14

IT Security - A crucial Success Factor for e-Government!

Martina Rohde, Andreas Schmidt and Timo Hauschild
GISA (German Information Security Agency)
Division "Concepts and Consulting for Applications"
Postbox 200363, D-53133 Bonn
{martina.rohde, and.schmidt, timo.hauschild}@bsi.bund.de;
+49 (0) 228 9582 {-285, -825, -824}

Abstract: More and more public administrations are moving towards electronic "business" processes based on information technology (IT). As public administration processes need to fulfil specific requirements, among them a high degree of correctness, IT security becomes increasingly important. Therefore, IT security requirements deserve special attention, when public administration business processes are being (re)engineered.

This paper reports on a process reengineering project in the German public administration and its relation to IT security. Section 1 extends the motivation before Section 2 describes the special characteristics of public administration services in Germany. Section 3 then shows how to integrate security into electronic governmental processes.

The main steps of a security analysis are explained by an example: the communication process that is taking place between the bidder and the party awarding the contract during public tendering procedures. The paper concludes with recommendations on how to implement electronic processes within the public sector.

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: 10.1007/978-0-387-35617-4_48

J. L. Monteiro et al. (eds.), *Towards the Knowledge Society*

1. INTRODUCTION

The initiative "BundOnline 2005" is one of ten areas within the German federal government program "Internet for all – 10 steps on the way to information society".[1] This "government initiative" aims at transforming all customer oriented federal services that are suitable into "electronic" processes until the year 2005, e.g., by making them accessible via the German federal government Web portal.[2] Federal offices are heading towards this aim for image reasons as well as economic reasons. Government is intended to focus on "modern, efficient and citizen-friendly" services rather than on the pure "fulfilment of governmental duties".

The use of information and communication technology (ICT) holds a lot of potential to optimize processes – but it all depends on whether the existing processes and underlying structures will be arranged and optimised according to the "real" needs such as effectiveness and usability. Especially that part of administration that provides services has to fulfil its function correctly and to satisfy the customers' needs. On the one hand, customers will only accept electronic processes that guarantee an appropriate amount of information security. On the other hand, many customers requesting some sort of on-line access are driving the demand towards providing all suitable processes via the Internet. There is a general aspect in the relation between citizen and government, too: A rich choice of secure and convenient ways to interact with the government will improve the government's image within its clientele.

The term "business process" can be defined as "coherent sequence of activities that are performed by people in order to achieve the business aims, that take place within a given framework of constraints or conditions, and that are supported with techniques and tools". In general, business processes are relevant in order to add value to an organisation. This understanding can be transferred to the sector of public administration: the term "electronic governmental processes" refers to processes that are "based on digital input data and/or digital output data communicated via electronic media and processed with the support of ICT in order to fulfil governmental tasks".[3] Parties communicating with the administration are, e.g., citizens, enterprises, and non-governmental/non-profit organisations.

Electronic processes within the public administration – so-called e-government processes – can be seen from three different perspectives: electronic information processing, modernisation of public administration, and democratic participation in political processes via electronic media. The notions "e-government processes", "electronic processes within public administration" and "electronic information processing" are used synonymously. E-government processes are characterised by 1) the exchange of digital documents via a *communication interface* between

customer and public administration and 2) the electronic information processing within the *internal procedures*.

The *communication interface* consists of the customers' front end, the actual data transmission and the office's internet portal (including some sort of electronic post office). Here usability and, especially, security are critical success factors that affect the acceptance by potential customers. The *internal procedures* comprise the employees' PC connected to the back office, and in some cases a third party (some sort of application service provider) that supports the service. Here, effectiveness and especially auditing acceptability (German: Revisionssicherheit) are critical success factors that affect the orderliness (German: Ordnungsmäßigkeit).

2. PUBLIC ADMINISTRATION SERVICES

2.1 Specifics within Public administration

Several characteristics of public administration authorities need to be taken into account while designing e-government processes and developing supporting ICT systems. Besides technical and economic issues, there are legal, political, and other aspects that have to be considered. For that reason, technical solutions for public administration differ from those for commercial enterprises – even if a similar problem is being addressed.

Most of the differences are caused by "principles that restrict the activities of public administration". Public services are bound to general laws and special directives, (numerous) specific procedural regulations further refine these laws and directives.[5] Four principles direct the activities of the public administration (in Germany):

1. Administration has to act in accordance with laws, directives and regulations (German: "Gesetzesmäßigkeit").

2. Administration has to treat all interested parties fair and equal and not to exclude any (interested) parties (German: "Gleichbehandlung").

Exceptions to both principles need to be explicitly justified and documented. Of course in some cases, decisions cannot directly be derived from the respective rules. In this case, the civil servant in charge of the decision has to make it based on his interpretation of the legal and factual situation. Regarding this, a third principle has to be looked at:

3. Administration has to choose appropriate means with regard to expense and benefit (in a non-economic meaning) (German: Verhältnismäßigkeit").

Last but not least, the forth principle is

4. Economic efficiency (German: "Wirtschaftlichkeit").

Based on this, an important consequence is that all relevant actions have to be put into writing in order to be auditable and controllable.

2.2 Example: The situation

Every year, 30.000 public administration authorities in Germany are awarding about 1 Million construction work contracts amounting to about 250 Billion (10^9) Euro. These contracts include services, deliveries and building works. Since 2002-01-17, the public administration authorities mentioned above have to accept tenders in electronic form[6]. Electronic copying and mailing enable the parties awarding the contract to significantly reduce the costs, e.g., for distributing the requirements' documents.

Considering that requirements' documents have an average length of 200 pages and have to be copied twice for 20 to 50 (potential) tenderers, transmission in electronic form instead of paper should help to save costs significantly. Additionally, the mailing of tenders allows tenderers to speed up processing time and to reduce errors caused by a change of media. Experts expect savings of 10 percent by electronic public awarding procedures.

Three aspects show that special security requirements are involved:

– There is a huge potential for attacks and damages because of the enormous financial volume of single orders.

– The tendering and awarding procedures are very complex.

– There is the strong aim to avoid any suspicion of corruption or faults as this would lead to extra examination procedures that can causing time delays or even the dismissal of the whole project.

3. SECURE ELECTRONIC GOVERNMENT PROCESSES

3.1 A systematic approach for integrating security

In our approach, security is seen as a part of the functionality of a system. Consequently, integrating security into an e-government process is the same as designing the functionality and implementing this functionality within a process. In other words, the main steps for the transformation of a government process have to be defined and, in each step, security has to be considered as a significant aspect.

The general model consists of six elements:

1. a *kick-off* meeting within the authority for *initialisation*,
2. considerations concerning the *objectives, policies and strategies*,

3. the *analysis* of the task to be transformed,
4. the *design* of the process,
5. the technical and organisational *implementation and integration* and
6. the *installation and the start-up* procedure.

Operation and maintenance are not part of this general model.

The focus of this article lies on the development of *secure* e-government processes; therefore the analysis (3rdstep) is described in detail in the following section and the security aspects are highlighted.

3.2 Essential aspects in the analysis, related to security

3.2.1 Process Analysis

In principle, an (electronic) process can be seen as a "black box" that transforms a (digital) input (e.g. an application) into a (digital) output (e.g. a notification). Within this black box, all activities for providing the service in question are performed.

The process should be analysed by determining the important "procedural steps", respectively "logical aspects". The processed information and the actors involved should be determined, too. To follow the methodology of business process modelling, functional components, organisational units, and "data flow" should be considered at the same time. The modelling leads to some sort of process description that shows the relation between events initiating or controlling activities and input-output data produced by or needed for these activities. While analysing the status quo of the process, weaknesses and potential improvements should be revealed and reported. Based on this process description of the status quo, the optimisation process (see 3.2.4) will be performed.

3.2.1.1 Example Part 1 – Process Analysis

The following actors are involved in the process: the enterprise as "interested party" or "bidder", the department as "party awarding the contract" with the roles "employee" and "session officer". The employee prepares and conducts the awarding procedure. The session officer is in charge of opening the sealed bids within the opening session. The processed information is: the requirements' documents (including the bid form) and the bids. The procedural steps/logical aspects are listed in the following figure (cf. Figure 1).

Each procedural step or logical aspect can be refined into sub-activities or described with scenarios until the desired depth of analysis is achieved. An in-depth analysis can be seen as a basis for further examination,

especially from the point of view of security. It is essential to understand what is happening – just to be able to answer the question "Who is doing what using which data?".

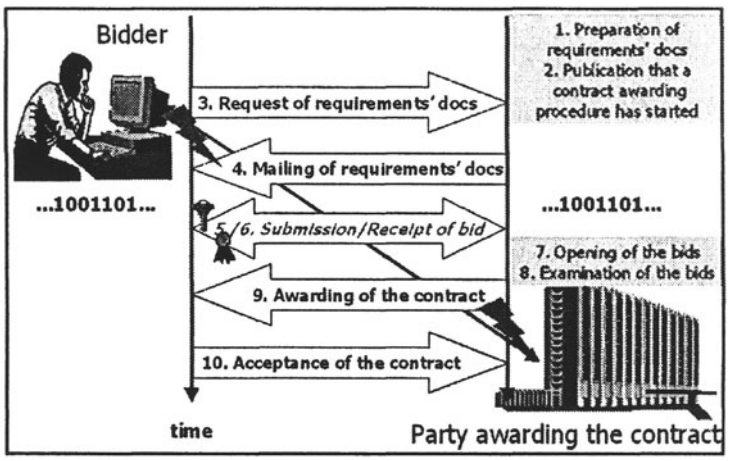

Figure 1: Procedural steps/Logical aspects

3.2.2 Requirements Engineering

Besides the legal and functional requirements, the security requirements concerning the process have to be examined[7]. For that purpose, security objectives and protection levels have to be determined in a way that allows to derive security requirements. Depending on the modelling approach, activities should be assessed in order to identify the (relevant) assets within the process. Before determining whether assets are valuable enough to warrant some degree of protection, an impact analysis has to be performed. This means: First, to categorise the kind of impact, e.g., an offence against law and regulation. Second, to classify the potential consequences of unwanted incidents, that affect the assets, i.e., none, basic, moderate, high, very high. And third, to estimate what this means in a given context. After performing an impact analysis, the assets can be rated and the results should be documented.[8] Because of the different participants with variant interests, the idea of multilateral security[9] is the means of choice in handling several security objectives. Assets rated higher than "moderate" have to be assessed by an additional threat and risk analysis – assuming one applies the methodology described in the baseline protection manual. Otherwise a detailed threat and risk analysis or some sort of combined approach has to be performed.[10]

3.2.2.1 Example Part 2 – Requirements Engineering

A bid is an essential asset. It must be signed with a qualified signature and be kept encrypted until the opening session has started.[11] The security objectives of a bid and the rated protection levels are[12]:

- Confidentiality of the bid until submission time – high,
- Integrity and authenticity of the bid – both high, and
- Legal liability of the bid – high, too.

In addition to these security objectives, the availability of the bid during transmission time is not part of this section. Because there is a hard deadline for handing-in bids, the bid has to be rated "very high" regarding its availability. This means that the technical solution must run on a system that is highly available.

Thinking about activity no. 5/6 "submission/receipt of bid" there are implicit requirements that will influence the functional design. Therefore it should be discussed beforehand, if these (security) requirements are still relevant. These implicit requirements are:

- Confidentiality of the ID of the awarding procedure,
- Non-repudiation of receipt, and
- Reliability of handing-in.

In the traditional procedure, the bid has been put into an envelope that again was put into another envelope: The "outer" envelope is addressed to the party awarding the contract. The "inner" envelope is titled with the ID of the awarding procedure. That is because of the *confidentiality of the ID of the awarding procedure*: The fact that a bidder has applied for a special awarding procedure should not be known by others than the bidder itself and the party awarding the contract. The "double" enveloping ensures that nobody knows which bidder has applied for which awarding procedure. If there is an explicit requirement about informing the bidder, the functional design of the acknowledgement should take into account that the confidentiality of the ID of the awarding procedure is warranted during the transmission of the acknowledgement.

In the traditional procedure, the bid is sent to the postal address of the party awarding the contract. The handing-in is registered, normally with an entrance stamp. That is because of *non-repudiation of receipt*: The fact that the bid has been handed-in is being recorded. This "stamping" ensures that the party awarding the contract can't deny that the bid had been handed-in. If there is an explicit requirement about informing the bidder, the functional design of the acknowledgement should take into account that the time in question is added to the acknowledgement.

In the traditional procedure the application is recognised as "untouched" in the postal office of the party awarding the contract. But only the status of the envelope(s) can be interpreted; nothing can be said about the status of the bid itself. That is because of *reliability of handing-in*: The fact that

modifications (to some certain degree) of the bid that has been handed-in can be recognised by the party awarding the contract. This ensures that changing the bid after the handing-in (until the opening session) is impossible without leaving a trace (assuming that the bid had been stored securely). The bid itself will be inspected after the opening of the sealed bids.

If the integrity of the bid is checked too late, there are two threats that have to be considered by the party awarding the contract. They both occur when bids are modified in some way and therefore are unreadable while the opening session takes place: On the one hand, those bids could principally not be accepted and are turned back. But as the electronic transmission is unprotected, this might happen too often. On the other hand, those bids could be accepted in principle while inquiring the original bid from the bidder once again. But because there is no way to prove that the original (old) bid and the received (new) bid are identical, a "bad" bidder could try to cheat by sending in an unreadable bid and taking advantage of the additional time.

3.2.3 Functional Modelling

Besides the modelling of functions that fulfil the legal and functional requirements, security functionality has to be modelled, too. To fulfil all security requirements, it is crucial to select appropriate security controls. Maybe there is more than one security functionality that fits; maybe there isn't any security functionality that fits. Alternative options should be described and the pros and cons should be discussed. Especially, if there are controls that don't suit well, one has to think about reducing the determined requirements, building some sort of work-around, or accepting a lower security level. Last but not least, one has to think about leaving the activity as it is – not modelled electronically. It is essential for the overall security of the process that all controls work together properly and perform as intended. The functional model should be a consistent technical solution that can be (really) implemented.

3.2.3.1 Example Part 3 – Functional Modelling

In this example the preferential technical solution is to implement cryptographic functions. Digital signatures and encryption are the means of choice. The digital signature certificate must be issued by a certification service provider that is compliant to the German digital signature law. The quality of encryption must be conformant to the technical state of the art. The bid is signed (with the private key of the bidder) and encrypted (with the public key of the session officer); the result is the so-called "signed & encrypted bid".

The functionality that matches the above mentioned implicit requirements can be implemented, too, as described below.

To model the requirement of *confidentiality of the ID of the awarding procedure*, the message that contains the "signed & encrypted bid" has to be sent to the party awarding the contract in an encrypted way. The functionality could be implemented by encrypting the "signed & encrypted bid" itself with the public key of the electronic post office of the party awarding the contract. This "2nd encryption" plays the role of the "outer" envelope.

To model the requirement of *non-repudiation of receipt*, the handing-in has to be documented by recording a reliable time. In principle, the creation of important signatures should be marked with a qualified time-stamp. But the party awarding the contract can not rely on the hope that the bid handed-in has a proper time-stamp. The functionality could be implemented by logging the time of handing-in or requesting a qualified time-stamp for the received bid.

To model the requirement of *reliability of handing-in*, the integrity of the received bid has to be checked immediately. An early integrity check can be implemented by verifying an additional signature. This means that the "signed & encrypted bid" has to be signed for a second time by the bidder before it is sent to the party awarding the contract. This "2ndsignature" is a technical feature to support the integrity check.

Please note that the combination of 2ndencryption and 2ndsignature means to first sign the "signed & encrypted bid" and to second encrypt the signed "signed & encrypted bid" as it is shown in Figure 2 below.

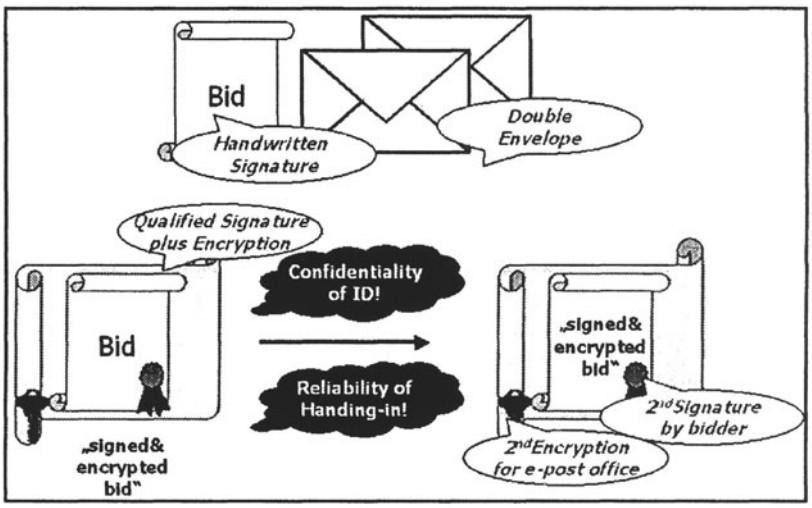

Figure 2: "Signed&encrypted bid" with 2nd signature and 2nd encryption

3.2.4 Process Optimisation

Based on the process description of status quo (see 3.2.1) the process can be optimised according to the departments' goals. There are external goals such as process transparency or service quality; and there are internal goals such as effectiveness. Besides those, security is an additional goal. It is very important not to simply transform all "traditional" activities, i.e., to model them without thinking about the reason, respectively, the purpose for doing the things just the way they (always) had been done. For each activity, it should be analysed if it is still relevant. By switching from paper to digital documents (communicated via electronic media), new conditions have to be taken into account. Non-relevant activities have to be eliminated or converted into other activities. New relevant activities have to be added.

3.2.4.1 Example Part 4 – Process Optimisation

In the traditional procedure, the bidder is not informed that the bid had been handed-in properly. There are several ways to hand-in a bid. The bidder can send it by mail, he can send it by recorded mail, or he can hand it in personally. Depending on the way he has chosen, the bidder knows more or less about the status of the bid. Sending by mail gives him no feedback, sending by recorded mail lets him know that the bid had arrived (in whatever status) at the party awarding the contract, handing it in personally gives him the knowledge that the bid had arrived properly.

Because of the options the bidder has and because of the insecurity of the electronic transmission, there is an explicit requirement to send an acknowledgement to the bidder. Especially if one looks at the fair splitting of risks between the bidder and the party awarding the contract, it is not acceptable to shift the responsibility for a proper handing-in to the bidder. This would be a disadvantage for a "good" bidder, because he has no chance to know anything about the status of his bid; therefore he can't send it again in case it had not been handed-in properly.

The functionality that fulfils the explicit requirement can be implemented, too, as described below.

The structure of the acknowledgement depends on the information that it should contain. The best solution is to sign the acknowledgement with a qualified signature as it is shown in Figure 3 below; the signing key is the private key of the electronic post office and the signed data structure is the "signed & encrypted bit" (or its hash value)[13]. Because of the signature, the acknowledgement is authentic and the signer can't deny the receipt of the bid. The bidder is able to verify the signature and therefore he can be sure that the party awarding the contract was the signer and had received his bid. Because of the content, the bidder is also able to check if the bid received by the party awarding the contract is identical to the one he had handed-in. If

there is no qualified signature, non-repudiation and authenticity are not guaranteed. If the "signed & encrypted bit" (or its hash value) is not part of the acknowledgement, the status of the bid after transmission to the party awarding the contract would not be reliably documented. There is also the possibility to add a time-stamp to the acknowledgement. This gives additional information about the time the bid had been received.

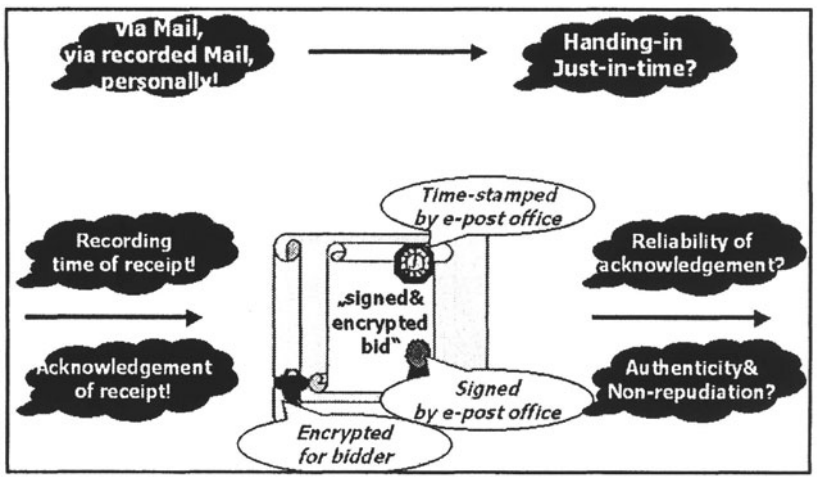

Figure 3: signed&encrypted acknowledgement (with time-stamp)

3.3 The next step: Design

By this stage, the requirements are determined, one or more way(s) to model them functionally are identified and alternative options to modify the whole process are detected. At this point, an appropriate solution has to be chosen. It could be helpful to conduct a vulnerability analysis in order to identify exploitable weaknesses. Another way to examine security breaches is to perform a residual risk analysis in order to be able to decide which risks had been eliminated or mitigated, and which have to be accepted or transferred. Especially, the boundaries of the process under construction – the technical and organisational context of the respective department – should be considered. This is a very significant step to avoid problems in further steps only by reviewing the facts.

Once the analysis is finished, the functionality that had been modelled has to be designed for the following technical implementation. Three sub-steps have to be performed.

First, the security controls, especially the cryptographic mechanisms have to be specified – until now the only specification was "encrypted with someone's private key". This leaves to clarify: how to manage the keys, who issues the certificates, and so on.

Second, the functional model has to be refined – until now, it is only specified which activities have to be considered, but not how the sub-activities look like.

Third, the security concept has to be established – until now there is only the claim that the technical system is part of a process meaning that it has to be integrated into the organisational environment.

4. LESSONS LEARNT

4.1 Doing the "right" things

The realisation of e-government processes is a highly interdisciplinary task. It is essential to understand "why things are the way they are and for what purpose they are done" in order to select the "right" control. The person who is responsible for the task (the so-called "process owner") has the background, especially the legal knowledge, that makes one able to interpret what is behind the process under question (see 3.2.1). This person is often the one who can decide between possible alternatives and options (see 3.2.4) or who can present the problem for decision to the senior management.

For example: A hand-written signature can be used for the purpose of matching an application to a citizen ID because it is a means for identifying a person. It can also be used for the purpose of avoiding the denial of applying within a legal context. Depending on the interpretation of the activity, several security mechanisms could be appropriate and different technical solutions could be implemented. In the first case, maybe it is sufficient to know someone's e-mail address for identification. In the second case, there must be a qualified signature for authentication.

Another example: In some processes payment is a "real" prerequisite for the start of the process or the continuation of the process. In other processes there is no need to wait until a fee had been paid.

Sometimes the selection of controls is limited by legal requirements; sometimes the process owner has the freedom to decide. In any case it is important to implement an appropriate security mechanism because otherwise it secures the "wrong" thing. To ease the development of an e-government process, GISA has published a module "Procedural model for e-government" – as a part of the so-called e-government manual.[14]

4.2 Doing things "right"

There are IT (and of course IT security) issues, organisational constraints and procedural conditions that have to be combined. Once the appropriate controls have been selected, it must be checked if there is a technical solution and whether the IT infrastructure is suitable to support the security mechanisms properly.

Regarding cryptographic mechanisms, there must be a consistent concept that describes and explains how the mechanisms are implemented. Having the overall technical-organisational system in mind, IT security management is something that should not be left aside. This means e-government asks for establishing a security policy, a security process and a security concept. To ease the selection of safeguards, GISA has published the so-called baseline protection manual.[15][16]

In general, to be present in the Internet means, that the organisation creates a certain "image" in the digital world. For example, a portal with active content forces customers to use a browser configuration that is inherently insecure. Therefore, a customer – especially one who is aware of the security risks that arise while being on-line – could have the impression that security was not intended to be implemented from the very start.

4.3 Thinking in terms of "processes"

This might be the most important part of e-government. Enterprises had been forced to think in terms of processes because of ISO 9000, total quality management, and so on; unfortunately, public administration is not accustomed to think in terms of processes. Administrative thinking mostly ends where another division starts. Thinking in terms of processes seems to be a change of paradigms. Determining the main processes concerning the "business" value chain is the starting point of e-government.

IT and IT security are no means of their own – they serve to ease the information processing, they avoid the media-change (from paper to digital form and vice versa) and they (hopefully) help to reduce the processing time. Security controls especially cryptographic mechanisms such as signing and encrypting have to be integrated into the workflow activities; unfortunately, the existing public key infrastructure (PKI) solutions cause severe interoperability problems. But on the other side, this hindrance is often over-used as an excuse for not doing anything.

Security controls should be aligned along the process in order to produce a security level that is acceptable and usable for customers and employees. And, security controls of one process should correspond to those within other processes in order to unify the technical infrastructure within a department. The first aspect is called vertical integration; the second aspect

is called horizontal integration. Nevertheless, it is very important to see the customer as a part of the whole process. Therefore, the customer has to be dealt with as a participant and, consequently, he or she has to be part of the security concept.

5. CONCLUSION

IT (and consequently IT security) are critical success factors for e-government. Therefore the way of integrating them into electronic processes within public administration is crucial, too. Security is always a question of the overall process – and it is not only a technical aspect. Understanding the problem(s) to be addressed in spite of trying to implement a nice technical mechanism (and later looking for an application to fit in) is the real challenge.

Regarding IT security within e-government processes, there are three aspects to highlight:

– Security needs early planning to be implemented appropriately. It is nothing that can be added to a process just before "going on-line". Security has to be viewed as a feature – if it is not, the entire system will be buggy.

– Security has to be derived from the process requirements. Most "traditional" processes contain some security elements – even if these are not obvious or made explicit; these security elements (therefore) have to be deliberately researched with regard to their transfer into the "new" process.

– Security is functionality like other functions. It has to be tested in order to give assurance that it works properly. Systems with "security inside" have a better quality than systems without.

Last but not least: E-Government processes combine aspects of organisation and technology. Besides technology, there are three other variables in an organisation that have to be taken into account and that interact with each other: people, structures and tasks. Taking this into consideration will help e-government to live up to its initial expectations.

6. ENDNOTES

[1] The starting point of this campaign was set by German chancellor, Gerhard Schröder, who held a speech at the D21-congress in Hannover on 18th of September 2000; whereas he launched the government initiative "BundOnline 2005".

[2] See *www.bund.de.*

[3] See *www.bsi.bund.de/literat/faltbl/egovernm.htm* and for further information see also *http://foev.dhv-speyer.de/ruvii/SP-Egov.pdf.*

[4] There is a legal regulation for public construction procedures (German: Verdingungsordnung für Bauleistungen - VOB) that describes how awarding procedures have to be conducted. For further information see (BAnz, 2000).

[5] Additionally, there is in Germany a special law that deals with the subject how public administration has to conduct its daily work (German: Verwaltungsverfahrensgesetz).

[6] In Germany there is a procedural regulation called "Verdingungsordnung für Bauleistungen – VOB" (BAnz, 2000) that is based on a special directive called "Vergabeverordnung" (BGBl, 2001). Both are implementing the European law called "EU-Richtlinie über den elektronischen Geschäftsverkehr" (ABl, 2000).

[7] See *www.bsi.bund.de/fachthem/egov/index.htm;* and here especially the module "Analysis of cryptographic requirements" as part of the e-government manual.

[8] See *www.bsi.bund.de/gshb/index.htm*; and here especially chapter 2 "Application of IT baseline protection manual" as a part of the baseline protection manual.

[9] For further information see (Rannenberg et al., 1999).

[10] For further information see (ISO13335).

[11] See VOB/A §21 Nr.1 in combination with VOB/A §22 Nr.1; where it is said that: "... the party awarding the contract can accept bids that are signed with a qualified signature and handed-in encrypted - ... and that they have to be stored encrypted".

[12] For further information see also *www.bsi.bund.de/fachthem/egov/download/006.pdf* (Seidel, 2001).

[13] If there is a 2nd signature, then it is possible to include the hash value (instead of the "signed & encrypted bid") within the acknowledgement.

[14] See *www.bsi.bund.de/fachthem/egov/index.htm;* and here especially chapter 3 "Analysis" and in addition, a module dealing with the selection of appropriate (cryptographic) mechanisms for authentication and encryption is following soon – both as part of the e-government manual.

[15] See *www.bsi.bund.de/gshb/index.htm;* and here especially chapter 3.0 "Security Management" and chapter 3.7 "Cryptographic Concept" as parts of the baseline protection manual.

[16] For further information about the certification scheme based on the baseline protection manual see *www.bsi.bund.de/gshb/zert/index.htm.*

7. REFERENCES

Seidel, Ingelore: *Öffentliches Auftragswesen.* Stand Mai 2001, S. 75-78. In: Dauses Handbuch des EU-Wirtschaftsrechts. Sonderdruck. Verlag C.H. Beck.

ABl 2000: *EU-Richtlinie 2000/31/EG über den elektronischen Geschäftsverkehr vom 8. Juni 2000.* In: ABl. L 178, 17.07.2000.

ISO 13335: *Guidelines for the management of IT security.* Part 3 and part 4.

Rannenberg, Kai; Pfitzmann, Andreas; Müller, Günter: *IT Security and Multilateral Security*; pp. 21-29 in Günter Müller, Kai Rannenberg: Multilateral Security in Communications – Technology, Infrastructure, Economy; Addison-Wesley-Longman, München, Reading (Massachusetts) et al. 1999; ISBN 3-8273-1360-0.

BGBl 2001: *Verordnung über die Vergabe öffentlicher Aufträge vom 09. Januar.* 2001. In: BGBl. Teil I Nr. 3, 18.01.2001.

BAnz, 2000: *Verdingungsordnung für Bauleistungen Teil A (VOB/A)* vom 30. Mai 2000. In: BAnz. Nr. 120a, 30.06.2000, S. 19125.