Bundesamt für Sicherheit in der Informationstechnik

E-Government Phase Plan

Phase 4 – “High-Level Design”

This text is a module of the

E-Government Manual

http://www.e-government-handbuch.de

Editorial staff: E-Government Project Team
Federal Office for Information Security (BSI)

Contact details: egov@bsi.bund.de

Contents

Information on this module

Status	BSI contribution
Authors	Dr. Blum (BSI)
Point of contact / contact details	Dr. Blum (BSI), mailto:egov@bsi.bund.de

Amendment History

Date	Name	Change
18.03.2004	Horn	Some changes introduced
08.07.2003	Horn	Editorial revisions
08.12.2002	Horn	Correction of margin notes
16.12.2002	Dr. Hauschild	Integration of recommended changes by the authors of the module “Authentication in E-Government” – further revision to follow in connection with the publication of Phase 5 or 6.
31.10.2002	Dr. Blum	Version 1

© 2002
Federal Office for Information Security BSI
Godesberger Allee 185-189, 53175 Bonn, GERMANY

4 Phase 4 – "High-Level Design"

Summary of the input from Phases 1-3

Process analysis

Following the initialisation of the E-Government Project in Phase 1, Phase 2 is intended to identify the public agency's online-capable services (Activities 2.3 to 2.7). Phase 3 consists of a systematic process analysis, during which the online-capable services are first subdivided into sub-processes at activity level and then combined into groups with identical activity content (e.g. advising, checking, analysing, researching, decision-making). The sequence and logical links between these sub-processes are then visualised in the form of flow diagrams. In particular, the input and output of each sub-process is identified.

Process optimisation

In subsequent stages, the analysis of processes which are critical to the agency is fine-tuned down to the level of work operations (Activity 3.2). Wherever this reveals weaknesses such as long processing times, long waiting times, media discontinuities etc., the corresponding sub-processes are, if possible, optimised in Activity 3.3 in order to increase the efficiency of the workflows.

Assessment of protection requirements

After the e-government-specific assessment of protection requirements (Activity 3.4), the IT security requirements relating to the online services that are to be provided are identified in Activity 3.5. This security analysis provides an important basis for the modelling of the online processes (Activity 3.6). In concrete terms, this stage examines which sub-processes can be linked together through the use of IT in order to form process chains that are as extensively automated as possible and, taken as a whole, provide an online service. Finally, the e-government services that have been modelled in this way are checked for conformity with the legal framework conditions in Activities 3.7 to 3.10, subjected to a cost-benefit analysis and agreed on with all the parties involved.

High-level technical concept

The output from Phase 3 is a high-level technical concept for all the online services that the public agency intends to offer within the e-government framework. In particular, it defines the interfaces both to any online services that are already up and running and to other existing IT procedures.

Objectives of Phase 4

Detailed technical concept

Detailed description of all functions and interfaces

Taking this high-level concept as its input, Phase 4 encompasses the step-by-step development of the detailed technical concept for the projected e-government services. Here it is necessary to further subdivide the sub-processes of an e-government service – identified within a task-related, organisational perspective in Phase 3 – until a level of detail is reached that can be directly transferred to the technical IT solution. This demands a detailed description of all the application's functions and their interactions within the framework of an e-government procedure. Moreover, it is necessary to define and describe in detail the interfaces between the processes.

High-level IT concept

Unlike the detailed IT concept that will be drafted during the subsequent implementation phase, this detailed description of the future e-government application is not as yet formulated in a formal notation but in language that can be understood even by non-specialists. Thus, the detailed technical concept does not contain any program structure plans (for example, in pseudocode or similar) or full database designs. However, it does include technical IT details on, for example, the hardware and software, databases, operating systems and cryptographic components that have to be procured. This part of the overall high-level design is therefore also referred to as the high-level IT concept.

Focus: e-government and security-specific aspects

As many of the activities described in this chapter would also be conducted as part of a "normal" IT project, those aspects that are specific to e-government and security considerations are stressed below. Where more detailed information on "ordinary" IT project management is required, the appropriate specialist literature should be consulted.

Compatibility requirements for the new e-government components

The detailed concept for the implementation of an e-government service should start with a survey of the IT landscape that already exists within the public agency together with any other in-house standards (Activity 4.1). On the one hand, this provides an overview of existing IT components that can be employed within the framework of the new procedure and, on the other, it makes it possible to derive the requirements that the new components must satisfy in terms of compatibility.

Basic components

Alongside the in-house hardware and software, it may also be possible to take over basic components developed elsewhere for the new services. Examples and information relating to the legal basis for such a transfer can be found in the section devoted to Activity 4.2.

Communication channels, authentication, encryption

Activities 4.3 and 4.4 then define suitable communications channels and mechanisms for secure authentication and encryption for the planned e-government services.

Data model, functionality of the application

Security concept

Restructuring the IT landscape

At the heart of the detailed technical concept lie Activities 4.5 to 4.8, in which the data model is first developed (Activity 4.5) and the functionality of the new applications is then defined in detail (Activity 4.6). In accordance with the approach set out above, special attention should be paid to the question of how best to ensure the basic requirements of confidentiality, integrity and availability in the new e-government service through the adoption of appropriate technical and organisational measures (Activity 4.7). These considerations then form the basis for the planning of how the existing IT landscape is to be restructured in order to integrate the new e-government service (Activity 4.8).

Review of the detailed technical concept

This by and large concludes the high-level design work relating to the new IT application itself. Before any further activities are undertaken, the drafted detailed technical concept and the associated high-level IT concept should now be subjected to a critical review. Alongside a check of whether the desired objectives can actually be achieved with this high-level design, this audit also includes an economic feasibility study.

Documentation of the IT security concept

If the result of the review of the overall planning is positive, the organisational and technical security measures defined in Activity 4.7 should be set down in writing in the form of an IT security concept (Activity 4.10). Alongside the documentation of problem management measures and contingency planning, this should also include a cryptographic and firewall concept.

Planning the implementation phase

The approach to be adopted during the implementation phase can then be planned in Activity 4.11. This comprises the creation of flowcharts and the definition of how to handle suggested changes.

Invitation to tender and award of contract

Activity 4.12 then consists of an invitation to tender and the award of the contract for the IT side of the project if this cannot be performed in-house. Alongside the general framework conditions, such as VOL and the Federal Budget Ordinance (BHO), the "Special Contractual Conditions for the Creation of IT Programs" (SCC) or the the revised version of this, the "Extended Contractual Conditions for the Procurement of DP Services" (ECC-IT), are of particular importance here.

Training plan for staff and e-government customers

The high-level design phase (Activity 4.13) should also include a training plan for staff who will subsequently be involved in the provision of e-government services. It may be necessary to specify the corresponding training in the newly developed product as part of the contractual obligations of the external contractor. However, the public agency needs to consider more than just its own staff. Since e-government is based on interaction between public agency and customer, i.e., for example, the public, it is necessary to provide the latter with assistance that will facilitate the use of the system. This can extend from simple operating instructions through the completion of online forms to manuals on installing and operating the plug-ins or special software packages required for the e-government procedure and which customers must first install on their PCs. Attention must also be paid to the implementation of the Accessibility project so that the content is accessible to all members of the public.[1]

Information to all involved parties

In the final activity, Activity 4.14, all the parties affected should be informed about the results of the high-level design phase. A particularly in-depth dialogue should be conducted with the staff representatives in order to assure them that staff interests will be in no way harmed through the introduction of the new e-government service.

Modifications to the Phase Plan

The sequence of the individual activities proposed in this chapter represents a logically constructed proposal which may not necessarily be the most appropriate solution in any given case (depending on the type of e-government project or the specific circumstances of the public agency in question). The intention is not, therefore, to insist that the flowchart be slavishly applied in the presented sequence. Instead, each agency is advised to adapt the proposed sequence as it thinks fit. In some circumstances, it will prove beneficial to conduct certain activities in parallel. In the case of public agencies that do not possess the know-how required to plan the detailed technical concept, Activity 4.12 "Invitation to tender and award of contract" will have to be the first in the sequence. Furthermore, Activity 4.9 (Review of the detailed concept) may make it necessary to repeat earlier activities a number of times (see flowchart below) in order to recursively develop a final concept that can stand up to critical review.

[1] See "Accessible E-Government" module, Chapter 1.

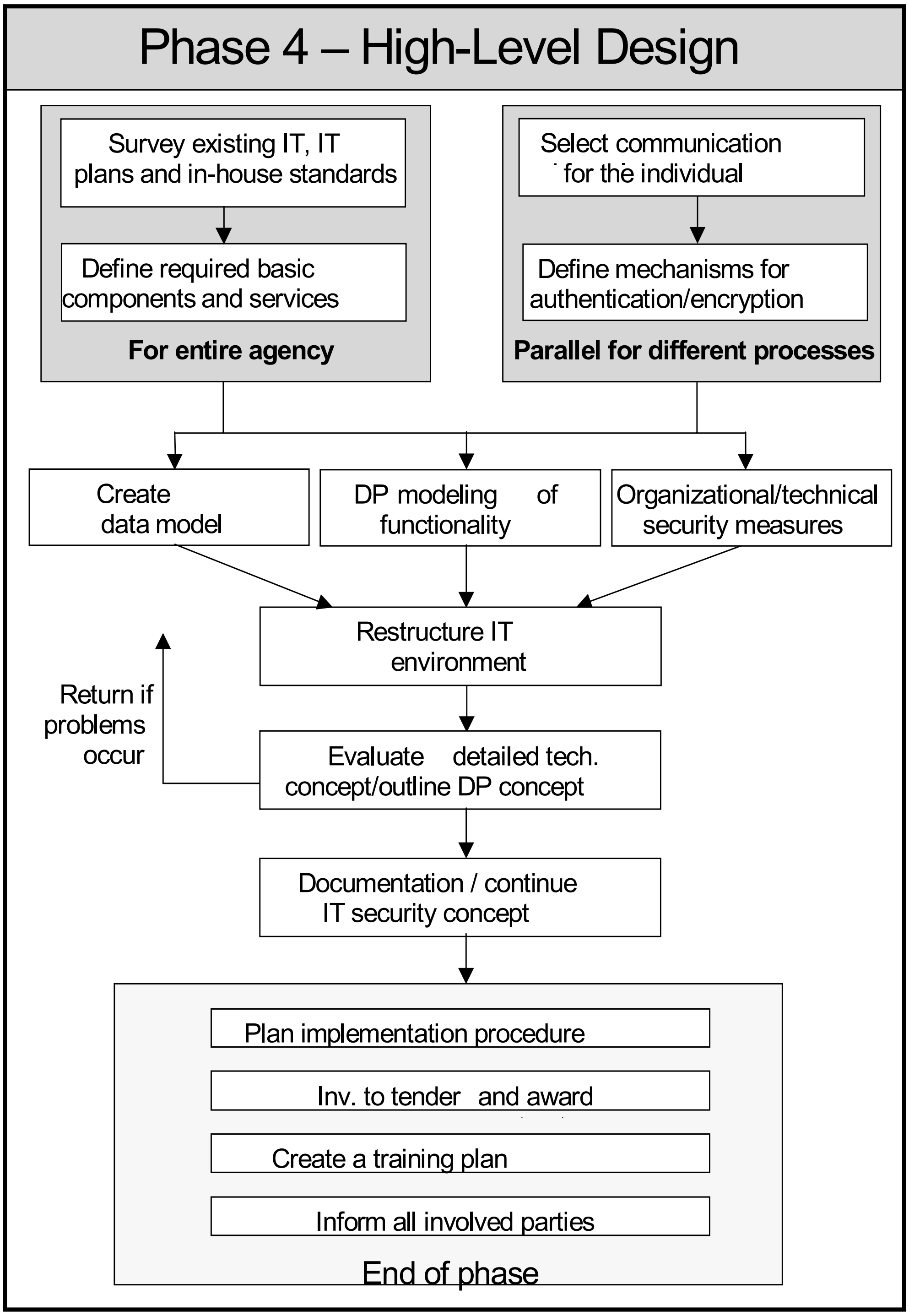
Phase 4 – High-Level Design
Survey existing IT, IT plans and in-house standards
Define required basic components and services
For entire agency
Select communication for the individual
Define mechanisms for authentication/encryption
Parallel for different processes
Create data model
DP modeling of functionality
Organizational/technical security measures
Restructure IT environment
Return if problems occur
Evaluate detailed tech. concept/outline DP concept
Documentation / continue IT security concept
Plan implementation procedure
Inv. to tender and award
Create a training plan
Inform all involved parties
End of phase

Figure 1: Flowchart illustrating Phase 4 – High-level design

4.1 Activity “Surveying the existing IT landscape”

Initiation responsibility: E-Government Team Leader

Implementation responsibility: E-Government Core Team, IT System Administrators, persons responsible for the technical procedure

Consideration of other planned IT activities

The high-level design phase for new e-government services should start with a comprehensive survey of the existing IT systems, applications and in-house standards. It should be noted that other planned IT activities that are independent of e-government will have to be included in order to prevent the duplicated development of system components within one and the same organisation.

This stocktaking process is necessary for the following reasons:

- Cost savings through the exploitation of existing resources
- Time savings through the avoidance of new developments
- Optimum integration of the planned e-government applications in the existing IT landscape.

In addition, the identified information provides an essential basis for the IT security concept which is drafted in Activity 4.10.

IT Structure Analysis

A detailed description of how to proceed when creating this type of overview of the in-house IT environment is provided in section 2.1, “IT Structure Analysis”, of the IT Baseline Protection Manual. Below, we simply outline the most important steps.

Creation of a network plan

Network plan

To gain an initial overview, it is advisable to visualise the existing IT landscape in the form of a graphical network plan[1]. This should contain:

- The servers:domain controllers, communications servers, application servers, database servers etc.
- The client PCs, possibly subdivided on a task basis (e.g. 10 client PCs for Human Resources)
- The network connections between these systems as well as active network components (switches, routers)
- External connections (e.g. internet connection, leased lines to other sites, dial-in access via modem or ISDN)

Alongside the IT systems themselves, the plan should also contain information on the operating systems installed on them.

[1] Unlike in the context of systems analysis, the term “network plan” is not intended here in the sense of a project planning and control tool. Instead, it simply describes the graphical depiction of the topology of a computer network.

A simple example of such a network plan can be seen in Figure 2 below:

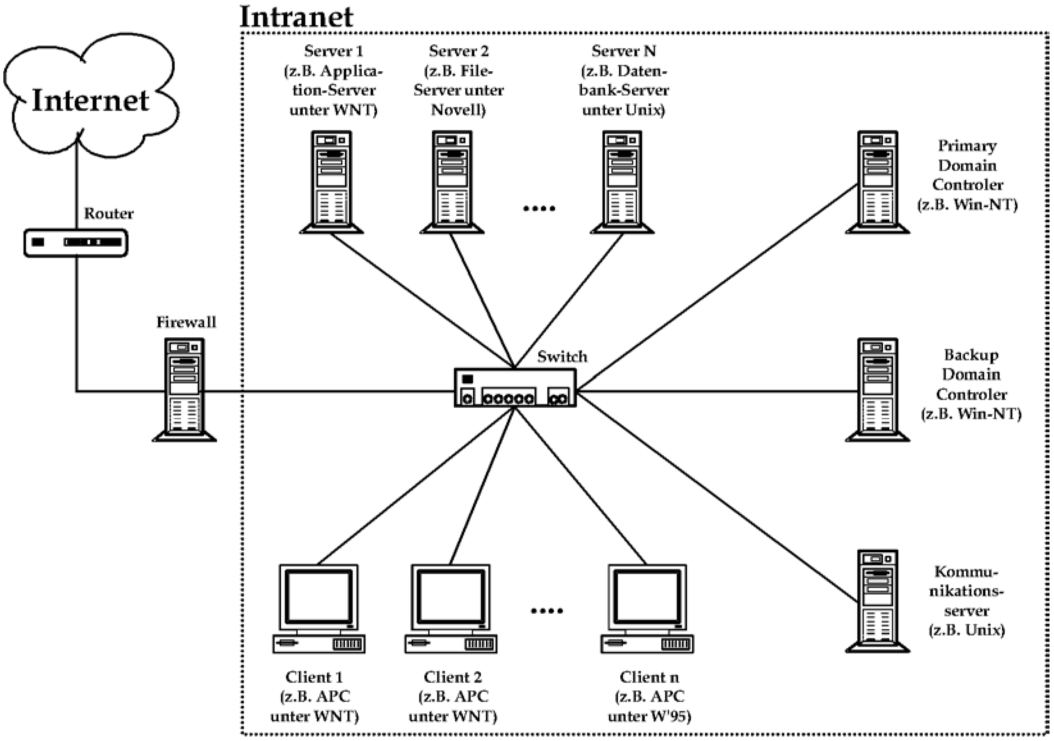
Intranet
Internet
Router
Firewall
Server 1 (z.B. Application-Server unter WNT)
Server 2 (z.B. File-Server unter Novell)
Server N (z.B. Datenbank-Server unter Unix)
Primary Domain Controler (z.B. Win-NT)
Switch
Backup Domain Controler (z.B. Win-NT)
Kommunikations-server (z.B. Unix)
Client 1 (z.B. APC unter WNT)
Client 2 (z.B. APC unter WNT)
Client n (z.B. APC unter W'95)

Figure 2: diagram showing a computer network typical of many government agencies

Summary table of the existing IT systems

Overview of the existing IT landscape

Of course, the network plan can only provide an outline view of the existing IT landscape. In order to provide more detailed information concerning the employed systems, the following properties should be recorded in a table:

- unique name of the IT system
- short description of its type and function
- platform (e.g. hardware architecture/operating system)
- in the case of groups, number of IT systems grouped together
- location of the IT system
- status of the IT system (operational, being tested, planned)
- Anwender/Administrator des IT-Systemsusers/administrator of the IT system

Group creation

When considering the introduction of e-government services it is, of course, not necessary to record every single workstation computer or every single printer here. Instead, it makes more sense to combine the devices into groups in which, for example, multiple clients or even servers which perform the same tasks and are configured in the same way, are grouped together and treated as a single device.

Compatibility of new IT components

The list must be detailed enough to make it possible to plan which of the existing components can be integrated into the new e-government applications and identify those systems that must be procured separately. In the latter case, the list should assist in the decision as to which system types can be most successfully integrated into the existing IT landscape.

Surveying the existing IT environment

Just as important as a precise list of the hardware already present in-house is an overview of the software products and IT applications in use. To conduct this type of survey, it is advisable to conduct interviews with the individuals responsible for the various technical procedures and, for each area of responsibility, to record the

Overview of existing or planned IT applications

- standard software
- special software, subdivided into
  - in-house developments
  - external developments
  - databases
- planned IT applications

employed there. This list should also indicate the assignment of each IT application to the previously recorded IT systems. This must make clear which server and which network components support the application in question.

During the subsequent design of the new e-government services, care must be taken to ensure that these can be integrated with the minimum of difficulty into the existing IT procedures and that they offer the highest possible level of compatibility with these.

4.2 Activity “Definition of the basic components, services and standards to be employed”

Initiation responsibility: E-Government Team Leader

Implementation responsibility: E-Government Core Team, persons responsible for the technical procedure, persons responsible for organisation, IT Security Officer, IT System Administrators, staff representatives

Integration of externally developed basic components

Naturally, the technologies used within the e-government framework do not have to be re-invented in every public agency. The aim of the activities described in the last section was to re-use to the greatest possible extent the hardware and software resources present within the organisation for the provision of the new e-government services. It follows that procedures that have already been developed and become established elsewhere should also be employed wherever possible. The advantage is obvious: by avoiding the need to perform new development work it is possible to save time and money. To this should be added the benefits of increased compatibility and interoperability that accrue when the largest possible number of public agencies use the same products[1].

Model projects

At the start of the high-level design phase, it is therefore advisable to find out where e-government projects similar to those planned in the public agency in question have already been implemented. A collection of model projects is presented in the module “E-Government Model Projects of the BundOnline 2005 Initiative” of the present E-Government Manual as well as on the BundOnline 2005 website at www.bundonline2005.de. The knowledge management offered within the framework of the central co-ordination of BundOnline 2005 by the Federal Ministry of the Interior (BMI) should also be pointed out here.

Kiel decisions

If this research indicates that an e-government application planned in-house has indeed already been developed by another public agency then it is possible to transfer this solution. The legal framework for such operations is provided by the so-called “Kiel decisions” arrived at in 1979 by the “General Data Processing” co-operative committee (KOOPA/ADV) which included representatives of the government, the states and municipal authorities. These specify that IT applications developed within the public service should be made available to other public agencies free of charge on a reciprocal basis (installation and maintenance costs may, however, be invoiced). Further information on the Kiel decisions can be found at this URL:
www.koopa.de/Schwerpunktthemen/Kieler_Beschluesse/kieler_beschluesse.htm.

[1] However, it should also be mentioned here that “technological monocultures” can also have their drawbacks. For example, in such cases a system malfunction may not simply affect individual agencies but large sections of the overall public administration. It is also easier for malicious programs such as viruses or worms to propagate in a homogeneous environment and thus impair the functioning of large numbers of clients.

Another objective of the national E-Government initiative is to commission the development of components that are typically used in e-government applications and then make these available to all public agencies. In some cases, standardised components are already commercially available or can be taken over from the e-commerce sector either unchanged or with slight modifications.

Transferring basic components from the e-commerce sector

The concept of centrally developed basic components which are then made available for use by the public agencies either centrally or locally is presented in detail in the "Implementation Plan for the BundOnline 2005 E-Government Initiative". This document can be downloaded from the BMI website at the address:

Implementation Plan for the BundOnline 2005 E-Government Initiative

http://text.bmi.bund.de/downloadde/16396/download.pdf

A few examples of basic components are presented below:

Virtual mail room

Even in the case of "conventional" communications between the public and the administration, it is not generally helpful for external messages to be personally addressed to individual members of staff within the agency. The responsibilities within an organisation are defined by an internal task allocation plan with which external communication partners are not familiar. The person who is to process an operation is therefore determined within the public agency on the basis of defined rules. This allocation is usually undertaken by a central mail room which opens letters received from the outside of the organisation and then forwards these to the responsible person on the basis of the defined responsibilities In the case of "electronic data traffic", a similar task is performed by the "virtual mail room" in which the necessary tasks are, to the greatest possible extent, performed automatically. The process chain that is worked through here comprises the following steps:

Central reception and forwarding of electronic messages

1. "Open", i.e. decrypt the incoming message if necessary
2. Check the message for malicious software (e.g. viruses)
3. Authenticate the sender, i.e. check the signature if necessary
4. Determine the content of the message
5. Forward to the responsible person
6. If necessary, encrypt, sign and timestamp outgoing messages
7. archivieren der KorrespondenzArchive the correspondence

It is clear that these tasks cannot be automated in the same way for *all* incoming documents. In particular, the fourth step (check of contents) is subject to limitations here. It is therefore useful to subdivide the incoming electronic mail into three categories:

- Completed forms, for example such as those filled in via a form server (see below)
- E-mails which can be clearly assigned on the basis, for example, of a transaction number, reference number or similar

Criteria for the automatic processing of electronic messages

- All other electronic messages sent by customers to the public agency which cannot generally be clearly assigned

In the case of the first and second document categories, forwarding of the message to the responsible person can be easily automated via the virtual mail room. In the case of the third category, messages may be routed on to a connected document management system (see below) which checks the contents on the basis of formal criteria (e.g. identification as invoice, tender or similar). The remaining electronic messages can then only be assigned and forwarded "manually".

The decryption of messages and the verification of the electronic signature also have some problems associated with them. One important reason for performing these tasks in a virtual mail room is that this makes it unnecessary to install a complex key administration solution at every workstation). It also makes it unnecessary for every member of staff to access a directory service themselves in order to check the existence and validity of certificates.

End-to-end encryption

At the same time, it is perfectly conceivable that some of the transactions conducted within a public agency may, for reasons of confidentiality and data privacy protection, make end-to-end encryption between the sender of a message and the person responsible for dealing with it desirable or, indeed, obligatory.

Development project: "virtual mail room" as a basic component

However, in the light of the benefits described above it can be assumed that in most cases the virtual mail room will meet the security requirements for online services. It therefore seems sensible to use the virtual mail room as a basic component and implement end-to-end encryption in individual cases. The virtual mail room is currently being developed as a high-priority basic component under the aegis of the BSI.

Document management system (DMS)

Electronic filing cabinet

As mentioned in the section above, the use of a document management system usefully complements the virtual mail room. Furthermore, a DMS forms the basis for any IT-assisted workflow management. Thus, for example, it makes it possible to press forward with the construction of an "electronic filing cabinet" and get one step closer to the desired reduction of paper in the office. In principle, this electronic filing cabinet can be accessed from any IT workstation and the data is available at all times as an input to other specialist applications without the need for any media discontinuity. It is important here that a suitable concept for the granting of rights is implemented in order to ensure that staff only have access to the data that is intended for them. Many DMSs include a database and therefore permit extensive research and search functions as well as appropriate archiving.

Document management systems, often specially tailored to meet the needs of different types of business process, are marketed by a large number of commercial suppliers. However, when selecting a system, only products certified using the DOMEA concept should be considered. The same criteria as are described in detail in the next section on workflow management systems apply here.

Workflow management systems

A DMS is often an integral part of a more comprehensive workflow management system. This permits the IT-assisted management of workflows which largely eliminates the problem of media discontinuity. First of all, the incoming documents are registered, scanned and then combined to form an electronic dossier. This dossier is then electronically routed to the various stations involved in processing via a channel which is specifically implemented in the system for each business process. This process can be aborted, halted or restarted at any time. Each processing step is logged and instructions, review signatures, comments, action reviews etc. are added to the electronic dossier as required. In this way, the steps involved at any stage within the administrative process for any given operation are documented in a transparent, traceable way.

IT-assisted workflow management with no media discontinuity

It is self-evident that workflow systems must be tailored as precisely as possible to the individual business processes implemented within a public agency. For this reason, it would make no sense to attempt to equip all the agencies with the same workflow management system. Instead, and in accordance with the "Implementation Plan for the BundOnline 2005 E-Government Initiative", the aim is to achieve the greatest possible level of conformity between the various systems on the basis of negotiations with the different product suppliers.

Compatibility of workflow systems

The basis for this takes the form of a catalogue of minimum requirements which workflow management systems must meet in terms of both their functionality (IT-assisted document management, construction of an electronic filing cabinet, workflow management, storage and search functions, archiving) and their compatibility and interoperability with other systems. This catalogue of requirements was drafted as part of the "Paperless Office" concept (DOMEA concept) under the aegis of the "Co-ordination and Advisory Bureau of the Federal Government for Information Technology in the Federal Administration" (KBSt). The document can be downloaded as Volume 53 in the KBSt series of publications from the web address:

DOMEA concept

http://www.kbst.bund.de/domea

In agreement with the "Co-ordinating committee for information technology in the federal administration" (IMKA), KBSt recommends taking this requirements catalogue as a basis for the planning and implementation of any electronic workflow management within the federal administration.

An overview of the certified products and the corresponding test reports will soon be published on the KBSt's website. Furthermore, the Federal Administration Office (BVA) will soon be setting up a Competence Centre which will advise and assist public agencies in the choice, introduction and operation of workflow management systems.

Certified products

Form server

As already mentioned in the section on the virtual mail room, rational, automated, electronically-assisted workflow management which avoids media discontinuities is easiest to implement if the associated data is already present in the formats required for subsequent input into the specialist applications at the time it enters the public agency. Data is available "ready-for-processing" in this way, for example, when it is entered in online forms and then electronically transferred to the public agency. Technically, this can be achieved by using a so-called form server which the public can access externally via the home page or a public agency portal.

The government's Online Form Centre

Since the middle of March 2002, the government has been running a so-called Online Form Centre which can be accessed via the portal www.bund.de. This currently offers visitors approx. 1000 public agency forms. The concept behind this is that, on the one hand, these forms are stored locally on the servers belonging to the individual public agencies (thus simplifying maintenance and minimising the associated costs and effort) while, on the other, the public can also access these forms in a convenient way via the central government portal.

All public agencies are able to use this existing infrastructure for their e-government services.

Payment platform (payment server)

Secure payments via a central government payment server

To enable the secure handling of public agency online services for which fees are payable, an electronic payment platform is required within the e-government framework. Naturally, such a payment system must satisfy very high requirements in terms of both security and availability. Ensuring that these requirements are indeed fulfilled at a very high level demands considerable technical effort. It is not therefore sensible for each public agency to operate its own payment server. Instead, payments should be handled at a central system which must be implemented within an especially secure environment

The German government is currently developing just such a central payment platform. An interface will be available to enable the integration of all decentralised public agency online services, thus ensuring secure, reliable payment operations 24 hours a day.

SAGA

The SAGA paper[1,2]. published as part of the "BundOnline 2005" initiative provides a collection of "Recently developed IT standards, procedures, methods and products for E-Government". This document is intended to help guide decision-makers in the organisational and information technology sectors of the German administration in the high-level design of technological architectures as well as in the high-level technical design of individual IT applications. The aim is to avoid duplication of cost-intensive development work within the public administration through the use of defined standards and architectures. Furthermore, the use of simple, clear standards should make it possible to achieve interoperability of the employed information systems. To this end, three classes of standards have been defined:

[1] SAGA = acronym for "Standards and Architectures for e-Government Applications"

[2] At the time of completion of the present module of the E-Government Manual, Version 0.9 of the SAGA paper was available in draft form. This can be downloaded from http://www.bund.de/BundOnline-2005/Saga-.6431.htm. In the future, it is planned to incorporate the SAGA document as a separate module in the E-Government Manual.

Orientation aid for the high-level design of technological architectures and IT applications

- Obligatory: standards are obligatory if they have proved their value in practice and are the preferred solution. These standards are binding.
- Recommended: standards are recommended if they have proved their worth in practice but are not absolutely necessary, if further harmonisation is required before they can be considered obligatory or if they are not the preferred solution.
- Under consideration: standards are under consideration if they follow the desired line of development but are not yet mature or have not yet been sufficiently proven in practice.

Binding nature of SAGA

SAGA-conformity is fundamentally binding for all processes and systems that provide federal e-government services. In the case of systems that have no direct interface to e-government, migration is recommended if the cost-benefit analysis is positive.

The binding nature of SAGA within the business areas is determined by the federal ministries.

“Basic components” module

A more detailed, substantive discussion of the basic components together with an overview of the public agencies responsible for their provision and a list of the relevant contact persons will be collated in a separate, future module of the E-Government Manual.

4.3 Activity "Selection of suitable communication channels for E-Government services"

Initiation responsibility: E-Government Team Leader

Implementation responsibility: E-Government Core Team, IT Security Officer, persons responsible for the technical procedure, persons responsible for organisation

First and foremost, secure e-government means ensuring the confidentiality, integrity and authenticity of the data exchanged between customer and public agency. This can only be guaranteed if the communication channels via which the data is exchanged are appropriately protected (see Activity 4.4). However, this also presupposes that *suitable* communication channels have been chosen for each e-government procedure.

Online services as a complement to the traditional communication channels

When implementing e-government services it should not, however, be forgotten that the conventional communication channels such as letters, telephone, fax and personal visits to public agencies by citizens will continue to exist. As set out in the "BundOnline 2005" initiative, the new online services represent an *additional* facility available to those customers who possess the basic know-how required for electronic communications together with the appropriate equipment (PC with internet connection). The challenge here is to combine the "new" and "conventional" communication channels and integrate these within uniform administrative processes.

Web applications

Ergonomically designed input forms

All provided e-government services should be designed in such a way that the data exchanged between the customer and the public agency is as structured as possible. In principle, "conventional administrative processes" pursue the same aim since, here too, information is exchanged via forms wherever possible. Unfortunately, printed forms are viewed by the public as the "incarnation of bureaucracy" and therefore arouse a negative image. Here, however, electronic forms have a considerable advantage: because they allow far more freedom in terms of their functional design than is possible with paper forms, they can be made much easier for users to handle in ways which increase their acceptance. For example, they may possess direct input aids, plausibility checks of the entered data and so on. However, it is important here to exploit the technical possibilities. It is not enough simply to transfer the printed appearance of the paper form element-by-element to the electronic input form.

Consequently, any consideration of the issues of communications and data transfer within e-government services should start with an examination of all the ways in which procedures can be implemented on the basis of electronic forms. Wherever possible, it is advisable to perform communications via a web-based application. Customers enter their data in an electronic input form connected to the agency's form server (see section 4.2). Skilful user guidance can make this process very much easier for users than the often cumbersome and time-consuming task of completing a paper form. Thus, for example, the data can be queried in a dialogue using questions which are comprehensible for “everyday citizens”. A plausibility check can be performed to inform users immediately of any obvious inconsistencies in their responses and allow them to correct errors straightaway. This does away with the need to re-contact the user with queries and accelerates processing. Quite apart from the time saved due to the elimination of bureaucratic processes, this procedure also has the advantage of offering customers a more user-friendly way of submitting their forms.

XML files for the automated further processing of data

From the public agency’s point of view, the advantage of this communication channel lies in the fact that the incoming data, e.g. as received by a virtual mail room (see Section 4.2), can be automatically identified and immediately read in to a workflow management system. If, for example, the web application works with XML[1], then it is a simple matter to transfer the data in different formats for further processing. Thus when it is necessary for public agencies and private companies to communicate, for example in the case of invitations to tender, it is a simple matter to convert XML data to EDI[2]- format which is commonly used for order processing. Furthermore, this procedure is relatively easy to merge with the traditional processing of printed forms: during an intermediate stage, the data must be converted into electronic form either manually or, wherever possible, by means of scanning.

Encryption of communication

In principle, it is a relatively simple task to ensure the confidentiality of communications using established technologies. The latest versions of the most commonly used internet browsers are able to work with the current SSLv3.0[3] protocol. This makes possible encrypted communications for web applications based on powerful cryptographic procedures which guarantee an adequate level of security (for a more detailed description, see section 4.4).

Server and client authentication

Reciprocal authentication between server and customer poses a greater problem. Citizens want to be certain that they are actually entrusting their confidential data to the public agency’s server and not to a so-called “man in the middle”, i.e. someone who simply pretends to possess the public agency identity in order to acquire confidential information. In order to prevent this so-called “spoofing”, the server requires a certificate from an authority that is trusted by the customer in question. Such certificates can, for example, be provided by the administration PKI which is co-ordinated by the BSI. When an SSL connection is established between client and server, the so-called “SSL handshake”, the server sends its certificate to the client whose browser then checks whether it is trustworthy. If the result of this check is positive, the customer can be certain that he or she is

[1] In simple terms, XML (abbreviation for “E**X**tensible **M**arkup **L**anguage”) is an extension of the HTML (abbreviation for “**H**yper**T**ext **M**arkup **L**anguage”) standardised programming language for the development of web pages. XML is especially well suited for data transfer. This can be presented very flexibly in specific formats on the basis of rules that can be freely defined by the programmer. (e.g. in the form of tables) and thus be used as the input for downstream processing software.

[2] EDI (abbreviation for “**E**lectronic **D**ata **I**nterchange”) is a standard that has been in use since the late 1980s for the electronic transfer of order data between business partners (for example, it is extensively used for “just-in-time” orders).

[3] SSL stands for “**S**ecure **S**ocket **L**ayer”.

actually connected to the public agency's server. As of Version 3.0, the client can also authenticate itself to the server within the framework of the SSL protocol provided that the client also possesses a valid certificate issued by a certification authority which is trusted by the server.

Despite the fact that the SSLv3.0 protocol permits reciprocal authentication, identification of the customer remains particularly problematic. The reliability of the procedure described here is crucially dependent on whether both client and server are located within a secure environment, whether the certificates and private keys are securely stored etc. While, as far the public agency is concerned, all the necessary measures can be taken at the server to ensure that the security requirements are met, it has no control over the client side circumstances.

Electronic signature

If the administrative procedures that are to be performed using the web application are subject to procedural requirements, then the citizen must be authenticated by means of a qualified electronic signature in accordance with the Digital Signatures Act. However, this requires a not insubstantial client side technical configuration (smartcard, reader) which adds to the customer's costs accordingly.

Since solutions that make use of qualified electronic signatures are still relatively expensive because of the equipment required[1], it is necessary when introducing online services, to consider abandoning the requirement for media continuity or to slightly reduce the confidentiality requirements relating to electronic documents – even if only for a transitional period.

Thus, for example, in the ELSTER[2] procedure for electronic tax returns which is currently employed, the form and the data it contains are transmitted electronically to the financial authorities. However, the personal signature which is required in order to give the return binding legal force is supplied on a paper print-out which is then sent to the tax authorities by conventional mail. On the one hand, this media discontinuity makes it possible to comply with the requirement for tax returns to be legally binding for relatively little additional effort while, on the other, workflow management itself is fully automated. Both the citizen and the financial authorities benefit in equal measure from this procedure. The former because his or her tax returns are processed more quickly and an assessment can be expected more rapidly and the latter because of the rationalisation achieved through the elimination of the need to enter the data manually. For more information on ELSTER, see the module "E-Government Model Projects of the BundOnline 2005 Initiative" which forms part of the current E-Government Manual.

Pragmatic approaches to solutions

The other path, which consists of doing without qualified electronic signatures wherever these are not absolutely necessary, is the one that is adopted by the Federal Administration Office (BVA) with its service "Bafög-Online"[3] for the collection and administration of loans for students in higher education within the framework of the Federal Education and Training Assistance Act (BAföG). On

[1] A situation which will very probably change as the use of electronic signatures becomes more widespread and the number of manufactured devices increases.

[2] ELSTER stands for "**El**ektronische **St**eu**er**klärung" (=electronic tax return).

[3] http://www.bva.bund.de/aufgaben/bafoeg/antraege/index.html

this internet page, the BVA provides former beneficiaries of BAföG loans with a range of online forms which they can use, for example, to apply to make a premature repayment of the sums owing or to request a partial or full exemption from repayment of their loans. Because the data is transferred via SSL, confidentiality is ensured. However, the authenticity of the sender is not confirmed by any signature and it is only therefore possible to check the plausibility of the data content. This is clearly perfectly sufficient for the intended purpose. Declarations with legal force, such as an objection against a repayment ruling, still have to be lodged in writing. For the majority of communications between the BVA and former BAföG beneficiaries, the online data transfer procedure via a form server with SSL encryption is perfectly satisfactory in terms of the security it offers. In this way, it was possible to create the potential for considerable rationalisation without having to expend any unjustifiably large effort in order to ensure authenticity. Further information on "BAföG-Online" can also be found in the module "E-Government Model Projects of the BundOnline 2005 Initiative".

E-mail

In a number of e-government applications, it will not be possible to perform workflow management on the basis of forms. One example here is the question of legal correspondence: Statements sent by citizens and lawyers to the courts may relate to a wide range of different matters and may therefore be constructed in so many different ways that it would serve little purpose to attempt to replicate them as forms[1]. E-mail[2] correspondence may also be used as an alternative communication channel in such cases.

Standards for e-mail encryption and authentication

As far as the public agency is concerned, the provision of e-mail access is usually the simplest way, in technical terms, of creating a channel for communication with the public. In Mail-Trust V2 (MTT), which deals with encryption, and ISIS-MTT, which is devoted to authentication, we have two standards which form the basis for secure e-mail communication (see Activity 4.4) in accordance with the "Implementation Plan for the BundOnline 2005 E-Government Initiative" (see Activity 4.2).

Establishing an e-mail access

In this way, it is relatively easy to guarantee the secure transfer of messages from the public to the public agency. However, some problems arise in connection with communication in the opposite direction. At least in the case of official documents whose date of delivery may set a deadline, legally binding e-mail access must previously have been established by the member of the public concerned. Whereas in "normal" correspondence, the address of the place of residence represents a clear point of access for postal delivery, this is not necessarily the case when electronic communication is used. Even if the person possesses an electronic mail

[1] Of course, this does not mean that it is necessary to do completely without form-based workflow management here. On the contrary, the field of legal correspondence comprises many procedures which can benefit greatly from the use of form-based processing. Thus, for example, in several German states the introduction of form-based collection procedures is already a possibility.

[2] In the discussion that follows, the term "e-mail" is understood to mean the transfer of messages using the SMTP protocol (abbreviation for **S**imple **M**ail **T**ransfer **P**rotocol).

box, the public agency cannot simply use this as the delivery address for official decisions.

Administrative procedures and the Law on Service in Administrative Procedure

There is as yet no clear answer to the question of what conditions must obtain before electronic communications have been "established" in a legally binding way. The legislature intends to come to a definitive decision on this matter in the form of amendments to the laws governing administration procedures and the delivery of administrative correspondence (Administrative Procedures Act, Law on Service in Administrative Procedure).

Closed user group

While e-mail communications between public agencies and the public continue to present certain problems for the reasons mentioned above, no such restrictions apply to the delivery of electronic documents from one public agency to another or between a public agency and a "closed user group". In this case, the absence of legal regulations is not a problem since the parties can come to an agreement in which each provides a binding e-mail address. Taking the above example of electronic legal correspondence, the "closed user group" could, for example, consist of the lawyers who are licensed to practise before the court. As individuals who are responsible for the administration of justice, lawyers are naturally already subject to additional, legally defined obligations concerning due care and diligence from which, in particular, the binding nature of any e-mail access given to the court as a delivery address can be derived.

As an alternative to sending decisions directly to the citizen's e-mail address, it is also possible to set up electronic mail boxes on the public agency's server. To this end, it would be possible to stipulate, for example, that such a mail box be assigned to an applicant the first time he or she contacts the agency. The applicant would then have to undertake to check the mail box at defined intervals. This would ensure that when a decision is delivered to the assigned mail box, the electronic document comes under the citizen's control. This could then be defined as the time of delivery as is currently the case with conventional mail.

4.4 Activity "Concrete definition of the protective mechanisms for authentication and encryption"

Initiation responsibility: E-Government Team Leader

Implementation responsibility: E-Government Core Team, IT Security Officer, IT System Administrators

Adaptation of cryptographic standards to technological development

Following the definition of the communication channels for the various e-government services, which was the subject of the last activity, it is now possible to develop a more concrete specification of the mechanisms necessary to protect this communication. However, it should be pointed out here that developments in the field of cryptographic methods, as in the IT world generally, are constantly changing. Thus "standards", such as "SSL" for example, have only a very limited lifetime and must constantly be adapted to the current state-of-the-art. Consequently, wherever such standards are referred to below, they must always be considered to represent a minimum requirement. As a result, in each individual case it is necessary to check whether these requirements still correspond to the state-of-the-art and whether the procedures are appropriate for the task in question.

The security requirements identified in Activity 3.5 form the basis for the choice of technical protection mechanisms. There are a number of different ways in which they can be implemented. Examples of these are presented below: A more detailed examination is undertaken in the modules "Encryption and Digital Signatures" and "Authentication in E-Government". The "Authentication in E-Government" module also serves as a guideline for the identification of the authentication mechanisms that are appropriate for a given technical procedure.

Protection goal: confidentiality

- Protection requirements "basic" or "moderate":
  - Web application as communication channel: no encryption or SSLv3.0[1]
  - E-mail as communication channel: no encryption or encryption in accordance with the S/MIME standard[1]

Protection goal: confidentiality

- Protection requirements "high" or "very high"
  - Web application as communication channel: encryption using at least SSLv3.0 is an essential requirement
  - E-mail as communication channel: encryption using at least the S/MIME standard is an essential requirement

[1] For information on the SSLv3.0 and S/MIME specifications, see reference [1] at the end of this section.

Protection goal: authenticity

Protection requirements: citizen's authenticity

- Authenticity of customer applications (input):
  - No protection requirements regarding authenticity:
    - Web application as communication channel: client does not need to authenticate itself to the server
    - E-mail as communication channel: no authentication necessary.
  - Protection requirements regarding authenticity are "basic":
    - Web application as communication channel: authentication of customer through specification in an online form is sufficient, e.g. specification of an e-mail or postal address
    - E-mail as communication channel: authentication of customer on the basis of the e-mail address is sufficient
  - Protection requirements regarding authenticity are "moderate":
    - Web application as communication channel: authentication of customer by means of a secret specification in an online form is sufficient, e.g. specification of a password
    - E-mail as communication channel: authentication of documents created by the customer by means of an advanced electronic signature
  - Protection requirements regarding authenticity are "high":
    - Web application as communication channel: authentication of documents created by the customer by means of a qualified electronic signature[1]. Technically, this can be implemented using a signature application component with the capabilities set out in Section17, para 2, Digital Signature Act[2] and Section15 Digital Signature Ordinance[2].
    - E-mail as communication channel: authentication of documents created by the customer by means of a qualified electronic signature, similar to the procedure for web applications.
  - Protection requirements regarding authenticity are "very high":

[1] This explicitly refers to ensuring the confidentiality of a document created by the customer (e.g. a completed online form). However, if an authentication is required from customers before they can use the web application itself then the signature key should **not** be used for this purpose. If necessary, a separate authentication key should be used instead. Since the signature key serves a specific legal purpose (Section 2, para. 4, SigG), it should only be used in the corresponding, precisely delineated circumstances.

[2] The texts of the Digital Signatures Act (SigG) and the Digital Signatures Ordinance (SigV) form part of this manual. The conformity of a product to these legal requirements must be guaranteed in writing by the manufacturer (manufacturer's declaration). It is not therefore the task of those responsible for implementing E-Government to check whether the technical implementation of each employed application component complies with the requirements of SigG and SigV.

Currently there is no way of implementing an adequate electronic procedure for such protection requirements.

- Authenticity of the public agency (input)
  - Protection requirements regarding the authenticity of the public agency as recipient are "basic":
    - Web application as communication channel: the authenticity of the public agency is established on the basis of the public agency server's generally known web address (or IP address)
    - E-mail as communication channel: authenticity is established on the basis of the public agency's generally known e-mail address or on the basis of the domain name (e.g. @...bund.de)
  - Protection requirements regarding the authenticity of the public agency as recipient are "moderate":
    - Web application as communication channel: server authentication via SSLv3.0 protocol with X.509 certificate from a registration authority with a defined security level similar to that provided by the public service PKI
    - E-mail as communication channel: for customers to be sure that their data can only be read by the public agency's staff, they require a public encryption key from the agency, coupled with an X.509 certificate from a registration authority with a defined security level similar to that provided by the public service PKI. This can, for example, be made available to the public via the public agency's web server.
  - Protection requirements regarding the authenticity of the public agency as recipient are "high":

Protection requirements: authenticity of the agency

    - Web application as communication channel: server authentication via the SSLv3.0 protocol with X.509 certificate from a trusted certification authority; the server must provide the powerful mechanisms described in [1], section 5.2.1.
    - E-mail as communication channel: for customers to be sure that their confidential data (e.g. electronic tax return) can only be read by the staff of the public agency, they require the agency's public encryption key together with an X.509 certificate from a trusted certification authority. This can, for example, be made available to the public via the public agency's web server.
  - Protection requirements regarding the authenticity of the public agency as recipient are "very high":

    Currently there is no way of implementing an adequate electronic procedure for such protection requirements.
- Authenticity of the service provided by the public agency (output)
  - Protection requirements regarding the authenticity of the public agency service are "basic":

Protection requirements: authenticity of the agency

  - Web application as communication channel: the authenticity of the public agency is established on the basis of the public agency server's generally known web address (or IP address) from which customers can download forms and other material made available on the web.
  - E-mail as communication channel: in the case of notifications which do not involve forms from the public agency to a customer, the agency's authenticity is established on the basis of its generally known e-mail address or on the basis of the domain name (e.g. @...bund.de)

- Protection requirements regarding the authenticity of the public agency service are "moderate":
  - Web application as communication channel: the authenticity of the public agency is established on the basis of the public agency server's generally known web address (or IP address) which is accompanied by an X.509 certificate from a registration authority with a defined security level similar to that provided by the public service PKI.
  - E-mail as communication channel: in the case of notifications sent to the customer by the public agency, the agency's authenticity is established on the basis of a signed e-mail; the corresponding certificate must have been issued by a registration authority with a defined security level similar to that provided by the public service PKI.
- Protection requirements regarding the authenticity of the public agency service are "high":
  - Web application as communication channel: it is extremely unlikely that this channel would ever be used to deliver official decisions[1].
  - E-mail as communication channel: documents issued by the public agency, such as decisions, must be accompanied by a qualified electronic signature.
- Protection requirements regarding authenticity are "very high":

  Currently there is no way of implementing an adequate electronic procedure for such protection requirements.

[1] One possible technical solution would be the use of a "decision server" from which it would be possible to download the qualified, signed document after authentication.

- Authenticity of the customer (output)
  - Protection requirements regarding authenticity are “basic”:
    - Web application as communication channel: Customers can, for example, download information or forms made available by the public agency from the server after entering a password.
    - E-mail as communication channel: the public agency sends messages (e.g. information material) to the e-mail address that the customer has already notified to it.
  - Protection requirements regarding authenticity are “moderate”:
    - Web application as communication channel: customers can, for example, call a service made available by the public agency from the server after entering a PIN or a TAN.
    - E-mail as communication channel: the public agency sends messages (e.g. the requested service) in an e-mail. If the public agency is to be certain that only the authorised customer can read these messages, it requires a public encryption key from the customer, coupled with an X.509 certificate from a registration authority with a defined security level similar to that provided by the public service PKI. The customer can also send this public key to the public agency via e-mail.
  - Protection requirements regarding the authenticity of the customer as recipient are “high”:
    - Web application as communication channel: it is extremely unlikely that this channel would ever be used to deliver official decisions.
    - E-mail as communication channel: if the public agency is to be certain that a decision, for example, can only be read by the person for whom it is intended, it requires this person’s public encryption key together with an X.509 certificate from a trusted certification authority. The customer can also send this public key to the public agency via e-mail.
  - Protection requirements regarding the authenticity of the customer as recipient are “very high”:

    Currently there is no way of implementing an adequate electronic procedure for such protection requirements.

Protection requirements: citizen’s authenticity

Reference to cryptography in e-government

[1] The specifications relating to the cryptographic standards referred to in this section can be found in the module “Cryptography on the Internet” which forms part of the current E-Government Manual. The module can also be downloaded online from the BSI’s website at the URL:

http://www.bsi.bund.de/fachthem/egov/download/4_Krypto.pdf

For information on SSLv3.0, see section 5.2.1

For information on S/MIME, see section 8.1.4

4.5 Activity “Creating the data model”

Initiation responsibility: E-Government Team Leader

Implementation responsibility: E-Government Core Team, IT specialists, persons responsible for the technical procedure, IT Security Officer

After the communication channels for e-government services have been defined in Activity 4.3 and the protection mechanisms to be used for the transferred data have been given a concrete definition in Activity 4.4, these elements should now be categorised and mapped to a data model. Within the technical DP implementation of the e-government procedure, this data model forms both the basis both for the programming of the user interface (front-end) and for the underlying database structure (back-end). Given the variety of tasks addressed by different e-government services, the individual data models may differ greatly. It is therefore only possible to provide a few general comments on their design here.

Data catalogue

Data dictionary

The data catalogue (often also referred to as the data lexicon or data dictionary) contains all the data that accrues during the conduct of the technical procedure. The data stock is described on the basis of its content and format and is subdivided to eliminate any ambiguity. The criteria for this categorisation could be, for example:

- Data name and specialist designation (not the technical IT name; this is defined later by the programmer) to provide a unique identification
- Precise description of the contents of the data (e.g. “Name of applicant”) to distinguish it from other data (e.g. “Name of the responsible person in the public agency”)
- Description of the data format (e.g. “alphanumerical”)
- Specification of the data length (e.g. “maximum 255 characters”)
- Specification of the range of values (e.g. “[-0.999999*10^6, +0.999999*10^6]”)

Data structure

Entity-Relationship Model

Neben der inhaltlichen und formalen Beschreibung sind für die spätere Konzeption der Datenbanken im Rahmen des DV-Feinkonzeptes vor allem die Beziehungen und Abhängigkeiten zwischen den Daten von besonderer Bedeutung.Alongside the description of the contents and format of the data, the relations and dependencies between the data entities are of particular importance for the subsequent high-level design of the database as part of the detailed implementation concept. Um diese zu ermitteln, sollte zunächst eine möglichst detaillierte Kategorisierung der Daten nach ihrer Bedeutung im Rahmen des Fachverfahrens vorgenommen werden.To identify these aspects, the next step is to perform as detailed as possible a categorisation of the data in the light of its significance for the technical procedure. Eine formale Methode, diese Kategorisierung in geeigneter Weise durchzuführen, bietet das „Gegenstands-

Beziehungs-Modell“ (Entity-Relationship-Model, abgekürzt ERM), aus welchem sich später relativ einfach die konkrete Datenbankstruktur ableiten lässt.One formal method that is suitable for performing such a categorisation is the “Entity-Relationship Model (or ERM) from which it is subsequently relatively easy to derive the concrete database structure. Wie der Name schon sagt, unterscheidet dieses Modell zwischen Gegenständen (Entitäten, entities) als eindeutig unterscheidbaren und gegenüber anderen Gegenständen abgegrenzten Elementen eines Geschäftsprozesses sowie Beziehungen (Relationen, relationships), welche die Gegenstände miteinander verknüpfen.As the name suggests, this model differentiates between entities (objects), i.e. uniquely identifiable elements within a business process that are separate from any other elements, and relations which link these entities. Den Gegenständen und Beziehungen werden Eigenschaften (Attribute) zugeordnet, die diese in eindeutiger Weise charakterisieren.The entities and relations are assigned attributes which uniquely characterise them. Ein einfaches Beispiel eines Entity-Relationship-Diagramms ist in Abb. 3 für den Geschäftsprozess „Bürger stellt Antrag“ dargestellt.A simple example of an Entity-Relationship Diagram is presented in Figure 3 for the business process “Citizen submits Application”.

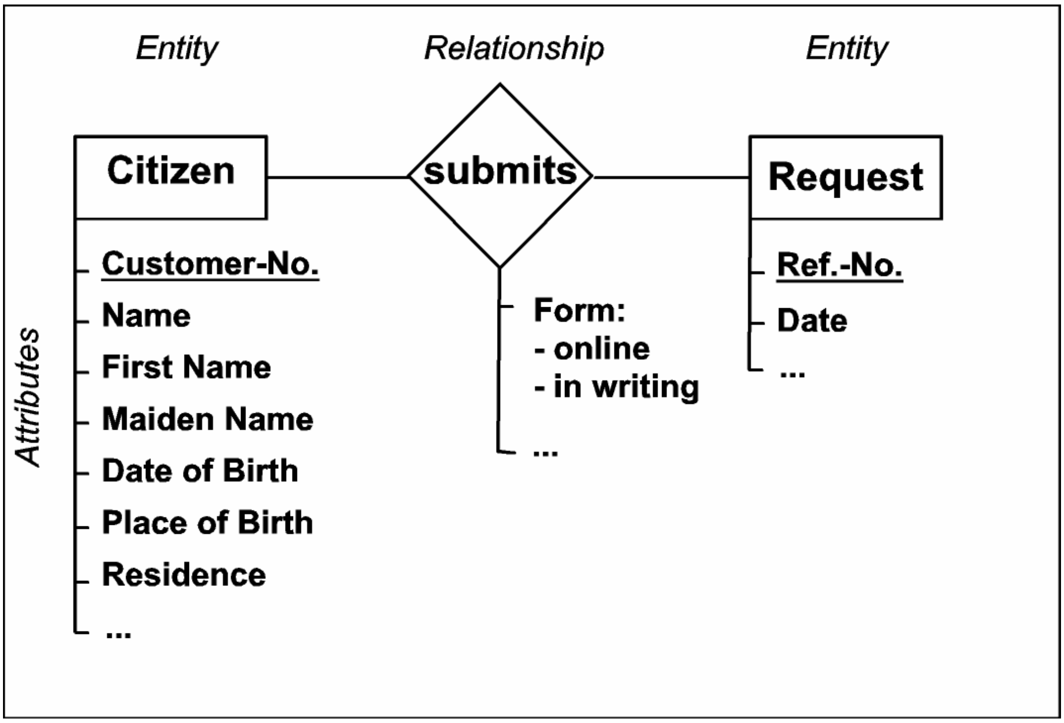

Figure 3: Entity-Relationship Diagram using the simple example of an application.

Here, the entities “Citizen” and “Application” are linked by the relationship “Submission”. This submission can be made in writing or online and the form of the application is noted in the attribute.

Key attributes

In the example, those attributes which *uniquely* identify an entity within one and the same set of objects are specially emphasised. These are known as key attributes. In the example above, a specific citizen within the entity set “Citizens” can be uniquely identified on the basis of the customer number. The name would be unsuitable as such an identification criterion since if two citizens have the same name they can no longer be uniquely identified. If necessary, uniqueness could be restored by combining several attributes, such as name, date of birth and place of birth, to form a so-called composite key. This type of key which is highly informative as to the content of the item to which it refers has the advantage of simplifying database searches. The disadvantage compared to "abstract" key systems which, like the customer number, consist of randomly generated figures, is that a very small risk of ambiguity persists even when multiple attributes are combined. Even more serious effects can arise in the case of key systems which are not generated automatically if it is not possible to be absolutely certain of the integrity of the data. A typing error in one of the key attributes can mean that the record can no longer be located.

Uniqueness of keys

When creating the data model as part of the detailed technical or high-level IT concept, special attention should be paid to the selection of the characteristics that are suitable for the identification of records, i.e. of the key system. Since, in this case, the most important control characteristics of the technical procedure are taken over directly into the database design and IT implementation of the e-government service, particularly close co-operation between technical managers and DP planners is necessary here. Any mistakes that are made at this stage can only be eliminated subsequently through far-reaching, time and cost-intensive interventions in the overall procedures and often prove to be a severe long-term burden handicapping the entire project.

Data flow

Database design

Data flow diagram

If the e-government service is expected to generate large quantities of data then an attempt should be made during the implementation design stage to obtain a realistic assessment of the data flows. A graphical visualisation using a data flow diagram may prove particularly valuable here. This should make it possible to identify the

- sources
- destinations
- branches

of the data flows. Moreover, these should be specified on the basis of the

- data volumes
- times of occurrence (are certain peak values expected at given times?)
- processing times

involved. This information is important for the IT planners if they are to configure capacities correctly when selecting the technical equipment.

Role and access right concept

The data model must also define which functional positions (roles) are to be authorised to access which data. However, we shall not discuss this question here but postpone our examination until Activity 4.7 "Organisational and technical security measures".

4.6 Activity “IT modelling of the functionality”

Initiation responsibility:	E-Government Team Leader
Implementation responsibility:	E-Government Core Team, IT specialists, persons responsible for the technical procedure, IT Security Officer

In Activity 3.1, the online-capable services were systematically analysed in order to record the relevant process information. The corresponding technical processes were subdivided into sub-processes and analysed down to activity level. The chain of sub-processes that was identified in this way was then visualised in the form of a flowchart. In the activity that is presented below, this process chain serves as the input for the IT modelling of the online service which, in the subsequent implementation phase, is used by the programmer to create the source code that represents the IT implementation of the model.

Process execution and structure

Subdivision of the process chain

Generally speaking, the sub-processes that result from Phase 3 are still insufficiently detailed to permit direct IT implementation. For this reason, the sub-processes must first be subdivided in greater detail. If such a sub-process exists within the framework of an e-government procedure – for example in the submission of an application by a citizen (see also the corresponding example for the Entity-Relationship-Model in Figure 3), then the granularity of the process chain can be successively refined in the following iteration as illustrated in Figure 4.

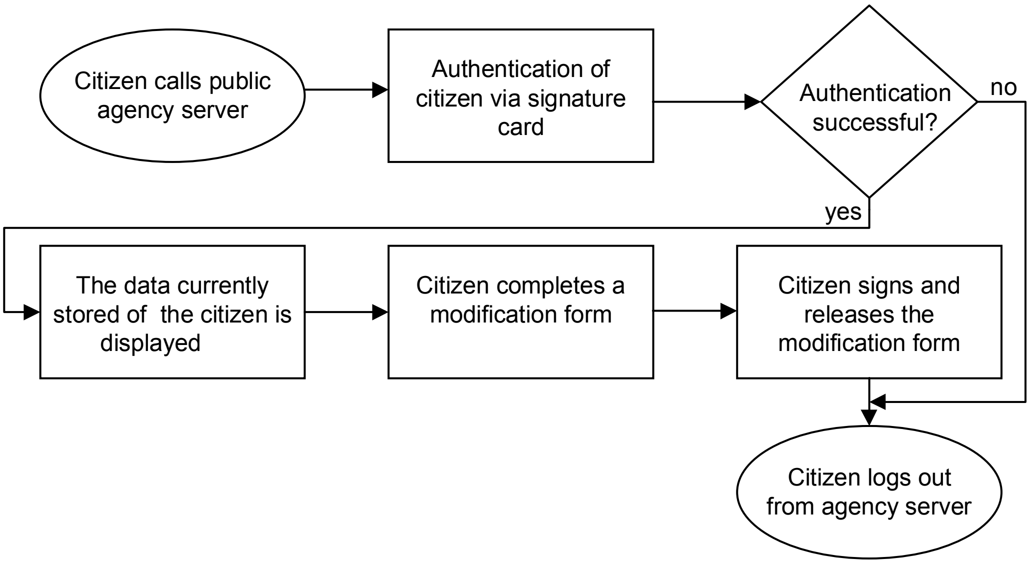
Citizen calls public agency server
Authentication of citizen via signature card
Authentication successful?
no
yes
The data currently stored of the citizen is displayed
Citizen completes a modification form
Citizen signs and releases the modification form
Citizen logs out from agency server

Figure 4: example of how sub-process “Request for modification” is further subdivided

This (sub-)process chain now possesses a level of detail which already permits the transition of sub-tasks, such as the display and processing of customer data, to the next stage of IT modelling, namely the design of the corresponding forms and editing screens (see below).

Depiction of the sub-processes in sequence diagrams

In contrast, the sub-process “Authentication” still needs to be specified in greater detail since, alongside simple processing steps, it also contains control elements and an additional interface to an external trust centre. Graphical visualisation here is best achieved by means of a sequence diagram. This describes the temporal sequence of the interactions between different objects (comparable to the entities in the Entity-Relationship Diagram) within the framework of the temporally delineated execution of a process. The broken lines below the objects “Client”, “Server” and “Trust Centre” in Figure 5 delineate the time axis.

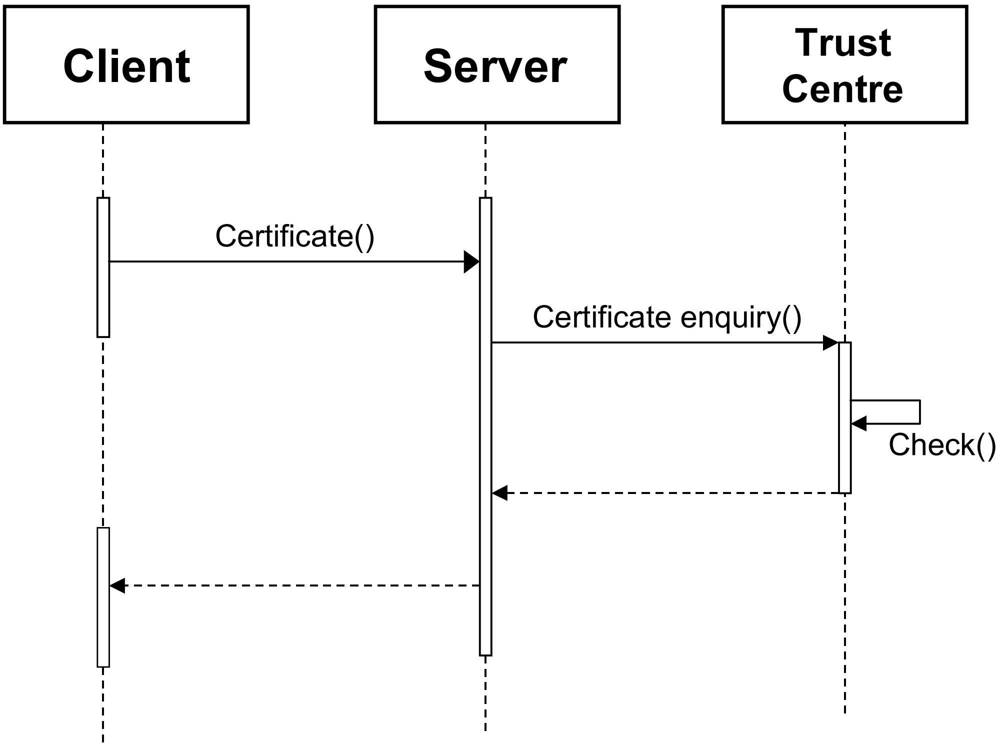

Figure 5: Presentation of the execution of an authentication process in the form of sequence diagram. The client (citizen) sends the certificate to the server (public agency). This then queries the certificate at the Trust Centre. This checks the certificate and returns the result to the server. Depending on the result, the server either continues the session with the client or terminates it with an error message.

If one object is communicating with another then a bar is drawn on its time axis. Messages exchanged between the objects and the corresponding responses are indicated by solid or broken arrows.

Subdivision down to elementary process level

The iterative refinement of the process chain must be continued until, finally, the so-called elementary processes, which represent self-contained, logical units, are identified. In particular, in their internal operation these should be independent of the internal operations involved in other elementary processes. The structuring of the process is complete when

- the technically formulated elementary processes can be used directly as the basis for subsequent modular programming.
- the processing and control steps are clearly separated from one another.
- the interfaces are clearly defined.

Interfaces

Identification and description of the interfaces

As mentioned above, it is essential that all the interfaces between the components have been uniquely identified and described before the IT implementation of the technical process can be carried out. In particular, this type of interface analysis comprises the following:

- Communication interfaces between clients and servers via the internet (e.g. between the customer's PC and the public agency's server)
- Communication interfaces in the public agency's internal network (e.g. between the application server and the mail server)
- Interfaces to data storage systems (e.g. databases, document archiving systems)
- Interfaces to hardware components (e.g. card readers)
- Administrator interfaces (e.g. for database administration, for reading in updates)
- Interfaces to other technical processes (e.g. housekeeping, cost-benefit analysis)
- Interfaces to external service suppliers (e.g. trust centres)

System components

Once process execution has been clarified down to the level of elementary processes and the interfaces have been defined, the next step is to define and describe the precise functionality of the individual system components.

Layer structure of client-server applications

Advantages of intermediate layers

The majority of e-government services should be designed as client-server applications. In the past, it was customary to distinguish between two layers (2-tier[1]- architecture): on the one hand, there is the front-end which is the part of the application which is directly visible to the user and, on the other, there is the back-end which generally consists of a database. In modern applications, additional layers are implemented between the front-end and back-end. Depending on the number of these layers, we talk in terms of a 3-, 4 ... n-tier architecture. The purpose of interposing these additional layers is to free the front-end and back-end from tasks which have nothing to do with their primary objective within the framework of the application. Alongside improved performance, this extended architecture has other benefits to offer. On the one hand, the security of the application is considerably enhanced due to the fact that it is no longer possible for any given client to access the back-end databases (which may sometimes contain extremely sensitive data. On the other, this architecture considerably

[1] Tier = layer or level

simplifies system administration. This can be illustrated most easily using a simple example:

Reduction of maintenance times through n-tier architectures

If one of the application's functions consists of performing a currency conversion (e.g. in a procurement system) then, in the case of a 2-tier architecture, this is usually implemented in the client. However, this means that the conversion rates must be constantly updated (i.e. at least once a day and sometimes more frequently) at all the clients (and there may be a lot of these). By contrast, if the part of the application that contains the conversion module is moved to an application server between the front-end and the back-end then the update need only be performed on this one machine.

Of course, an architecture which contains additional layers between the front-end and back-end requires the use of more hardware and thus leads to higher costs. When deciding on the system architecture to be used for a given e-government architecture, it is therefore necessary to weigh the advantages described against the necessary expenditure and then select the most economically efficient solution.

Front-end

In order to perform the IT implementation of the application's user interface (the front-end), the programmer requires precise, unambiguous specification of the specialist requirements which the system must fulfil.

First of all, it is necessary to gather together all the documents and document types used in the technical procedure, such as

- forms
- lists
- logs
- receipts
- notifications
- applications
- decisions
- ...

Collection of all document types used in the e-government procedure

and provide a detailed description of these. This description must comprise the function of these documents within the technical procedure, the way they are created in the application (e.g. automatic generation of a decision from the data submitted in the application) and the layout.

Modelling of the input forms

In the case of the documents that are to be processed online, it is necessary to develop a role concept (see also Activity 4.7) which defines which user group is to be able to process which data in which form view. Thus, in general, processing of the application (by the responsible person in the public agency) requires data to be entered in fields other than those involved in the submission of the application (by the customer). It is therefore necessary to create different views of the form for the two user groups. Certain data fields which, for example, will accept input in the processing view, should either be invisible or visible but not editable in the application submission view. The input data formats have already been defined during the creation of the data model (see Activity 4.5).

Every form implemented in the user interface should adhere to certain general layout rules. Usually, this type of form consists of four basic elements:

Description of front-end functionality

- title bar
- information bar
- navigation bar
- content area

These elements should be described in terms of the characteristics

- layout
- functions
- plausibility
- help

for every screen form. Further front-end functionality, in particular as far as the issue of IT security is concerned, is discussed in the next activity.

Intermediate layers and the back-end

Transfer of functionality from front-end to intermediate layers

In a conventional two-tier architecture, almost all the application's functionality is implemented in the front-end while the back-end, i.e. the database, serves only for the storage and administration of the data received. However, as mentioned above, in modern client-server architectures there is a tendency to transfer some of the functionality from the front-end to the intermediate layers (middle tiers). The IT modelling must therefore provide a precise definition of which functionality is to be implemented on which application server. These functions which are transferred from the front-end must then be described in the same way as presented in the last subsection.

As explained in connection with Activity 4.7 below, it may also be particularly advisable to move security functions, such as the verification of access rights, from the front-end to the back-end, i.e. the database.

Overall, the use of a multi-tier architecture opens up new design possibilities which permit an IT modelling of the application which is optimally adapted to e-government requirements.

4.7 Activity “Definition of the organisational and technical security safeguards”

Initiation responsibility:	E-Government Team Leader
Implementation responsibility:	E-Government Core Team, IT Security Officer, IT Administrators, persons responsible for the technical procedure, persons responsible for organisation

As noted in the introduction to this phase, the planning of IT security measures forms an important part of the detailed technical concept. One aspect which is particularly relevant to e-government, i.e. the protection of the communication channels by means of data encryption, has already been discussed in Activity 4.4 in conjunction with the issue of authentication. Additional security measures which protect the application from both external and internal attacks are discussed below. Since these security functions also form a criterion for the selection of the new hardware and software that is to be procured as part of the E-Government Project, this examination must precede the activity “Restructuring of the IT environment”. In contrast, documenting of the new or extension of the existing security concept should be performed after restructuring has been completed and evaluated (see Activity 4.10).

IT Baseline Protection

Modelling in accordance with IT Baseline Protection

The IT modelling of the new online services performed in the last two activities provides the direct basis for commencement of the corresponding modelling in accordance with IT Baseline Protection (see section 2.3 of the IT Baseline Protection Manual (BPM)). Once an analysis of the protection requirements for the planned e-government procedure has been performed (see section 2.2 of the BPM), the components of the associated IT infrastructure must be mapped to the modules of the IT Baseline Protection Manual. Here, we recommend using a layer model in which the various IT security aspects are grouped together by subject category. The layer model, which involves progressively more refined levels of detail – from the IT infrastructure as a whole down to the specific security requirements of the individual IT components – includes the following stages:

Layer concept for IT Baseline Protection

- Higher order aspects: Issues such as IT security management, organisation, data backup concept, computer virus protection concept which are of similar importance for all the components in the system as a whole.
- Infrastructure: Physical security measures (e.g. access protection, power supply, protection against fire, water, lightning etc.).
- IT systems: Security considerations relating to servers, clients, stand-alone systems and communication systems (e.g. PBX).
- Networks: Protection of network connections, firewall concept.
- IT applications: All security considerations that guarantee the integrity of the individual IT application.

Once modelling has been performed on the basis of the outline diagram, the IT Baseline Protection Manual supplies a set of suitable security measures for each component in the overall system. If these measures require the use of special hardware or software then this should be taken into consideration during the restructuring of the IT environment described in Activity 4.8.

Supplementary security analysis

Safeguards extending beyond IT Baseline Protection

The standard security measures provided within the framework of IT Baseline Protection provide an adequate and appropriate level of protection for the majority of IT systems. However, in the field of e-government there are a particularly large number of sub-components that require a security analysis which goes beyond the confines of baseline protection. On the one hand, this necessity results from the fact that the transmission channels (internet) would currently be extremely insecure in the absence of appropriate security measures and, on the other, from the great value of respecting and promoting respect for the data privacy protection regulations within the framework of e-government.

The issue of protecting the transmission channels has already been addressed in Activity 4.4. Two further sets of problems relating to e-government, namely the control of access to data and the use of firewalls, are examined separately below. A separate security analysis which goes beyond the confines of the baseline protection concept must be performed for any e-government sub-systems which are subject to particularly stringent security requirements (see also the discussion in section 2.5 of the BPM).

Data privacy protection and data security requirements

Data privacy protection and data security measures can be categorised along various lines. On the one hand, they can be categorised on the basis of conventional, fundamental IT security values as measures designed to ensure:

Fundamental IT security values

- confidentiality
- integrity
- availability

However, they can also be subdivided, as suggested by the title of this activity, into:

- organisational and
- technical

safeguards.

Below, we use the latter mode of categorisation to provide the outline structure and the former to provide a more detailed specification of the security measures.

Organisational safeguards

Transaction logging

Whenever the question of security is considered, there is often a tendency to rely exclusively on technology. The fact that a properly thought out organisational concept often makes it possible to achieve the objectives more effectively and at less cost and effort is frequently ignored. Often, even technical security measures which make perfect sense, for example end-to-end transaction logging, come to nothing because of the lack of an organisational concept which defines when or how often these logs are to be checked and by whom. As long as no one actually analyses these files, all that will happen is that large volumes of data will accrue in the log files without in any way helping to improve the security level.

The basis for all data security measures consists of a concept which defines the roles to be assigned to all the parties involved in the e-government procedure and the data access rights that are to be associated with these roles

A1) Role concept

Overview of all the roles in the technical procedure

In the section devoted to the planning of the front-end (Activity 4.6), it was pointed out that before users can carry out certain transactions within the framework of an e-government service, they must possess the corresponding access rights. For example, the person who handles an application in the public agency may be able to consult data which is not usually available to the applicant. The following simple example illustrates the principle: “Responsible member of staff” and “applicant” are in themselves roles whose functions within the procedure automatically delineate their individual rights to access specific data stocks or their right to carry out specific transactions.

The first step during planning therefore consists of listing all the roles that may be involved in the procedure.

Definition of access rights for each role

The next step involves the definition of all the rights that must be assigned to a role if it is to be able to properly fulfil its function within the procedure. The general guideline here is “as many as necessary, as few as possible” or, as it is often formulated in other contexts, “on a need-to-know basis”. Furthermore, the specification of privileges should be as differentiated as possible, e.g. following the scheme “read”, “write”, “execute”, “delete” etc., as they are used in modern computer operating systems.

Finally, the result of the two steps can be summarised in a table with a structure similar to that presented in Figure 6.

Permission	Role 1	Role 2	Role 3	...
Data set 1: read	X	X	X	
Data set 1: write		X	X	
Data set 1: delete			X	
Data set 1:			X	
Data set 2: read	X	X	X	
Data set 2: write		X	X	
Data set 2: delete			X	
Data set 2:			X	
...				
Action 1: execute	X	X	X	
Action 2: execute		X	X	
...				

Figure 6: Schematic representation of a role concept

Further details involved in the implementation of this type of role concept will be examined below in the discussion of technical security measures.

A2) Deputising arrangements

Key management in the event of deputisation

If, for any reason (e.g. illness, holiday), a member of staff in the agency should be unable to complete an operation that is currently in progress, then there must be a defined procedure for transferring the task to a deputy. Unlike paper files, for which this type of delegation can be easily performed by simply handing over the relevant documents to another member of staff, this task is not quite so straightforward when electronic dossiers are used due to the highly desirable, security measures implemented to protect data confidentiality and integrity. Even if, for example, only an administrator is able to "release" the data in the event of deputisation (an operation which is itself far from unproblematic in terms of data privacy protection legislation); serious difficulties will arise if the data has been stored in encrypted form. Without the absent staff member's decryption key, it will no longer be possible to view the electronic dossier or to continue processing the operation.

There is consequently no alternative to developing a deputisation concept which defines how tasks an be delegated if a member of staff is absent. Here, it is necessary to distinguish between two cases:

Arrangements for scheduled and unscheduled staff absences

- planned absences (e.g. holidays)
- unplanned absences (e.g. illness, accidents)

Whereas, in the former case, the transfer of responsibilities can be performed in an "orderly" manner in accordance with defined rules before the absence occurs, unscheduled absences, especially if they are long-term, demand recourse to planned contingency measures such as key recovery of the absent staff member's now inaccessible private decryption key. The corresponding arrangements must conform with the cryptographic and contingency concept (see Activity 4.10).

A3) Auditing and monitoring

Regular checks of the security measures

Because they are particularly in the public interest, e-government services are exposed to a greater risk of internal or external attack than other IT applications. Alongside the technical mechanisms designed to ward off such attacks, it is essential for IT security management to make certain organisational arrangements that will assist in affording the necessary protection. On the one hand, these include the continuous registration and evaluation of all security-relevant system activities. On the other hand, it is necessary to undertake periodic examinations in order to determine whether the security measures are actually being observed in practice and identify the extent to which they genuinely contribute to the purpose of providing protection.

For further information on this subject, please refer to the IT Basic Protection Manual, in particular modules 3.0 "IT Security management" and 3.1 "Organisation" and especially the following safeguards:

- Safeguard **S 2.64**: Checking the log files
- Safeguard **S 2.65**: Checking the efficiency of user separation on an IT System

- Safeguard **S 2.133**: Checking the log files of a database system
- Safeguard **S 4.81**: Auditing and logging of activities in a network

B) Technical safeguards

First step: implementation of IT Baseline Protection

The following presentation of technical measures designed to protect IT systems is simply intended to give a brief account of certain issues that are of special relevance for e-government applications. While many of these issues also apply to other IT systems, it is not possible to present in detail all the technical mechanisms implemented in all IT systems here. For the purposes of the following discussion, it is assumed that standard protection mechanisms, such as securing workstations by means of a password or the use of virus scanners, have been implemented. For further details on such mechanisms, please refer to the IT Baseline Protection Manual.

The discussion below is subdivided on the basis of underlying IT security requirements: confidentiality, integrity, availability.

B1) Technical safeguards for the protection of confidentiality

Technical implementation of the roles/rights concept

So far, we have considered the protection of confidentiality within the e-government framework in terms of data encryption and authentication (Activity 4.4). The most important role that these mechanisms have to play is in warding off external attacks. However, in order to ensure that individuals who are directly involved in the procedure (internal perpetrators) cannot gain knowledge of data that is not intended for them, it is necessary to implement the role concept outlined in section A1 at the technical level in a way which ensures the desired results.

In the “System components” section of Activity 4.6, we briefly examined the layer structure (n-tier architecture) of modern client-server applications. Here, we also alluded to the advantage they offer of permitting the flexible distribution of security functions across the various layers. In order to further investigate this point, which is of crucial significance for the high-level design of e-government services, we want to briefly examine the alternatives with their associated advantages and drawbacks.

In most client-server applications, the transaction and data access rights are verified in the front-end. Whenever the user wants to perform an action, the client installed on the user’s PC immediately checks whether the necessary rights are available for the role assigned on the basis of the authentication. If they are, the client performs the action. If not, it aborts the transaction.

The advantage of this solution is that it is the simplest and most straightforward to programme. The drawback is that it may leave security loopholes. For the purposes of this discussion, we shall not consider simple programming errors (bugs) in the implementation of the security functionality here. The greatest potential security loophole lies in the fact that the application program is directly controlled by the user (it is installed on the user’s computer) who can “try out” all the possible methods of attack in order to overcome the security functions.

Security risks due to internal perpetrators

If data access rights are checked only in the front-end, then internal perpetrators (i.e. individuals who have the right to log on legally to the application at least with the least privileged role) have even more sophisticated ways of circumventing access restrictions at their disposal. To do this, they simply need to program their own database client (or download existing freeware programs from the internet) which will permit direct access to the entire data stock without performing the inconvenient authorisation checks that are conducted by the original application. If the user logs into the database using this “home-made” front-end (to which, as an “internal agent”, he or she possesses the required authorisation) then full permissions are immediately available despite the user’s low level of privilege.

Enhanced security through layer architecture

Given the backdrop of this potential type of attack, one alternative solution is to perform rights verification in the database itself. Although this is technically possible, it generally requires considerable administrative effort. A better alternative is to move at least part of the security functionality to one (or more) application servers connected between the front-end and the database. As already mentioned, this frees the application level and database administration level from tasks which have no direct connection with the business process in question. In addition, this results in a considerable gain in terms of data security because users no longer log on to the database directly via the front-end. Instead, communication is carried out in a controlled way via the application server.

B2) Technical safeguards for the protection of integrity

When considering the threats to data integrity within the e-government framework, the first thing that comes to mind is intentional fraudulent activity committed with malicious intent (e.g. the manipulation of data in order to obtain financial benefits under false pretences). Protection against this type of threat is provided mainly by the security mechanisms described in Activity 4.4.

Unintentional data corruption

One reason for incorrect data, which may appear much more harmless, is unintentional corruption, i.e. simple typing mistakes or other entry and transmission errors. Since the subsequent correction work, which usually has to be performed manually, requires considerable effort, such problems result in high costs. If they are allowed to accumulate, entire data stocks may become unusable, thus obviating the point of the entire automated workflow management process.

When implementing any data entry front-end, it is therefore necessary to make the greatest possible use of all the available plausibility check mechanisms. These include, for example:

- Verification of the data formats: it should not, for example, be possible to enter a floating point value in an integer field.

Plausibility checks

- Text entries should, wherever this is at all possible, be performed by means of selections in predefined lists (e.g. town names, ZIP codes etc.)
- Entry of date specifications via a calendar module (to prevent, for example, dates of birth such as 29.02.1967).
- Consistency check of the data contents (to make sure, for example, that no 11-year-old fathers can apply for their old age pensions).

Firewalls for the protection of the integrity of the local area network

Alongside data integrity, another import protection objective consists in maintaining the integrity of the local area network run by the public agency offering the e-government service. Here, the most important technical protection component is the firewall which secures the intranet against direct attacks from the internet. For practical assistance in the choice of a suitable product, please refer to the BSI firewall study which can be found in the “Toolbox” of the current E-Government Manual. Alongside a detailed examination of the different products conducted on the basis of a predefined catalogue of security criteria, this study also contains the results of performance tests, i.e. a criterion that is of considerable relevance with reference to e-government applications involving large volumes of data.

Strengthened operating systems for exposed servers

Alongside the firewall, the central components of the e-government service, such as web servers, form servers, FTP servers etc. are also particularly highly exposed to risk. As a result, robust devices running specially strengthened operating systems should be selected for such tasks. In order to restrict to the greatest possible extent the points at which hackers whose manipulations (for example, falsification of the website) can result in a considerable loss of image, the following guideline should be adopted in connection with the services that are to be implemented: as little as possible, as much as is absolutely necessary.

B3) Technical security measures for increasing availability

When planning e-government services, it is important to pay special attention to the availability requirements that the systems must meet.

Availability requirements for the e-government service

On the one hand, the task itself may impose high or very high availability requirements. For example, if the submission of an application implies legally binding deadlines then the public agency is, of course, obliged to make it possible for the customer to respect these deadlines by making access to the e-government application available at all times. In this case, the situation is analogous to conventional business transactions where, for example, the publication of a fax number directly entails the obligation to guarantee that the corresponding device is operational at all times.

Cost-benefit assessment

At the same time, it is important to be aware that high availability generally implies considerable effort and very high costs. Consequently, in the absence of any imperative legal obligations, a critical cost-benefit assessment should be performed in order to determine the system availability requirements before any decision is reached. Thus, there would be little point in ensuring the *permanent* availability within a few minutes of a service which simply provides information.

The technical safeguards that ensure the availability of data and systems can therefore be subdivided into two categories:

- Standard safeguards designed to ensure correct business transactions within the “usual” framework
- Special safeguards designed to ensure high or very high levels of availability with a maximum down time of a few minutes or even a few seconds

Standard security measures falling within the first category are described in detail in the IT Baseline Protection Manual. These include, for example, the installation of an independent power supply (UPS) or ensuring scheduled data backups. It is particularly important to ensure that there is an operational contingency concept (see also Activity 4.10).

Redundancy in all critical system components

The safeguards in the second category include, in particular, the redundant configuration of all critical system components. This starts with the mirroring of the data stock to independent disks or even to different servers and continues with the, initially, local duplication of all the major network components. If it is also necessary to protect against localised disasters (major fires, natural catastrophes etc.) then the next stage consists of setting up a second data centre in another location at which all the data can be mirrored (again with local redundancy if required).

Recovery service provider

It is clear that this type of effort is only justified under special circumstances. High availability requirements can also be met by concluding an agreement with a commercial service provider specialised in so-called recovery services. If a disaster occurs, then this service provider re-establishes the entire infrastructure that the public agency needs in order to continue processing business transactions.

4.8 Activity “Restructuring the IT landscape”

Initiation responsibility: E-Government Team Leader

Implementation responsibility: E-Government Core Team, IT Administrators, IT Security Officer, persons responsible for the technical procedure, persons responsible for organisation

After IT modelling of the planned e-government services has been performed in Activities 4.2 to 4.7, it is now possible to start the design of an IT environment which is adapted to the new requirements.

Creation of a network plan incorporating the new e-government components

Outline plan of the new network architecture

In a similar way to Activity 4.1, when the existing IT environment was surveyed, it is advisable to start by sketching an outline plan of the new network architecture. An example of such a plan is illustrated in Figures 7 and 8.

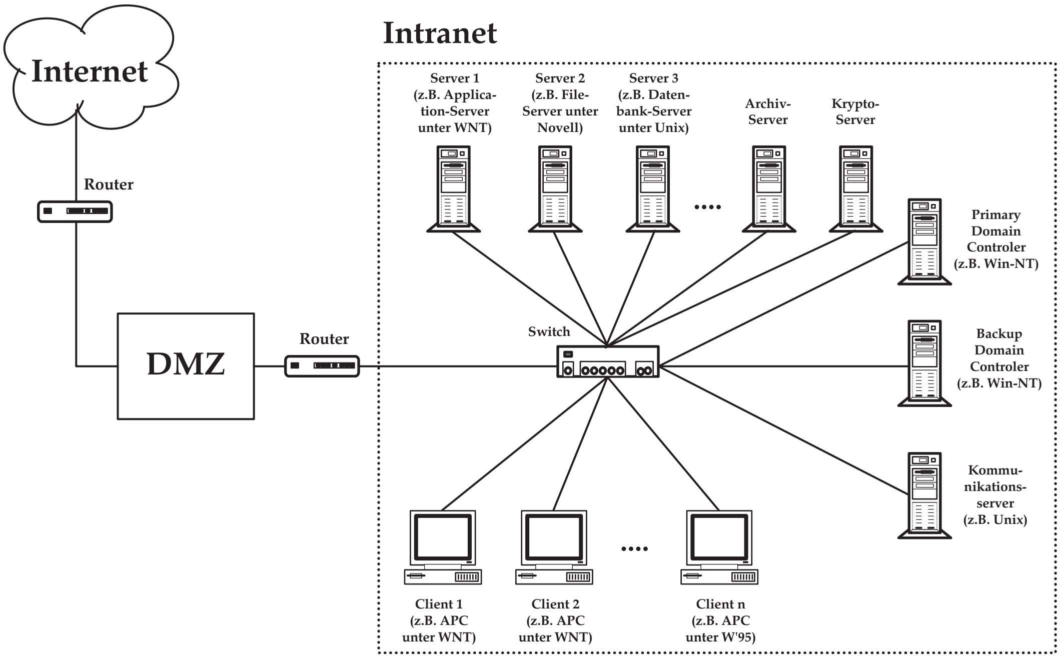
Internet
Intranet
Router
DMZ
Router
Switch
Server 1 (z.B. Application-Server unter WNT)
Server 2 (z.B. File-Server unter Novell)
Server 3 (z.B. Datenbank-Server unter Unix)
....
Archiv-Server
Krypto-Server
Primary Domain Controler (z.B. Win-NT)
Backup Domain Controler (z.B. Win-NT)
Kommunikations-server (z.B. Unix)
Client 1 (z.B. APC unter WNT)
Client 2 (z.B. APC unter WNT)
....
Client n (z.B. APC unter W'95)

Figure 7: Im Rahmen von E-Government möchte die Behörde, deren bisherige IT-Landschaft in Abb. 2 dargestellt war, nun mehrere Informationsserver betreiben.As part of its e-government effort, the public agency whose existing IT environment was presented in Figure 2 now wishes to operate multiple information servers. Die einfache Firewall-Architektur aus Abb. 2 wird hierzu durch eine sog. „demilitarisierte Zone“ (DMZ) ersetzt.To this end, the simple firewall architecture in Figure 2 is replaced by a so-called “demilitarised zone” (DMZ). In dieser sind die Server in einer Weise geschützt aufgestellt, dass ein „legaler“ Zugriff auf sie sowohl aus dem Internet als auch aus dem Intranet möglich ist, sie jedoch vor Angriffen sowohl von innen als auch von außen sicher sind.This protects the servers in such a way that “legal” access to them is possible from both the internet and the intranet. They are, however, protected against both internal and external attacks. Weiterhin wird das Intranet der Behörde gegen Angriffe aus dem Internet geschützt.At the same time, the public agency’s intranet continues to be protected against attacks from the internet.

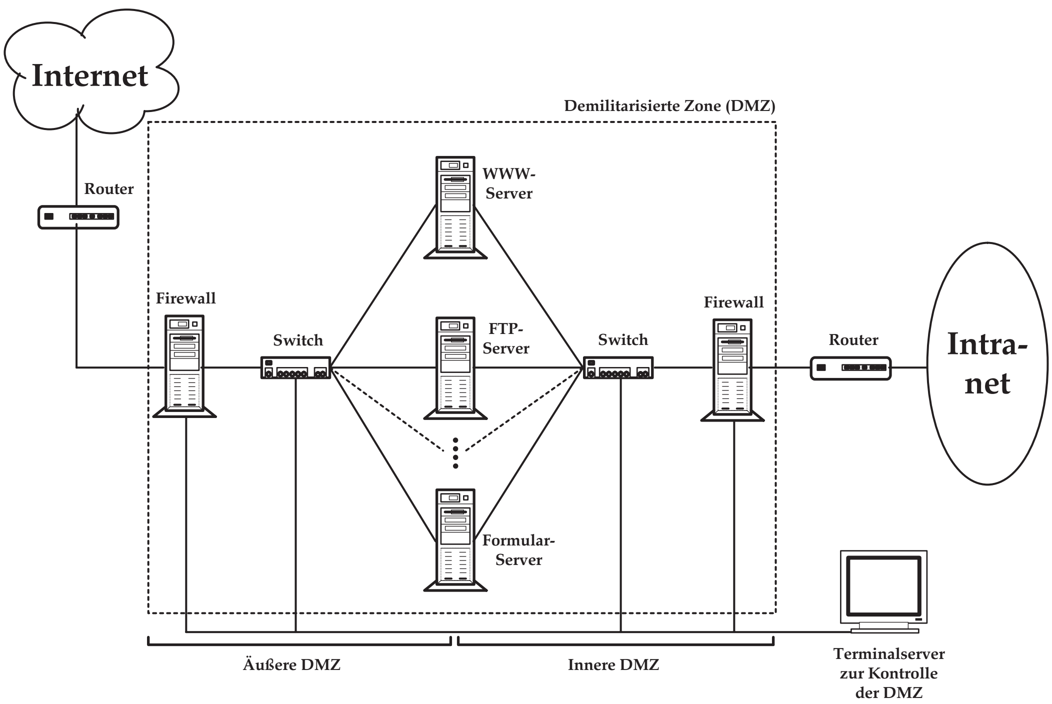

Figure 8: Detailausschnitt der in Abb. 7 als „Black Box“ abgebildeten demilitarisierten Zone.Detailed view of the demilitarised zone which is presented as a “black box” in Figure 7. Im Zentrum der DMZ stehen die Server.At the centre of the DMZ are the servers. Die beiden Switches leiten Zugriffe sowohl aus dem Internet als auch aus dem Intranet auf den jeweils „zuständigen“ Server weiter (http -> www, ftp -> ftp, usw.).The two switches forward access attempts from the internet and intranet to the “responsible” server (http -> www, ftp -> ftp, etc.). Sie dienen auch zur Abschottung der Server gegeneinander und verhindern „unerlaubten Netzverkehr“ *zwischen* diesen.They also help to isolate the servers from one another and prevent “unauthorised network traffic” *between* them. Die linke und die rechte Firewall-Router-Kombination schützen die Server jeweils gegen unerlaubte Zugriffe von außen, aus dem Internet bzw. von innen, aus dem Intranet.The left and right firewall-router combinations protect the servers against unauthorised external (from the internet) and internal (from the intranet) access attempts. Die Administration der Sicherheitskomponenten erfolgt durch einen vom Intranet unabhängigen Stand-alone-Rechner.Administration of the security components is performed from a stand-alone computer which has no intranet connection.

Demilitarised zone

In this example, the public agency offers its e-government service by means of a web server, an FTP[1]- server and a form server. On the right-hand side of Figure 7, we can see the public agency’s intranet just as it was in Figure 2. On the left, however, the firewall which protected the intranet against attacks in the earlier configuration has been replaced by a demilitarised zone (DMZ). In Figure 7, this is simply represented as a “black box” whose internal structure is presented in Figure 8. An explanation of the precise function of each of the components at this

[1] Here it should be noted that, within the framework of E-Government, FTP servers (FTP= **F**ile **T**ransfer **P**rotocol) should be used, if at all, for information services involving data for which there is absolutely no confidentiality requirement. When pure FTP is used, the data is not encrypted for transmission. FTP is primarily suitable for the transfer of large volumes of data, e.g. long legal texts which should be accessible to everyone. However, it is possible to transfer encrypted data with sFTP (**s**ecure **F**ile **T**ransfer **P**rotocol). In practice, however, this protocol is not yet in widespread use.

point would require us to go into too much detail. However, the caption accompanying Figure 8 gives a broad overview. This example is simply intended to provide an idea of what a part of the network plan for the restructured IT environment might look like.

Definition of the new hardware to be procured

Priority of security over cost considerations

The complete network plan for the restructured IT environment should immediately make clear what hardware from the old configuration can be taken over and used and what new hardware needs to be procured. In particular in the case of the security components, as presented, for example, in Figure 8, the quality of the products should take precedence over pure cost considerations. (The term "product" here is used to designate the device *type* and not the product offered by specific suppliers. The choice of products in the second sense cannot be made until the tendering procedure has been concluded).

Definition of the new software to be procured

Compatibility with the existing IT environment"

As has already been mentioned a number of times, when choosing the software, the prime consideration should be to ensure compatibility with products employed in the existing IT environment (e.g budget management software or similar already installed)[1]. It is also desirable to achieve compatibility with products that are already used (or whose use is planned) by other public agencies as part of their e-government services. Wherever possible, the simplest and cheapest solution is to take over existing basic components (see Activity 4.2). However, in many cases there will be no alternative to developing at least some agency-specific solutions. First of all, of course, the new product that is to be developed must provide the functionality defined in the previous activities. Beyond that, however, it is of primary importance to ensure that the new software is based on existing standards (see the SAGA paper cited in Activity 4.2) and can be integrated without difficulty into the existing IT environment.

Selection of databases

Professional SQL database

The majority of e-government procedures should make use of client-server databases. Alongside the front-ends, which provide the functionality, and any intermediate application servers (n-tier architecture, see Activity 4.6), the back-end, i.e. the database, is the application's third main component. Consequently, it must be chosen with great care. The most important point here is that a professional SQL database[2] must be chosen and not a proprietary product which will generally be incompatible with other databases.

[1] This applies only if the existing procedures make use of standardised products which are compatible with other commonly used applications (for more information, see the comments on databases in the next subsection).

[2] SQL (**S**tructured **Q**uery **L**anguage) is a standardised database query language which is "understood" by all commonly used databases. Products which do not support SQL are unsuitable as a back-end for the client-server application that is to be programmed. Frequently, this type of proprietary database forms the core of an entire application (e.g. budget management or procurement systems) which suppliers market only in the form of global packages. Choosing such products, however, commits the public agency to this one supplier. In such cases, extensions to the

Problems may occur during the introduction of e-government services if any existing applications which are essential for the agency's functioning are based on this type of incompatible database. In such cases, instead of "tailoring" the new e-government application to match the old database, the public agency should consider abandoning the old product rather than creating an additional isolated solution for the entire agency.

Scalability and portability as selection criteria

If large volumes of data are involved in the provision of an e-government service then it is, of course, essential to consider the performance of the database. Another selection criterion (along with price) takes the form of the so-called scalability and portability of the system, i.e. whether the database can be distributed over multiple servers and whether it can be transferred to larger, faster servers as technology develops or the utilisation level of the e-government service grows.

application are usually impossible or extremely expensive. Data exchange with other applications via import/export interfaces may not be possible, and if it is, is also usually cumbersome.

4.9 Activity “Evaluation of the detailed technical concept”

Initiation responsibility:	E-Government Team Leader
Implementation responsibility:	E-Government Core Team, persons responsible for the technical procedure, persons responsible for organisation, IT Security Officer, Budget Manager, Data Privacy Officer, staff representatives

The detailed technical concept for the new e-government service, i.e. the specification of the IT implementation of the processes involved in the technical procedure, was concluded in Activities 4.1 to 4.8. Before undertaking the next steps through to implementation, it is now advisable to subject this concept to a critical examination.

Comparison with the original objectives

Critical examination of the detailed concept

The first thing to check is whether the IT modelling of the procedure actually meets all the functional requirements that were formulated during Phase 3. In particular, the new procedure must make it possible to achieve the objectives defined in Activity 3.3 “Process optimisation”. The planned security measures form another critical point: are these sufficient to ensure the protection requirements identified in Activity 3.4?

At the same time, it is possible that the development of the detailed technical concept has revealed that some of the objectives were too ambitious, i.e. they cannot be implemented at the technical or organisational level. In this case, the e-government strategy itself must be reviewed as in Activity 3.9.

Economic feasibility study

In order to prevent incorrect decisions entailing major economic consequences for the public agency Section 7, para 2 of the Federal Budget Ordinance (BHO) stipulates that an economic feasibility study must be conducted for all “measures with financial implications”. This should, as far as possible, aim at establishing a favourable relation between the pursued objective and the means used to achieve it. This is possible either

- by achieving a given result using the lowest possible level of resources (minimum principle) or
- obtaining the best possible result from a predefined level of resources (maximum principle)

The economic feasibility study should comprise the following points:

Comparison of alternative solutions

- A description of the starting situation and a justification of the necessity of the operation
- A comparison of alternative solutions

- A justification of the approach selected from among these alternatives
- A cost-benefit analysis from the financial and non-financial perspectives
- An estimate of the overall expense of the project distributed over the different budgetary years
- A time schedule for the project
- A result with a concluding recommendation

Check of framework conditions in terms of employment and data privacy protection law

A check of the legal framework conditions relating to the e-government procedure per se has already been conducted in Activity 3.7 and should not be repeated here. This section is intended to deal with potential legal problems that may arise from the *functional* high-level design of the procedure, in particular as far as the public agency's employees are concerned.

In Activity 4.7, we stressed the need for an as complete as possible logging of system-critical transactions. However, the analysis of these logs can give rise to problems in connection with data privacy protection law since they make it possible to reconstruct all the operations that a member of staff has performed at the system.

Conflict of objectives: data privacy protection vs. logging

From the staff representatives' viewpoint, this results in a conflict of objectives. On the one hand, they must oppose any possible misuse of the log files as a means of monitoring staff. On the other, the logs serve to protect every individual user of the system. If inconsistencies occur within an employee's area of responsibility then the logged data can provide important evidence making it possible to clear him or her of improper behaviour if, for example, illegal manipulations by third parties are revealed.

In order to exclude such potential conflicts of objectives from the outset, all the relevant parts of the detailed technical concept should be subjected to a critical review conducted in co operation with the staff representatives. By reaching specific agreements, for example concerning the way log files are to be analysed, it is then possible to decide on the security mechanisms required for the protection of the application and all its users without infringing employees' demands in terms of data privacy protection law.

Review of accessibility

Has accessibility already been considered in the concept? To avoid unnecessary costs, accessibility should be considered already as the e-government application is being designed. Subsequent amendments to the website will be cost-intensive and therefore not sensible.[1]

[1] See also "Accessible E-Government" module.

4.10 Activity "Documenting the IT security concept"

Initiation responsibility: E-Government Team Leader

Implementation responsibility: IT security officer

Once the high-level design of the e-government application has been terminated and subjected to a thorough re-examination in a concluding review, the next step is to document the organisational and technical security measures in detail.

Since all public agencies will have some form of IT infrastructure even prior to the introduction of e-government, it can be assumed that there is already an IT security concept which complies with IT Baseline Protection. Consequently, the documentation does not have to be produced from scratch but can build on what has been produced in the past.

Updating the IT security concept

However, once Activity 4.8 has been performed, this old security concept will very likely no longer correspond in all respects to the new, restructured IT environment. On the one hand, the network has been extended by the addition of new, e-government-specific components while, on the other, modifications to existing components will have become necessary due to the integration of these new elements. Correspondingly, the procedure for updating the security concept comprises the following steps:

- Documentation of the security requirements for the new e-government components (hardware, software).
- Review of the old security concept and, if necessary, documentation of changes resulting from the integration of new components in the old IT environment.
- Addition of new e-government-specific organisational arrangements (e.g. crypto concept, construction of a PKI).

In principle, the first two steps broadly require the same procedure, as set out in the IT Baseline Protection Manual, as the creation of an "ordinary" IT security concept. Consequently, we briefly address only some of the topics that are associated with e-government-specific considerations below.

Crypto concept

As we have frequently stressed throughout this manual, cryptography plays a key role in the security concept designed for e-government applications. However, even the use of the most powerful cryptographic algorithms and the most sophisticated cryptographic technology are pointless without the implementation of the organisational measures necessary to ensure that these are applied correctly. The associated rules must be set out in the public agency's crypto concept.

PKI and key management

One of the most important components of the crypto concept is key management. This requires the development of a key administration which organises the distribution of keys and certificates.

Key management in the event of deputisation

One of the issues that has to be settled as part of the crypto concept is the question of key recovery that was briefly alluded to in Activity 4.7 (sub-section A2). In the event of an "unscheduled" absence on the part of a member of staff (e.g. due to illness), this procedure makes it possible to restore documents which were encrypted using the staff member's public key to plaintext. In order to prevent the misuse of this key recovery procedure, the cryptographic concept must include clear rules specifying the narrowly defined circumstances under which such a procedure may be conducted in a strictly controlled way.

Further information on the content of a cryptographic concept and a concrete example of its structure can be found in safeguard S 2.161 of the IT Baseline Protection Manual.

Firewall concept

Every public agency which has an internet connection should possess a firewall concept even before the introduction of e-government. As the example in Activity 4.8 indicates, the implementation of e-government services may change the IT environment so fundamentally in this area that the firewall concept has to be completely redesigned.

Rules governing the configuration of active network components

A comparison of Figure 2 (before the introduction of e-government) and Figure 7 or Figure 8 makes the changes obvious. Whereas in the situation as depicted in Figure 2, it was only necessary to configure functions and rules for a router and a firewall, the situation in Figure 8 is far more complex due to the creation of a demilitarised zone. The new firewall concept must now define dedicated rules for the configuration of a router-firewall-switch combination for both internal (intranet) and external (internet) attacks.

For specific information on how to create a firewall concept, see safeguard S 2.70 of the IT Baseline Protection Manual.

Problem management, contingency planning

Increased availability requirements due to e-government

As already touched on in Activity 4.8 (sub-section B3), the introduction of e-government services can dramatically increase system availability requirements. In general, this fact has far-reaching consequences for the public agency's problem management and contingency planning procedures. Whereas, in the past, it may have been acceptable for systems to be up and running again 1-3 days following an incident, the legal provisions relating to e-government may stipulate maximum down times of just a few hours or even minutes.

This may lead public agencies to adopt a new contingency planning strategy, for example by leasing capacity in a backup data centre. The new framework conditions associated with such a change of strategy, for example the logistical support required for a switch-over to a backup data centre, must be defined in the revised contingency planning concept. Information on creating a contingency planning concept can be found in module 3.3 of the IT Baseline Protection Manual.

4.11 Activity: “Planning the implementation procedure”

Initiation responsibility: E-Government Team Leader

Implementation responsibility: E-Government Core Team, persons responsible for the technical procedure, persons responsible for organisation

Once the detailed technical concept for the new e-government services has been completed with the documentation of the IT security concept, it is possible to start planning the procedure for project implementation.

Definition of priorities, flowchart

In the description of the preceding activities, we have intentionally avoided specifying whether we are dealing with the introduction of a single e-government service or a bundle of measures. Here, too, the distinction must be made flexible since it is perfectly possible that, on the one hand, a number of different online services may support a single (administrative) procedure (e.g. a form server for the submission of applications, a web server to track the processing status, a mail server to send decisions) or, on the other, that a single online service may be associated with a number of different procedures (e.g. a form server with application forms for various procedures).

Step-by-step project implementation

Depending on the type of service or because of financial framework conditions (see the distribution of costs over multiple budgetary years as part of the economic feasibility study presented in Activity 4.9) it may be advisable, or indeed essential, to carry out the project in a number of stages. In such cases, it is necessary to subdivide the project into a number of sub-projects. To implement these sub-projects, it is then necessary to define priorities which take account of the strategic objectives on the one hand and material or personnel resources on the other. It is advisable to visualise this subdivision of the overall project in the form of a project structure plan in order to ensure that the logical sequence of project phases is easy to follow even for individuals not involved in its planning.

Milestones

The project structure plan serves to convey a complete overview of the entire project. The attainment of concrete interim results should be indicated here in the form of milestones. On the one hand, these indicate the completion of important steps in the project and, on the other, they make it possible to decide on corrective measures for the subsequent procedure.

A suitable way of depicting the project structure plan is a bar chart in which the milestones should be both entered clearly and scheduled as accurately as possible. This plan acts as a tool for efficient project control and the long-term monitoring of deadlines.

Handling change proposals

Change request procedure

Experience shows that even during project implementation, it is often necessary to deviate from or improve on the original planning. At the same time, in order to avoid the progress of the project from being impeded by constant change requests which are not necessarily consistent with one another, these should be routed through a systematic change request procedure and dealt with in the appropriate channels.

As already mentioned above, milestones are particularly well suited to intermediate revisions of project progress and make it possible to implement corrective measures to improve upcoming activities. Within this framework, it is necessary to consider change requests provided that these are defined in the form of a written application which covers at least the following points:

Change request

- On the part of the applicant:
  - applicant, date
  - precise description of the change request
  - reason for the request
- On the part of the relevant technical manager:
  - statement of position
  - explanation of the consequences for the procedure in question
  - explanation of the consequences for other procedures
  - comparison of the work/costs involved and benefits

On this basis, project management can then decide whether to accept or reject the change request.

Appointment of sub-project managers

Nachdem im Projektstrukturplan die Teilprojekte gegeneinander abgegrenzt wurden, sollten nun die Teilprojektleiter sowie die zugeordneten Projektteams bestimmt werden.Once the sub-projects have been clearly identified as separate parts of the project structure plan, it is necessary to appoint the sub-project managers and the associated project teams. Die Teilprojektleiter unterstehen dem E-Government-Team und sind diesem für die termingerechte Abwicklung ihrer Teilprojekte verantwortlich.The sub-project managers report to the E-Government Team and are responsible to it for completing their sub-projects on schedule.

4.12 Activity “Internal or external commissioning”

Initiation responsibility: E-Government Team Leader

Implementation responsibility: Budget Department representative, persons responsible for the technical procedure, persons responsible for organisation

In the introduction to this high-level design phase, it was pointed out that the sequence of the presented activities is based on a logically structured flowchart from which, in practice, it may sometimes be necessary to deviate depending on the way the public agency is organised and the type of e-government project. This is at its clearest in the activity that is described below. It is perfectly logical for the results of the planning phase to be set out in a so-called schedule of specifications which then forms the basis for the subsequent invitation to tender and award of the contract.

In-house or contracted planning and implementation

Here, however, it is necessary to distinguish between different types of public agency. For example, large public agencies which made intensive use of IT procedures even before the “e-government era” may possess highly competent IT departments which are able to programme the implementation of e-government projects themselves. In such cases, the schedule of specifications represents the formal catalogue of requirements for the in-house IT development project. There is no need to issue an invitation or award a contract.

The second type of public agency that we wish to identify corresponds precisely to the logic of the Phase Plan that we have presented here: although such agencies do not have the ability to implement their e-government projects themselves, they nevertheless possess the know-how necessary to conduct the high-level design activities described in Phase 4.

However, many public agencies do not correspond to either of these two cases. In such cases, the activity described in this section will have to be carried out at the very beginning of Phase 4 rather than at the end. That is the reason why we wish to examine this particular situation briefly below.

Contracting of the implementation *and* planning of the E-Government Project

To perform the activities described in the previous sections, it is necessary to possess a planning team which already has practical experience in the introduction of new IT procedures. Due to the increased security requirements relating to e-government services, qualified expertise must also be present in the fields of encryption, IT network security, firewall administration etc.

If a public agency does not possess appropriately qualified members of staff or if these are so busy with “everyday work”, i.e. with ensuring the operation of the existing IT procedures, that they do not have the time to plan the new e-government services, then the activities described within the framework of Phase 4 must be entrusted to an external contractor[1].

Here, there are two possibilities:

Planning phase undertaken by external contractor

1. The same company that subsequently undertakes the implementation work also performs planning
2. Planning and implementation are performed by separate IT service providers

Advantages and disadvantages of commissioning planning *and* implementation from the same supplier

In both cases, there are advantages and disadvantages that must be carefully assessed as a function of the type of project in question. It is plainly simpler to commission planning and implementation from the same source. The public agency only needs to deal with one contractor and the project can generally be concluded more quickly and efficiently if the programmers are involved at an early stage in the high-level design phase.

At the same time, however, this approach may also have disadvantages for the contracting agency. To a very large extent, the contractor determines the individual services that he has to provide. This type of conflict of interests is, of course, excluded from the outset if the second course of action is chosen. In this case, however, there is the danger that the measures specified during the planning phase cannot be implemented or can be achieved only with considerable effort, thus inevitably resulting in higher costs and delaying project completion.

Schedule of specifications

However the contracting agency finally decides to award the contract, one fundamental rule should always be observed: the planning phase must always result in the drafting of a schedule of specifications for the subsequent implementation operations. This must describe in detail all the functional and security-related requirements for the new procedure (see also the discussion in the following sub-section). Implementation cannot commence until the contracting agency has made sure that the high-level design of the new e-government service defined in this schedule of specifications actually corresponds to the initial intentions.

Drafting a design specification

Even if the contracting agency does not possess the necessary expertise to draft a schedule of specifications and therefore entrusts the planning of the new online procedure to an external contractor, it still has to provide concrete specifications concerning the type and scope of the required services. This service description, which is generally extremely concise and which sets out the key requirements for the new system from the contracting agency's perspective, is commonly known as a design specification. It in no way possesses the scope or level of detail of the subsequent schedule of specifications.

SCC and ECC-IT

As mentioned in the Introduction, the award of contracts within the framework of public service IT projects is subject to the "Special Contractual Conditions for the Procurement of DP Services" (SCC) or the revised version, the "Extended

[1] Federal public agencies may also consult a competence centre set up by the BSI.

Contractual Conditions for the Procurement of DP Services" (ECC-IT)[1]. SCC planning provides for a so-called planning document which serves as the basis for contractual agreements with contractors. Alongside the usual conditions which this regulates, such as fees, modes of payment, guarantee periods etc., this document also includes a service description which is formally equivalent to the above-mentioned design specifications. The planning document contains the following specifications:

Content of the design specifications (planning document)

- Brief presentation of the task
- Description of requirements, e.g. delineation of planning scope, service priorities and objectives, characteristics, requirements in terms of personnel resources and materials, processing times, benefits, restrictions, interfaces to existing procedures, methods, regulations
- Applicable standards and guidelines
- Documentary requirements
- Technical qualifications to be met by the personnel fulfilling the contract
- Cooperation to be provided by the contracting agency, e.g. provision of staff, material etc., deadlines and schedules
- Points of contacts with the contracting agency and contractor organisations
- Start of work, hand-over, acceptance
- Discussion of documentation: specification of the number of days on which the contractor must be available for discussions, specification of the period following hand-over during which such discussions must be conducted.

Drafting a schedule of specifications

As we have mentioned a number of times, the planning phase results in the drafting of a schedule of specifications which forms the basis for the implementation of the e-government procedure.

DIN 69901 defines the schedule of specifications as a "detailed description of the services (e.g. technical, economic, organisational) which are required or requested in order to achieve the project objectives".

Documentation of the detailed technical concept

In other words, the schedule of specifications constitutes the written documentation of the detailed technical concept as developed during the steps presented in the preceding activities. The relevant definition can be found in the SCC (or ECC-IT) cited in the sub-section above:

"Complete definition of a procedure through the detailed description of its functions, the interfaces and the interaction between the functions as well as the information they require or generate. In the case of IT procedures, any functions that are performed automatically are identified as such."

[1] These documents can be downloaded from the website run by the Co-ordination and Advisory Bureau of the Federal Government for Information Technology in the Federal Administration (KBSt) at http://www.kbst.bund.de.

Schedule of specifications as a contractual element

When defined in these terms, it becomes necessary to include the schedule of specifications itself as an element in the contract for the creation of the IT system[1]. If this is not the case then it will subsequently be very difficult for the customer to prove any deficiencies in the supplied product or enforce any guarantee claims. This is because only if the characteristics and functionality of the IT system are precisely described in a legally binding form will it subsequently be possible to judge whether or not the product that is ultimately supplied presents any defects.

The contents of the schedule of specifications result from the activities presented in this module, i.e. the detailed technical concept. The most important points are summarised again below:

Contents of the schedule of specifications

- Presentation of the requirements the system must fulfil: functionality, hardware, software, user interface etc.
- Hardware/software architecture
- Hardware/software interface architecture
- Database architecture
- Encryption and authentication mechanisms
- Security functionality to ensure data confidentiality, integrity and availability
- Legal framework conditions, e.g. Decree on Barrier Free Information Technology (BITV)
- ...

Formal characteristics of the schedule of specifications

Alongside such requirements in terms of content, it is also necessary to observe certain formal criteria. Thus, in the same way as in the design specification, the schedule of specifications should contain a time schedule for project implementation.

It is also necessary to ensure that the notation is clear and comprehensible for all involved. Technical terms must be explained separately in a glossary.

[1] It is irrelevant here whether the schedule of specifications was drafted by the contracting agency or by a company entrusted with the development of the detailed concept (in particular, and as specified in the two preceding sub-sections, this company may be the same one that is responsible for the creation of the DP system itself).

4.13 Activity "Creation of a training plan for future system users"

Initiation responsibility: E-Government Team Leader

Implementation responsibility: E-Government Core Team, persons responsible for the technical procedure, persons responsible for organisation

The high-level design phase should conclude with the creation of a training plan for the future users of the e-government application whose detailed technical design is now complete. When compared to "normal" IT projects, online services present certain special characteristics since, as far as the public agency is concerned, the potential user group does not just consist of in-house employees.

Documentation

Documentation as a part of the contractual services

A precondition for and valuable aid to training activities is proper documentation of the application. The drafting of this documentation by the company commissioned to develop the IT procedure should be defined as an element in the services to be provided[1] at the time the contract is concluded. This documentation must be drafted in a way which addresses the individual target groups. Consequently, it must be structured to deal with components that are of specific interest to the various user groups:

Target group-oriented documentation

- Technical personnel (e.g. network administrators, database administrators)
- Non-technical personnel (e.g. administrative staff)
- Non-specialist users (e.g. members of the public who use the online service)

Drafting of a training plan

In the same way as the documentation, the training plan must also be designed to focus on the needs of the different target groups. First of all, it is necessary to define:

Target group-oriented training plan

- the requirements that the new procedure imposes on the different user groups
- the capabilities which these users already possess
- the areas in which training is necessary for the individual groups

Focal points of the training plan

Before embarking on the task of developing the training concept on the basis of this information, it is first necessary to decide whether the training of the public agency staff should be performed externally (in this case the company that developed the system would clearly be the first choice) or whether it is to be provided internally by the agency's own training personnel. In the first case, the

[1] Even if development is performed in-house, the documentation must be drafted with the same care as would be expected of an external supplier. Since it is well known that developers are particularly reluctant to document their work, this requires a certain level of insistence on the part of the individuals responsible for organisation or the management of the public agency.

basic framework of the training programme will probably already exist. However, if training is performed in-house then the programme must first be developed. Typically, training will focus on the following issues depending on the staff target group in question:

For technical staff

- For technical staff:
  - network topology (integration of the new e-government components in the existing network)
  - firewall configuration
  - system control, system configuration
  - setting up of user accounts, assignment of rights
  - database administration
  - backing up
  - creation of barrier free web pages
  - ...

For non-technical staff

- For non-technical staff:
  - introduction to the procedural implementation of the service
  - system operation (operation of the front-ends)
  - functional overview
  - dialogue-based operation
  - ...

In addition to these direct training measures, it is also advisable to provide users within the public agency with an "electronic information pool" on the intranet available at their workstations as a supplement to the paper documentation. This makes it possible to present everything there is to know about the system in an attractive form which staff can study at their leisure or call up as reference material when the need arises.

Training of e-government customers

User guides for e-government customers

The training concept presented in the sub-section above can, to some extent, be re-used for all newly introduced IT procedures. As already mentioned in the introduction, the specific nature of e-government services resides in the fact that the majority of users, i.e. the e-government customers, are not specialists. Furthermore, they are not usually able to benefit from face-to-face training measures[1]. It is therefore necessary to design completely new concepts in order to train this user group in the operation of the e-government application.

[1] There are, however, exceptions, for example when the e-government services are intended for a relatively limited group of (specialist) users (for example lawyers or solicitors who need to correspond with a court using electronic media). In such cases, it is possible to design training measures similar to those used for public agency staff.

FAQ

The first and most important consequence of this situation is that the user interface presented to e-government customers must be as simple and self-explanatory as possible. The greatest possible use should be made of all the available online help options. In addition, customers must be provided with downloadable written operating instructions and FAQ (= documents with answers to "Frequently Asked Questions").

E-learning and web-based training

In the case of simple e-government services in which, for example, the customer simply needs to fill in a form, this type of assistance can be provided instead of training. However, in the future there will undoubtedly be more complex online procedures. This will necessitate the use of training methods which are referred to using terms such as "e-learning" (electronic learning) or WBT (web-based training).

CD tutorials

One method, for example, is to provide members of the public with a CD available on request (by e-mail), which contains a tutorial program which they can study by themselves. At the same time, it might also be possible for this CD to include a program which installs a client designed to facilitate operation of the e-government application on the user's PC.

In the case of e-government services which are not excessively complex, this procedure could also be performed online, i.e. customers can learn using a tutorial program available from the public agency's server (web-based training). However, such a concept is limited by the restricted data transmission speed and the connection costs that the customer has to pay.

4.14 Activity "Briefing of all those concerned"

Initiation responsibility:	Agency management
Implementation responsibility:	Agency management, Public Relations, staff representatives

As in the previous phases, the high-level design of the new e-government service should conclude with a briefing of all the parties concerned as to the achieved results.

Briefing of agency staff

First of all, of course, it is necessary to brief the staff of the public agency because their work will generally be directly affected by the subsequent implementation and commissioning phases. Consequently, staff should be informed in detail of the now fully developed concept as well as of the specific consequences for their everyday tasks. When introducing this type of new procedure, it is especially important to assuage the ever-present, latent fear that rationalisation effects resulting from the introduction of electronic procedures could jeopardise employees' own positions.

Briefing of staff representatives

Since this latter consideration is of particular relevance for staff representatives, it is important to inform them openly and transparently from the very outset in order to gain their confidence in all respects. Constructive co-operation with staff representatives is, as was stressed in Activity 4.7, particularly important within the framework of the organisational measures designed to guarantee data security since such measures also affect the legal rights of members of staff in terms of data privacy protection.

Information to e-government customers

While caution was urged at the end of Phase 3 (Activity 3.10) with regard to informing e-government customers, in order to avoid over-optimistic expectations (in particular with regard to the schedule), it is now possible to make much more realistic forecasts on the basis of the developed concept. In order to allow industry to concretise its planning with regard to the utilisation of the new e-government services, information should again be supplied openly on the basis of a realistic appraisal of the duration of the impending implementation phase.

Checklists

The following checklist can be used to ascertain whether all the essential results of the present phase are available. It can also be used where the above activities have been carried out in a different order or in a different form.

Checklist for Phase 4

Outcome(s)	**Who?**	**When?**	**Done?**
Existing IT environment, in-house standards and basic components that are to be employed recorded			
Suitable communication channels for e-government services and security measures necessary for their protection defined			
Detailed technical concept drafted			
IT security concept for the new e-government services created and documented			
Schedule of specifications created and project implementation commissioned internally or externally			
Training plan for future users created			

Author Profile

Dr. Herbert Blum, BSI

Herbert Blum studied physics and electrical engineering at Saarbrücken University. After graduating, he moved to the University of Mainz where, in 1992, he was awarded a doctorate in nuclear physics. The many calculations he was required to perform as part of his thesis resulted in a concentration on IT-related issues. He subsequently spent several years working on large-scale IT projects in industry and the public services with a special focus on the development of client-server database applications. As a project manager, one of his achievements was to implement an electronic procurement system for Mainz University. In 1998, Herbert Blum took up a position in the Bundesamt für Sicherheit in der Informationstechnik where he was initially responsible for providing IT security training. As of September 2001, he has been contributing to the development of the E-Government Manual in the field of "application concepts and consultancy".