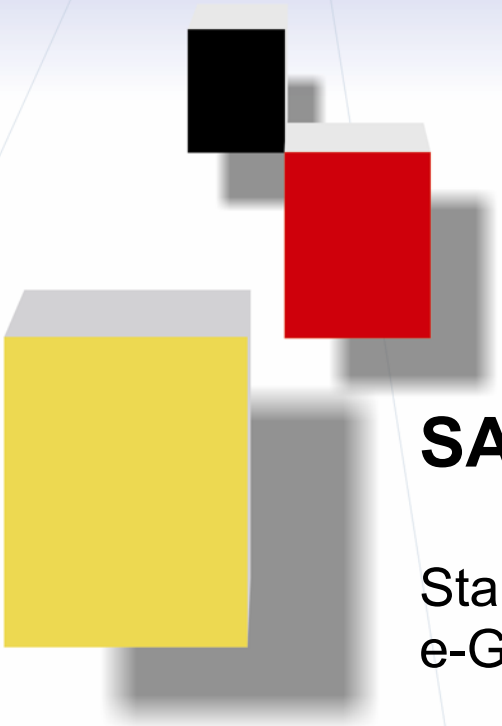
Bundesministerium
des Innern



SAGA

Standards and Architectures for e-Government Applications

Version 1.1

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

KBSt

KBSt Publication Series
ISSN 0179-7263
Volume 56
February 2003

KBSt Publication Series
Volume 56
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,]init[AG, Booz Allen Hamilton and the Fraunhofer Gesellschaft.

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 eGovernment Applications
Version 1.1

February 2003

Published by the
Federal Minister of the Interior

Word of thanks

The 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 the updating of the document.

Introduction:

This document presents standards, processes, methods and products of state-of-the-art IT development for e-government applications in a 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 by certain manufacturers or standardization 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, the editors, authors and experts consulted cannot accept any responsibility for the technical functioning, compatibility or completeness of the standards discussed. This version 1.1 was published on 12 February 2003. Please send any comments, amendments or corrections to: Bundesministerium des Innern, Referat IT2 (KBSt) and via 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 on which conditions (single/group license) a product can be economically used must be examined from case to case.

Version numbers are stated when they are relevant in the specific context discussed. Failure to state a version number, however, does 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

Mandatory standards

Standards are mandatory if they are tried-and-tested and represent the preferred solution. Such standards are binding and must hence be observed and applied with priority.

Competing standards can be mandatory parallel if they have clearly different functionalities or 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 in justified, exceptional cases only.

Recommended standards

Standards are recommended if they are tried-and-tested, but 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 functionalities or 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 be adopted in justified, exceptional cases only.

Standards 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.

0 Revision history and status

This document, version 1.1, is the first released publication of SAGA (Standards and Architectures for eGovernment Applications) and is binding.

0.1 Amendments to version 0.9

This document is based on SAGA version 0.9 that was already published and the subject of intense discussion with experts from Federal Government, Federal-State governments, municipal administrations and business. More than 150 comments were processed, and around 95 of these comments resulted in amendments to the document.

These amendments mainly refer to the following:

a. Clearer presentation of standards in order to improve readability and ease of handling
b. Revision of the architecture kit using RM-DDP (breaking down applications into viewpoints)
c. Revision of the "Presentation", "Middleware", "Communication" and "Data integrity" chapters

In the field of client technology, even active contents, such as Javascript and plug-ins, as well as the use of cookies were permitted subject to certain restrictions.

A chapter on "Basic components and competence centres" was added. The basic components are core elements of the e-government architecture of BundOnline 2005. Their applications for the implementation of e-government applications are defined in SAGA.

0.2 Future issues

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.

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

a. New access channels, such as digital TV, game consoles, etc.
b. Methods, processes and tools (including testing for conformity with SAGA)
c. Technical and specialized process and data models
d. Basic components and their linking to the backend
e. Integration of first practical experience with the application of SAGA

The "Basic components" chapter, in particular, will be extensively amended in the next version. This results from the progress of the projects for the individual basic components and the pertinent detailed requirements.

1 Introduction

1.1 Background

With the Standards and Architectures for eGovernment Applications (SAGA), the Federal Government is making an important contribution towards modern and service-orientated administration.

In September 2000, Chancellor Gerhard Schröder launched the BundOnline 2005 e-government initiative and obliged the Federal administration to provide its more than 350 Internet-enabled services online by the year 2005. Federal administrations, agencies and authorities have started implementing this initiative. Since the end of 2002, more than 160 administration services have now become available online.

Co-ordinated by the Federal Ministry of the Interior (BMI), an implementation plan was drafted and basic components defined. These basic components and applications that were developed according to the "one-for-all" principle, as well as new e-government applications to be created during the years to come are to smoothly interact with each other. A uniform "look and feel" system is to be made available to users. Following the development of the implementation plan, the Federal Ministry of the Interior set up a project group responsible for developing concrete technical procedures for this implementation plan.

The first step involved taking stock of existing standards which was carried out by a group that included eight experts from industry and another six experts from Federal-government, Federal-state and communal administrations.

This was the basis for the development of the Standards and Architectures for eGovernment Applications (SAGA) proposed in this document.

The resolution by the Federal Government on security in electronic legal and business matters with the Federal administration of 16 January 2002 was taken into consideration, as was the "Verordnung zur Schaffung barrierefreier Informationstechnik nach dem Behindertengleichstellungsgesetz (Barrierefreie Informationstechnik Verordnung BITV)" (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)).

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 detailed solutions whenever the standards presented herein are not sufficient for the implementation of technical requirements.

The standards and architectures defined are designed to avoid costly parallel work within public agencies and to enable offensive utilisation of any synergies which become possible via the Internet. The Federal Government also considers 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 to find their way through public agencies and to promote nation-wide e-government offers.

1.3 Purpose and structure of the 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 their frontend, unless the services to be implemented cannot be reasonably handled via a browser.
b. They forego active contents, to that users are not forced to reduce the browser's security settings which could result in damage by invisible Internet pages, or they at least use only signed and quality-secured applications of the type referred to in chapter 5.2.
c. E-government applications do not store any program parts or data on the users' computers beyond the users' control.

1.3.2 Objectives

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 (re-usability). Federal-state governments and communal administrations have the opportunity to make use of the development results of the BundOnline 2005 initiative.

c. To provide specifications in the form of publicly accessible documentation (openness)

d. To consider developments on the market and in the field of standardization (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 Scope

SAGA is a standardization 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 in order to be likely to become a standard in the new future

e. are not desired because they 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 (refer to chapter 4).

Two parts of the document describe standards in particular:

a. Chapters 4 to 6 describe the architecture kit and its elements.

b. Chapter 7 describes standards for the basic components defined within the scope of the BundOnline 2005 project.

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: services which the Federal Government offers its citizens directly

b. Government to business: services which the Federal Government offers to companies

c. Government to government: Federal Government services for public agencies.

More than 350 services of the different Federal administrations were identified. An analysis of the services along the value chain enabled the identification of eight service types (refer to www.bundonline2005.de). 73 percent of the services used today already belong to the three following types:

a. Gathering, processing and providing information

b. Processing applications and requests sent to public agencies

c. Processing subsidy and assistance applications

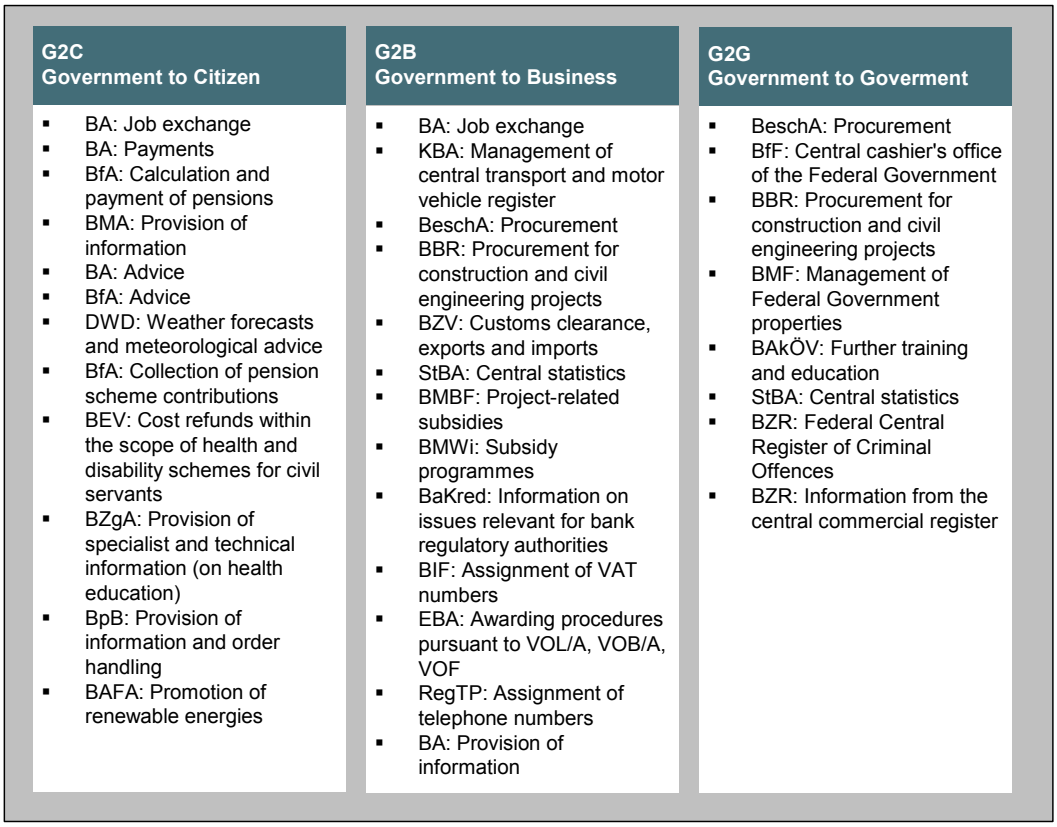


Figure 1-1: Selected services by the Federal Government

1.5 Success factors for standardization

Trials with standards and architectures for e-government have been underway for some years now in Germany and in other countries[1]. Experience from these trials and international exchange contribute towards facilitating the definition and implementation of SAGA. Some generally accepted factors for the success of e-government are as follows:

Legislative framework

The legislative framework must enable a user-friendly and efficient supply of services on the Internet.

Customer data (i.e. data on citizens, companies or public agencies), for example, must be electronically stored to a certain extent in order to offer users a user-friendly interface and to more than just information services.

Customer expectations

The use of e-government is strongly dependent on customer acceptance of the services offered. Expectations of citizens, companies and public agencies need to be identified on an ongoing basis. The service portfolio and the service rendering process must be adapted to these expectations.

Process definitions and meta data

A uniform and standardized process and data definition is a precondition for uniform and standardized hardware, applications and interfaces.

Training

The use and updating of standards means an ongoing exchange of information and training process. Activities of this kind are organized via the Federal Ministry of the Interior and/or the BundOnline 2005 project group.

[1] Refer to the corresponding documentation for the UK (eGIF: eGovernment Interoperability Framework), the US (GOSIP: Open System Interconnection Profile), Australia (APEC e-Business: What do Users need?) and Europe (IDA: Interchange of Data between Administrations)

Integration of partners and outsourcing

Close co-operation with partners and outsourcing of activities other than government activities can help save costs and boost the efficiency of e-government services.

2 The evolution of SAGA

2.1 Tasks

SAGA is a full-scale standardization 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 4). 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 chapter 5.3) 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 standardized description of the data communicated within the scope of e-government processes (applications) as a whole or in part (refer to chapter 5.3) 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. Six basic components have already entered into the implementation phase (refer to chapter 7).

2.2 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 is subsequently responsible for co-ordination with the Federal departments.

The process and data models are developed on the basis of the individual e-government projects of the public agencies. Process models of general relevance are standardized by the Bundesverwaltungsamt (BVA) as the competence centre for processes and organization. A steering unit yet to be identified is to be responsible for standardizing the data models. The Federal Ministry of the Interior will co-ordinate this development.

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

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.

2.2.1 Public discussion forum

A public forum (http://foren.kbst.bund.de) offers Internet users the possibility to register and discuss SAGA-related issues.

2.2.2 Request for comments (RFC)

Interested parties are invited to comment on up-to-date contents while new documents or new document versions are published. The SAGA homepage (http://www.kbst.bund.de/saga) offers a contact form for this purpose. The next version of the relevant document then takes these comments into consideration.

2.2.3 Expert group

The Federal Ministry of the Interior sets 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.

2.2.4 Request for proposals (RFP)

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

3 Binding effect and conformity of the applications

3.1 Scope of validity and binding effect of SAGA

SAGA describes the technical boundary conditions recommended for the development, communication and interaction of IT systems for 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[2] to be used should, whenever possible, comprise products or product versions which are compatible with the architecture recommended in SAGA.

The Federal Ministries lay down rules for the binding effect of SAGA within their spheres of business.

3.1.1 Classification of standards

Standards are divided into three categories. Competing standards which are not stated should not be used or only if absolutely inevitable.

Mandatory:

Standards are mandatory if they are tried-and-tested and represent the preferred solution. Such standards are binding and must hence be observed and applied with priority.

Competing standards can be mandatory parallel if they have clearly different functionalities or 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 in justified, exceptional cases only.

Recommended:

Standards are recommended if they are tried-and-tested, but are not mandatory and/or do not represent the preferred solution or their classification as mandatory still requires further agreement. In the event that no competing mandatory standards

[2] Software that is simply installed and configured

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 functionalities or 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 be adopted in justified, exceptional cases only.

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.

3.1.2 Definition of conformity

Conformity of an IT system with SAGA is given if:

a. The technical standards and architectures described are adhered to
b. Process models that are already standardized are applied
c. Data models that are already standardized are taken into consideration
d. Existing basic components are used

3.2 Responsibility for conformity

The public agency responsible for a process or system is also responsible for ensuring the conformity of e-government applications with SAGA. The public agencies are also responsible for examining ways of migrating specialist applications.

The Federal Ministries lay down rules for responsibility within their spheres of business.

The provision of conformity tests forms part of the future development of SAGA (refer to chapter 0).

3.3 Migration for conformity

3.3.1 Transition phase

SAGA is relatively new. It is subject to ongoing updating and adaptation to new requirements. This means that individual processes and systems are temporarily not in conformity with SAGA.

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

A pragmatic approach is recommended in order to ensure conformity with SAGA.

3.3.2 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 is specified as a mandatory criterion for government contracts.

3.4 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 centres are limited or even impossible.
c. Interfaces with such systems cannot be supported.
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.

4 Architecture kit for e-government applications

4.1 Functions and principles of the kit

The model of the architecture kit in SAGA serves the following purposes:

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

b. IT 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 standards that can be used when it comes to the implementation of e-government projects.

A view of an application under different viewpoints is helpful in order to describe complex, distributed e-government applications. Breaking down into viewpoints reduces the complexity of the individual viewpoints.

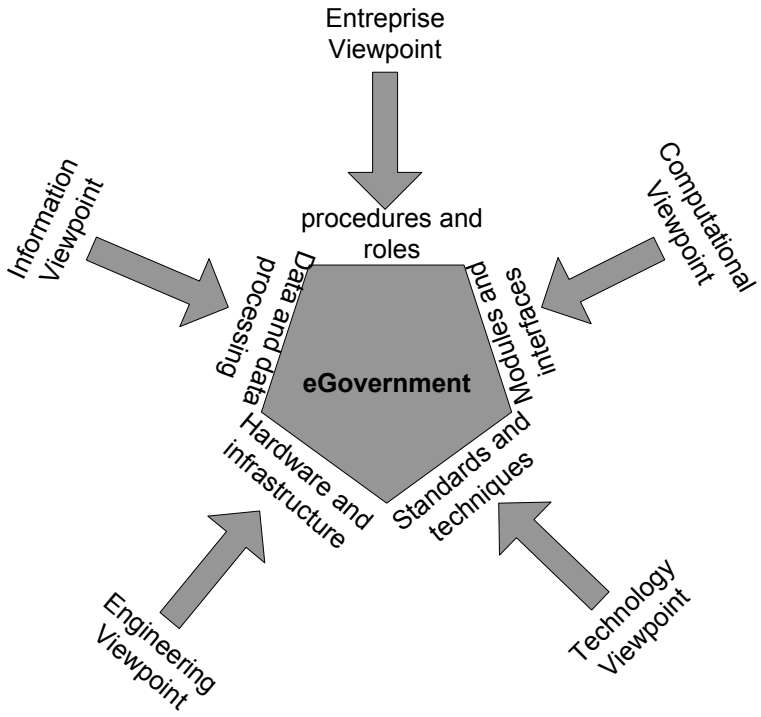


Figure 4-1: Viewpoints according to RM ODP

The architecture kit thus shows the basic structure of e-government applications from the different viewpoints and provides models, standards and technologies for modelling and implementing the applications.

The Reference Model for Open Distributed Processing (RM ODP[3]) proposes five viewpoints for a system which are adopted for SAGA.

- The Enterprise Viewpoint specifies purposes, scope, processes and policies for an application.
- The Information Viewpoint describes the characteristics and semantics of the data processed, as well as the detailed processes for data processing.
- The Computational Viewpoint represents the breaking down of an application into functional modules and their interaction interfaces.
- The Engineering Viewpoint represents the distribution of the individual elements of the system to physical resources and their connections.
- 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.

4.2 Modelling specialist applications in the viewpoints

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.

[3] ITU-T Rec

4.2.1 Fundamentals of e-government

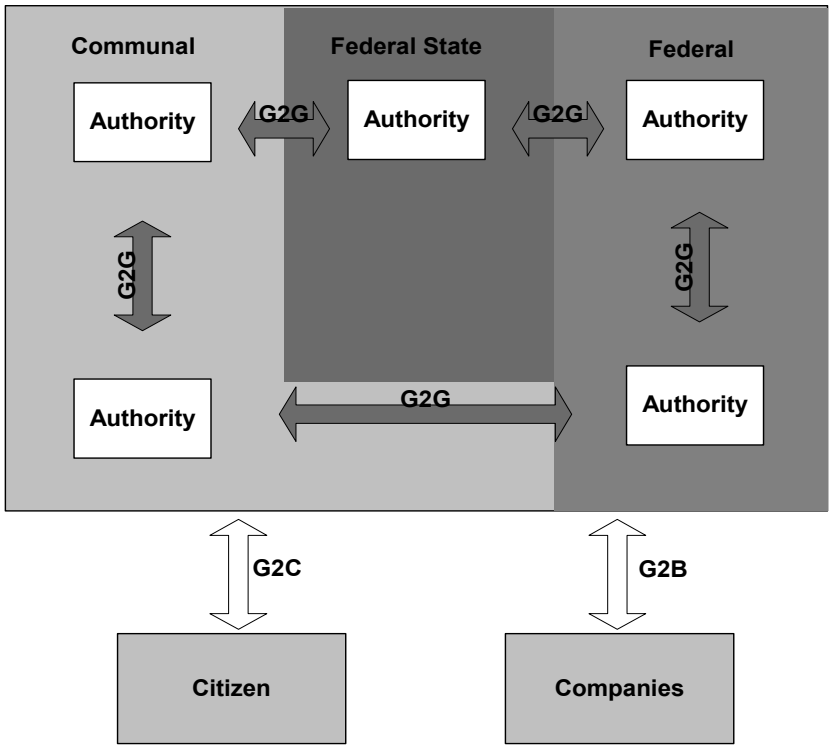


Figure 4-2: Overview of e-government interactions

E-government interaction can be divided into three categories as follows (refer to Figure 4-2: Overview of e-government interactions):

1. Public agencies interact with each other in order to implement processes. This is referred to as government-to-government (G2G) interaction.
2. Interaction between citizens and public agencies is termed government-to-citizen (G2C) interaction.
3. Government-to-business (G2B) interaction is the interface between companies and public agencies.

The architecture kit is valid for all three interfaces. One aspect that is currently not included is the internal operation and use of the processes by employees in public agencies:

4. The use of an application within a public agency is part of government-to-employee interaction (G2E).

SAGA distinguishes between three different major communication scenarios for each interaction interface, depending on its position in the value chain (refer also to the E-Government Manual):

a. *Information:* information is made available and retrieved as required.

b. *Communication/interaction*: bilateral communication for simple, general transactions, such as advice or co-operation.

c. *Transaction/integration*: complex, specialized transactions with a multi-stage value chain between communication partners with the aim of performing a individual-related service, such as an application procedure, a purchasing project and supervisory measures. Transactions can be performed both online and offline.

4.2.2 Enterprise viewpoint

This is where the overall environment for the system and its purpose are described. Furthermore, 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

Chapter 5.3 of the SAGA document provides the descriptive tools and procedure models needed to define the enterprise viewpoint.

4.2.3 Information viewpoint

This viewpoint determines the structure and semantics of the system's information. Further items include the definition of information sources and sinks, as well as processing and transformation of information by the system. Integrity rules and invariants exist for this purpose. Chapter 5.3 of SAGE provides the tools needed to define the data models. The basic components described in chapter 7 ensure the interoperability of specialist applications and their integrating capability. These basic components define the data models to be used and provide a common database.

4.2.4 Computational viewpoint (view of the system's structural and modular layout)

This is where a system is broken down into logic, functional components which are suitable for distribution. This results in objects which feature interfaces where services are offered and/or used.

Figure 4-3: Structural view – tier model

A specialist e-government application is generally divided into four tiers (refer to Figure 4-3: Structural view – tier model):

1. The client tier represents different access channels reflecting different users, terminal devices, transmission routes, as well as different applications in order to interact with the specialist applications. SAGA 1.1 refers to the following terminal devices:
   a. Web access via web browsers or special browser plug-ins
   b. Mobile phones and personal digital assistants (PDAs)
   c. External systems (such as ERP systems by industrial companies)
2. The presentation describes the processing of information in the client and the user's interaction with the specialist application. The presentation component includes all the standards for communication with the relevant terminal devices of the client tier.
3. 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 specialist 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 extent of integration is expected within the scope of e-government solutions. The medium tier processes the data from the backend or from the persistence tier.
4. The persistence tier is responsible for data storage, usually in databases.

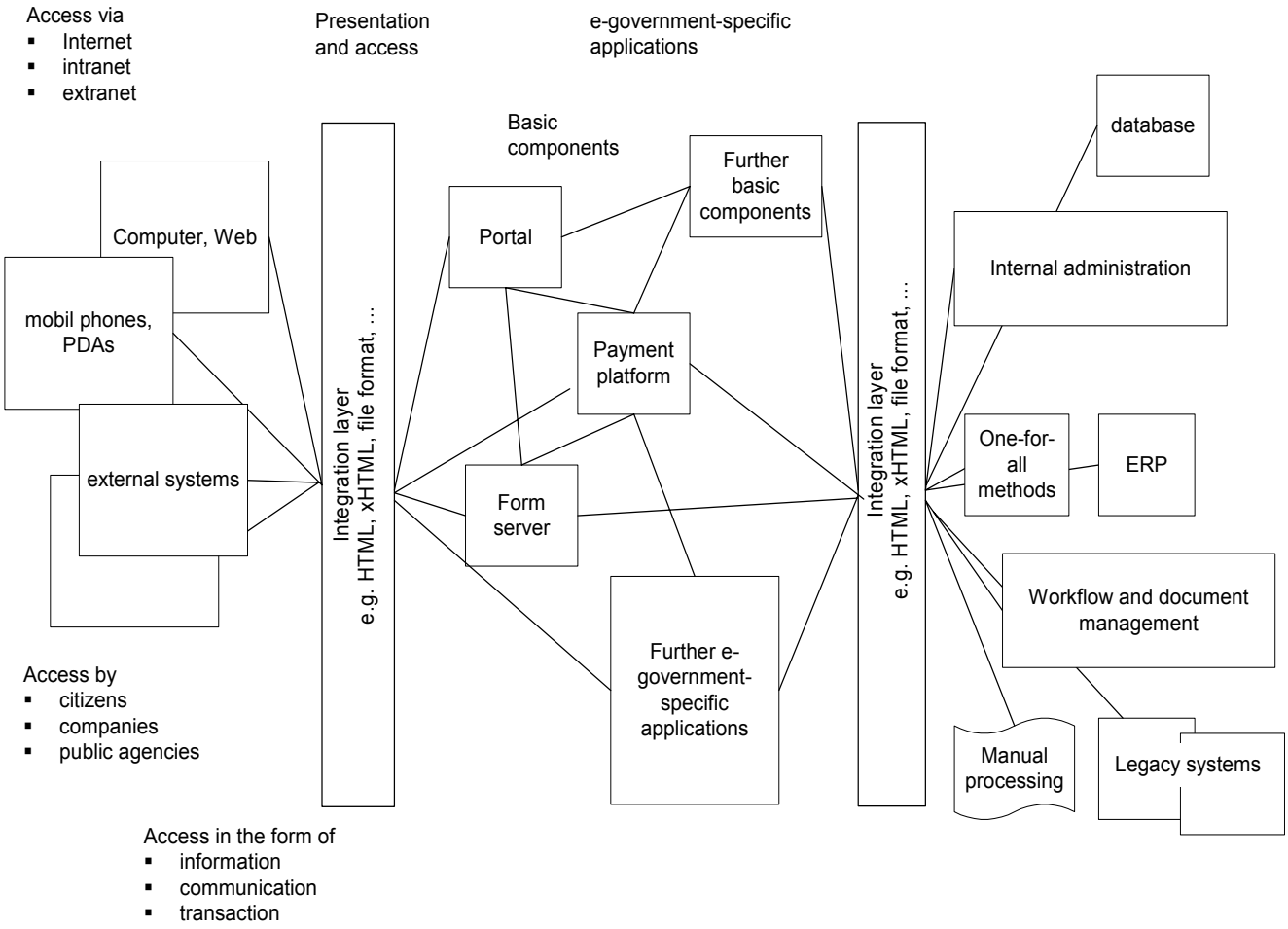


Figure 4-4: The architecture model abstracts terminal devices, as well as data integrity systems and methods, processes and tools

The backend mostly refers to the "old" world (i.e. legacy systems). These systems represent specialist applications and are seldom needed for e-government purposes.

Within these tiers, a specialist 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 chapter 7 provide functional modules for the implementation of e-government applications.

Terminal devices, users, communication scenarios and transmission media sum up to a host of possible applications. SAGA always refers to all applications, with exceptions being explicitly mentioned.

Safe and secure interaction between all the modules must be ensured. These security requirements include the following:

a. The authentication of the individuals and systems involved in order to ensure that all the identities present in the system can be trusted.
b. The authorisation of actors in order to ensure that the actors are authorised to perform the respective interaction.
c. The integrity of data and processes in order to ensure the undistorted transmission of data during communication, as well as the correct execution of all processes.
d. The confidentiality of data in order to ensure that no parties other than the communication partners have access to such data. Eavesdropping of communications, in particular, must be prevented.

Chapter 6 of the SAGA document defines standards and modules designed to ensure safe and secure interaction.

4.2.5 Engineering viewpoint (view of the system's physical distribution)

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

4.2.6 Technology viewpoint

This section describes the selection of concrete technologies for implementing the system.

Chapter 5 of the SAGA document describes the mandatory and recommended standards, with a structure corresponding to the tiers of the computational viewpoint. Models and standards which are relevant for and which support security issues are linked to all the other models and standards and are hence specified in chapter 6 for all the areas of the architecture kit at a generally applicable level.

5 Standards for the IT architecture

In this chapter, technical standards are assigned to the individual elements of the architecture kit introduced in chapter 4. 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.

5.1 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 offers in order to interact with public administrations, with access to information being possible via different media. In Germany, the following media are currently the most popular, so that optimum conditions for the wide-spread 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)

Standardization 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.

5.1.1 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 called 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 chapter 1.3.1).

5.1.1.1 Web browsers

In order to enable wide-spread use the of e-government applications on offer, web browsers should be used as the frontend device that must be capable of processing and presenting the presentation-tier formats (refer to chapter 5.2). The following browser-based client technologies are permitted in this context:

1) The use of cookies is permitted on condition that these are

   a) not persistent and

   b) linked to the issuing domain.

   The recommendations for the HTTP protocol according to chapter 5.6.3 must be taken into consideration in this context.

2) The use of Javascript is permitted on condition that a server certificate and an SSL connection (refer to chapter 6.3.1) are used in order to enable the client to identify this as authentic and integer. Chapter 5.2.1.5 must be taken into consideration when Javascript is used.

3) The use of Java applets is permitted on condition that they are signed by the server, so that the client can identify them as authentic and integer and further on condition that a manufacturer-independent software firm has performed quality assurance.

4) A positive list of supported plug-ins is kept and published at: http://www.kbst.bund.de/saga-plugins.

5) Configuration examples are prepared for usual browser types and made publicly available by the BSI on the Internet.

6) The confidentiality of form data must be ensured by the use of SSL-encrypted channels and the pertinent server certificates.

7) The statutory instrument (ordinance) on barrier-freedom remains fully applicable to the use of permitted client technologies.

5.1.1.2 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 considered as 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:

1) Any personal and security-critical data is stored in encrypted form on the local data medium.

2) Secure data transmission to the server is supported, for example, in accordance with the OSCI transport specifications. No protocols other than those defined in chapter 5.6.1.2 are permitted for any other client/server communications.

3) The formats documented in SAGA for the exchange of user data with other applications should be supported.

4) A manufacturer-independent software firm assures the quality of the application.

5) The application is supplied along with a software certificate which is verified during the course of the installation.

6) Besides an option to download the application from the Internet, distribution on CD-ROM is also offered.

7) The statutory instrument (ordinance) on barrier-freedom must be taken into consideration.

5.1.1.3 E-mail client

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

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

Note that the communication of these clients is standardized 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 chapter 5.6.3 must be used.

5.1.2 Access to information via mobile phone / PDA

Protocols which are served at the server end (refer to chapter 5.2.2) 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.

5.1.3 Access to information via external systems

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

Refer to "Data integration", "Middleware", "Communication" and "Linking to the backend" (chapters 5.4 to 5.7).

5.2 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 sub-chapters. 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.

5.2.1 Information processing – computer / web

5.2.1.1 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)"; refer to: http://www.bmi.bund.de/Annex/de_22681/BITV.pdf; are to 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 of W3C in version 1.0 which can be accessed at: http://www.w3.org/TR/WCAG10.

5.2.1.2 Interchange formats for hypertext

Mandatory:	Hypertext Markup Language (HTML) v3.2

The HTML v3.2 (http://www.w3.org/TR/REC-html32) format must be supported in order to ensure that older browser generations are supported.

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 (http://www.w3.org/TR/html401/), 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, happen 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 (http://www.w3.org/TR/xhtml1/) 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.

5.2.1.3 Style sheets

Style sheets can be used in order to ensure 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 by W3C can be used:

Recommended:	Cascading Style Sheets Language Level 2 (CSS2)

Cascading Style Sheets Language Level 2 (CSS2) (http://www.w3.org/TR/REC-CSS2/) should be used to design HTML pages.

Recommended:	Extensible Stylesheet Language (XSL) v1.0

The Extensible Stylesheet Language (XSL), version 1.0, (http://www.w3.org/TR/xsl/) should be used to transform and present XML documents in HTML files.

5.2.1.4 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. This specification is available at: www.unicode.org.

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

UTF-16 encoding should be used for documents in Greek or in 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.

5.2.1.5 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 read 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 runtime. **Active contents** are computer programs which are contained on Internet pages (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 chapter 5.1 must be taken into consideration.

Mandatory:	HTML format

If *information* is to be provided, HTML pages should be used on the basis of the hypertext interchange formats defined in chapter 5.2.1.2. The support of active contents and plug-ins may only be taken for granted to the extent defined in chapter 5.1.

Mandatory:	ECMA-262 – ECMAScript Language Specification

In as far as Javascript is used within HTML pages according to chapter 5.1.1.1, this must comply with the ECMA 262 specification (refer to: www.ecma.ch).

Recommended:	Servlets and Java Server Pages or XSL

Servlets and Java Server Pages (JSP, refer to: http://java.sun.com/products/jsp/) or Servlets and XSL (refer to: http://www.w3.org/TR/xsl/) should be used for the server-based, dynamic generation of HTML pages.

5.2.1.6 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 chapter 5.2.1.2).

Mandatory:	Portable Document Format (PDF) Version 4

Text documents that cannot be edited should be provided in the platform-independent Portable Document Format from Adobe Acrobat as (.pdf) files in the Acrobat Viewer Version 4 (www.adobe.de).

Recommended:	Extensible Markup Language (XML)

XML can also be used to describe documents and offers more design and layout options than HTML. For detailed specifications, please refer to: http://www.w3.org/TR/2000/REC-xml-20001006.

Under observation:	Portable Document Format (PDF) Version 5

In order to support forms and barrier-free text documents, it is also possible to use version 5 of the Portable Document Format from Adobe Acrobat as (.pdf) which is not yet very widely used. If this format is used for forms, the recommendations of the "Sicherer Internet-Auftritt" [Secure Internet Presence] of the E-Government Manual must be considered with regard to active contents (refer to chapter 5.2.1.5).

Mandatory:	Multipurpose Internet Mail Extensions (MIME)

The Multipurpose Internet Mail Extensions (MIME) format must be used for the standardized 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.

5.2.1.7 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) Version 4

Analogous to chapter 5.2.1.6.

Under observation:	Portable Document Format (PDF) Version 5

Analogous to chapter 5.2.1.6.

5.2.1.8 File types for presentations

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

Mandatory:	Hypertext Markup Language (HTML)

Presentations that can be edited should be exchanged as hypertext documents in HTML format as (.html) files (refer to chapter 5.2.1.2 Interchange formats for hypertext).

Mandatory:	Portable Document Format (PDF) Version 4

Analogous to chapter 5.2.1.6.

Under observation:	Portable Document Format (PDF) Version 5

Analogous to chapter 5.2.1.6.

5.2.1.9 Interchange formats for graphics

Mandatory:	Graphics Interchange Format (GIF)

In view of its wide-spread use, the Graphics Interchange Format (.gif) should be used to interchange 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 to interchange 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)

Whenever possible, the Portable Network Graphics (.png, http://www.w3.org/TR/REC-png) format should be used. 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 fifth-generation browsers have become 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.

Recommended:	Enhanced Compressed Wavelet (ECW)

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

5.2.1.10 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.

Under observation:	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). 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 rather than on document type definitions (DTD).

Under observation:	Scalable Vector Graphic (SVG)

W3C defines SVG as a language that describes two-dimensional graphics in XML. SVG supports three types of graphic objects:

- Vector graphics (such as lines, curves, polygons, paths)

- Pixel images
- Text

SVG enables graphic objects to be grouped, transformed or broken down into other previously rendered objects. Clipping paths, alpha masks or filter effects are special features of SVG. Furthermore, SVGs can also have interactive and dynamic properties.

Under observation: Vector Markup Language (VML)

The presentation of vector graphics can be supported by the Vector Markup Language (.vml) file format. (.vml) is an XML-based markup language for two-dimensional graphics embedded in HTML. It uses the structures known from CSS to this effect.

5.2.1.11 Interchange formats for audio and video files

Mandatory: MPEG-1 Layer 3 (MP3)

The customary (.mp3) format should be used to interchange 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. A suitable plug-in enables a browser to "play" such files. For further information concerning (.mp3), please refer to: www.iis.fhg.de.

Mandatory: Quicktime (.qt, .mov)

The customary Quicktime format should be used to interchange video sequences. A suitable plug-in enables a browser to "play" such files. For further information concerning Quicktime, please refer to; quicktime.apple.com.

5.2.1.12 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 is 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:	HTTP

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 is recommended because this is currently supported by all customary products. For further information concerning Quicktime, please refer to quicktime.apple.com.

Under observation:	Ogg

Ogg 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. For further information concerning Ogg, please refer to: www.ogg.org.

5.2.1.13 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 product of choice here. With this format, several individual GIF images are stored in a file and it is possible to define their sequence, display time and number of repetitions.

5.2.1.14 Data compression

Compression systems should be used in order to enable the exchange of large files and minimize 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 (www.ietf.org).

5.2.2 Information processing – mobile phone / PDA

In the event that an information offer for mobile phones and PDA's is to be developed, preference should be given to the SMS system because this is widely accepted by citizens. The presentation of Internet pages 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; refer to: www.smsforum.net. The SMS Forum is an international forum of all major IT companies.

Under observation:	WML v1.x

The Wireless Markup Language (http://www.wapforum.org/what/technical.htm) was defined for use in narrow-band environments, in particular, for wireless communications, and is the WAP markup language. All wireless communications providers in Germany support WML 1.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:	WAP v1.x

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

Under observation: XHTML Basic

XHTML Basic (http://www.w3.org/TR/xhtml-basic/) 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 1.0, WML 2.0 is once again based XML. It is, however, a subset of the xHTML Mobile Profile Specification which, on its part, is a subset of xHTML.

5.2.3 Information processing – external systems

Refer to "Data integration", "Middleware", "Communication" and "Linking to the backend" (chapters 5.4 to 5.7). However, only a subset of the standards mentioned in the middleware area is relevant for communication with external systems. XML and web service technology form the heart of communication with external systems. Existing interfaces that are based on OSI technology will be gradually migrated.

5.3 Technical and specialized process and data models

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 and that the necessary data is defined rather than placing information technology into the foreground. XMeld, which was developed by the Federal state of Bremen, is one example of this approach.

5.3.1 Technical and specialized process models

Services can and should be described in the form of technical process models. This means that all the work steps should be considered from the beginning to the end, i.e. from the customer's inquiry to the rendering of the service. At a first stage of development, these process models should remain at a relatively high level, and should be typically limited to a maximum of 20 work steps.

New proposals for 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 centre in charge of processes and organization should offer support in this respect. With support from work groups, this competence centre should also define the process types a and b referred to below.

Three types of process variants are generally distinguished as follows:

a. Reference models define templates for work processes which are not specific for a particular service. Rather than being specific for a particular public agency, they should describe the process between a customer and a service provider in a general form.
b. General processes are identical for all or most of the services involved (such as navigation, login, basic components and key applications).
c. Specific processes differ from service to service. Specific processes should be based on reference models. In cases of doubt, differences must be justified.

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 be orientated in a broader

sense towards DIN 66001: "Informationsverarbeitung, Sinnbilder und ihre Anwendung" [Information processing, symbols and their use].

Recommended:	Unified Modeling Language (UML)

The Unified Modeling Language (UML, refer to: www.omg.org) should be used for object-orientated modelling in order to prepare and document 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.

5.3.2 Technical data models

A coherent process definition calls for the use of general data definitions for major data identities (such as citizens) 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 centre in charge of processes and organization should offer support in this respect. A steering unit yet to be identified in more detail, as well as work groups managed by it should perform the work on standardizing the data models (refer to chapter 2.2). Prior to formulating data models, one should check whether comparable models are already available in Germany or Europe.

Three detail levels are distinguished as follows:

a. Functional data models describe major data identities and their mutual relations without going into specifics. This presentation is recommended for the development of the coarse technical concept.
b. Object-orientated reference classes define the basic data elements of e-government applications and include those elements that can be generalised.
c. Derived classes or objects inherit all the data elements of the reference classes and add further specific features.

Mandatory:	Entity Relationship Diagrams

Functional data models of detail level a. as aforestated must be presented using Entity Relationship Diagrams.

Mandatory:	Extensible Markup Language Schema Definition (XSD) v1.0

The data specification of detail levels b. and c. as aforestated is to be implemented as an XML schema (refer to chapter 5.4).

Under observation:	Unified Modeling Language (UML)

The Unified Modeling Language (UML, refer to: www.omg.org) can be used for object-orientated modelling in order to prepare and document large projects. XML schemas can be directly generated from the corresponding specifications.

5.4 Data integration

5.4.1 Data description

Mandatory:	Extensible Markup Language (XML)

XML (Extensible Markup Language) is to serve as the universal and primary standard for the exchange of data between all the information systems relevant for administrative purposes (http://www.w3.org/XML).

New systems to be installed should be capable of interchanging 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:	Extensible Markup Language Schema Definition (XSD) v1.0

XML schemas according to W3C definitions (www.w3.org) are to be generated using the Extensible Markup Language Schema Definition (XSD) for the structured description of data.

5.4.2 Data transformation

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

If applications use different XML schemas, conversion from one format to another may become necessary for data interchanging purposes. This format conversion is performed by the W3C-defined XSLT (http://www.w3.org/TR/xslt) language as part of XSL (Extensible Stylesheet Language).

5.4.3 Character sets

The standards already defined in chapter 5.2 "Presentation" are applicable to the exchange of data. The character set of individual parts of XML schemas can be further restricted in this context.

5.5 Middleware architecture

This chapter defines the standards in the middleware element of the e-government architecture kit, with special emphasis being laid on the application integration aspect. The specifications and recommendations in this area are based on the design principles that were laid down in the implementation plan of the BundOnline-2005 initiative, i.e. operating-system neutrality, interoperability and portability.

Other 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.

Mandatory:	J2EE v1.3

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

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

require the use of Java 2 Platform Enterprise Edition (J2EE) 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. The system architecture of J2EE includes several Java and Java middleware technologies (Servlets, JavaBeans, Enterprise JavaBeans, etc.) which form the basis for commonly used e-business frameworks. The J2EE Software Developer Kit includes standard programming interfaces (APIs) and technologies, such as JDBC 2.0 API, JMS 1.0, JTA 1.0, JAXP 1.1, J2EE Connector API 1.0, JAAS 1.0, JavaMail API 1.2, JAXR. For detailed information concerning J2EE in its current version 1.3, please refer to: http://java.sun.com/j2ee.

Mandatory: J2SE

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). The individual technologies should be used in accordance with J2EE Specification 1.3 in order to create a compatible migration path to J2EE.

JAAS v1.0

Authentication and authorization are to be implemented using the Java Authentication and Authorization Service (JAAS). JAAS offers modules for integration into the authentication of Unix, Windows NT and Kerberos. JAAS forms part of the Java 2 Platform Standard Edition (J2SE).

JDBC v2.0

JDBC should be used for access to databases.

JAXP v1.1

The Java API for XML Parsing (JAXP) is to be used for processing XML documents..

JMS, J2EE Connector Architecture

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

JNDI v1.1.2

JNDI should be used for access to and for creating directory services. JNDI offers access to LDAP and other directory services.

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

Core components of the .NET middleware were standardized by international standardization organizations. Projects are currently underway which aim at implementing 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.

5.6 Communication

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

5.6.1 Middleware protocols

In the case of middleware protocols, a distinction is made between server applications that communicate within an administration (chapter 5.6.1.1) and client applications outside the administration which communicate with an administration server (refer to chapter 5.6.1.2).

5.6.1.1 Server-to-server communication within the administration

Mandatory:	Remote Method Invocation (RMI)

Remote Method Invocation (RMI) 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. For further information concerning RMI, please refer to: http://java.sun.com.

Mandatory:	Mandatory: SOAP v1.1

SOAP (Simple Object Access Protocol) can be used for communication between applications or application components which are based on a J2EE architecture if the requirements of 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). For further information concerning SOAP, please refer to: www.w3.org.

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

The Web Services Description Language (WSDL) should be used for service definition purposes. WSDL is a standardized language 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:	Mandatory: Extensible Markup Language Schema Definition (XSD)

The data elements to be transmitted are to be specified via XML schema.

Recommended:	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.

5.6.1.2 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 chapter 5.4 "Data integration" as a universal and primary standard for the exchange of 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 1.0, SOAP 1.1, WSDL 1.1, and UDDI 1.0.

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

The Web Services Description Language (WSDL) should be used for service definition purposes. WSDL is a standardized language 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:	Extensible Markup Language Schema Definition (XSD) v1.0

The data elements to be transmitted are to be specified via XML schema.

Mandatory:	SOAP v1.1

SOAP (Simple Object Access Protocol) can be used to exchange structured data as XML objects between applications or application components via an Internet protocol (e.g. via HTTP). For further information concerning SOAP, please refer to: www.w3.org.

Under observation:	UDDI v2.0

The UDDI (Universal Description, Discovery and Integration) project, in its latest version 2.0 (www.uddi.org), is an XML-based technology initiative that is pursued by companies from all industries with the aim of publishing web services, their structured administration and their offering to users.UDDI is based on standards issued by the World Wide Web Consortium (W3C) and the Internet Engineering Task Force (IETF), such as XML, HTTP, DNS protocols and SOAP.

5.6.2 Network protocols

Mandatory:	IP v4

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

Under observation:	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/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 (www.sicherheit-im-internet.de) or of the German Federal Office for Information Security (www.bsi.de).

Mandatory:	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.

5.6.3 Application protocols

Chapter 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 standardized user interfaces for different file system types, and transfers data in an efficient and reliable manner. In contrast to HTTP, FTP foresees re-starting and restoration after an interruption.

Mandatory:	HTTP v1.0

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

Mandatory:	SMTP/MIME

E-mail protocols in conformity with the SMTP/MIME specifications for the exchange of 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 chapter 5.2.

Mandatory:	POP3/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.

5.6.4 Directory services

Mandatory: LDAP v3

LDAP v3 (Lightweighted Directory Access Protocol, 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 queries.

Under observation: UDDI v1.0

The UDDI (Universal Description, Discovery and Integration project, www.uddi.org), is an XML-based technology initiative that is pursued by companies from all industries aiming at the publishing, structured management and offering to users of web services. UDDI is based on standards issued by the World Wide Web Consortium (W3C) and the Internet Engineering Task Force (IETF), such as XML, HTTP, DNS protocols and SOAP.

Under observation: DSML v2

Directory Services Markup Language (DSML, www.oasis-open.org) is a definition in XML, which enables access to directory services. It enables the handling of several directories at the same time.

5.7 Connection to the backend

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 time and budget available, as well as the functions to be supported during the integration of the legacy system.

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

5.7.1 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 development of user interfaces 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 product converts legacy dialogues to user interfaces that can be handled by a browser.

5.7.2 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 chapter 5.4 "Data integration". This opens up new options and increases the flexibility of interfaces.

5.7.3 Program-to-program communication

Certain interfaces are widely used at Federal administrations, such as the F15 interface described in chapter 7.3. Widely used interfaces of this kind should remain in use, and should be upgraded.

Recommended:	Extensible Markup Language (XML)

Information interchange via XML documents has become the established procedure when it comes to adapting processing interfaces of this kind 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 that the development of a separate connector functionality may no longer be necessary.

Recommended:	J2EE Connectors, Java Message Service

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

Recommended:	Web Services

Web services are the medium of choice for data transmission.

Certain standards are very commonly used in industry. They should remain in use. For example:

Recommended:	UN/EDIFACT

This method of electronic data interchange (EDI) which is chiefly used in B2 environments is still possible. The "UN Electronic Data Interchange for Administration, Commerce and Transport (UN/EDIFACT)" standard has been the international standard since 1987. This standard must be adhered to when establishing EDI communications, unless more recent, SAGA-compliant technologies can be adopted.

6 Data security standards

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 trusted and secure communication between citizens, public agencies and business.

The e-government architecture kit (refer to chapter 4) 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 classical protection aims are fulfilled.

As the relevance of security measures has extremely increased in recent years due to the growing use of the Internet, standardization efforts 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.

6.1 Aims and principles of the data security

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

6.1.1 Protection aims

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

a. *Confidentiality* – protection against disclosure to unauthorized parties:
   no data is made available or disclosed to unauthorized individuals, entities or processes.

b. *Integrity* – protection against manipulation:
   unauthorized modification or destruction of data is not possible.

c. *Authenticity* – protection against fake 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 authorized 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.

6.1.2 Protection requirements

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

The IT Baseline Protection Manual (Chapter 2.2 Assessment of Protection Requirements, www.it-grundschutzhandbuch.de) explains the procedure for determining protection demand. In the E-Government Manual (Module: e-government phase plan – phase 3 "Analysis", www.e-government-handbuch.de) this demand is broken 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 6-1: Protection requirement categories

In order to evaluate applications in terms of their security, a protection requirement category can be defined for each protection aim. Examples of protection requirements identified in this way are to be found in the E-Government Manual (module: e-government phase plan – phase 3: "Analysis").

A determination of protection requirements must, in particular, consider the potential processing of personal data in order to ensure adherence to the general data protection requirements.SAGA does not explain any data protection measures. Data

protection information by the Federal Data Protection Commissioner with regard to risks and recommended measures can be found in the proposed data protection chapter for the IT Baseline Protection Manual of the German Federal Office for Information Security (http://www.bfd.bund.de/technik/DS-KAP/35.htm); future editions (presumably as of the 1st quarter 2003) of the E-Government Manual will include an additional chapter on data protection.

6.1.3 Data security structure model

In order to facilitate the understanding and use of security standards, the e-government architecture kit described in chapter 4 was broken down further in the form of a structure model with security-relevant issues (refer to Figure 6-2).

The structure model is not a layer model, but instead illustrates the different specification processes to be carried out in order to achieve the relevant security aims. This model shows the complexity of the IT security issue.

Since a data security standard typically encompasses more than just one structure level, a classification is deliberately not set up. It is, however, possible to view each standard from the point of view of the individual structure levels.

The structure model and the data security standards mentioned do not release the experts in charge from the need to scrutinize any given application with regard to its legal conformity and compliance with data protection requirements, as well as to check and adhere to the relevant security level during all instances and processes of the communication chain. An application-specific risk analysis, a determination of the protection requirements, as well as a security concept should be prepared.

Protection aims, protection requirements and applications (refer to chapter 4) define the aims of security measures.

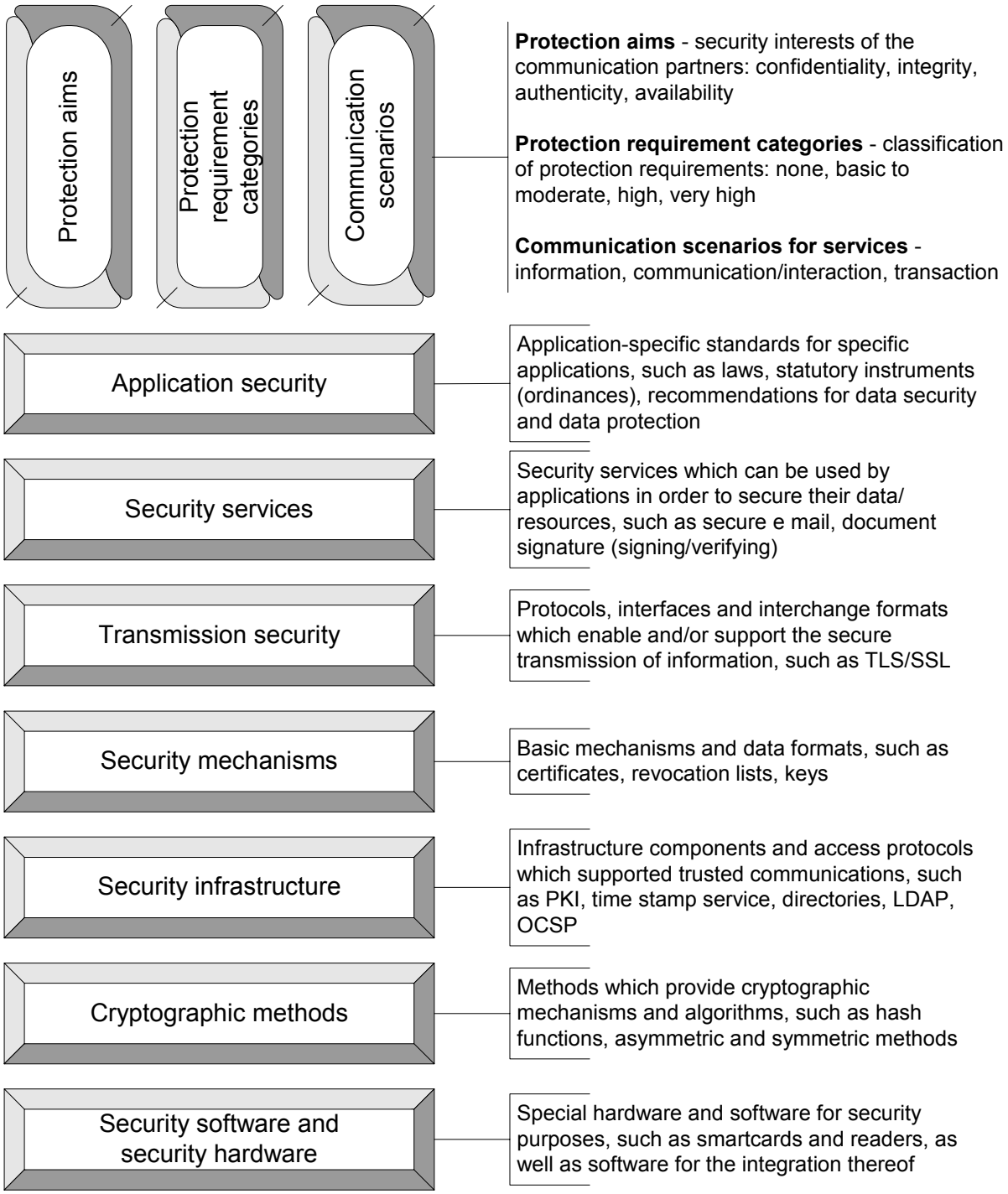


Figure 6-2: Structure model for security standards

6.2 Security standards for determining protection requirements

Laws and decisions by the Federal Government must be generally regarded as mandatory instruments. They are rounded off by recommendations and guidelines for IT security.

The recommendations and guidelines issued by the German Federal Office for Information Security and the KoopA committee [Co-operation Committee of the Federal Government and the Federal-state Governments for Automated Data Processing] listed below should be used to determine protection requirements. If protection requirements were identified for an IT application and/or components, the use of these recommendations and guidelines is mandatory.

Mandatory:	BSI, IT Baseline Protection Manual

The use of the IT Baseline Protection Manual issued by the German Federal Office for Information Security (manual for the development of IT security guidelines for low to medium security requirements; refer to: www.it-grundschutzhandbuch.de) is required. The IT Baseline Protection Manual enables the simple implementation of IT security concepts with reasonable effort. The structure of the IT Baseline Protection Manual supports a component-orientated approach.

Recommended:	KoopA, Guideline for action for introducing the electronic signature and encryption to public administrations

The "Handlungsleitfaden für die Einführung der elektronischen Signatur und der Verschlüsselung in der Verwaltung" [Guideline for action for introducing the electronic signature and encryption to public administrations] issued by KoopA ADV (www.koopa.de) is designed to facilitate solutions to cryptographic problems for selected projects in public administrations, primarily in the form of a work document for public agencies. Typical problems are defined in the form of scenarios for which possible solutions are described.

Recommended:	BSI, E-Government Manual

The E-Government Manual of the German Federal Office for Information Security (www.e-government-handbuch.de) was prepared in order to support the BundOnline 2005 initiative. The manual contains recommendations concerning the organization of and the use of IT in e-government. The manual, in particular, also deals with security recommendations.

6.3 Standards for specific applications

In order to enable the realistic assignment of security standards, common applications are formulated from a security point of view (refer to Figure 6-3 and chapter 4).

	Information	*Communication/interaction*	*Transaction/integration*
Secure transmission of web contents (integrity and confidentiality)	▸ SSL/TLS		
Web server authenticity			
Securing e-mail communications		▸ MTT Version 2 ▸ ISIS-MTT	
Secure interchange 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 6-3: Security standards for specific applications

6.3.1 Secure transmission of web contents and web server authenticity

When a client communicates with the web server of a public agency, this client must be certain that this is in fact the agency's server (web server authenticity). The retrieval of information – i.e. the transmission of web contents requiring integrity and/or confidentiality – must be secured during the process of transmission via the Internet.

Mandatory:	SSL/TLS

SSL (Secure Sockets Layer) is a cryptographic protocol that ensures integrity, confidentiality and authenticity on the World Wide Web. SSL was developed further to the TLS (Transport Layer Security) protocol (http://www.ietf.org/ rfc/rfc2246.txt).

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

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

SSL/TLS also supports the unilateral authentication of the public agency's server in relation to the client of the communication partner, so that the latter can convince itself that it is actually 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 the communication contents
d. Symmetric message authentication (via MACs) and protection against the replaying of messages

Chapter 5.2.2 of the KoopA guideline provides an exact description of how SSL/TLS works. The combination of different methods is referred to as "Cipher Suite" in SSL/TLS. An SSL/TLS Cipher Suite always contains four cryptographic algorithms, i.e. a signature process, a key interchange process, a symmetric encryption process and a hash function.

The KoopA guideline features the following recommendations:

a. A maximum key length should be defined for symmetric methods, i.e. currently 128 bits or 112 bits 3-DES, whilst single-DES and RC2 are not advised.
b. SHA-1 should be used as the hash function.
c. RSA modulo should have at least 1024 bits.

6.3.2 Securing e-mail communications

The secure exchange of e-mails is one possible application of the "communication/interaction" scenario. Secure e-mail communication includes the securing of e-mails on their way from a sender to a recipient. This application considers e-mails in their entirety. Chapter 6.3.3 Secure exchange of documents addresses the issue of securing documents, including e-mail attachments.

Mandatory:	MTT Version 2/SPHINX/PKI-1 administration

MTT Version 2

The MTT specification, version 2 (www.teletrust.de), is a development by the German TeleTrusT e.V. association. This standard includes:

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 rated 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 powerful cryptographic processes used in SPHINX form part of the MTT specification. Within the scope of the "SPHINX – Secure E-mail" project, the end-to-end security of e-mails using public key cryptography was tested on a manufacturer-independent basis. The entire project was set up on the basis of the MailTrusT specification (MTT version 2) and covers the underlying standard for the electronic signature and for encryption, as well as the infrastructure measures and organizational procedures necessary for the introduction of security technology. This concept was used as a basis upon which a security infrastructure was set up for the participating public agencies and organizations that enables a secure exchange of documents between the participants.

PKI-1-Verwaltung – Public key infrastructure for public administrations

Drawing on the experience from the SPHINX pilot project, the German Federal Office for Information Security has implemented a public key infrastructure (PKI) for the area of public administrations (PKI-1-Verwaltung). The root certification authority (Policy Certification Authority: PCA) of PKI1-Verwaltung must be used. Federal-state authorities, municipal authorities and other public institutions operate their own certification agencies which, on their part, are certified by the PCA for public administrations (PCA-1-Verwaltung). Information concerning the use of SPHINX in the context of PKI-1-Verwaltung is available from the German Federal Office for Information Security at www.bsi.de.

Mandatory:	ISIS-MTT

The ISIS-MTT specification considers a host of applications for methods to secure electronic transactions (such as mail, file, transaction and time "protection") based on the basic functions, i.e. electronic signature, encryption and authentication.

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

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

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

The latest versions of the specifications can be downloaded from the websites www.teletrust.de and www.t7-isis.de.

ISIS-MTT is rated 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 (as of around 2003), ISIS-MTT will replace the MTT v2 standard.

6.3.3 Secure exchange of documents

The "communication/interaction" scenario requires the exchange of secure documents. This includes, for example, the securing of documents attached to e-mails and the securing of documents for any communication channels whatsoever.

The MTTv2 and ISIS-MTT standards are relevant with regard to the securing of e-mail attachments. The XML-specific XML Signature and XML Encryption standards are becoming increasingly important for the secure exchange of XML documents (for forms that can be processed further, for example).

Mandatory:	MTT Version 2/SPHINX/PKI-1-Verwaltung

The MTT version 2 specification (refer to chapter 6.3.2 Securing e-mail communications) also defines an interoperable data interchange format for signed and encrypted data. MTT particularly considers the securing of binary data, so that the secure transmission of any 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. MTTv2 will in future be replaced by ISIS-MTT (refer to chapter 6.3.2).

Mandatory:	ISIS-MTT

ISIS-MTT (refer to chapter 6.3.2 Securing e-mail communications) fully integrates MTT version 2 and will replace this standard in future.

Recommended:	XML Signature

XML Signature is a joint standard of the W3C and IETF (W3C, XML-Signature Syntax and Processing, W3C Recommendation and IETF RFC 3275, March 2002, http://www.ietf.org/rfc/rfc3275.txt).

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

Three options are available for placing the XML signature:

a. Enveloped: The signature can be enveloped. This means that the XML fragment that represents the signature is integrated into the signed document.

b. Enveloping: The signature can serve as an envelope, i.e. it is applied to a document to which the reference is made within the signature.

c. Detached: The signature can be independent (i.e. detached). This means that it is stored separate from the source, either in the same or in another XML document.

One central feature of XML Signature is that it is possible to sign only certain parts of the XML document rather than the complete document. Both asymmetric encryption algorithm and symmetric processes can be used which must be chosen depending on protection requirements.

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. An example is a signed XML form that is sent to a user. The user can then fill in 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/addition would have meant a violation of the document's integrity.

The following encryption algorithms are specified:

a. Hash function: SHA1

b. Encryption: base64

c. MAC: HMAC-SHA1 (symmetric keys); (HMAC RFC 2104)

d. Signature: DSA-SHA1 (DSS); additionally recommended: RSA-SHA1

Specialization of the cryptographic preferences for particular communication scenarios has not yet taken place.

Recommended:	XML Encryption

XML Encryption is a W3C standard, but in contrast to XML Signature not yet an RFC (XML Encryption Syntax and Processing, W3C Candidate Recommendation, 4 March 2002, http://www.w3.org/TR/xmlenc-core/).

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

Encryption can be carried out using a symmetric or an asymmetric key.

The following encryption algorithms are specified:

a. Block encryption: 3DES, AES

b. Key transport: RSA (RSAES-PKCS1-v1_5 algorithm, RFC 2437)

c. Key agreement: Diffie-Hellman (optionally)

d. Hash function: SHA1, RIPEMD-160

e. Encryption: base64

XML Encryption is recommended as a supplement to XML Signature. However, acceptance of this standard is not equivalent to the acceptance of XML Signature.

6.3.4 Transactions

Transactions refer to complex, technical business transactions with a multi-stage value chain between the communication partners.

Mandatory:	OSCI-Transport v1.2

OSCI (Online Service Computer Interface) was developed within the scope of the MEDIA@Komm competition. OSCI covers a host of protocols which are suitable for e-government applications and which are prepared by the OSCI steering group. The aim is to support transactions in the form of web services and their complete handling 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 exchange unit – the so-called intermediary – which is capable of rendering value services without jeopardising confidentiality at transaction data level is characteristic for the secure implementation

of e-government processes using OSCI. As a secure transmission protocol, it enables online transactions with a binding effect (including SigG-conforming transactions).

OSCI-Transport supports the asynchronous communication via the intermediary as well as end-to-end encryption for the confidential transmission of data. OSCI-Transport standardizes both message contents as well as transport and security functions, and is based on international standards (including, but not limited to, XML Signature, DES, AES, RSA und X.509), for which concrete details are laid down in a suitable manner.

Major design criteria for OSCI-Transport, version 1.2, were the following:

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

6.3.5 Web services

The increasing importance of XML as a data interchange and specification format even for security applications, as well as the introduction of web services as an integrative middleware are leading to an active standardization of XML security standards in the W3C and OASIS committees. A full assessment of the relevance and final scope of drafts is currently not yet possible.

Under observation: WS-Security

WS-Security is a new industry standard for the security of web services. WS-Security defines amendments to the SOAP protocol in order to provide confidentiality, integrity and the binding effect of SOAP messages in order to secure web services. It should be possible to use different security models and different cryptographic methods as a basis.

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 regarded as a kind of foundation document for Web Services Security which is to be followed by further documents (WS-Policy, WS-Trust, WS-Privacy, WS-Secure Conversation, WS-Federation and WS-Authorization) in future.

WS-Security is a joint draft by IBM, Microsoft and Verisign and hence features strong manufacturer support. Although a final assessment of the relevance of this standard is not possible at the moment, it might turn out to be a crucial element for SOAP communication of web services of the future.

6.4 Generally applicable data security standards

Generally applicable security standards are standards that cannot be assigned to particular applications and/or communication scenarios.

	Information	Communication/ interaction	Transaction/integration
Security infrastructure integration		▸ ISIS-MTT	
Smartcard integration	▸ ISO/IEC 7816		
Encryption algorithms for the electronic signature	▸ Publication by RegTP ▸ Hash functions: RIPEMD-160, SHA-1; signature algorithms: RSA, DSA, DSA variants)		
Symmetric encryption algorithms	▸ Triple-DES, IDEA, AES		

Figure 6-4: General security standards

6.4.1 Authentication

In order to warrant the "authenticity" requirement, certain e-government applications require the identification and authentication of the communication partners. Different mechanisms are available for authentication, such as user ID / password, PIN/TAN or certificates. An assessment of the various authentication options from a security point of view will be the subject of a separate module of the E-Government Manual (presumably at the end of 2002).

6.4.2 Security infrastructure integration

The security infrastructure includes directory, certification and time stamp components which support the distribution and handling of certificates, revocation lists and time stamps for both e-mail and web environments. These components are accessed via operational protocols.

Mandatory:	ISIS-MTT

Part 4 "Operational Protocols" of ISIS-MTT (refer to chapter 6.3.2 Securing e-mail communications) describes protocols and profiles for the integration of security infrastructures. These include access to directories via LDAP V.3, Online Certificate Status Protocol (OCSP), FTP and HTTP as well as the Time Stamp Protocol (TSP).

6.4.3 Smartcard integration

The integration of smartcards, smartcard readers and their driver architectures and of complete, multi-function "smartcard/reader bundles“ is necessary for the client infrastructure for several reasons, including the use of qualified electronic signatures.

The D21 (www.initiatived21.de) initiative addresses this issue in its work group 5 – smartcards project. The results of this project group will supplement the standards mentioned for the integration of smartcards.

Mandatory:	ISO/IEC 7816

Smartcards (chip cards) must comply with the ISO/IEC 7816 standard. Components which support the universal "Cryptographic Token Interface (Cryptoki)" interface must conform with ISIS-MTT part 7 (Cryptographic Token Interface).

6.4.4 Encryption algorithms for the electronic signature

The security of an electronic signature depends primarily on the strength of its underlying encryption algorithms.

Mandatory:	Encryption algorithms according to RegTP for the electronic signature

The regulation authority for telecommunications and postal services (RegTP) issues the suitable encryption algorithms that meet with the requirements pursuant to SigG and SigV for the forthcoming 6 years in the Bundesanzeiger (Federal Gazette) (www.regtp.de). The German Federal Office for Information Security can identify additional processes as suitable.

For the purposes of the law, an electronic signature includes the following encryption algorithms:

a. An algorithm for the hashing of data (a hash function) which reduces the data to be signed to a hash value, i.e. a bit sequence with a constant length. The hash value of the data rather than the data itself is then signed.

b. An asymmetric signature method which consists of a signing and a verifying algorithm. The signature process depends on a key pair, i.e. a private (i.e. secret) key for signing (generation of the signature) and the pertinent public key for verifying (checking) the signature.

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

Suitable hash functions:

a. RIPEMD-160
   RIPEMD-160 is a cryptographic hash function which – like SHA-1 – generates hash values with a length of 160 bits.

b. SHA-1
   SHA-1 (Secure Hash Algorithm) is a widely used cryptographic hash function. SHA-1 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 also termed public key method, and is the most important asymmetric method. The security is based on the difficulty to factorise large natural numbers. Usual modulus lengths are 512, 1024 and 2048 bits, whilst 512-bit keys are no longer recommended.

b. DSA
   The Digital Signature Algorithm (DSA) is the signature method which was developed and specified in 1991 in the Digital Signature Standard (DSS). DSA is a pure signature algorithm (in contrast to this, RSA enables both the electronic signature and the exchange of keys). Although the US government has patented 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 characteristics of the algorithms to be applied can be influenced by the applicable standards. ISIS-MTT part 6, for example, specifies the cryptographic algorithms that are valid for ISIS-MTT.

6.4.5 Symmetric encryption algorithms for encryption

Cryptographic algorithms for encryption can be applied to the data and/or keys to be transmitted on a confidential basis.

When symmetric methods are used, they use the same private key for encryption and decryption. These methods are generally very performant.

Although RegTP does not specify any encryption algorithms as binding, the algorithms laid down in ISIS-MTT part 6 (Cryptographic Algorithms) are adopted here. In cases of doubt, the specifications in the ISIS-MTT standard are applicable. With regard to the mode/padding of an algorithm, reference is made to ISIS-MTT part 6.

Mandatory:	Triple-DES

Triple-DES, also termed 3DES, is a triple DES (Data Encryption Algorithm) 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 safe, it is not very performant.

Mandatory:	IDEA

IDEA (International Data Encryption Algorithm) was developed in Europe and uses a key length of 128 bits.

7 Basic components and competence centres

The implementation of the around 400 Internet-enabled services identified within the scope of BundOnline 2005 is supported by so-called **basic components**. The basic components centrally offer technical functionalities which can be used by different services and public agencies. They provide technology platforms which – once developed – are widely used within the Federal administration, either in identical form or in a customised configurations.

So-called **competence centres** were set up in addition to the basic components. The main purpose of the competence centres is to support public agencies in introducing the relevant basic components.

7.1 Basic components

The basic components provide function blocks which form part of many services and which are integrated as services or modules into the e-government applications.

The basic components differ in terms of their development level. Whilst the first version of the basic component "Portal www.bund.de" went into operation as early as during the 1st quarter of 2001, the basic component "Call Center" is still in the demand analysis stage.

The basic components are implemented in several stages, so that new versions of the basic components with a gradually enhanced functionality will be made available during the course of time.

The basic components identified as mandatory must, as a general rule, be used when e-government applications are implemented. Any temporary use of alternative approaches for functionality blocks implemented by the basic components should be restricted to justified exceptions if subsequent migration costs can be avoided in this way.

Mandatory:	Basic component: payment platform ("e-payment“)

The implementation of many online services is contingent upon the possibility to electronically collect and pay fees for administrative services. This makes it possible to make full use of the efficiency advantages of electronic payment in conjunction with the digitisation of administrative services.

The **basic component "payment platform"** is an e-payment service that can be integrated into all kinds of e-government processes. The central provision of this service is designed to avoid parallel development and to ensure cost-effective operations.

The necessary integration into the Federal Government's budget, collection and accounting system (HKR) forms part of the e-payment platform, so that it does not have to be implemented separately by every e-shop. The e-payment platform is to offer the following core functionalities:

- A service for fee collection
- To ensure the collection of fees
- Communicate the success or failure of a transaction
- To pass on the revenue to the budget, collection and accounting system for posting

Recommended:	Basic component: "data security" ("virtual post office“)

The **basic component "data security"** (virtual post office) ensures secure, traceable and confidential communication between public agencies and external communication partners within the scope of e-government services. One of its purposes is substantial relief for all the parties involved when it comes to routine work which is often still connected to communication secured by electronic signatures and encryption.

In conjunction with the use of electronic communication channels, the virtual post office is to work as a largely automatic, central security gateway, providing the authentication, signature verification and signature generation, as well as decryption and encryption functions. Although the virtual post office generally acts as a central service provider (central contact point) in a public agency and primarily supports indirect communication with the public agency, direct secure e-mail communication with individual officers will be possible parallel to this function.

E-mails, e-mail attachments and data structures for a web interface are regarded as the inputs and outputs of the virtual post office. Apart from these functions, it will also offer further security checks as required.

As long as the basic component "data security" is not yet available, the "Data Security" competence centre offers advice on how interim solutions can be established which simplify a future introduction of the basic component.

Mandatory:	Basic component: Portal www.bund.de

The **basic component "Portal www.bund.de"** is the central point of access to the Federal Government's online services and information offers. The portal is thus responsible for providing citizens, business and administrations with quick and user-friendly access to the Federal Government's electronic services. The portal functions as an information guide, providing user-specific information and services and thereby enhancing communication with the Federal administration.

The start page of www.bund.de was designed in analogy to commercial websites, featuring search windows and a list of subjects. Data of public agencies on the portal, including an address directory, is updated by the public agencies themselves via a decentralised editorial function.

Mandatory:	Basic component: form server

The **basic component "form server"** is an overview of the Federal Government's forms for citizens, business and administrations which is made available as a form centre via the www.bund.de portal. The decentralised offering and linking of forms is possible via the distributed content management system of the portal.

The aim is to enable partially or fully digital communication between public agencies and citizens. The use of digital forms and the digital transmission of forms via the Internet can reduce operating costs and simplify and accelerate their handling on both ends.

The medium-term is to fully process all forms via the Internet using a single medium.

Recommended:	Basic component: content management system

The **basic component "content management system"** (CMS) is made available to all the agencies of the Federal administration for their Internet, intranet and extranet applications. The system is prepared on the basis of the design guidelines (Internet styleguide of the Federal Government) published by the Press and Information Office of the Federal Government, as well as on the basis of the disabled-friendly requirements for "barrier-free" Internet.

The CMS basic component will be implemented on the basis of the CAP 4.0 content management systems by CoreMedia, and will be specifically adapted to the requirements of the public authorities landscape. The pre-configured system can be made available to the individual Federal agencies both centrally (by way of hosting) and in a decentralised form (by way of subsequent distribution of the adapted application).

Under observation:	Basic component: call centre

The customary user assistance tool (information pages, help assistants, etc.) are often insufficient when it comes to handling complex e-government services. In cases like these, a call centre can offer users additional valuable support. The prospective users' demand for call-centre services is currently being explored.

7.2 Competence centres

Four competence centres have been set up in order to support the BundOnline 2005 e-government initiative. The main purpose of the competence centres is to provide expertise for the distributed implementation of online services. This includes, in particular, consultancy services with regard to the implementation of basic components and online services.

The **Data Security Competence Centre** at the German Federal Office for Information Security offers advice to public agencies with regard to the security of e-government methods and the use of the digital signature. Trustworthy infrastructures must be created, administrative processes must be re-structured and existing applications in public agencies must be fitted with suitable security solutions in order to enable the transmission of sensitive data via the Internet. This ensures smooth, legally valid and confidential online communications with the external environment of the Federal administration, as well as secure communications within and between public agencies.

The **E-Payment Platform Competence Centre** will provide the entire Federal administration with methods and concepts for implementing and operating e-payment applications. Furthermore, it will gather and process technical expertise for the integration of e-shops into the central e-payment platform, offer consultancy services and provide market expertise for other e-payment systems (suppliers, products, services, price models, trends, etc.). The E-Payment Platform Competence Centre will start work in spring 2003 when the first stage of the e-payment platform goes on stream.

The **Content Management System Competence Centre** (CMS) offers implementation advice to public agencies within the Federal administration wishing to use the CMS basic component for the online offering of their services. It also takes part in the concept work on the demand-orientated implementation of the CMS basic component and, following completion of the CMS basic component, will be available as a contact partner for optimisation suggestions and customised adaptation.

The **Transaction Handling, Processes and Organization Competence Centre** will support public agencies in optimizing the relevant business processes prior to implementing online services. This is considered as a mandatory organizational precondition for using the existing potential for optimization. The main task of the competence centre is to enable Federal agencies to effectively implement their services under their own responsibility. Federal agencies are to be offered technical and methodological support in order to adapt their structures, processes and administrative procedures.

8 Appendix

8.1 Overview of standards for the IT architecture

8.1.1 Presentation

8.1.1.1 Information processing – computer / web

Chap-ter	Component	Technical specification
5.2.1	Presentation for the disabled	▸ Barrier-free information technology ordinance BITV
5.2.1	Interchange formats for hypertext	▸ HTML v3.2, http://www.w3.org/TR/REC-html32 ▸ HTML v4.01, http://www.w3.org/TR/html401/ ▸ XHTML v1.0, http://www.w3.org/TR/xhtml1/
5.2.1	Style Sheets	▸ CSS2 (Cascading Style Sheets) as supplementary language for HTML, http://www.w3.org/TR/REC-CSS2 ▸ XSL v1.0, http://www.w3.org/TR/xsl/
5.2.1	Character sets	▸ ISO 10646-1:2000/Unicode V3.0 in UTF 8 and/or UTF 16 encryption, www.unicode.org ▸ ISO 8859-1 ▸ ISO 8859-15
5.2.1	Static and dynamic, passive and active contents	▸ HTML format ▸ ECMA-262 – ECMAScript Language Specification ▸ Servlets and Java Server Pages or XSL
5.2.1	File types and type identification for text documents	▸ Text (.txt) ▸ Hypertext Markup Language (HTML) ▸ Portable Document Format (PDF) Version 4 ▸ Extensible Markup Language (XML) ▸ Portable Document Format (PDF) Version 5 ▸ Multipurpose Internet Mail Extensions (MIME)

5.2.1	File types for spreadsheets	▸ Comma Separated Value (CSV) ▸ Adobe Acrobat as (PDF) file Version 4 ▸ Adobe Acrobat as (PDF) file Version 5
5.2.1	File types for presentations	▸ Hypertext Markup Language (HTML) ▸ Portable Document Format (PDF) Version 4 ▸ Portable Document Format (PDF) Version 5
5.2.1	Interchange formats for graphics	▸ Graphics Interchange Format (GIF) ▸ Joint Photographic Experts Group (JPEG) ▸ Portable Network Graphic (PNG) ▸ Tag Image File Format (TIFF) ▸ Enhanced Compressed Wavelet (ECW)
5.2.1	Interchange formats for geographical information (grid data, vector data)	▸ Geography Markup Language (GML) ▸ Scalable Vector Graphic (SVG) ▸ Vector Markup Language (VML)
5.2.1	Interchange formats for audio and video files	▸ MPEG-1 Layer 3 (MP3) ▸ Quicktime (.qt, .mov)
5.2.1	Interchange formats for audio and video streaming	▸ HTTP as transport protocol ▸ Quicktime (.qt, .mov) ▸ Ogg
5.2.1	Animation	▸ Animated GIF
5.2.1	Data compression	▸ ZIP v2.0 ▸ GZIP v4.3 (.gz)

8.1.1.2 Information processing – mobile phone / PDA

Chap-ter	Component	Technical specification
5.2.2	SMS	▸ Specification as defined by the SMS Forum, http://www.smsforum.net/doc/public/Spec/
5.2.2	WML 1.x	▸ www.wapform.org
5.2.2	WAP 1.x	▸ Specification as defined by the WAP Forum, www.wapforum.org

5.2.2	XHTML-BASIC	▸ http://www.w3.org/tr/xhtml-basic/

8.1.2 Technical and specialized process and data models

Chap-ter	Component	Technical specification
5.3.1	Process models	▸ Role models and flow charts (DIN 66001) ▸ UML
5.3.2	Data models	▸ Entity Relationship Diagrams ▸ Extensible Markup Language Schema Definition 1.0 (XSD) ▸ Unified Modeling Language (UML)

8.1.3 Data integration

Chap-ter	Component	Technical specification
5.4.1	Data description	▸ Extensible Markup Language (XML) ▸ Extensible Markup Language Schema Definition 1.0 (XSD)
5.4.2	Data transformation	▸ Extensible Stylesheet Language Transformation 1.0 (XSLT)
5.4.3	Character sets	▸ The standards described in chapter 5.2 "Presentation" are used. ▸ Certain parts of the XML schema can be restricted further in the character set.

8.1.4 Middleware

Chap-ter	Component	Technical specification
5.5	Middleware architecture	▸ J2EE v1.3 ▸ J2SE ▸ Microsoft .NET Framework

8.1.5 Communication

8.1.5.1 Middleware protocols

Chap-ter	Component	Technical specification
5.6.1	Middleware protocols for server-to-server communication	▸ Remote Method Invocation (RMI) ▸ SOAP ▸ WSDL 1.1 (Web Services Description Language) ▸ Extensible Markup Language Schema Definition (XSD) ▸ RMI-IIOP
5.6.1	Middleware protocols for client-to-server communication	▸ WSDL 1.1 (Web Services Description Language) ▸ Extensible Markup Language Schema Definition 1.0 (XSD) ▸ SOAP 1.1 ▸ UDDI 2.0

8.1.5.2 Network protocols

Chap-ter	Component	Technical specification
5.6.2	Internet Protocol	▸ IP v4 (RFC 791) with TCP and UDP ▸ IP v6
5.6.2	Name Services/ Naming Policy	▸ DNS (RFC 1034, RFC 1035, RFC 1591)

8.1.5.3 Application protocols

Chap-ter	Component	Technical specification
5.6.3	File transmission	▸ FTP (RFC 959, RFC 1123, RFC 2228, RFC 2640) File Transfer Protocol ▸ HTTP v1.0 (RFC 1945) and v1.1 (RFC 2616)
5.6.3	E-mail transport	▸ E-mail protocols in conformity with the SMTP/MIME

		specifications for message interchange ▸ POP3/IMAP for electronic mailboxes

8.1.5.4 Directory services

Chap-ter	Component	Technical specification
5.6.4	Directory	▸ LDAP V3 (Lightweighted Access Protocol) for general access to address book resources (according to X.500) (RFC 2251, 2252, 2253, 2256, 2798, 1777, 1823)
5.6.4	Web Service Request Registry	▸ UDDI v1.0 (Universal Description, Discovery and Integration, www.uddi.org)
5.6.4	Directory Services	▸ DSML V2

8.1.6 Connection to the backend

8.1.6.1 Batch processing

Chap-ter	Component	Technical specification
5.7.2	Batch processing	▸ Extensible Markup Language (XML)

8.1.6.2 Program-to-program communication

Chap-ter	Component	Technical specification
5.7.3	Information interchange	▸ Extensible Markup Language (XML)
5.7.3	J2EE Integration	▸ J2EE Connectors, Java Message Service
5.7.3	Data exchange	▸ Web Services
5.7.3	Data exchange	▸ UN/EDIFACT

8.2 Overview of data security standards

Chap-ter	Component	Technical specification
6.2	Security standards for determining protection requirements	▸ German Federal Office for Information Security, IT Baseline Protection manual www.it-grundschutzhandbuch.de ▸ KoopA ADV, Guideline for action for introducing the electronic signature and encryption to public administrations in the administration; new version in preparation ▸ German Federal Office for Information Security, Secure e-government: E-Government Manual, www.e-government-handbuch.de
6.3.1	Secure transmission of web contents and web server authenticity	▸ SSL and TLS ▸ TLS: T. Dierks, C. Allen: The TLS Protocol, Version 1.0, January 1999, RFC 2246, http://www.ietf.org/rfc/rfc2246.txt
6.3.2	Securing e-mail communications	▸ MTT v.2/SPHINX/PKI-1-Verwaltung ▸ TeleTrusT: “MailTrust”, Version 2, March 1999, www.teletrust.de ▸ German Federal Office for Information Security: "Sphinx" publication series, project on methods for the digital signature and encryption http://www.bsi.de/aufgaben/projekte/sphinx/dokument.htm ▸ ISIS-MTT: T7 & Teletrust; Common ISIS-MTT Specification for PKI Applications, Version 1.0.1, 15. November 2001, http://www.t7-isis.de/ISIS-MTT/isis-mtt.html • Part 1: Certificate and CRL Profiles • Part 2: PKI Management, in work • Part 3 Message Formats • Part 4 Operational Protocols (LDAP, OCSP, TSP) • Part 5 Certificate Path Validation • Part 6 Cryptographic Algorithms

		• Part 7 Cryptographic Token Interface
6.3.3	Secure exchange of documents	▸ MTT v.2/SPHINX/PKI-1-Verwaltung ▸ ISIS-MTT ▸ XML Signature: IETF und W3C, RFC 3275, XML-Signature Syntax and Processing, W3C Recommendation, 12 February 2002, http://www.w3.org/TR/xmldsig-core/ und http://www.ietf.org/rfc/rfc3275.txt ▸ XML Encryption: W3C XML Encryption Syntax and Processing., W3C Candidate Recommendation, 04. 03. 2002, http://www.w3.org/TR/xmlenc-core/
6.3.4	Transactions	▸ OSCI-Transport v1.2: OSCI steering group, specification, 7 June 2002, www.osci.de
6.3.5	Web Services	▸ WS-Security: IBM, Microsoft, Verisign: Web Services Security (WS-Security), v1.0, 5 April 2002, http://www-106.ibm.com/developerworks/library/ws-secure/
6.4.2	Security infrastructure integration	▸ ISIS-MTT part 4 (LDAP, OCSP, TSP)
6.4.3	Smartcard integration	▸ ISO/IEC 7816: ISO/IEC, Information Technology - “Identification Cards - Integrated Circuit(s) Cards with Contacts“ ▸ D21 initiative, work group 5
6.4.4	RegTP Encryption algorithms	▸ RegTP, Geeignete Kryptoalgorithmen [Suitable encryption algorithms], http://www.regtp.de/tech_reg_tele/in_06-02-02-00-00_m/03/
6.4.5	Symmetric encryption algorithms	▸ Triple-DES: FIPS 46-3, Data Encryption Standard, October 1999, http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf ▸ IDEA: International Data Encryption Algorithm

		▸ AES: Federal Information Processing Standards (FIPS PUB) 197: Advanced Encryption Standard (AES), November 2001, http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

8.3 Glossary

AES	Advanced Encryption Standard
APEC	Asia-Pacific Economic Cooperation
API	Application Programming Interface
BMI	Bundesministerium des Innern [Federal Ministry of the Interior]
BSI	Bundesamt für Sicherheit in der Informationstechnik [German Federal Office for Information Security]
BVA	Bundesverwaltungsamt [German Office of Administration]
CEN	Comité Européen de Normalisation
CORBA	Common Object Request Broker Architecture
CRL	Certificate Revocation List
CSS	Cascading Style Sheets Language
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Services
DSA	Digital Signature Algorithm
DSML	Directory Services Markup Language
DSS	Digital Signature Standard
ECW	Enhanced Compressed Wavelet
EDI	Electronic Data Interchange
e-GIF	e-Government Interoperability Framework
EIS	Enterprise Information System
ERP	Enterprise Resource Planning
ETSI	European Telecommunications Standards Institute
FTP	File Transfer Protocol
GIF	Graphics Interchange Format

GML	Geography Markup Language
GOSIP	Government Open Systems Interconnection Profile
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
IETF	Internet Engineering Task Force
IIOP	Internet Inter-ORB Protocol
IMKA	Interministerieller Koordinierungsausschuss für die Informationstechnik in der Bundesverwaltung [Inter-ministerial Co-ordination Committee for Information Technology in the Federal Administration]
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
J2EE	Java 2 Enterprise Edition
JAAS	Java Authentication and Authorization Service
JAXP	Java API for XML
JAXR	Java API for XML Registries
JDBC	Java Database Connectivity
JMS	Java Message Service
JTA	Java Transaction API
KBSt	Koordinierungs- und Beratungsstelle der Bundesregierung für Informationstechnik in der Bundesverwaltung im Bundesministerium des Innern [Co-ordination and Advisory Office of the Federal Government for Information Technology in the Federal Administration in the Federal Ministry of the Interior]
KoopA	Kooperationsausschuss ADV Bund/Länder/Kommunaler Bereich [Co-operation Committee for Automatic Data Processing for the Area of the Federal Government, Federal-state Governments, Municipal Administrations]
LDAP	Lightweight Directory Access Protocol
MAC	Message Authentication Code
MIME	Multipurpose Internet Mail Extensions

MPEG	Moving Picture Experts Group
MTT	MailTrusT
OASIS	Organization for the Advancement of Structured Information Standards
OCSP	Online Certificate Status Protocol
OSCI	Online Services Computer Interface
PCA	Policy Certification Authority
PDA	Personal Digital Assistant
PDF	Portable Document Format
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PKIX	IETF Working Group „Public-Key Infrastructure (X.509)“
PNG	Portable Network Graphics
RegTP	Regulierungsbehörde für Telekommunikation und Post [Regulation authority for Telecommunications and Postal Services]
RFC	Request for Comments
RFP	Request for Proposals
RMI	Remote Method Invocation
RPC	Remote Procedure Call
RSA	Rivest, Shamir, Adleman Public Key Encryption
SAGA	Standards und Architekturen für eGovernment-Anwendungen [Standards and Architectures for EGovernment Applications]
SGML	Standard Generalized Markup Language
SHA	Secure Hash Algorithm
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
TIF	Tag 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
VML	Vector Markup Language
W3C	World-Wide-Web Consortium
WAP	Wireless Application Protocol
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