infinity, should be possible.

For further information, please refer to the web address stated in the introduction.

A.2 Data security basic component ("virtual post office")

A.2.1 Introduction

The core element of the data security basic component is the virtual post office (VPS) which is to support e-government applications in the implementation of secure, traceable and confidential communications between two partners within the framework of e-government services offered by public agencies. It is, for example, designed to significantly relieve all the parties involved of sometimes complex and error-prone cryptographic operations which are still a frequent characteristic of communications secured by electronic signatures and encryption.

The verification component is another central element of the virtual post office. This component enables internal and external users to verify the signature of documents. This is carried out using program libraries of the virtual post office. The user interface is implemented on the basis of a client/server-based application.

Contact partner	Dr Christian Mrugalla egov@bsi.bund.de Bundesamt für Sicherheit in der Informationstechnik Postfach 20 03 63 53133 Bonn Tel. +49 1888 9582-232 Fax +49 1888 9582-405
Availability of the basic component in version 1.0	Early 2004
Availability of the basic component in version 2.0	Autumn 2004

Web address for information concerning the basic components and contents of the versions	http://www.kbst.bund.de/saga-bk-vps

A.2.2 Features

The virtual post office serves as a central security gateway and communication server, offering security services via standardised interfaces for secure communications between public agencies and external communication partners, such as other public agencies, citizens and businesses. To this effect, the virtual post office supports the special applications in warranting the following security targets.

a. Confidentiality – of information both transmitted and stored
b. Integrity – of information both transmitted and stored
c. Binding effect – authenticity and demonstrability
d. Authentication – support for web-based and other applications with different authentication methods
e. Monitoring and auditing

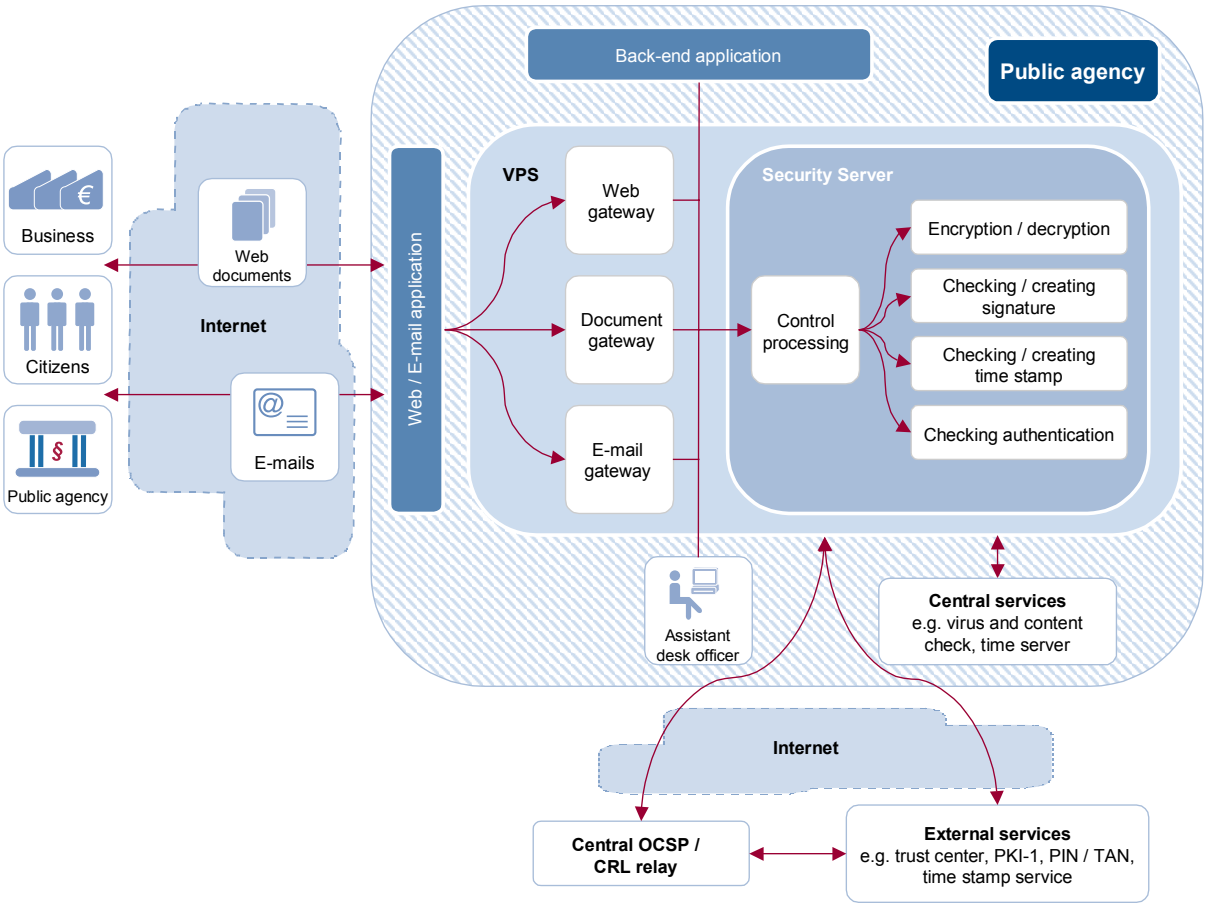


Figure A-2: Principle of the data security basic component

The security functions enumerated below are made available to the e-government services as uniform and – to the maximum extent possible – automatic functions via the interfaces offered.

a. Encryption and decryption
b. Signature check and generation
c. Time stamp check and generation
d. Security checks, such as virus or contents checks of e-mails and documents
e. Authentication on the basis of different credentials
f. Check of the security features of a document
g. Administration of the virtual post office

For the purposes of some of the aforementioned functions, the virtual post office uses central infrastructure services or external services; refer to Figure A-2 on page 118.

Besides indirect e-mail communication with a central address at public authorities, the basic components also supports strict end-to-end security with individual officers. This means that inbound and outbound e-mails are then passed on without being changed and without encryption or decryption. This is why individual features of the virtual post office can be deactivated in a flexible manner.

In line with the varying requirements of the different special applications of a federal authority, the central security gateway offers graded security mechanisms and algorithms. Furthermore, methods commonly used by citizens and business are also integrated, such as ISIS-MTT, SPHINX, PGP (in versions which support X.509 certificates) as well as OSCI.

External trust centers communicate with the virtual post office via an OCSP / CRL relay. This component will be centrally provided for all federal authorities, but can also be operated locally by a public agency. The central relay offers the advantage from the point of view of the individual public agencies that there is just a single, uniform interface for certificate verification.

Prior to using the data security basic component, every special application is responsible for classifying its protection requirements. The data security competence center (refer to section A.9.2, page 155), offers its advisory services in this context. The competence center has also developed a strategy for the introduction of the virtual post office.

A.2.3 Business cases

All business cases are classified as **recommended**. Pending completion of version 1.0 of the data security basic component, the pertinent competence center offers its advisory services for establishing transitional solutions which will facilitate future migration to the basic component.

Every business case is accompanied by a documentation of the relevant actions of the virtual post office in the form of a routing slip which is transmitted as an XML file. Access to the data in inbound-mail and outbound-mail records which may exist outside the virtual post office is restricted to administrators with special roles (supervision and audit). The preparation of such "records" is not a task of the virtual post office.

Public agency receives document as an e-mail

a. External mail user sends an e-mail to an internal recipient.
b. The incoming e-mail is checked and passed on.
    i. Decryption, if necessary.
    ii. Checking signature and time stamp of the e-mail, if necessary.
    iii. Virus check of the contents of the e-mail.
    iv. Further encryption, if necessary.
c. If necessary, use of an interface for entry in the inbound-mail record.
d. Sending an e-mail to internal recipients; observing out-of-office rules, if necessary.
e. If necessary, confirmation of receipt to the sender.

Public agency receives document via web browser / application

a. External browser user / application sends a document.
b. Authentication on the basis of the document's signature.
c. Incoming document is checked and passed on.
    i. Decryption, if necessary.
    ii. Checking signature and time stamp of the document, if necessary.
    iii. Virus check of the document.
    iv. Further encryption, if necessary.
d. If necessary, passing on for entry in a mail-in record.
e. Passing the document on to the application.

Public agency sends document as an e-mail

a. Internal mail user sends an e-mail to an external recipient.
b. Outgoing mail is checked and passed on.
    i. Decryption, if necessary.
    ii. Checking signature and time stamp of the e-mail, if necessary.
    iii. Virus check of the contents of the e-mail.
    iv. Time stamping.
    v. Signing the e-mail / further encryption, if necessary,
c. If necessary, passing on for entry in a mail-out record.

d. Sending the mail to the external recipient.
e. If necessary, confirmation of receipt to the sender.

Public agency sends document via web browser / application

a. Internal web user / application sends document to external recipient.
b. Outgoing document is checked and passed on.
    i. Decryption, if necessary.
    ii. Checking signature and time stamp of the document, if necessary.
    iii. Virus check of the document.
    iv. Time stamping.
    v. Signing the document / further encryption, if necessary.
c. If necessary, passing on for entry in a mail-out record.
d. Passing the document on to the application.

Internal processing of a document

a. Internal browser user / application sends a document for processing.
b. The incoming document is processed in accordance with the attached rules.
    i. Decryption / encryption, if necessary.
    ii. Checking / creating a signature, if necessary.
    iii. Checking / creating a time stamp, if necessary.
    iv. Virus check of the document, if necessary.
c. Passing the document on to internal browser user / application.

Verifying a signed and, if applicable, time-stamped document

a. Internal /external browser user / application sends a document for checking.
b. Application sends signature, hash value, certificate and, if applicable, time stamp to virtual post office.
c. Virtual post office verifies the document.
    i. Mathematical check of the signature.
    ii. Checking the time stamp, if necessary.
    iii. Checking the certificate chain.
    iv. Checking the root certificate.
d. The result of the check is passed on to the application (secured, if necessary).
e. The result of the check is displayed to the user of the browser / application.

Authenticating an internal / external user of browser / application

a. Browser user sends the data necessary for authentication.
b. Application sends the credentials to be checked to virtual post office.

c. Virtual post office checks credentials with regard to:
   i. correctness
   ii. validity
d. The result of the check is passed on to the application (secured, if necessary).
e. The result of the check is displayed to the user of the browser / application.

Public agency receives several documents in one e-mail

a. External mail user sends signed e-mails to internal recipient with several signed and encrypted attachments.
b. Incoming mail is checked by virtual post office in line with business case 1 and passed on to internal recipient.
c. Internal recipient breaks the e-mail down using an application which passes on every document individually to the virtual post office.
d. Virtual post office checks every document.
   i. Decryption.
   ii. Checking signature and time stamp of the document.
   iii. Virus check of the document.
e. Virtual post office sends the result of the signature check and the decrypted document to the application.

A.2.4 Roadmap

Early 2004	• Release 1.0 of the virtual post office can be used by selected BundOnline 2005 pilot applications. o OCSP / CRL relay o Verification and authentication module (restricted functionality) o (Rudimentary) kernel system using Governikus-1.1 components o SMTP product ("Stand-alone")
2nd quarter 2004	• Release 1.1 o Extended functionality of the kernel system, authentication even without OSCI o OSCI enabler on OSCI 1.2 basis o SMTP product using the OCSP / CRL relay
Autumn 2004	• Release 2.0 is the implementation of the virtual post office in accordance with the technical concept.

For up-to-date information, please refer to the web address stated in the introduction.

A.2.5 Interfaces

The published technical concept of the virtual post office (to be found at the web address stated in the introduction) includes a table with an overview of the interfaces of the virtual post office. A detailed interface description will be prepared during the implementation phase. Examples of selected interfaces are described in the following.

a. The MIME and S/MIME encapsulated in XML formats are used for communication with **mail applications**. The Java Message Service (JMS) is used to exchange data.
b. Communication with the **authentication component** proceeds via an XML-based protocol which is also transported by the JMS.
c. An XML-based protocol and JMS are also used for the **verification component**.
d. The LDAP protocol is used for access to **directory services** (internal users, external users, trust center). The transport proceeds via Secure Socket Layer (SSL).

A.3 The portal basic component

A.3.1 Introduction

The bund.de portal as a basic component is the central point of access to the federal agencies' electronic services and information offerings on the Internet. A content management system permits access by distributed users and enables all the public authorities and agencies to publish information via the portal.

The portal provides the addresses of the federal agencies and further information concerning organizational structures and services of the individual public agencies. The portal provides central information services, such as vacancies at administrations, publication of non-electronic invitations to tender, information on sales by administrations, etc. The portal's information offering, the number of services provided centrally and interfaces are being continuously expanded.

All public agencies are called upon to see to it – if necessary, with support by the portal editors – that the information on the portal is at all times up-to-date and complete.

Contact partner for organizational matters	Mr Andreas Polster pgbo2005@bmi.bund.de Bundesministerium des Innern Projektgruppe BundOnline 2005 Bundesallee 216-218 10179 Berlin Tel. +49 1888 681-4318 Fax +49 1888 681-54318

Contact partner for technical matters	Mr Thomas Schubert thomas.schubert@bva.bund.de Bundesverwaltungsamt Barbarastr. 1 50735 Köln Tel. +49 1888 358-3936 Fax +49 1888 358-2832
Availability of the basic component	Since 21 March 2001
Web address for information concerning the basic components and contents of the versions	http://www.bund.de/Service/Ueber-bund.de-.5977.htm

A.3.2 Features

The portal's underlying technology is currently the portal editing system from the company]init[and a search engine from FAST (formerly Altavista). The portal is migrated to the CMS basic component[123] BundOnline 2005 initiative (CAP 4.1 editor system from CoreMedia). The bund.de data is updated and maintained by local editors and a portal editing team working at distributed locations. The respective public agency always has the editorial control of the information to be presented.

The portal is implemented in several stages, with the second of three development stages currently underway.

Stage 1

Since the CeBIT in March 2000, the "search" and "find" core functions have been available at the first stage. The portal hence appears to Internet users in the familiar form of a catalogue with a search engine.

The catalogue helps to retrieve information offerings and services in the form of annotated links which are divided into subjects. The public agency database is updated in a de-centralised manner and covers the supreme constitutional organs, all the federal authorities and major institutional recipients of funds, such as large libraries, museums and research institutes. The federal states are represented with their constitutional organs, the supreme administrative levels and further public agencies, whilst the municipal level is represented with the central organizations and the large cities.

The central full-text search function is based on a search index which covers the complete offer from all public agencies. The geo-search function shows users maps with the locations of public agencies. Several columns of the portal offers users the

[123] Refer to section A.5 "The content management system basic component", page 132

possibility to register for e-mail subscriptions. Any information that is newly published via the portal editing system is immediately circulated by e-mail.

Users can send inquiries to public agencies via a contact form, by e-mail, fax or telephone. The portal editing team answers the inquiries or passes them on to the appropriate public agencies for further action.

Stage 2

The focal task of the second stage was the implementation of the ordinance on the creation of barrier-free information technology (BITV) which came into effect on 24 July 2002. At the CeBIT in March 2003, the federal administration's portal www.bund.de went online in a barrier-free condition.

Besides the revision of the portal in line with the ordinance on the creation of barrier-free information technology, the number of central services on offer was increased. In 2002, the most important forms of the federal administration, for example, were made available via the new online form centre of the portal[124]. Job centre, sales and invitations to tender were upgraded by adding new functions. The municipality search function now offers a full range of important communal data in an interactive format.

Stage 3

Stage 3 will mark the migration of the portal to the CMS basic component of the BundOnline 2005 initiative. The migration project is scheduled for completion by mid-2004. This will then be followed by the implementation of a knowledge-based online information system via the portal. This would help reduce portal editing costs and mean a further expansion of help desk functions.

When the federal government's electronic services will be implemented in 2005, these services will then be fully available for research via the federal government's service portal.

A.3.3 Business cases

The business cases discussed below can serve as an orientation aid for decisions concerning the use of the portal and of its functions.

Maintenance and updating of the federal government's central database (public agency master data)

a. The master data of public agencies to be published is compiled.
b. This data is imported to the portal via the portal editing system or via the import interfaces on an XML basis.
c. Data is exported on an XML basis. Web service is enabled.

---

[124] Refer to section A.4 "The form server basic component", page 128

This business case is **mandatory**. The parallel provision of addresses of public agencies on the portal and in the directory service of the Berlin-Bonn Information Network (IVBB) (around 860 federal authorities on the portal and around 100 in the Berlin-Bonn Information Network) will be replaced with an export of this data on an XML basis and the provision of this data for updating the directory of the Berlin-Bonn Information Network.

Maintenance and updating of the federal government's central database (services)

a. The service information to be published is compiled.
b. The portal editing system is used to publish this information on the portal.
c. Data is exported on an XML basis.

This business case is **mandatory**.

Maintenance and updating of the central information services (forms, vacancies, non-electronic invitations to tender and sales)

a. The offers to be published are compiled.
b. The portal editing system is used to publish this information on the portal.
c. Data is exported on an XML basis. Web service is enabled.

This business case is **recommended**. The exchange with external information services on an XML basis and/or via web services is planned for the future.

Maintenance and updating of the "Latest News" information offer

a. The latest news to be published is compiled by the editorial team.
b. The portal editing system is used to publish this information on the portal.

This business case is **recommended**.

Maintenance and updating of the information offered by the federal states

a. The federal-state information to be published is compiled.
b. The portal editing system is used to publish this information on the portal.

This business case is **under observation**. All the federal states generally have the possibility to update their public-agency information themselves using the editing system of the company]init[. Replacement with XML-based data exchange and/or via web services is planned during the course of the migration project.

Maintenance and updating of municipality data

a. Information concerning cities, districts and municipalities to be published is obtained from external sources.
b. A routine of the portal editing system is used to publish this information on the portal.

This business case is **recommended**.

Maintenance and updating of the BundOnline 2005 information offers

a. The information concerning BundOnline and the initiative's progress to be published is compiled.
b. The portal editing system is used to publish this information on the portal.
c. The data of the BundOnline services can be exported on an XML basis.

This business case is **mandatory**.

A.3.4 Roadmap

4th quarter 2003	• Publishing the invitation to tender for migrating the latest portal version to the CMS basic component
2nd quarter 2004	• Migration by 30 June 2004
3rd quarter 2004 and thereafter	• Further functional upgrading of the portal

A.3.5 Interfaces

The existing interfaces use the export and import functions of the editing system of the company]init[. The interfaces of the CMS basic component of the BundOnline 2005 initiative will be used following migration.

Web services

The following web services are currently implemented.

a. Master data of a public agency
b. Active invitations to tender
c. Active vacancies
d. Active sales
e. Geographic location of an address sent

These web services are available to a restricted user group and are hosted on a UDDI server.

Data export

The editing system of the company]init[includes intervention options for data export operations which the portal editor can use to export data records. The export functionalities include the following options.

a. Public-agency entries can be exported separately or together with the pertinent addresses (public agencies: address data = 1 : n).
b. Public-agency entries and addresses can also be exported as comma-separated files.

c. The complete address directory at bund.de can be downloaded (exported) as a PDF file.
d. The following extended organization data of a public agency can be exported in the XML format.
   i. Addresses / real property of a public agency
   ii. Contact partners
   iii. Lower-level agencies
   iv. Subjects in the catalogue
   v. Services and BundOnline services
   vi. Forms
   vii. Vacancies
   viii. Invitations to tender
   ix. Sales

X.500 export

Addresses of public agencies are made available in the CSV format to the directory service of the Berlin-Bonn Information Network for import via its X.500 interface.

Data import

Public-agency master data can be imported via the defined XML format for public-agency entries and addresses.

The "form server" basic component

The "form server" basic component includes the form centre in its first stage on the bund.de portal. For details, please refer to section A.4 below.

A.4 The form server basic component

A.4.1 Introduction

The "form server" basic component includes the form centre on the bund.de[125] portal in its first stage. The further upgrading of the basic component will depend on the result of an in-depth analysis of demand among public agencies which require a form-based exchange of data for BundOnline 2005 services.

[125] Refer to http://www.bund.de/formulare

Contact partner for organizational matters	Mr Andreas Polster pgbo2005@bmi.bund.de Bundesministerium des Innern Projektgruppe BundOnline 2005 Bundesallee 216-218 10179 Berlin Tel. +49 1888 681-4318 Fax +49 1888 681-54318
Contact partner for technical matters – Form centre	Mr Thomas Schubert thomas.schubert@bva.bund.de Bundesverwaltungsamt Barbarastr. 1 50735 Köln Tel. +49 1888 358-3936 Fax +49 1888 358-2832
Availability of the form centre	Since March 2002 at: http://www.bund.de/formulare
Web address for information concerning the basic component and the stages	http://www.kbst.bund.de/saga-bk-form

A.4.2 Features

A.4.2.1 Features of the form centre

The bund.de[126] portal offers a cadastre of e-forms[127] of the federal government for citizens, business and public administrations as the relevant target groups. Internet addresses and descriptions of the e-forms can be provided via the portal editing system.

The e-forms are sorted according to target groups on the top level. The structure is then broken down further into subjects and concrete issues. The individual e-forms are offered as PDF or HTML documents. A search engine and the catalogue of the portal enable the quick identification and retrieval of e-forms on the basis of form numbers. Addresses and descriptions of the e-forms are offered via a web service of the portal.

---

[126] Refer to http://www.bund.de/formulare

[127] The term *"paper form"* as used in this document refers to a printed form supplied by a public agency or on its behalf. The term *"electronic form"* (e-form) refers to the rendering of this paper form and/or its contents in digital form, including the related IT-based functionalities.

A.4.2.2 Further development of the basic component

Complete and media-consistent, form-based data exchange between users and administrations is a medium-term goal. This means that all relevant steps – from the creation and publishing of e-forms via their filling in, signing, encryption and mailing by users right through to the media-consistent receipt and passing on for further processing at public agencies – will be supported by suitable interfaces of the basic component. Paper forms and e-forms are expected to be used parallel for quite some time.

A.4.3 Business cases

A.4.3.1 The "form centre" business case

The following business case describes important uses of the form centre. The use is classified as **mandatory**.

Paper-based submission of an e-form to a public agency

a. Providing the e-form in conjunction with the public agency's online service and publication in the form centre
b. Retrieving the e-form from the form centre and access to the public agency's online service
c. Download and filling in of the e-form by the user
d. Printing the completed e-form, signature and sending by post
e. Paper-based or digital further processing of the application by the public agency

A.4.3.2 Business cases for the further development of the basic component

The following business cases describe possible uses of the "form server" basic component in the interaction with other basic components and the related e-government applications. Modifications in the form of amendments to and restrictions for functionality are possible depending on the result of the evaluation of the current demand among federal authorities and the concept developed as a result of this. Since further development of the form server has yet to take place, these business cases are still classified as **under observation**.

Electronic submission of an e-form to a public agency

a. Creation of the e-form by the public agency. Additional functionalities, such as validation of data, are possible.
b. Providing the e-form in conjunction with the public agency's online service and publication in the form centre
c. Filling in the e-form online or offline; local storage of the e-form by the user

d. Electronic signing, encryption if necessary, and electronic mailing of the completed e-form
e. Paper-based or digital further processing of the application by the public agency

Integrated data exchange for services using e-forms

a. Creation of the e-form by the public agency. Additional functionalities, such as personalisation or validation of data, are possible.
b. Providing the e-form in conjunction with the public agency's online service and publication in the form center; adapting the e-form to the user's specific requirements
c. Filling in the e-form online / offline at the computer; if necessary, indirect data reconciliation based on special features of the online services
d. Electronic signing, encryption, if necessary, and connection to further basic components (such as e-payment) and mailing of the completed e-form; if necessary, adding electronic attachments (such as proof)
e. Receipt by the virtual post office (signature check, decryption, if necessary) of the e-form and electronic transmission to the special applications belonging to the online service
f. Communication with the user (for example, acknowledgment of receipt, reporting incorrect information) as well as status inquiry by the user
g. Possibility to involve third parties (for example, other public agencies, financial institutions, etc.) for application processing

A.4.4 Roadmap

4th quarter 2003	The demand analysis is concluded. Public agencies that voiced interest in the basic components are polled to this effect. The demand analysis forms the basis for the following concept development exercise. A user advisory board is set up parallel to this.

A.4.5 Interfaces

The use of directory services in accordance with SAGA (refer to section A.7, page 143) is to be enabled for data administration purposes for access by users from within public agencies.

Furthermore, interfaces with the following basic components may become relevant in future.

a. Creation and provision of e-forms for the "form server" basic component are connected to the content management system (CMS) basic component.
b. The "data security" ("virtual post office") basic component is to handle the receipt, the verification of signatures and, if necessary, the decryption of e-forms.

c. Form-based payments are passed on to the "payment platform" ("e-payment") basic component.

d. The form centre is integrated into the portal basic component.

What's more, the further processing of e-forms by special applications should be generally enabled, for example, by electronic workflow and document management systems.

A.5 The content management system basic component

A.5.1 Introduction

The "content management system" basic component is designed to standardise and facilitate information management and updating in intranet and Internet environments of federal authorities. This system which is also known under the federal government's "Government Site Builder" brand is a content management solution which was specifically developed to meet the needs of the federal administration. It features a multi client solution, fulfils the requirements for "barrier-free" Internet, and offers a configurable layout which is orientated towards the design guidelines published by the Press and Information Office of the Federal Government ("Internet Styleguide of the Federal Government"). The system comes with pre-configured modules which public agencies can accept as their own standard solutions or adapt to any specific needs. The basic component supports the production process by a roles and privileges concept as well as workflows with related quality assurance mechanisms. The content management framework from CoreMedia AG serves as the technological platform.

The economically efficient use of a content management system by the federal administration is possible thanks to central development and joint use of upgrades.

The solution is available both as a central platform service of the Federal Office of Administration and as a distributed component for which the individual public agencies are then responsible.

Contact partner for organizational matters	Mr Andreas Polster pgbo2005@bmi.bund.de Bundesministerium des Innern Projektgruppe BundOnline 2005 Bundesallee 216-218 10179 Berlin Tel. +49 1888 681-4318 Fax +49 1888 681-54318

Contact partner for technical matters	Mr Claus Hackethal claus.hackethal@bva.bund.de Bundesverwaltungsamt 50728 Köln Tel. +49 1888 358-1549 Fax +49 1888 358-3899
Availability of the basic component in version 1.0	Since 1 October 2003
Availability of the basic component in version 2.0	2004
Web address for information concerning the basic components and contents of the versions	http://www.bva.bund.de/aufgaben/bol_docs/ For login information and password, please contact the above-named contact partner for technical matters.

A.5.2 Features

The CMS basic component is based on the Smart Content Technology (SCI) of CoreMedia AG[128]. This component constitutes a powerful enterprise content management system (ECMS) which enables, for example, hosting and administration of the online activities of several public agencies on one system (multi client solution).

The CMS is accessed via editors. An editor based on Java technology and a browser-based web editor are available.

The use of the CMS basic component enables the separation of design, contents and logic. Contents are provided and administered in a structured manner separate from the layout. This is carried out on the basis of so-called document types which are used to classify and provide the contents. This enables editorial staff to focus on their core task, i.e. creating contents, without requiring special technical skills.

Within the CMS, contents are structured on the basis of these document types and their mutual relations. A document type includes attributes (properties) which contain the real information. Relations describe the relationships between the document types and determine which documents can contain lower-level documents and which attributes they inherit from them.

The basic component offers several document types which can be edited or amended as required, such as press release, speech, picture, job vacancy, and interview. However, the CMS basic component also enables the administration of graphics, video and audio data as distinct document types.

[128] Refer to http://www.coremedia.com/

Uniform and standardised document types also contribute towards easier exchange. Media-neutral output and rendering of the contents provided in this manner are ensured by presentation templates which consider the federal government's Internet Styleguide.

A version management function within the CMS supports the administration of documents and enables access to the latest or earlier versions of a document. On the basis of the version selected, a new version is generated when a document is edited. The previous version of the contents is saved accordingly. The version management functionality of the CMS basic component ensures that any access by any other authorised users to a document which is currently being edited is restricted to read access. After editing, the document, including the changes carried out in it, is returned to the system where it is then available to other users again. The link management feature of the basic components ensures the checking and correct resolution of internal links and supports this function in the case of external links.

Further technical functionalities are enumerated below.

a. Support of multilingual capability and internationalisation
b. Workflows, including a notification system, in order to represent editorial processes (4-eyes and 6-eyes workflows, proxy procedures, possibility of adding client-specific workflows)
c. Authorisation system (roles, privileges)
d. Style definition and creation of HTML forms on the basis of configurable, modular systems
e. Newsletter mailing (such as e-mail push system for press releases)

A.5.3 Business cases

Three business cases were identified for the CMS basic component. Description and classification of business cases serve as a basis for decisions concerning the use of the basic component.

Information website

Different kinds of contents must be administered and presented in the case of pure information services, such as websites of public agencies or Internet offers focusing on specific subjects. Change frequency and document numbers are usually high enough to justify the use of a content management system.

The use of the CMS basic component is hence **recommended** for all information services.

Websites of public agencies with access to special applications

Special applications of a communication or transaction nature must often be presented and/or integrated within the framework of websites. The bundling of different

special applications and their uniform presentation, in particular, call for the use of a CMS solution. The CMS acts as an integration platform in cases like this.

This integration is achieved by communication between the CMS (as the integration component) and the special application (application interface) on the middle tier level, with the possibility to export contents from the special application on the basis of XML files to the CMS. Furthermore, the presentation tier can be used – irrespective of the real CMS – to retrieve and visualise contents directly from the application interface of the special application. Possible communication protocols include SOAP, CORBA, RMI as well as direct inter-process communications.

Furthermore, the editing system of the CMS can be used to integrate additional contents – such as help texts and background material – and to link these contents to the contents of the special application on the presentation tier. The web front-end of the special applications is implemented by the CMS basic component.

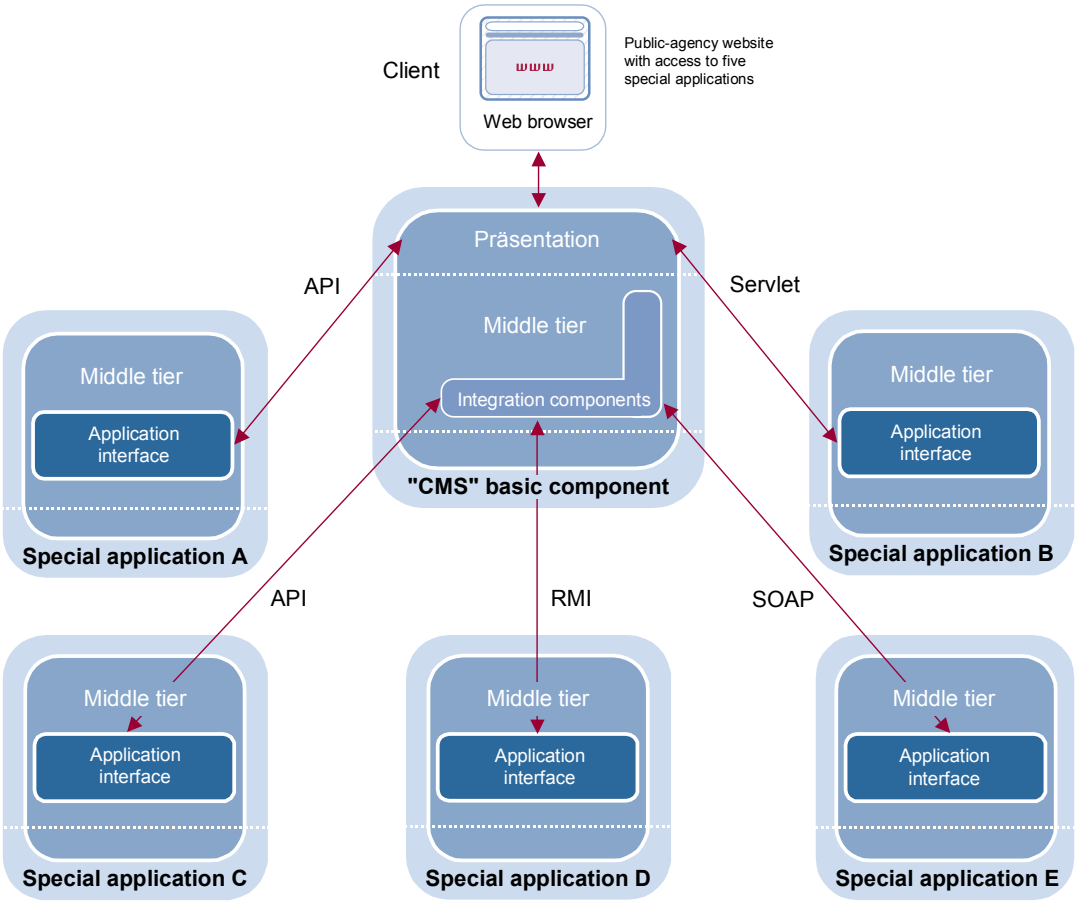


Figure A-3: CMS-based public-agency website integrates special applications

Figure A-3 shows five different special applications. Three of these special applications exchange contents with the CMS via different communication channels (such as API, SOAP or RMI). The data exchange format and the communication interfaces can be implemented on the basis of the interfaces provided by the CMS (refer to section A.5.6, page 138).

The other two special applications are integrated into the website irrespective of the CMS on the presentation tier in different ways (for example, using a special API or a servlet).

Communication via API or servlet means direct access to programming interfaces within the same runtime environment. In the case of communication via SOAP or RMI, the basic component and the special applications may be distributed to different computers in the network.

The use of the "content management system" basic component is **recommended** for integrating special applications on a public agency's website.

Special portal for a special application

The requirements for a special application often include the presentation of contents. These contents require special editing by the special application, depending on the underlying conditions. In order to avoid copying the functionalities of a content management system, the CMS should be integrated as a component into the special application. Depending on the concrete expectations, the export interfaces of the CMS can be adapted in such a manner that the contents are passed on to the middle tier of the special application. The contents are usually delivered in the XML format. It does, however, remain possible that the CMS already visualises the contents and passes these on in the HTML format to the presentation tier of the special application.

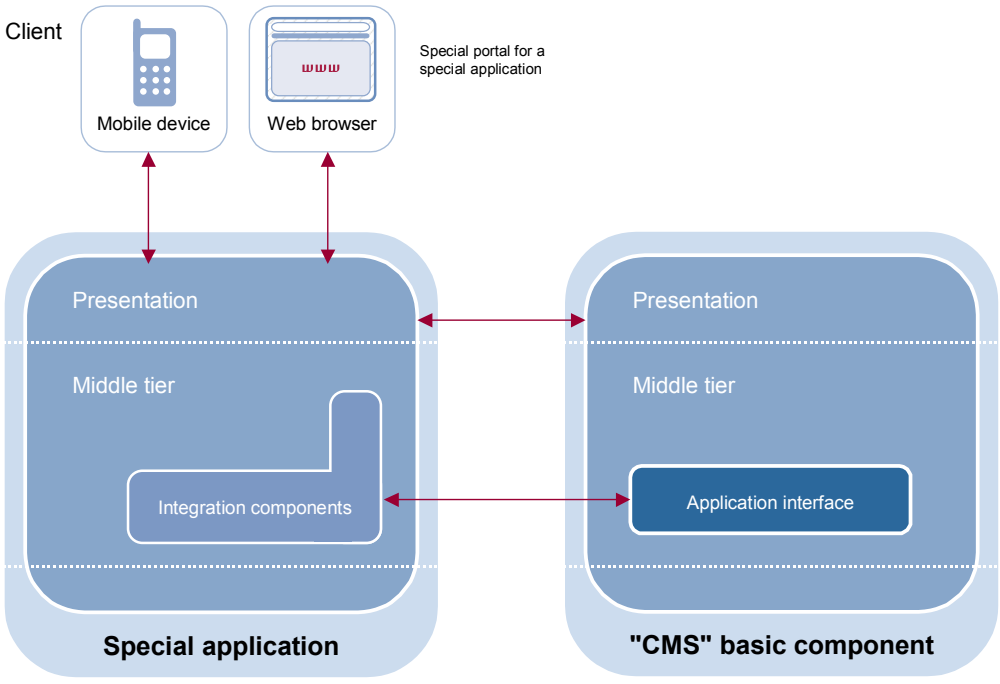


Figure A-4: Special application integrates functionality of the CMS

Figure A-4 illustrates the interaction between the special application and the CMS basic components, with the CMS integrated into the special application. Communica-

tion would typically take place directly either via an API or via servlets. However, it is also possible to use SOAP and RMI, so that the special application and the CMS can also run on different computers.

Besides the administration and visualisation of contents, further components of the CMS basic components can be used in conjunction with the implementation of a special application. In the case of personalised access, for example, the CMS could be used for user administration functions.

This business case is **under observation**. In view of the complex nature of the "content management system" basic component, costs and benefits of its use as a component of a special application must be carefully weighed up.

A.5.4 Application scenarios

Once the decision to use the CMS basic component has been made, two application scenarios can be considered for selection. The first option is to use the hosting environment which is available at the Federal Office of Administration (BVA). This is, for example, recommended for public agencies which do not run their own computer center, which operate only a limited technical infrastructure, or which prefer not to operate and administer the application themselves due to a lack of human resources. The shared use of a common solution can boost the economic efficiency of operations because infrastructures – such as computer center environment, networks, firewalls, server park, etc. – have to be installed and maintained only once.

Furthermore, it is also possible to use the basic component as software. This option can be exercised by public agencies running their own computer center and with high integration demands in conjunction with special applications. Furthermore, standalone operations feature higher performance compared to client mode. This scenario also enables the full use of the existing document model of the basic components and the pre-configured functionalities. If all of the features offered are not used, it is also possible to use just a subset.

The CoreMedia license is a variant of the second option. This variant is particularly useful if the document model or the editing interface have to fulfil special requirements. Due to the functional diversity of the basic components, larger upgrades of the system can require substantial adaptation effort, so that the use of the license and an agency-specific installation of the CoreMedia software can be the more economically feasible approach in the long term. Note that this variant requires new programming of the outside views and other elements.

When selecting the applicable scenario, the requirements for the e-government application as well as the agency's existing infrastructure and human resources situation must be considered. However, the CMS competence center should be contacted in any case before any decision in favour of central or de-centralised use. The decision in favour of a particular approach depends on the analysis of the economic efficiency of the particular case in question.

A.5.5 Roadmap

4th quarter 2003	• Start of productive operations of version 1.0 • Identification of requirements for version 2 • Compilation of practical experience from the first pilot projects
End of 2003	• Delivery of version 1.1 • Further development on the basis of the experience from the pilot projects
2004	• Start of development of version 2 of the basic component software on the basis of the identification of requirements

A.5.6 Interfaces

Up-to-date contents are a crucial factor for the success of a website. However, this information often stems from different systems or external partners. Furthermore, part of the contents must sometimes be disseminated to several partners. Moreover, existing contents of legacy systems are often to be reused in many intranet and Internet solutions and, when required, presented within the framework of the newly designed website. This will usually require further amendments or additional attributes for this legacy data.

The content management system from CoreMedia as the underlying system of the basic component hence includes interfaces for both XML import and XML export. However, since every system uses another XML specification, it is not possible to directly import this data into the target system. This is why special XML importers[129] are additionally offered, such as:

a. AP-Import (IPTC 7901)
b. dpa-Import (IPTC 7901)
c. dpa Newsfeed Interface

Interfaces with a more far-reaching functionality can be implemented in an event-driven manner on the basis of SOAP as web services in an J2EE-conforming software architecture. If additional interfaces and XML importers are needed, these can be developed in the projects and made available to the federal authorities. Following introduction of the basic component, the number of available interfaces increases with the number of public agencies using the component.

[129] The "special" XML importers listed here are not included in the license agreement between the federal government and CoreMedia.

A.6 The Federal Administration Information Network as an infrastructure component

A.6.1 Introduction

The Federal Administration Information Network (IVBV) is to facilitate communications and the supply of information within the federal administration by integrating existing and future information services into an intranet of the federal administration. All federal institutions and public agencies will be given the opportunity to join the network. They are offered a communication platform based on the Internet Protocol (IP) to this effect.

The Federal Administration Information Network (IVBV) is a further development of the Berlin-Bonn Information Network (IVBB) which disseminates information and communication services on a nation-wide level, integrates the entire federal administration as users and considers the public agencies' demand for long-distance communications.

Contact partner for organizational matters	Mr Friedrich Seifen seifen@kbst.bund.de Bundesministerium des Innern 10559 Berlin Tel. +49 1888 681-3355 Fax +49 1888 10 681-3355
Contact partners for technical matters	Mr Arnd van Dornick dornick@kbst.bund.de Bundesministerium des Innern 10559 Berlin Tel. +49 1888 681-2783 Fax +49 1888 681-2782
Availability of the infrastructure component	As of April 2004
Web address for information concerning the infrastructure component	http://www.kbst.bund.de/saga-ivbv

A.6.2 Structure

The Federal Administration Information Network (IVBV) consists of three levels are follows: IVBV services, IVBV network infrastructure and IVBV intranet.

In the federal administration, the Federal Administration Information Network is to bring together the providers of information services. It offers its users the federal government's information services in the form of **IVBV services** on the basis of vari-

ous sources, including, for example, the Federal Administration Information Network (IVBB) or BundOnline 2005.

Domain name services (DNS) and e-mail are important central services of the Federal Administration Information Network (IVBV). These services support communications between IVBV users as well as between IVBV users and users of connected networks, such as the Berlin-Bonn Information Network (IVBB). An Internet access does not form part of the IVBV. Internet access is implemented in the existing networks of the federal administration (such as the Berlin-Bonn Information Network) or from case to case by the Federal Administration Network (BVN).

The Federal Administration Network (BVN) will constitute an important basis for the **IVBV network infrastructure** and the common technical integration platform of the IVBV. The Federal Administration Network will connect existing networks of the federal administration and of the Berlin-Bonn Information Network to form an integrated IP network, i.e. the IVBV network infrastructure.

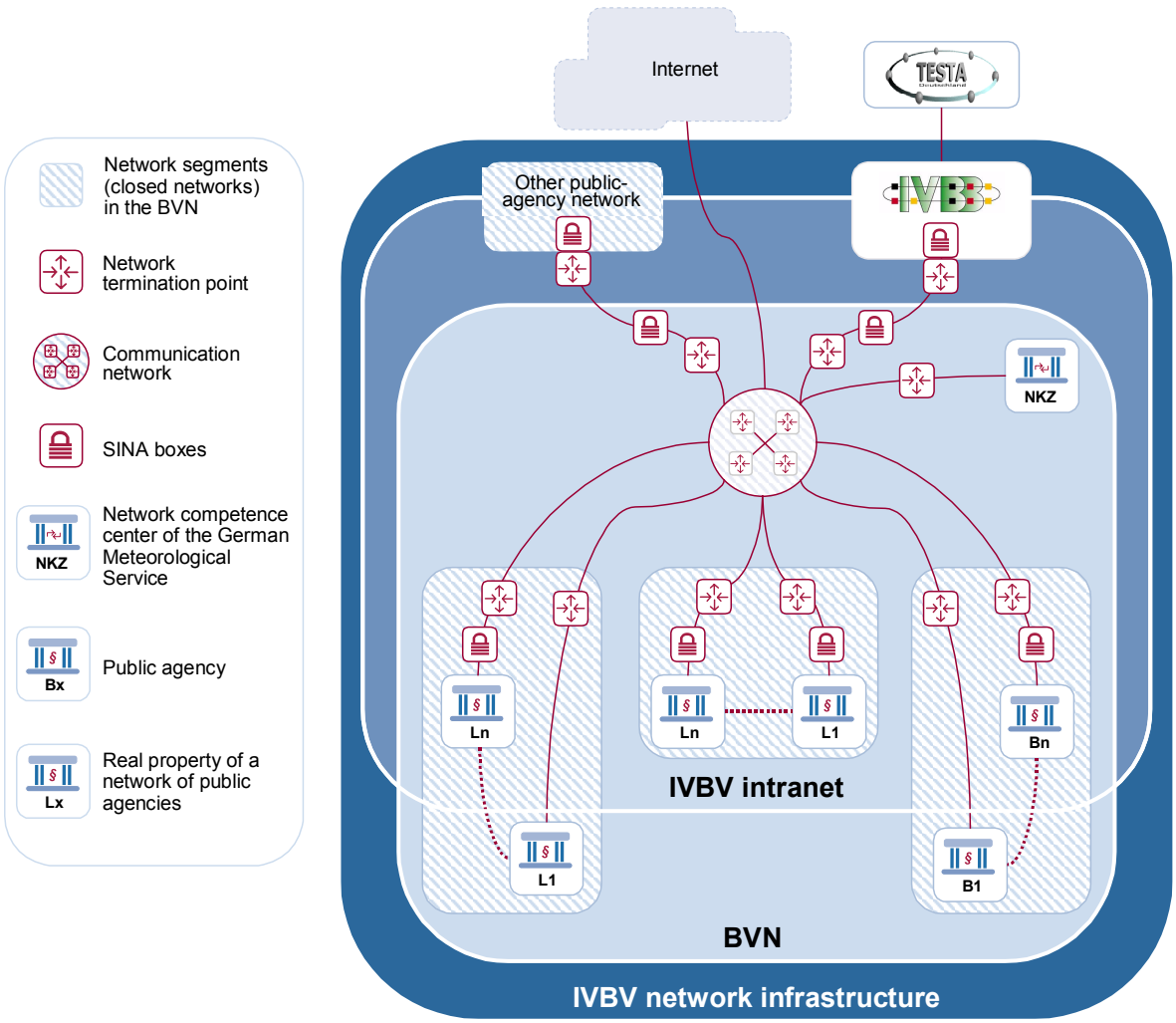


Figure A-5: IVBV network infrastructure and intranet

The services specified in the **skeleton agreement on the Federal Administration Network (BVN)** will enable federal administration authorities without network access of their own to implement their own, demand-orientated long-distance network for communication between distributed sites and for accessing the Federal Administration Information Network via their connection. The skeleton agreement also covers (transparent or secured, respectively) access to the Internet which public agencies can obtain in order to connect to the Federal Administration Network.

The **IVBV intranet** will constitute a separate information area which covers all the networks of the IVBV network infrastructure. Public agencies access the IVBV intranet via line encryption devices (SINA boxes) which ensure the confidentiality and integrity of the information transmitted. The IVBV intranet will constitute a virtual private network (VPN) on the basis of the IP networks which are integrated by the IVBV network infrastructure.

A **"Service Center IVBV"** (SC IVBV) will be set up with responsibility for monitoring network operation and representing the public agencies' interests in relation to the network operator, as well as for management and operational tasks in the IVBV.

A.6.3 Users and conditions of access

The users of the Federal Administration Information Network are chiefly members of the legal entity "federal government" with facilities throughout Germany. Either the Federal Administration Network or the Berlin-Bonn Information Network serve as points of access. Other networks of the federal administration will use the Federal Administration Network in order to enable their users to access the Federal Administration Information Network in this way. The operators of the sub-networks will continue for the time being to operate the relevant technical connection basis of the user.

In technical terms, the Federal Administration Information Network constitutes a self-enclosed communication network above the level of the federal administration's IP networks which is exclusively open to authorised users. A line encryption device – a so-called SINA box – approved by the German Federal Office for Information Security (BSI) is required at the user end (location of a public agency) as a precondition for implementing the Federal Administration Information Network. A central point of access to the Federal Administration Information Network will be established for users of the Berlin-Bonn Information Network who are connected to the IP backbone.

A.6.4 Features

The features covered by the skeleton agreement on the Federal Administration Network include an IP-based, non-public communication network of the federal administration to be used for largely unrestricted communications.

The services are always requested by the relevant user directly from the provider.

The basic services of the SC IVBV and the IVBB information services in the IVBV are centrally made available to the IVBV users. Furthermore, individual services of the

SC IVBV can be agreed to in the form of individual consultancy and operative services for BVN users which are directly settled with the SC IVBV.

Technical parameters of the Federal Administration Network (BVN):

a. Connection to the BVN via network terminal devices with an Ethernet port for access to the BVN, as well as another optional Ethernet port for transparent access to the Internet
b. BVN connection bandwidths of 128 kbps to 3x155 mbps in three service variants (including, for example, a high-availability connection with two-way routing) and further optional parameters (including, for example, four "quality of service" classes)
c. Transparent, individual Internet access with connection bandwidths of 128 kbps to 1x155 mbps in three service variants
d. Secured, central Internet access as an optional service at the user connection
e. Access to the BVN via dial-up and mobile telephone networks with user-related billing and authentication of mobile users

The following basic services in the Federal Administration Network (BVN) are performed by the SC IVBV.

a. Monitoring the rendering of services by the provider
b. Reporting on the services performed to BVN users
c. Co-ordination with operators of other public-agency networks
d. Management (personalisation and administration) of the encryption devices (SINA boxes) for access to the IVBV intranet
e. Operation of central components of the IVBV (DNS, e-mail)
f. Exchange of e-mails between IVBB and IVBV users via secure infrastructures

Information services made available from within the IVBB in the IVBV, i.e.:

a. Central services of the IVBB, such as directory and administration PKI
b. Database applications, such as EU document server, Central Aliens' Register (AZR), Legal Information System for the Public Administration (JURIS)
c. Web offers in the IVBB for the federal administration provided in an extranet area of the IVBB for the IVBV

Every IVBV user can also offer information services in the IBVB.

A.6.5 Business cases

The Federal Administration Information Network (IVBV) is the network of providers of information and communication services of the federal administration, and is hence without an alternative as an intranet. Two business cases are of special interest in this context.

Access to information offered by the IVBB

Public agencies which are not supreme federal authorities and which are hence not VBB users wish to access services and information which the IVBB offers to the federal administration.

Access is only possible if the required protection measures – for example, use of a line encryption devices as a means of securing communication – are taken and if the IVBB services was made available on the IVBB extranet with the appropriate access rights. Access hence takes place via the user connection to the IVBV to the IVBB extranet.

The resolution of the name of the information server requires the central DNS in the IVBV. As a precondition at the user end, the configuration of the name resolution must be configured accordingly in the user's local network.

Providing information services for the federal administration in a secure environment (G2G)

A public agency forms part of a process chain of a project of the BundOnline 2005 initiative. The public agency uses central components in order to make its processes available to other public agencies. As a provider of information and services, it requires a secure environment of communication and information services for its own operational purposes.

To this effect, the BVN offers the public agency high-availability access to the IVBV. The IVBV enables secure communication with other partners within the federal administration.

The public agency as an IVBV user makes its information available to other public agencies in the IVBV by providing an information server at the IVBV user connection and enabling the name of the information server in the central DNS of the IVBV.

A.7 The directory service as an infrastructure component

A.7.1 Introduction

The "directory service" infrastructure component provides a directory which is based on the X.500 standard via the Berlin-Bonn Information Network (IVBB). Agency-spanning address information, telephone numbers, addresses, e-mail addresses, etc. are made available to the users connected to the IVBB, typically public agencies. This service is designed to facilitate communication between public agencies.

The central directory service in the IVBB contains information concerning users and their staff. IVBB users can access the directory services using web browsers and LDAP-v2/v3 clients. The directory service offers public agency staff the advantage that up-to-dateness of the data is guaranteed without staff having to carry out time-consuming updates.

The directory service is available on the IVBB intranet and on the Internet. Contents of the X.500 directory are mirrored from the intranet into the Internet either completely or in adapted form. It is left to the users to decide to what extent the data is mirrored to the Internet. At present, just around three percent of the IVBB's data is also available on the Internet. The IVBB currently contains 48,000 entries and 600 certificates.

Contact partner for organizational matters	Ms Sabine Richter it2@bmi.bund.de Bundesministerium des Innern 10559 Berlin Tel. +49 1888 681-2763 Fax +49 1888 10 681-2763
Contact partners for technical matters	Mr Wilfried Kister referati12@bsi.bund.de Bundesamt für Sicherheit in der Informationstechnik 53133 Berlin Tel. +49 1888 9582-366 Fax +49 1888 9582-90-366
Availability of the infrastructure component	Already available in the IVBB, planned for the IVBV after its setting into operation (presumably in 2004)
Web address for information concerning the infrastructure component	http://www.kbst.bund.de/saga-x500

A.7.2 Features

Several options exist for making data available in the directory service.

a. Users with a directory system of their own can take part in the distributed X.500 directory (used here as a synonym for directory service). How and in what form the servers communicate must be decided from case to case.
b. If the user does not have access to a directory system of his own, a data interface is implemented via which data can be imported into the central X.500 directory.

The directory service on the intranet and on the Internet is operated by the company T-Systems. T-Systems is to administer the integration of distributed – shadow or distributed – directories at the user end, and is responsible for importing data via the file interface as well as for schema modifications and amendments.

The data model in the X.500 directory features a hierarchical structure. The topmost node that can be administered is c=de, o=bund, with c=de representing country=

Germany and o=bund meaning organization=federal government. Data administration is only possible below this node, i.e. the "administrative point".

The objects supported in the directory service are enumerated below.

a. Public agencies – being the supreme federal authorities and other agencies (ministries, organizations). They are stored as "organizationalUnit" in the directory.
b. Sites and locations – these are stored as "locality" in the directory.
c. Individuals – these are stored as "inetOrgPerson" in the directory. At present, however, many departments (that have a mail address) are also stored as individuals due to the formats in which the data is provided.
d. Rooms – these are stored as "room" in the directory. Video conference and meeting rooms can be distinguished.
e. Departments (or units) – are stored as "ivbbDepartment" in the directory.
f. Certification Authorities (CAs) – are stored as "applicationProcess" in the directory.

Although the structure of the X.500 schemas is largely orientated towards the X.509, X.520, X.521 (1997, 2000); X.402 (1988); RFC 1274 (COSINE / Paradise); RFC 2256 (X.500 Schema for LDAP v3); RFC 2798 (inetOrgPerson) standards, numerous additions – especially attributes – have been made which can be checked at the web address stated above.

A.7.3 Business cases

The use of the "directory service" infrastructure component is **mandatory** in all business cases.

Standard application
A user at a public agency needs the e-mail data of a recipient at the user's agency or at another public agency. The application, for example, Outlook, accesses the e-mail data from the X.500 directory in order to offer possible addresses.

As a precondition for this, the individual's name must be stored in the X.500 directory and the data must be complete (central synchronisation of the X.500 data).

Basic application

The public agency makes its address data available to other public agencies and users outside public agencies. Distributed data updating and central distribution are supported.

A.7.4 Interfaces

Section A.7.2 "Features" on page 144 lists standards and formats for creating, editing and exporting data in and from the X.500 directory.

A.7.5 Roadmap

The directory service is already available in the Berlin-Bonn Information Network (IVBB).

Presumably in 2004	• Available in the Federal Administration Information Network (IVBV)

A.8 "One for all" services

A.8.1 Introduction

Whilst the ministries and the pertinent public agencies are responsible for completely different areas of public life – from finance to defence and justice to consumer protection – the underlying processes implementing the different services are often very similar.

If the process of rendering a service is separated from the specific tasks to be performed and the information processed for this purpose, significant synergy potentials arise with regard to cost and effort when it comes to implementing the required IT support for the process to be brought online.

The subsidy process, for example, is more or less the same in every ministry, irrespective of the purpose of the subsidies granted. The subsidy application is followed by its examination, approval, by the earmarking of funds, monitoring and its final evaluation.

In order to make use of these synergy potentials, the cabinet decided in December 2002 to introduce so-called "one for all" services (in short: OFA services).

These "OFA" services – much like the subsidy example – are rendered by several public agencies in the same or a similar manner. They hence cover the identical IT support requirements of several public agencies for the business processes in question.

OFA services are developed and, if applicable, centrally operated by a ministry or by a public agency. The software and system configuration should be such that they can be adapted to changing user requirements with the smallest effort and at the lowest cost possible. Both the concept and the development process must hence focus strongly on a generic and configurable system and software design.

In a first step, a total of 15 BundOnline services were identified as OFA services. Within the framework of regular ministry meetings by members of the initiative, five of these services were identified as particularly high-priority issues in terms of their benefits for the ministries. They belong to the more complex, transaction-orientated service types.

OFA service	Service type
The "profi" project subsidy system	Service type 6: Subsidy programmes
eTendering	Service type 7: Procurement programmes
Electronic legal transactions	Service type 5: General application procedures
Recruitment	Service type 9: Other services
Preparation of political and regulatory decisions	Service type 3: Preparation of political decisions

In order to enable the ministries and public agencies which use these services to contribute their own demands and requirements for OFA services, a user advisory board is made up of representatives from interested public agencies. The members of this advisory board are to ensure that the various requirements are compiled at an early stage and considered during the concept and implementation phases.

A.8.2 The "profi Online" project subsidy information system

One important function of the federal administration is to promote and subsidise all kinds of plans, programmes and projects. The Federal Ministry of Education and Research (BMBF) alone is spending more than two billion euro on project subsidy programmes in 2003. This relevance is also reflected in the BundOnline initiative. Around ten percent of the BundOnline services are related to subsidy programmes by federal ministries. Even before the launch of BundOnline, the Federal Ministry of Education and Research had developed the "profi" project subsidy system and subsequently upgraded this system in co-operation with project sponsors and other ministries, such as the Federal Ministry of Economics and Labour. Profi offers IT support for subsidy programmes, from the invitation to tender via the application process right through to administrative handling. The kernel of profi consists of a jointly used, uniform and central database from which authorised users can retrieve data for further, decentralised processing and editing.

Contact partner for organizational matters	Dr Peter Mecking pl.profi@bmbf.bund.de Bundesministerium für Bildung und Forschung Heinemannstr. 2 53175 Bonn Tel. +49 1888 57-3815 Fax +49 1888 57-83815

Contact partners for technical matters	Mr Michael Noack profi@dlr.de Deutsches Zentrum für Luft- und Raumfahrt Linder Höhe 51147 Köln Tel. +49 2203 601-3613 Fax +49 2203 601-2965
Availability of the kernel system	In productive use since 2000
Availability of profi-online	May 2004
Web address for information concerning the OFA service	http://www.kp.dlr.de/profi/

The use of profi offers a range of advantages, including, for example, better data quality and more up-to-date information, as well as more effective and more speedy procedures. profi, for example, replaces the conventional procedure of manual orders for payment with an automated procedure with multiple payment orders. In this way, the Federal Cash Office also benefits from the electronic interchange of payment-relevant data.

By 2002, four federal ministries were using profi. In 2003 it was introduced at the Federal Ministry for the Environment, Nature Conservation and Nuclear Safety. Further ministries and public agencies are currently preparing to use profi. At present, 1,800 users at 28 locations are currently working on more than 19,000 projects and programmes.

Profi is currently being upgraded by adding further components. As a means of ensuring secure communications with external users, the "profi-online" component is implemented on the basis of Governikus in analogy to the data security basic component. Start of productive operations is scheduled for May 2004. The multi client solution of profi is to be implemented by July 2005. A target concept for integrating a workflow and document management system was developed in 2003 for filing and managing documents in the subsidy area. The implementation of this link is scheduled to be completed by December 2005.

A.8.3 eTendering

Every year, the 600 or so awarding offices of the federal government buy products and services with a value of around euro 63 billion. In view of this large volume, electronic awarding procedures can yield significant savings both in terms of process costs and in terms of the prices for the goods and services to be bought. Besides the public sector, private business can also benefit from a uniform, electronic procurement solution.

Contact partner	Mr Jörg Funk joerg.funk@bescha.bund.de Beschaffungsamt des Bundesministeriums des Innern Postfach 30015 53181 Bonn Tel. +49 228 610-1202 Fax +49 228 610-1610
Availability	Since May 2002
Web address for information concerning the OFA service	http://www.bescha.bund.de/egovernment/

Within the framework of the "Öffentlicher Eink@uf Online" (Public Procurement Online), the Procurement Office of the Federal Ministry of the Interior has therefore implemented an electronic awarding platform, the so-called "e-Vergabe" (eTendering) platform. Partners in the development of the platform were the Federal Ministry of Defence as well as the Federal Ministry of Transport, Building and Housing, with the Federal Ministry of Economics and Labour sponsoring the project. In May 2002, the first fully electronic procurement process was transacted via the system.

Figure A-6: Homepage of the eTendering OFA service

eTendering enables the electronic handling of procurement processes via the Internet. Communications between the awarding office and prospective suppliers are conducted in a legally binding manner without the need to change from one medium to another. These communications range from the publishing of the invitation to tender via the distribution of the contracting documents, the electronic submission of offers right through to the awarding of the job. Smartcards are used to provide documents with the qualified electronic signature prior to encrypted transmission.

The system features a multi client solution and incorporates all the relevant contracting rules for awarding contracts. eTendering is currently used by several authorities, such as the Procurement Office of the Federal Ministry of the Interior, the Federal Office for Building and Regional Planning, as well as the Federal Office of Defence Technology and Procurement, as well as federal-state and communal authorities, such as the Office for Equipment and Procurement of the Police in Mecklenburg-West Pomerania. The platform is technically operated by the Wiesbaden-based Federal Statistical Office on behalf of the Procurement Office of the Federal Ministry of the Interior. It is available on the Internet at: http://www.evergabe-online.de/

The federal administration is determined to improve the organization of public procurement on the basis of new information technologies. At the heart of this effort is a seven-point programme with the following statements relevant for eTendering.

a. The eTendering service is offered to all public institutions for use. By the end of 2005, all federal authorities will successively introduce eTendering.
b. Consistent (electronic) process chains with well-defined interfaces are developed between buyers and suppliers.

A business model shows how the further development of the system can be ensured (including, for example, adaptation to new legislation or technical innovation) and how a fair and equitable distribution of costs to users can be achieved.

A.8.4 Electronic legal communications

The "electronic legal communications" service covers the electronic transmission of litigation-relevant statements, including exhibits, by parties to courts and vice versa[130]. The introduction of electronic legal communications is particularly effective for standardised and highly repetitive procedures.

Contact partner	Mr Bernd Tödte post@dpma.de Deutsches Patent- und Markenamt Zweibrückenstr. 12 80331 München

[130] The exchange of documents within a public agency or court does not form part of "Electronic legal communications" or of the OFA service.

	Tel. +49 89 2195-3927 Fax +49 89 2195-2221
Availability of the first stage	1st quarter 2004
Availability of the second stage	2nd quarter 2005

Electronic legal communications are based on the electronic patent application procedure of the German Patent Office. The service has parallels with electronic awarding procedures (service type 5) which account for around one fifth of all services. The development of this application to an OFA service will enable the implementation of a host of registration and application procedures which involve requirements in terms of law conformity, data protection and privacy as well as integration into the special procedures of specific service providers.

Electronic patent registration is already implemented, and will be available to the general public by the end of 2003. Plans also exist to harmonise this service with the corresponding procedure of the European Patents Office by the end of 2003. The user advisory board offers its services to further ministries and public agencies when it comes to identifying and co-ordinating their requirements for electronic legal communications.

Electronic legal communications will be implemented in two stages within the BundOnline framework. The first stage, i.e. "harmonisation of patent application procedures of the German Patent Office and the European Patents Office" as well as "pilot migration to the virtual post office basic component", is scheduled to be available during the first quarter of 2004. The second stage, i.e. "addition of further industrial property rights", will be completed during the second quarter of 2005.

A.8.5 Recruitment

The Federal Ministry of Defence (BMVg) offers its "recruitment" OFA service with contents and functionalities which can also be used by other ministries for their recruitment demands.

Contact partner	Mr Peter Pörsch peter1poersch@bmvg.bund400.de Bundesministerium der Verteidigung Fontainengraben 150 53123 Bonn Tel. +49 1888 24-3642 Fax +49 228 12-6429
Availability of the first stage	End of 2003
Availability of the second stage	2004

The recruitment service offers comprehensive and up-to-date information on job descriptions and career opportunities in the ministry. In this way, the Federal Armed Forces present themselves as an employer with career information, vacancies and hiring procedures. The information on offer is tuned to the situation of job-seekers and is broken down in terms of educational and vocational qualifications as well as specialist departments. It hence forms an efficient marketing tool for customer-orientated, state-of-the-art jobs in the federal administration.

The recruitment area offers job-seekers the latest vacancies in the ministry's public agencies. This can take the form of concrete job advertisements or more general offers related to the recruitment of young talent. Applications can be filed online. The functionality is such that the data from the applicant's online application is entered into the public agency's back-end system. This helps reduce processing time to the benefit of both public agencies and applicants alike.

Ministries using the OFA service can adapt the information supplied by the Federal Ministry of Defence to their specific demands and advertise their vacancies in a uniform structure. This can then form the basis for a joint "career portal" of the federal administration at www.bund.de with links to the offers by ministries and public agencies.

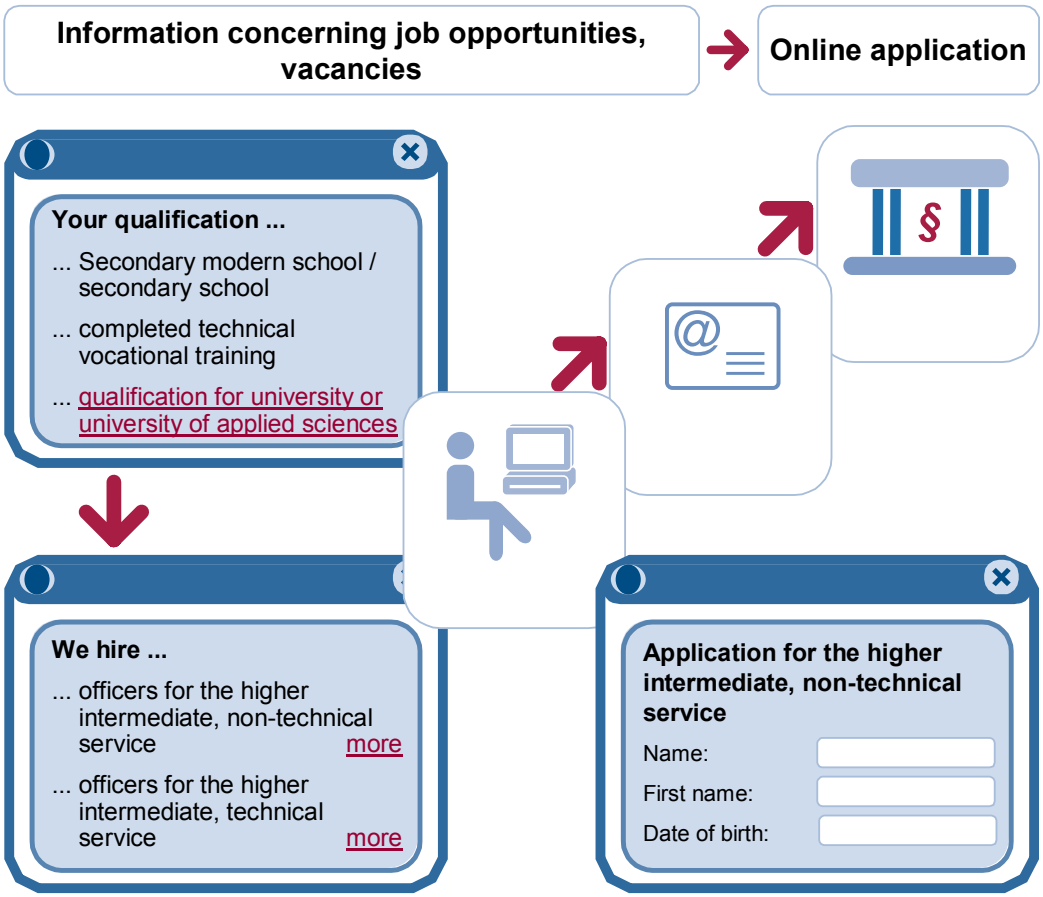


Figure A-7: The "recruitment" OFA service

The first development stage of the recruitment service which will be completed by the end of 2003 includes the basis structure for the target-group orientated information offering (initially for military personnel) as well as the online application. In 2004, information and job offerings for civilian personnel in the technical and non-technical service will be added. The use of the "data security" and "form server" basic components is also planned.

A.8.6 Preparation of political and regulatory decisions

The "preparation of political and regulatory decisions" OFA service relates to government bills. The aim is to use a single medium to enable the exchange of documents for the preparation and adoption of bills and regulations between the ministries involved and the Federal Chancellery as well as the Bundesrat and the Bundestag. The system is to be used by all the parties involved in order to document all voting, co-ordinating and decision-making processes and to exchange the bills. At the same time, the data format is designed to speed up the printing process.

Contact partner	Dr Rainer Mantz ref-114@bk.bund.de Bundeskanzleramt Willy-Brandt Str. 1 10557 Berlin
Availability of the OFA service	2004

Sub-projects of this service are pursued by the Federal Chancellery (as the leading unit) as well as the Federal Ministry of Health and Social Security (BMGS) and the Federal Ministry of Economics and Labour (BMWA).

Guidelines form part of the procedure in order to support staff in the preparation of drafts, so that the examination of the legal basis and situation can be directly integrated into the system. This saves time and costs. Parliamentary publications and laws that have been enacted can be produced and published faster in this way.

The center of excellence for workflow management, processes and organization has started identifying and describing the actual processes. An easy-to-implement preliminary solution will go online before the end of 2003 in order to meet the Bundestag's requirements for electronic supplies. The Federal Ministry of Economics and Labour (BMWA) will make the so-called "planning online" service also available in 2003.

The final solution of the OFA service "preparation of political and regulatory decisions" as well as the majority of the components in other ministries involved will be available in 2004. Prior to these functions going online, interaction of the individual components in the ministries and smooth data transmission will have to be tested.

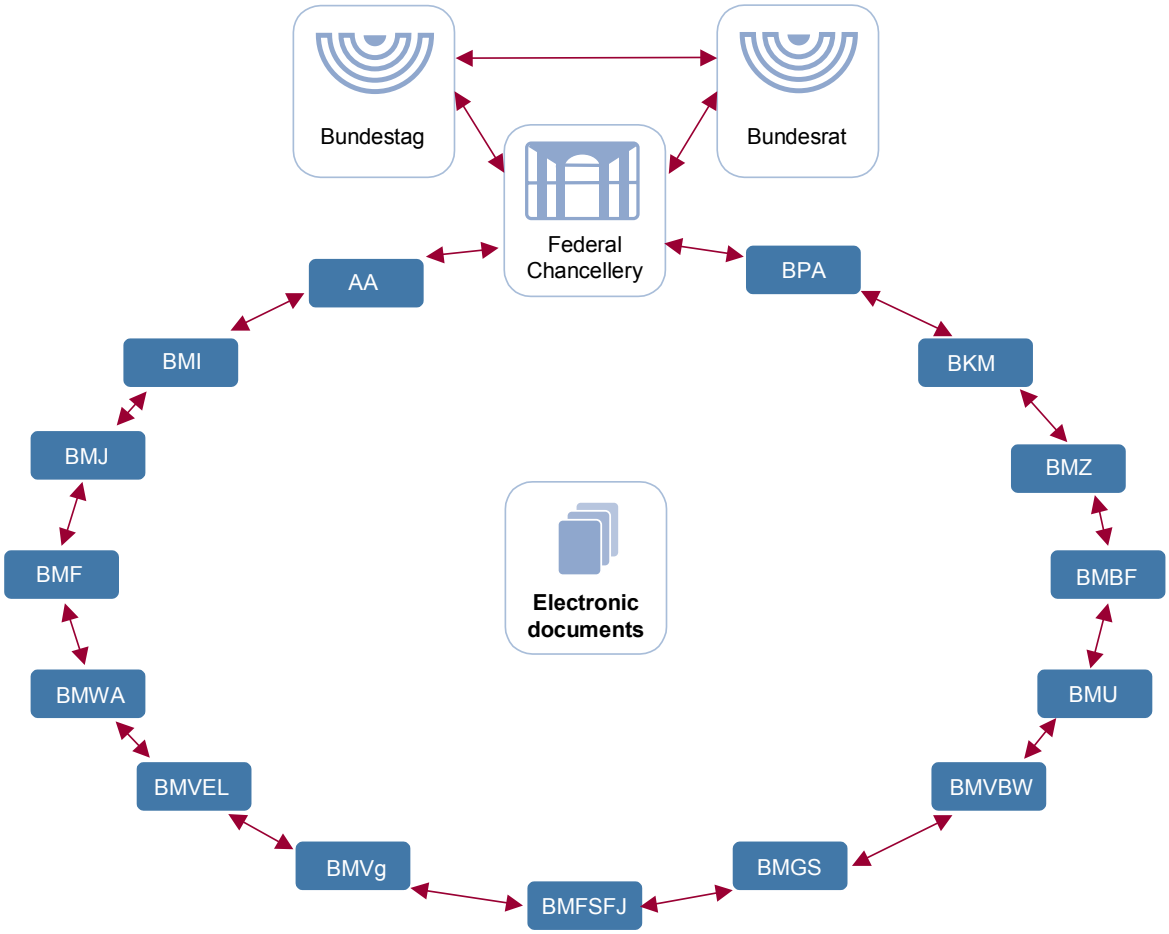


Figure A-8: The electronic exchange of government bills

A.9 Competence centers

Four competence centers were set up in order to support the BundOnline 2005 e-government initiative. The main task of the competence centers is to provide know-how for the de-centralised implementation of the online services. This includes, in particular, advice and consultancy services when it comes to implementing basic components and online services.

A.9.1 The payment platform competence center

The "payment platform" competence center offers methods and concepts for the implementation and operation of e-payment applications throughout the entire federal administration. It additionally compiles technical expertise for linking e-shops and other processes to the central payment platform and adapts these processes accordingly. The competence center offers presentation and advice related to e-payment offerings of the federal government and supports public agencies in technical matters with regard to the integration of the payment platform. The competence center also monitors the markets with a view to further payment methods, such as micropayments or mobile payments. The competence center has been available since 31 July 2003.

Contact partner	Mr Volker Walgenbach ePayment@bff.bund.de Bundesamt für Finanzen Friedhofstrasse 1 53225 Bonn Tel. +49 228 406-2905 Fax +49 228 406-2241

A.9.2 The data security competence center

The "data security" competence center at the German Federal Office for Information Security (BSI) advises public agencies in matters related to the security of e-government applications and the use of the digital signature. The transmission of sensitive data via the Internet calls for trustworthy infrastructures, re-organization of administrative processes, and implementing suitable security solutions for existing applications at public agencies. This enables smooth, legally binding and confidential online communications between external users and the federal administration and also ensures secure communications between public agencies.

Contact partner	Mr Kurt Klinner kurt.klinner@bsi.bund.de Bundesamt für Sicherheit in der Informationstechnik Godesberger Allee 185-189 53175 Bonn Tel. +49 1888 9582-132 Fax +49 1888 9582-90132

A.9.3 The content management system competence center

The "content management system" (CMS) competence center advises public agencies of the federal administration in implementation matters in conjunction with the use of the CMS basic component for the online offering of services. The competence center also supports the development of concepts for the demand-orientated implementation of the CMS basic component and, following its completion, will be available as a contact partner for optimisation suggestions and case-specific demand adaptation.

Contact partner	Mr Claus Hackethal claus.hackethal@bva.bund.de Bundesverwaltungsamt 50728 Köln Tel. +49 1888 358-1549 Fax +49 1888 358-3899

A.9.4 The workflow management, processes and organization competence center

The implementation of e-government solutions calls for prior optimisation of the relevant business processes as a mandatory organizational precondition for exploiting actual efficiency gains. This means that an IT solution should be based on optimised target processes rather than on conventional actual processes.

The "workflow management, processes and organization" competence center (WMPO CC) at the Federal Office of Administration offers support during business process optimisation projects as well as product-neutral consultancy services for the introduction of workflow management systems.

Contact partner	Mr Elias Paraskewopoulos elias.paraskewopoulos@bva.bund.de Bundesverwaltungsamt 50728 Köln Tel. +49 1888 358-1546 Fax +49 1888 358-2801

Target

The top priority of the competence center is to support federal authorities in the economically efficient implementation of BundOnline 2005 services under their own responsibility. The competence center is to offer technical and methodological support for adapting organization and processes as well as administrative procedures. The aim is to generate the following benefits for public agencies.

a. Cost-neutral, customer-orientated and professional support for federal authorities
b. Standardised procedure for the provision of online services
c. Creation of sustainable competence within public agencies by coaching project managers
d. Development of efficient business processes and targeted provision of information
e. Co-ordinated, technical solutions for workflows and optimised business processes

Services

The competence center offers the following services in order to achieve the above-stated targets.

a. Support for the preparation of contracts for process analyses and rough concepts for the introduction of workflow management systems
b. Support during the analysis and reorganization of particularly complex processes
c. Support during the introduction of workflow management systems
d. Development of sample processes on the basis of selected services and basic components
e. Project-specific information events and workshops

f. Development of a toolbox for the provision of methods and concepts for process analysis and optimisation as well as for the introduction of an IT-based workflow management system
g. Compiling practical examples on the basis of selected consulting projects

The consultancy approach

A consultancy project includes the following optional phases.

a. During the analysis phase, public agencies are supported in exploring optimisation potentials.
b. During the concept development phase, the identification of functional requirements for the technical components is supported on the basis of the process model.
c. During the implementation phase, the public agency is offered support with regard to the independent implementation and testing of the new processes.
d. If necessary, the WMPO CC offers coaching services while the systems are being set into operation during the launching phase.

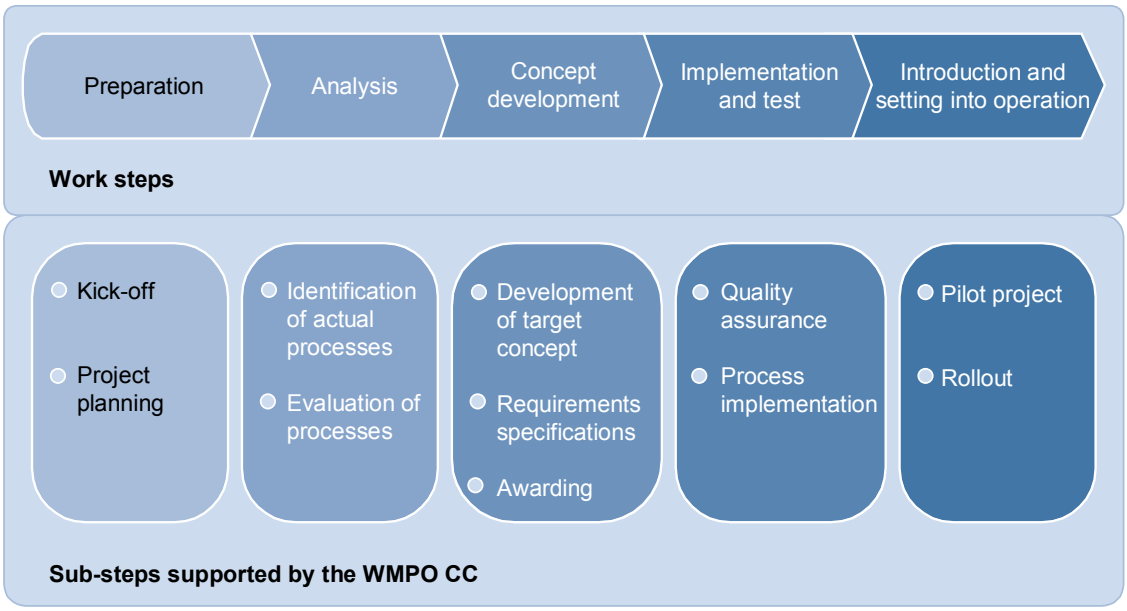


Figure A-9: Phases of consultancy projects

Appendix B Example of an online service with basic components

This appendix discusses an example of how basic components can be integrated into the processes of an online service. The example[131] relates to a special method which is based on a special database. All the parties involved in the process at the administration end have access to this database. The applicants in this case are companies which trigger the application process often enough to be entitled to obtain signature card readers. The companies must pay a fee when the application is approved. The application procedure ends when the receipt of payment is recorded in the special database. The activities applied for are carried out outside the Internet, however, with administrative staff using the special database.

All the basic components are used to support this application procedure. Four of them are directly integrated into the processes, with the fifth one, i.e. the **portal basic component** offering access to the online service. The **CMS basic component** implements the web interface of the online service with explanations, background information and statistics. Furthermore, the CMS also stores applicant data.

The **form server** basic component generates the application form and supports the applicant when completing the form. User data stored by the CMS basic component is used to enter default data in the form. The **data security basic component** ("virtual post office") is used for the secure transmission of this personal data, for signing the completed form and for the secure transmission of the form data. Libraries of the virtual post office are also used to ensure secure communications when receipt confirmations and cost statements are sent to users by e-mail.

The **e-payment basic component** is used to generate a debit entry at the Federal Cash Office when the application is approved. The applicant pays the bill by bank transfer. Information concerning debit entries already settled can be retrieved from the e-payment system.

Figure B-1 on page 160 shows all the process steps.

1. User data available in the special database is sent to the CMS basic component, so that applicants do not have to re-enter their complete personal data after logging in each time they submit an application.
2. The applicant logs in to the website of the application process, with the digital signature being used for authentication.
3. Transmission of the login data from the applicant's web client to the web server of the application process (use of the "data security" basic component for verifying the signature)
4. Transmission of the user identification to the CMS

[131] The process examples were designed on the basis of an application procedure for the import and export of protected plant and animal species.

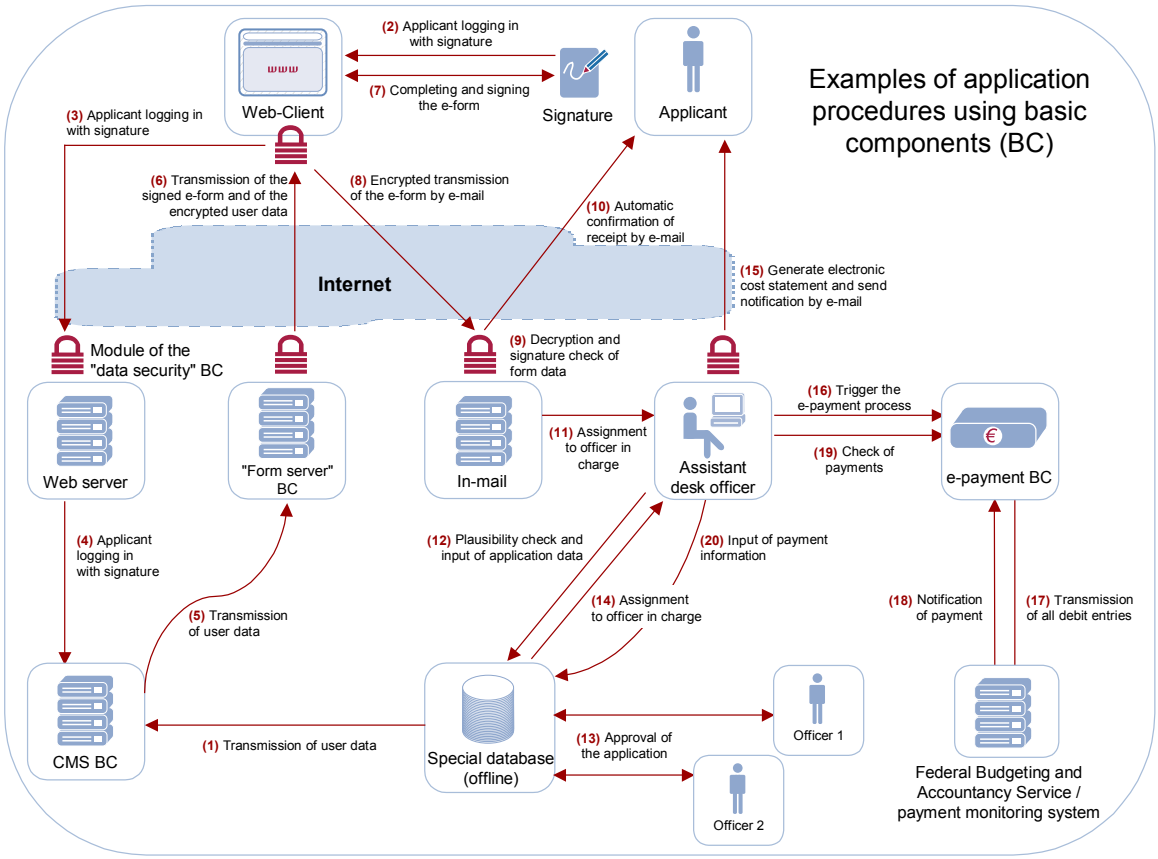


Figure B-1: Use of several basic components for an online service

5. Activation of the "form server" basic component by the CMS; transmission of all the user data necessary to complete certain boxes of the form in advance
6. Transmission of the e-form with encrypted user data in order to pre-complete individual boxes (use of the "data security" basic component or HTTPS for encryption)
7. The user completes the application form and adds scanned data as file attachments to the form; the completed form, including attachments, is digitally signed by the user.
8. Encrypted transmission of the e-form to the "in-mail" function of the application process (use of the "data security" basic component by the software of the form server)
9. Decryption of the form data and verification of the signature (use of the "data security" basic component)
10. Transmission of automatic confirmation of receipt of the form data to the applicant by e-mail; signing of the e-mail by the "data security" basic component; encryption, if necessary
11. Assigning the case to an officer
12. Checking the plausibility of the user information, and entering the application into the special database by the officer
13. Approval of the application by two officers via access to the special database

14. Further processing of the case by the officer
15. The officer generates an electronic cost statement and sends it to the applicant; signing and encryption of the e-mail by the "data security" basic component
16. The officer uses the appropriate basic component in order to trigger the e-payment procedure.
17. Once a day, the debit entries are sent to the payment monitoring system (ZÜV) of the Federal Budgeting and Accountancy Service (HKR).
18. As soon as the applicant has paid the bill, the payment monitoring system notifies the e-payment server thereof.
19. The officer retrieves the latest payment information from the e-payment system.
20. Payments are recorded in the special database whereupon the application process is completed.

If an application is rejected, the procedure would end with step 15 by sending a corresponding cost statement to the applicant.

Appendix C Templates for a SAGA conformity declaration

C.1 Conformity declaration

With regard to the application: _____

Name of the application, reference to performance specifications / features

the following components were identified which the applicant declares to be in conformity with SAGA according to SAGA 2.0 as evidenced by the check-lists attached hereto.

Self-developed components

Self-developed components of an application are created by the supplier on the basis of the customer's requirements and are hence modules of the applications which are specifically adapted to the purpose of use and the system architecture.

The following self-developed components were identified.

1. _____
2. _____
3. _____
4. _____

Product components

Product components of an e-government application are completed software modules which are solely installed and configured by the supplier.

The following product components were identified:

1. _____
2. _____
3. _____
4. _____

_____	_____
Customer	Supplier
_____	_____
Represented by	Represented by
_____	_____
Place, date, signature	Place, date, signature

C.2 Check-list for self-developed components

_____

Name of the component, brief description

_____

Name of the pertinent application

In order to ensure SAGA conformity of the above-stated components, the following criteria and the related standards specified in SAGA 2.0 must be examined with a view to their relevance for the application:

a. Process models
b. Data models
c. Technical standards and architectures
d. Use of existing basic components

Process modelling

The modelling of processes necessary for the creation of software components is described in chapter 8.

Process modelling (refer to section 8.1)

Relevant conformity aspect	Standard	SAGA conformity? Yes / no

Data modelling

The modelling of data necessary for the creation of software components is described in chapter 8.

Data modelling (refer to section 8.2)

Relevant conformity aspect	Standard	SAGA conformity? Yes / no

Technical standards and architectures

The technical standards and architectures relevant for creating a component are based on the standards for the IT architecture and the standards for data security described in chapters 8 and 9.

Furthermore, chapters 5, 6 and 7 also describe certain procedures and concepts which can be important for implementing a component. Concrete details of such requirements must be specified by the customer outside the following tables, depending on the specific project which is the subject matter of the invitation to tender.

Application architecture (refer to section 8.3)

Relevant conformity aspect	Standard	SAGA conformity? Yes / no

Client (refer to section 8.4)

Relevant conformity aspect	Standard	SAGA conformity? Yes / no

Presentation (refer to section 8.5)

Relevant conformity aspect	Standard	SAGA conformity? Yes / no

Communication (refer to section 8.6)

Relevant conformity aspect	Standard	SAGA conformity? Yes / no

Connection to the back-end (refer to section 8.7)

Relevant conformity aspect	Standard	SAGA conformity? Yes / no

Data security (refer to chapter 9)

Relevant conformity aspect	Standard	SAGA conformity? Yes / no

Basic components

When implementing components, it must be determined whether the required functions can be performed – in part or in full – by one of the basic or infrastructure components described in Appendix A of the SAGA document.

Use of basic modules (refer to Appendix A)

Basic module	Relevant functions of the basic module	Use of basic module planned? Yes / no
Payment platform		
Data security		
Portal		
Form server		
CMS		
IVBV		
Directory service		

C.3 Check-list for product components

_____

Name of the component, brief description

_____

Name of the pertinent application

In order to ensure SAGA conformity of the above-stated product component, the technical standards described in SAGA 2.0 must be examined with a view to their relevance for the use of the product.

The focus of the examination is on interoperability. The SAGA conformity of a product is hence evaluated on the basis of user interfaces, data exchange formats, communication interfaces and APIs of this solution.

Technical standards

The technical standards relevant for the interfaces and APIs of a product are based on the standards for the IT architecture and the standards for data security described in chapters 8 and 9.

Client (refer to section 8.4)

Relevant conformity aspect	Standard	SAGA conformity? Yes / no

Presentation (refer to section 8.5)

Relevant conformity aspect	Standard	SAGA conformity? Yes / no

Communication (refer to section 8.6)

Relevant conformity aspect	Standard	SAGA conformity? Yes / no

Connection to the back-end (refer to section 8.7)

Relevant conformity aspect	Standard	SAGA conformity? Yes / no

Data security (refer to chapter 9)

Relevant conformity aspect	Standard	SAGA conformity? Yes / no

Appendix D References

[Adnovum]
Adnovum Informatik AG: *Guichet Virtuel der Bundeskanzlei. Spezifikation der Software-Architektur*, online publication, 2002
http://www.admin.ch/ch/d/egov/gv/themen/architektur/architektur.html
http://www.admin.ch/ch/d/egov/gv/themen/architektur/software_architektur_1.0.pdf

[APEC]
National Office for the Information Economy / CSIRO: *APEC e-Business: What do Users need?*, 2002
http://pandora.nla.gov.au/tep/25067
http://www.dms.csiro.au/Reports/APEC_E-commerce.pdf

[BOL]
Bundesministerium des Innern (editor): *Umsetzungsplan für die eGovernment-Initiative BundOnline 2005*, Paderborn 2001
http://www.bund.de/Anlage66411/Umsetzungsplan.pdf

[e-GIF]
Office of the e-Envoy: *e-Government Interoperability Framework Version 5.0*, 2003
http://www.govtalk.gov.uk/schemasstandards/egif.asp
http://www.govtalk.gov.uk/documents/e-gif_v5_part1_2003-04-25.pdf
http://www.govtalk.gov.uk/documents/e-gif_v5_part2_2003-04-25.pdf

[GOSIP]
National Institute of Standards and Technology (NIST): *U. S. Government Open Systems Interconnection Profile (GOSIP)*, Version 2.0, 1990
http://www.i-n-t.de/ccie/Artikel/Gosip.pdf

[IDA]
European Commission: *Interchange of Data between Administrations*, 2003
http://europa.eu.int/ISPO/ida/

[ISO 1996]
ISO/IEC 10746-3: *Information technology – Open Distributed Processing – Reference Model: Architecture*, Geneva 1996

[ITG 2000]
Informationstechnische Gesellschaft (ITG) im VDE: *Electronic Government als Schlüssel der Modernisierung von Staat und Verwaltung*. Ein Memorandum des Fachausschusses für Verwaltungsinformatik der Gesellschaft für Informatik e.V. (GI) und des Fachbereichs 1 der Informationstechnischen Gesellschaft (ITG) im

Verband der Elektrotechnik, Elektronik und Informationstechnik (VDE), Bonn / Frankfurt 2000 [Memorandum by the expert committee on computer science in administrations of Gesellschaft für Informatik e.V. (GI) and specialist unit 1 of Informationstechnische Gesellschaft (ITG) in the Association for Electrical, Electronic & Information Technologies (VDE)]
http://www.mediakomm.net/documents/memorandum.pdf

[Kudraß 1999]
Kudraß, Thomas: Describing Architectures Using RM-ODP, online publication, 1999
http://www.imn.htwk-leipzig.de/~kudrass/Publikationen/OOPSLA99.pdf

[Lenk et al. 2000]
Lenk, Klaus / Klee-Kruse, Gudrun: *Multifunktionale Serviceläden*, Berlin 2000

[Lenk 2001]
Lenk, Klaus: *Über Electronic Government hinaus Verwaltungspolitik mit neuen Konturen*, Vortrag auf der 4. Fachtagung Verwaltungsinformatik in der Fachhochschule des Bundes für öffentliche Verwaltung am 5. September 2001 [Paper on the 4th specialist conference on computer science in administrations at Fachhochschule des Bundes für öffentliche Verwaltung on 5 September 2001]

[Lucke et al. 2000]
Lucke, Jörn von / Reinermann, Heinrich: *Speyerer Definition von Electronic Government*. Ergebnisse des Forschungsprojektes Regieren und Verwalten im Informationszeitalter, online publication, 2000
http://foev.dhv-speyer.de/ruvii/Sp-EGov.pdf

[New Zealand]
E-government Unit, State Services Commission, New Zealand: *New Zealand E-government Programme Home Page*, 2003
http://www.e-government.govt.nz/

[Schedler et al. 2001]
Schedler, Kuno / Proeller, Isabella: *NPM*, Bern / Stuttgart / Vienna 2001

[Schreiber 2000]
Schreiber, Lutz: *Verwaltung going digit@l. Ausgewählte Rechtsfragen der Online-Verwaltung*, in: Digitale Signaturen, in: Kommunikation & Recht Supplement 2 to Volume 10/2000

[Switzerland]
Bundeskanzlei, Switzerland: *E-Government*, Homepage of the Swiss Federal Government's e-government initiative, 2003
http://www.admin.ch/ch/d/egov/egov/

Appendix E Overview of classified standards

Appendix F Abbreviations

AES	Advanced Encryption Standard
APEC	Asia-Pacific Economic Cooperation
API	Application Programming Interface
B2B	Business to Business
BGG	Law on Equal Opportunities for the Disabled
BITV	Barrier-free Information Technology Ordinance
BMI	Federal Ministry of the Interior
BOL	BundOnline 2005 initiative
BSI	German Federal Office for Information Security
BVA	Federal Office of Administration
BVN	Federal Administration Network
CAP	Content Application Platform
CEN	Comité Européen de Normalisation
CMS	Content Management System
CORBA	Common Object Request Broker Architecture
CRL	Certificate Revocation List
CSS	Cascading Style Sheets Language
CSV	Comma Separated Value
CVC	Card Verification Code
DES	Data Encryption Standard
DIN	Deutsche Industrie-Norm [German Industry Standard]
DNS	Domain Name Services
DSA	Digital Signature Algorithm
DSML	Directory Services Markup Language
DSS	Digital Signature Standard
ECMA	European Computer Manufacturers Association
ECMS	Enterprise Content Management System
ECW	Enhanced Compressed Wavelet
EDI	Electronic Data Interchange
e-GIF	e-Government Interoperability Framework
ERP	Enterprise Resource Planning

EStdIT	Development standards for IT systems in the federal administration
ETSI	European Telecommunications Standards Institute
FTP	File Transfer Protocol
G2B	Government to Business
G2C	Government to Citizen
G2E	Government to Employee
G2G	Government to Government
GI	Gesellschaft für Informatik e.V. [a German association dealing with computer science]
GIF	Graphics Interchange Format
GML	Geography Markup Language
GOSIP	Government Open Systems Interconnection Profile
HKR	Federal Budgeting and Accountancy Service
HMAC	Keyed-Hash Message Authentication Code
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
IDA	Interchange of Data between Administrations
IDEA	International Data Encryption Algorithm
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IIOP	Internet Inter-ORB Protocol
IMAP	Internet Message Access Protocol
IP	Internet Protocol
IT	Information technology
ITG	Informationstechnische Gesellschaft [a computer science association]
ISDN	Integrated Services Digital Network
ISIS	Industrial Signature Interoperability Specification
ISO	International Organization for Standardization
IVBB	Berlin-Bonn Information Network
IVBV	Federal Administration Information Network
J2EE	Java 2 Platform, Enterprise Edition
J2SE	Java 2 Platform, Standard Edition

JAAS	Java Authentication and Authorization Service
JAXP	Java API for XML Parsing
JAXR	Java API for XML Registries
JCE	Java Cryptography Extension
JDBC	Java Database Connectivity
JDO	Java Data Objects
JMS	Java Message Service
JMX	Java Management Extensions
JNDI	Java Naming and Directory Interface
JPEG	Joint Photographic Experts Group
JSP	Java Server Pages
JSSE	Java Secure Socket Extension
JSTL	JSP Standard Tag Library
JTA	Java Transaction API
KBSt	Co-ordinating and Advisory Agency of the Federal Government for Information Technology in the Federal Administration
KoopA ADV	Co-operation Committee for Automatic Data Processing for the Federal-government, Federal-state Government and Municipal Administration Sector
LDAP	Lightweight Directory Access Protocol
MAC	Message Authentication Code
MIME	Multipurpose Internet Mail Extensions
MPEG	Moving Picture Experts Group
MTT	MailTrusT
NAT	Network Address Translation
OASIS	Organization for the Advancement of Structured Information Standards
OCSP	Online Certificate Status Protocol
OFA	One-for-all Services
OGC	Open GIS Consortium
OSCI	Online Services Computer Interface
OSS	Open Source Software
PCA	Policy Certification Authority
PDA	Personal Digital Assistant

PDF	Portable Document Format
PHP	PHP: Hypertext Preprocessor
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PKIX	IETF Working Group "Public-Key Infrastructure (X.509)"
PNG	Portable Network Graphics
POP	Post Office Protocol
RegTP	Regulatory Authority for Telecommunications and Posts
RFC	Request for Comments
RFP	Request for Proposals
RIPEMD	RIPE (RACE Integrity Primitives Evaluation) Message Digest
RMI	Remote Method Invocation
RM-ODP	Reference Model of Open Distributed Processing
RSA	Rivest, Shamir, Adleman Public Key Encryption
SAGA	Standards and Architectures for e-Government Applications
SC	Service Center
SGML	Standard Generalized Markup Language
SHA	Secure Hash Algorithm
SigG	German Signature Act
SigV	Digital Signature Ordinance
SINA	Secure Inter-Network Architecture
S/MIME	Secure Multipurpose Internet Mail Extensions
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SOAP	Simple Object Access Protocol
SSL	Secure Sockets Layer
SVG	Scalable Vector Graphic
TCP/IP	Transmission Control Protocol / Internet Protocol
TIFF	Tagged Image File Format
TLS	Transport Layer Security
UDDI	Universal Description, Discovery and Integration
UDP	User Datagram Protocol

UML	Unified Modeling Language
URL	Uniform Resource Locator
UTF	Unicode Transformation Format
VDE	Association for Electrical, Electronic & Information Technologies
VML	Vector Markup Language
VPN	Virtual Private Network
VPS	Virtual Post Office
W3C	World Wide Web Consortium
WAP	Wireless Application Protocol
WCAG	Web Content Accessibility Guideline
WMPO CC	Competence Center for Workflow Management, Processes and Organization
WSDL	Web Services Description Language
WWW	World Wide Web
XHTML	Extensible Hypertext Markup Language
XML	Extensible Markup Language
XSD	Extensible Markup Language Schema Definition
XSL	Extensible Stylesheet Language
XSLT	Extensible Stylesheet Language Transformation
ZÜV	Payment Monitoring System