A Holistic Approach for Providing Security Solutions in e-Government

Maria Wimmer  
University of Linz, Austria  
mw@ifs.uni-linz.ac.at

Bianca von Bredow  
University of Zurich, Switzerland  
bvonbred@ifi.unizh.ch

Abstract

E-Government is now in a stage where effective and secure online transaction services have to be provided. Yet, initial security are primarily technical. Many technical concepts and tools have been developed in the scope of e-Commerce. Applying these to the scope of e-Government need careful investigations. Security aspects do not, however, concern technical aspects only. The particular security needs of e-Government must be established from a non-technical viewpoint as well, and differentiated from the scope of e-Commerce. This presents a unique challenge regarding processes, judicial factors and strategies. In this contribution, we suggest a holistic concept that integrates security aspects from the strategic level down to the data and information level in order to address different security aspects in a comprehensive way.

1. Introduction

The global IT revolution is growing rapidly. Governments and businesses have to be ready to meet the increased demand for effective and secure online services. Providing secure online services in e-Government requires careful deliberation on different levels and for the distinct domains of e-Government.

The security issues first coming to mind concern of course technical aspects. Here, much has been done to provide secure transactions, to protect against unauthorized access to information and data, to protect against hacker attacks etc. Many methods and security systems which have been developed for e-Commerce in the private sector may also be adapted for e-Government without much change. Indeed, regarding security from a technical perspective, no big differences exist between e-Government and e-Commerce solutions. The differences are embedded in issues regarding processes, judicial factors, and strategies. For example, the data and information being manipulated within an e-Government process may be more sensitive than that within an e-Commerce process. Filling in a tax declaration requires the personal data of a citizen or confidential data of a company, whereas the quantity and price of electronically offered products is to be considered rather public.

On a strategic layer, public administration has security obligations and responsibilities for a wide range of electronic processes in the various e-Government fields having many involved parties. These security strategies are not very clear upon first inspection. By comparison, e-Commerce builds on clearly defined strategies and goals based rather on obvious security strategies for two-way interaction.

Further detailed differences between e-Commerce and e-Government will be found in section 2 before the discussion of distinct security threats that may be important for e-Government (section 3). Section 4 introduces a three-dimensional security concept for e-Government addressing the different domains of e-Government, the distinct levels of electronic processing and four distinct abstraction layers of a holistic view on e-Government systems. Based on this holistic security concept, some solutions for security are deliberated for a specific e-Government application, namely car registration (section 5).

2. e-Government vs. e-Commerce

Security issues have to be carefully investigated for the public sector’s electronic processes. However, one might claim that – since many security approaches already exist in the commercial sector – concepts from e-Commerce could be adopted right away. In the following, we will

![Figure 1: Differing aspects of issues demarcating e-Government from e-Commerce](image-url)
demonstrate some demarcations between e-Government and e-Commerce that stress the need for more thorough deliberations of security concepts for e-Government. Thereby, we will employ the distinct abstraction layers put forward in the holistic security concept as developed in section 4. As Figure 1 indicates, the higher the abstraction layer, the more differences exist between e-Government and e-Commerce.

On a strategic level, an important demarcating factor between e-Government and e-Commerce is that the administrations’ core business and responsibility deals with society’s safety, secure life, organized living together, etc. In order that Government can guarantee such a well-structured quality of life, these objectives are detailed in many administrative and governmental processes, also reflected in laws and legal norms. On the other hand, the commercial interests of private companies involved is much broader than in the commercial field.

Governmental rationality is highly bound to the legal framework defined by the constitutional state. One can recognize a marked influence of laws on administrative processes, where optimization and standardization are not always possible; conflicting trade-offs may exist between process optimization and governmental policy that may not be neglected. Hence, security issues supporting governmental policy have to be high on the agenda when developing e-Government systems.

Furthermore, the variety of governmental processes may require a variety of differing security measures. Even if some concepts for well-structured processes in e-Commerce may be adopted for e-Government, the core business of Government concerns individualized case processing and specific negotiation processes. A high degree of non-instrumental rationality is involved and concerned parties may have rather conflicting interests. Here, each case has to be considered on its own and requires specific security measurements. On the other hand, in the commercial domain, attempts to optimize and standardize business processes are always based on goals such as cost reduction and benefit increase.

Additionally, commercial business mainly is oriented towards bi-directional business transactions with rather homogeneous interests. Here, security issues may be settled once among the two business partners and used without changes for any future transactions. In e-Government, most processes have to be seen as individual cases and therefore require individual security treatment as well.

On a rather technical level of protecting information and data, however, no big differences exist. Information in e-Commerce is as vulnerable as in e-Government due to technical malfunctions and disruptions. The vulnerability of the flow of information and of information itself has increased along with a higher dependence on data processing as well as on information and communication technology.

Moving onto e-Government requires, therefore, careful investigation of security issues. For electronic transactions in particular, security is a major concern for the public sector, due to numerous risks that may threaten our technology-dependent systems. This may touch raw data and information as well as applications, the processes, or even the whole systems themselves (cf. [9]).

To define security requirements for e-Government systems, analyzing security threats may be a good starting point.

3. Security threats in e-Government

3.1. Technical security threats

From a technical viewpoint, Saarenpää et al [10] have defined at least 20 different risk types with relevance to data security. In a general classification, these can be grouped into the following three basic threats [9], [10] which are not specific to e-Government, but also exist in e-Commerce:

- Loss of confidence or credit (unauthorized information access or uncompleted transactions)
- Loss of integrity (unauthorized modification)
- Loss of availability (damage of functionality).

In more detail, these threats can be divided into inter-communication, intra-communication and system threats. Inter-communication threats may be passive or active. Passive threats are manipulations which cannot be proved, described as “leaking” out of information. Possible passive threats are e.g.:

- keeping violation of data and communication relations secret
- revelation of identities in anonymous communication relations
- analysis of web traffic.

Active threats are caused by manipulation of objects or relations. In comparison to passive threats, they can be recognized but cannot be prevented. Examples are:

- Masquerading assuming an unauthorized identity
- Message sequence manipulation (diverting or re-sending of messages)
- Modification (corruption of messages and routing information).
Intra-communication threats are caused by the communication participants themselves such as:

- repudiation of origin and of receipt of communication content
- computer fraud and computer forgery
- injuries of security marks like access marks or classification marks.

The third type of threats refers to systems or resources. They are manipulations of resources like overloading, reconfiguring or reprogramming. Examples are the misuse of access rights, Trojan horses, Viruses, Spooling, Flooding etc.

From a technical viewpoint the presented threats are similar for e-Government systems as well as for other IT systems in the private sector. Technical security solutions are similar in implementation in the two scopes of e-Commerce and e-Government.

Knowing classification schemes for analyzing threats within an IT infrastructure is not enough, though. Security threats have to be investigated from a non-technical viewpoint as well. These investigations have to be carried out with a sense of strategic, tactical, and operational security deliberations, especially for transactions, processes and even within a whole community.

3.2. A non-technical viewpoint

From a non-technical viewpoint, additional security deliberations and threats arise. In e-Government, almost all data are more security-sensitive. This is clear when considering that the consequences of misuses of stored citizen data are more important than in the scope in e-Commerce. For example, the consequences of misusing stored citizen data for committing crimes are more dire than the disadvantage of a credit card misuse when shopping on the Internet.

Citizens feel vulnerable when using e-Government systems. They want to have security solutions which provide subjective trust. Citizens have no opportunity to verify provided security. They have to accept a certain security uncertainty. The difference with e-Commerce is that citizens using e-Government will not accept the same uncertainties as they might when using e-Commerce systems. They need more trust when they use e-Government systems.

Additionally there are important differences between the scopes of e-Commerce and e-Government which influence the whole security context and the existence of different threats.

In the scope of e-Commerce transaction participants are able to pick out with whom they want to have business relationships. In the scope of e-Government public administration must consider the needs and the specific situation of all citizens. On the one hand, this fact causes a certain transparency of administration acts and citizen data for understanding and reproducing of individual cases. On the other hand it has to prevent that this transparency leads to unauthorized data access and the invasion of privacy.

Additionally, making profit is the main stimulus for signing contracts in e-Commerce. These contracts have allowed structures and are embedded in a well-structured legal framework. The processes in e-Government are not profit-oriented and they are not necessarily well-structured like most processes in e-Commerce. Security threats and deduced security requirements result from the unstructured and semi-structured realities of administration processes as well. Analyzing specific security threats and requirements for such administration processes needs consideration of context, participants, as well as of all further special conditions. Specifying general security threats and requirements in e-Government is not possible. It is necessary to look at the specific situation of each transaction process.

Additionally, security threats have to be investigated for the specific scopes of each of the different e-Government domains: e-Administration, e-Assistance, e-Democracy, e-Voting, e-Justice, etc.

Finally in each of the distinct levels of electronic processing (information, communication or transaction), selective security requirements need to be specified. A portal solely providing information has fewer different security requirements than an e-Government system which has to support comprehensive transaction possibilities with highly sensitive data. Therefore, in the following section, we suggest a three-dimensional model for comprehensive security threat analysis in e-Government in order to develop adequate and secure e-Government processes.

4. A holistic framework for developing secure e-Government solutions

To provide security solutions for e-Government, we postulate a holistic approach with the main focus on the processes to be carried out. This approach is based on investigations in three dimensions (see Figure 2): the specific scope of the various domains of e-Government, the level of advancement in electronic processing and the distinct abstraction layers. With a holistic approach, security is considered beyond the technical aspects: social, political, cultural, and legal impacts on security requirements are considered as well.
Security threat analysis is a very complex task. The 3-dimensional model promotes and supports a comprehensive security threat analysis from different points of view. Furthermore, deep insights in security requirements and security solutions are gained. In this way, a security model in the scope of e-Administration takes into account:

- security issues of e-Administration that might affect the other three domains. E.g. are there privacy problems when the same databases are used?
- what level of advancement in electronic processing is striven for? Electronic transactions present other security issues than simple information provision;
- on which level must security threat analysis be made? Security requirements comprise strategic security deliberations (level of general business models), tactical security deliberations (level of processes), operational security deliberations (level of transactions and technical issues) and investigations on the level of data and information.

To take into account all three dimensions at the same time is quite a difficult and complex activity. Furthermore, from a practical point of view, concrete implementations of e-Government systems concentrate around a specific field of application. Hence, the generic model proposed above should, at first glance, provide a general framework for security investigations which, for the solutions, has to be fleshed out in the respective context of the domain and for the processes to be developed there. In section 5, we will provide more concrete solutions for one of the four e-Government domains. The three dimensions of the above holistic security concept must be detailed first, however.

4.1. Holistic view throughout the different abstraction layers

Security aspects should not only be considered as technical issues. They also need careful investigation from a non-technical viewpoint. We suggest a holistic concept that integrates security aspects from the strategic level to the data and information level. The classification of the abstraction layers we use here is based on two basic sources: the Information Architecture of Mok [6] and the Business Media Reference Model (BMRM) of Schmid [11].

Mok’s Information Architecture reflects a bottom-up approach from data to concepts which starts with understanding the various data and information. It continues with determining the relationships and behavior thereof in order to build object clusters and structures. Then, the layout and representation of these object structures at the interface are developed and integrated in a user interface in the next layer (interactivity design). The interactivity layer is also the layer where Mok defines the shift from the data and information layer to the conceptual layer. Based on the interface layer, the content design (processes and workflow) is carried out and, finally, the identity design (strategies, organization’s philosophy and rationale) is built.

By comparison, Schmid’s BMRM provides a top-down four-layer concept to describe different views on electronic business media: Community, Implementation, Transaction, and Infrastructure. The community view describes the relevant business community and the underlying business model for defining relevant roles of involved agents and their information flows. The implementation view concentrates on business procedures and processes. The transaction view offers generic services for supporting the realization of the defined business processes. On the level of infrastructure, components for building respective IT infrastructures are provided. The BMRM is a two-dimensional model that, at the same time, provides insight into the four transaction phases (which we adopt for the dimension "levels of electronic processing", see next subsection).

For the dimension of abstractions within the three-dimensional framework we suggest, parts of the Business Media Reference Model and the Information Architecture have been adopted. The result is a four-layer structure that is traversed in a middle up-and-down design policy in order to address different security aspects in a comprehensive way:

1. on a community level a strategic e-Government security model is needed that fits to the overall purpose of the e-Government system and represents an integrated overview of potential security threats to participants and their information flows;
2. on the process level, starting from the above strategic security model, the different administrative and/or governance processes have to be analyzed regarding possible security problems;
3. on the interaction level, process models and security models have to be implemented and integrated with specific focus on two-way and multicast communications and transactions;
4. on the infrastructure and data & information level, security mechanisms address access control, data protection etc.

On the highest level of abstraction (community level), the organization which intends to develop an e-Government system has to define overall security strategies. These determine the scope within which security decisions should be made on the tactical (processes and operational interactions, technical, data & information) level. Issues such as the degree of confidentiality, integrity, identification, authentication and non-repudiation are thereby settled. Further, a general security architecture should be provided including a broad security management that also decides about corresponding security services and mechanisms.

Administrative structures have a lot of critical functions where responsibilities cannot be sacrificed for the sake of process optimization. The general security strategies from the upper layer are detailed into specific service delivery processes and workflow. The overall strategies need to ensure that the procedures reflected in the processes do not violate the underlying rules, that these protect the rights of citizens and even provide a control mechanism for safeguarding legal validity. Therefore, at the process level, the objective is to define governmental and administrative procedures and processes that may be distinguished between structured, semi-structured, and unstructured processes (according to Lenk [5]). Here, single processes and whole workflow are investigated and designed that may have specific security requirements. Transaction processes in particular need careful attention regarding security problems.

The aim of a comprehensive security strategy is to provide special security concepts for different processes and transactions. This is the core prerequisite for secure communications and transactions in the scope of e-Government. Because of the specifics of processes in public administration, security models and process models have to be developed in parallel and these have to correlate. By that, all necessary security aspects can be uncovered and mapped into security requirements.

The interaction layer deals with the execution of processes. Depending on the process type and the stage in a process, different security issues become important. Security issues mainly concern two-way and multicast communications regarding transaction processes. Here, the conceptual solutions of the process model layer have to be implemented. In this respect, the security management has to clarify the following aspects for each process:

- What has to be secure? Some exemplary answers are: whole applications, transactions, data, server, clients, communication, etc.
- For whom or what it has to protect for? - Exemplary answers are: hacker or employees.
- What kind of services and applications are needed? - Exemplary answers: access control services or monitoring and checking applications.
- Which services from the internet are needed? - Exemplary answers are: downloads, SSL or certificates.

Though a lot of technical security solutions and architectures already exist on an infrastructure layer in the scope of private business. Here the main focus is put on certain aspects or functionality of security such as digital signatures, PKI-infrastructures, firewalls or anti-virus mechanisms. Many of them have to be adapted for the special context of e-Government. However, the specific responsibilities embodied in governmental work, and especially the requirement for multicast communication, require security mechanisms that do not hamper the core responsibilities and functionality of public administration.

At the data and information level, issues such as access rights and control as well as data protection etc. have to be addressed and implemented.

With the four-layers of abstraction, security issues should be deliberated in a comprehensive way for a specific e-Government application domain. At the same time, the security issues should be detailed for the requested level of advancements in electronic processing.

### 4.2. Changing security issues in the various fields of e-Government

In the actual discussion on e-Government, several distinctions of e-Government domains can be found. Here, we adopt the distinction by Gisler and Spahni [2] that name the following fields of e-Government: e-Administration, e-Democracy, e-Voting and e-Assistance. The selection of this distinction is based on the different security requirements that arise for the various e-Government domains. For example, e-Administration requires other security issues than e-Voting or e-Democracy because democratic discussions on the web requires the promotion of political opinions whereas in a tax declaration, sensible data of a citizen or a company are transferred and processed. Further, e-Voting requires at first hand the authentication of the voter, but when it goes to process the votes, traceability of a single vote to the voter is to be avoided. E-Assistance is still another domain with distinct security issues.
In this paper our emphasis will be on the domain of e-Government. But in the sense of a holistic approach we have to take into account the influences and dependencies of the three other domains to our crucial domain e-Administration as well.

4.3. Different security requirements on distinct levels of electronic processing

Most important for successful e-Government are two-way or multicast communications and transactions between administrations and their external partners (citizens, companies and other administrations). Contrary to that, simple information providing normally does not require so much security effort. To explain and elicit security requirements for the different instances of electronic processing, the three core business concepts of electronic Government have to be investigated: information, communication and transaction (cf. [1]).

In order to deepen security requirements for the purpose of e-Government transactions, we will adopt once again the BMRM transaction model of the University St. Gallen [11]. The BMRM was developed and successfully applied in the scope of e-Commerce. According to the BMRM, the four phases of e-Government transactions are: knowledge, intention, contracting and settlement.

Following we put forward some examples of security requirements that have to be addressed in the different phases of an e-Government transaction in the domain of e-Administration.

In the knowledge phase of an e-Government transaction, security is not yet so high on the agenda, because no real private and personal data is transferred over the net, yet. Only general information on a specific public service is searched and collected. The security aspects rather regard public authorities that have to protect the information they provide over the net against active and passive attacks like masquerades, denial of service, viruses etc.

In the intention phase, first personal data may be sent over insecure nets and hence, the most important security requirement is to guarantee a secure transfer of such sensitive data. Nobody else than the citizens themselves and people who are authorized for the special administrative process may work with personal data. Confidence of data and protection of privacy are more important than in the scope of e-Commerce.

In the contracting phase, mechanisms for secure electronic contracts like document containers have to be provided.

In the settlement phase, mechanisms for secure document deliveries and secure payment transactions are necessary. Further, monitoring and checking functions have to be secured. Each involved person - especially citizens - have to know who has processed which personal data when and why. By that, the trust in e-Government systems and their acceptance can be improved.

5. Exemplifying security solutions for e-Administration

In e-Administration, the core objective and rationale is to implement policies that have been negotiated and agreed upon within e-Democracy. To work out security solutions not only at a technical level is of paramount importance. Security must be carefully integrated within the respective system context and application domain starting from strategic decisions. Only by that can comprehensive security solutions be provided. Within the process perspective, non-technical issues like law, confidence in systems etc. have to be taken into account as well. The holistic framework we introduced in the last section provides a good guideline for developing such comprehensive, secure and successful e-Government solutions.

In the following, we will exemplify the holistic framework for secure e-Government systems through an application in the domain of e-Administration on the rather well-structured process of car registering based on the Austrian law case (cf. Figure 3). We start with the development of security strategies within the community view. In accordance to the suggested holistic framework (cf. Figure 2), security models are, then, developed. These will be detailed for the transaction view and even for the infrastructure layer. Despite of that, influences and dependencies of the other three domains to the specific e-Administration process will be investigated. Security issues from a data and information layer point of view are not detailed here, instead, the reader is referred to scientific literature in the field of data and information security [4], [8], [13].

5.1. Community view

On the highest level of abstraction, the very first step is to select the specific application domain and to determine, on a very coarse grained level, the key players within that domain (i.e. involved participants with their respective roles and responsibilities as well as strategic decisions and constraints having to be born in mind). In the next step, the respective underlying governmental and administrative model can be sketched. It is important to set up this general frame for the development of any e-Government system, because once (most reasonably at the beginning of the project) the underlying requirements and goals have to be made clear and visible to every party being somehow involved during the development process.
authority or – such as in the Austrian case, where car registering is outsourced to insurance companies - from a private organization that is officially entitled to do so.

Starting from this strategic measurements, the process of car registering can be deliberated in more detail and for the purpose of describing the whole workflow as well as the respective security models.

5.2. Process view

Within the process view, the main participants of the process under consideration are identified and their relationships and dependencies are elicited. Further, their roles and responsibilities are described. In the case of car registering, these are the citizen (or a company or an institution), the insurance company and different involved authorities. In general, these are the provincial authority in charge of the car registering process and the municipality that issues the register record on the citizen’s place of residence.

In e-Government, the two authorities may still be involved depending on the overall strategy of data exchange and data access. In the scenario strategy we introduced within the community view, though, only one authority might be visible/transparent for the applying citizen. In addition, also business partners like banks performing the payment of the registering fees or car shield manufacturers might be involved. Finally, in case of a conflict, jurisdiction might be needed. Figure 4 sketches the different categories of parties that might potentially be involved in a car registering process (the minimal number of parties is highlighted in gray).
<table>
<thead>
<tr>
<th>Step</th>
<th>Involved party</th>
<th>Required Objects</th>
<th>Resulting Objects</th>
<th>Underlying rules</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Citizen</td>
<td>report § 57a, car-type booklet, contract, mandate</td>
<td>application form</td>
<td>Insurance agent is entitled to carry out the preparing steps for applying for registering a car</td>
</tr>
<tr>
<td>2</td>
<td>Insur. Agent</td>
<td>mandate</td>
<td>confirmation of residence of the citizen</td>
<td>With the mandate, the insurance agent is entitled to receive the confirmation of residence of the citizen from the municipality</td>
</tr>
<tr>
<td>3</td>
<td>Admin Munic.</td>
<td>Application form, report § 57a, car-type booklet, contract, confirmation of residence</td>
<td>Administrative file</td>
<td>For each incoming application form, an administrative file has to be created</td>
</tr>
<tr>
<td>4</td>
<td>Admin Prov./Med. Ins.</td>
<td>Ibid.</td>
<td>“accept” for further processing, “request for further material”, “reject” of application</td>
<td>The administrator has to control the application form and accompanying objects for their completeness</td>
</tr>
<tr>
<td>5</td>
<td>Other Admin.</td>
<td>Ibid., Administrative file, internal data bases and files</td>
<td>“accept” for further processing, “reject” of application</td>
<td>The administrator has to control the data entries in the internal databases regarding the car and the citizen in order to avoid misuse, fraud, etc.</td>
</tr>
<tr>
<td>6</td>
<td></td>
<td>Registering fees</td>
<td>Car tag, official allowance certificate, report § 57a, car-type booklet, contract</td>
<td>When all data is okay and the control process goes for “accept”, then the case can be processed</td>
</tr>
<tr>
<td>7</td>
<td></td>
<td>Registering fees</td>
<td>Ibid.</td>
<td>The insurance agent collects the administrative fees and hands out the material to the citizen</td>
</tr>
</tbody>
</table>

Figure 5: Scenario workflow description of the car registering process showing the different steps, the involved parties in a given step and the material and underlying rules being part of a specific step.

Eliciting security threats and deducing security requirements for car registering should be developed in parallel. Regarding electronic car registering, the dimension of advancement in electronic processing requires the clarification of the following issues:

1. information:
   - Decide on what kind of information processes (including their content) that is provided via public accessible nets needs to be protected?
   - What are the underlying legal aspects to be realized?
   - For which information processes are security measures required?

2. communication:
   - Which processes require protection for communication
   - What and when does communication need protection?

3. transaction:
   - Which transactions need specific security measures?
   - What needs to be secured?

According to the scenario given in Figure 3, in general, car registering is a well-structured process. The citizen acquires her car where she also receives the control report (§ 57a), the car-type booklet and the contract (cf. Figure 5). With that material she contacts her insurance agent and issues a mandate with which the agent acts on behalf of the citizen (1). At the same time, the agent fills in an application form, lets the citizen sign the application and goes to the municipality to get the confirmation of residence of the citizen (2). Finally, the agent goes to the agency or to the authorized mediator at the insurance company to complete the registering process (3). The mediator or administrator controls the application form and creates an administrative file (4). In the next step, s/he controls the entries that may already exist regarding the citizen or organization (5). If all data is complete and no exceptions exist, the case is processed, i.e. the tag is handed out together with the official allowance certificate for the car holder and the insurance agent pays the fees.
(6). In the next step, the agent contacts the car holder and settles the administrative act (7).

Independently from the strategic decision whether the process will be outsourced to a major part to the insurance company or not, in future, the citizen might handle several steps of car registering via the Internet. E.g. she might contact the insurance agent via the electronic way and most of the required documents might be available in an electronic form. According to the holistic framework for security issues, the development of respective security models has to be defined for the whole workflow.

Above process description already provides a good basis for where security measures are required: For each step in the process description, security models have to be investigated. Let us imagine the first step of the above description in an electronic mode and, thereby, exemplify the required security models: Which is the best way to identify the citizen? How can it be granted that only the respective citizen and authorized administration employee have access to personal citizen data? How can it be granted that the required material has not been manipulated? How can the digital signature be applied in an appropriate way? etc.

In a modified scenario for electronic processing, step 2 might be replaced by a direct request from the provincial authority. Also here, adequate security models have to be developed that address, amongst others, the following issues: access rights (authority – authority), secure that only the required data can be extracted and not more, secure transfer of the data via Internet, etc. Still other security aspects have to be handled, when it goes on settling the administrative act: provide secure transaction on payments, establish a secure communication to transfer the result of the process to the citizen/organization, etc.

This simple scenario of car registering shows in a very effective way how many security aspects have to be taken into account for implementing electronic car registering. These issues not only regard a technical level. Instead, many of them rather address non-technical issues. It has to be stressed that generic security solutions are not possible for such complex processes. For e-Government processes, a holistic approach is required that allows comprehensive deliberations (cf. the holistic model as put forward in Figure 2) which provide deep insights into the special context where the security solution should be applied.

5.3. Interaction layer

The interaction layer represents the most sensitive and dynamic layer of the concept. Here, generic services are offered for supporting the realization of the defined processes mentioned above. In this view, we keep a clear separation between the four key phases of an electronic transaction: knowledge, intention, contracting and settlement (cf. [11]).

In the knowledge phase, citizens acquire knowledge and information on what kind of procedure they have to follow when carrying out a car registering process, what material is required and which parties they have to contact (especially whom to contact: citizens/oranizations not only want to be forwarded to a role, they rather request the name of the person in charge). Further, they want to know the specific rules and laws they have to follow and bear in mind regarding their tentative. In the interaction layer, services which support the effective allocation of responsibilities and resources are needed. Citizens want to be trustful when they send their personal data. Only the right person should get the data.

In the intention phase, the crucial point is that the citizen can express her intention to register her car. In order to proceed with the process, generic security services like digital signature mechanisms, authentification, secure communication facilities, etc. are necessary in an appropriate way.

In the contracting phase, all necessary process documents have to be linked together. The course of a process must be provable. We can imagine that a container solution like from Greunz et al [3] is an appropriate solution to offer a generic service in this way.

In the settlement phase, services for secure deliveries of documents etc. and services for secure payment transactions are necessary.

5.4. Infrastructure layer

On the technical level, components for building the respective infrastructures should be provided. According to the proposed services in the above interaction layer, three possible solutions for providing security in e-Administration seem promising and feasible:

- Public Key Infrastructure (PKI) [7], [8]
- Attribute Certificates (AC) [12] and
- secure XML Document Container (XML-DC) [3].

For the allocation of responsibilities in the knowledge phase we suggest the concept of AC [12]. In the knowledge phase the biggest problem is the allocation of responsibilities of administration and their employees. The publication of authorizations for signing certain types of notifications can be done by introducing attribute certificates and making them publicly available in a directory. An unambiguous and secure way of identifying records and location of the responsible persons for handling certain requests is thereby feasible. An attribute certificate is a reference to the base certificate(s) according to the X.509 standard which it belongs but it contains no public key. It is a separate structure with additional attributes like clearance or authorizations. By
using attribute certificates allocation problems can be solved, the response speed on inquiries can be improved and unauthorized inspections of data records can be prevented.

For the intention, contracting, and settlement phases, PKI [8] and XML-DC [3] seem the more appropriate solution. When a citizen intends to register a car electronically he needs a document container where all forms and additional documents can be stored. Such a container is not merely necessary for bundling all documents but also for security aspects concerning reconstructions of processes as well. A document container ensures the availability of all evidence in case of conflicts. Additionally, a document container is a secure database where access rights can be defined for each transaction case uniquely. Using the document container in the subsequent transaction process steps as well (contracting, settlement) he will create a collection of all necessary documents with possibilities of evidence and secure settlement of the whole process.

For compliance with legal conditions of transactions in e-Government a Public Key Infrastructure (PKI) in the sense of the appliance of digital signatures is a necessary prerequisite. Only PKI ensures that the requirement of legally binding transactions can be fulfilled. Citizens, administration, and business partners need public and private keys and certificates, and an appropriate infrastructure has to be provided. The problems and cost of smart cards and smart readers are well known as are the problems and costs of certification. Alternative solutions, e.g. applications like Pretty Good Privacy (PGP) should also be considered. For further technical aspects and legal considerations we refer the reader to the literature [4], [7], [8].

6. Conclusions

In this paper, we have presented first deliberations on how existing security solutions can be applied in the scope of e-Administration in an appropriate manner. However, further security questions raised in the implementation view still have to be investigated. Additionally, further research in the field in e-Government investigating the application of existing security solutions for the other three domains of e-Government is necessary. The crucial point will be the investigation of dependencies between security solutions between all four domains of e-Government. Additionally, research questions concerning providing security solutions for gaps between defined security requirements and existing security solutions have to be answered. We presented the application of existing security solutions and the development of newer solutions will be an interesting scope of further research work.

References

[5/6/2001]