Tallinn University of Technology

FACULTY OF SYSTEMS ENGINEERING
Department of Automation

E-State From a Data Security Perspective

Arne Ansper

Tallinn, 2001

With editorial notes as of 2009

ABSTRACT

At the time of writing the original paper in 2001, Estonian public administration databases were still isolated from each other and the data exchange between these databases has been slow and inefficient. In the same year, the completion of a fast, reliable data communications network between state agencies which utilizes the Internet removed a major obstacle by promoting tighter integration of public administration databases, and created the opportunity to make communication between state agencies faster, more secure, and more efficient. To take advantage of this opportunity, public administration databases should cease to be isolated and be made accessible not only to the agency it belongs to, but to all authorized persons (regardless of agency) who require the information to help perform their jobs more efficiently, thereby improving the speed, security, and efficiency of public services. The new Internet-based public administration database network is referred to as the e-State.

This paper analyzes security problems which arise when public administration databases are opened to widespread electronic access. The analysis presented is based on the current legal situation as defined by Estonian law. Separate analysis is presented for agency-to-agency and citizen-to-government data exchanges.

This paper reaches the important conclusion that, due to substantially different scopes of risks and the countermeasures currently available, information security solutions developed for business organizations cannot be directly adapted for use in a public administration environment. To support this conclusion, a model for the e-State architecture is presented that, together with the appropriate legal framework, allows for the achievement of its main security objectives.

Additionally, the paper proposes the creation of an Internet portal and identification system for citizens (as in 'legal residents of Estonia') that would secure communication with public administration and state registries. The major security problem in such a portal is user *authentication*, but the Estonian electronic ID card is seen as a solution to this problem.

Table of Contents

1 INTRODUCTION

The rapid development of computing and communications technologies during the 1990s created a new kind of business environment. Today, the term "e-Commerce" implies business processes that are faster and more effieient, and that are driven by the Internet and the Public Key Infrastructure (PKI). Notable examples of e-commerce include Internet stores, online banking, and Business-to-Business (B2B) solutions. At the time of writing *[2001 –ed.]*, Estonia has ignored the rising use of Internet resources; however, this situation may soon change for the following reasons.

Firstly, there is no reason why technology developed for business organizations wouldn't be appropriate for government use. After all, the state can be viewed as an enterprise, the purpose, business processes, and organizational structure of which are defined by the existing business law.

Secondly, the general public is growing impatient with the outdated methods of conducting business. At present, even for trivial matters, state agencies must be visited in person. Only paper documents are considered official, but getting utilization of paper documents costs time and money. Instead, people would like to settle state matters quickly and easily over the Internet [47].

Thirdly, the Estonia government acknowledges the need for change [40]. While government expenses should be reduced to keep the national budget in balance, there is little that can be achieved with current methods.

The second and third reasons listed above, are not inherent to all countries. For instance, at the time of writing *[2001 –ed.]* most United States consumers are still suspicious of e-commerce, considering it too insecure [10]. In contrast, the widespread, positive attitude of consumers in Estonia towards utilizing e-commerce has created a fourth reason is created: by undergoing quick and radical public administration reforms, positive attention is created for Estonia [21].

These reasons have been understood for a long time, and ideas about the emergence of a so-called "e-State" have been more or less radically expressed several times [33], [34], [16]. While the objectives are clear and stated repeatedly by Estonian visionaries, how they can be accomplished is unclear. Some analysts believe the Internet should be available to every person [25]; others think that it is crucial to put the digital signature in use as soon as possible [34]; still others put their hopes on XML to tidy the disarray in the information technology (IT) landscape [49].

The problems inherent to an emerging e-State are being studied in several research organizations including the Institute for Electronic Government, at International Business Machines (IBM); the Center for Technology and Government at the University of Albany; the John F. Kennedy School of Government at Harvard University; and the Institute for Development Policy and Management at Manchester University, England.

The e-State is more than just an information technology problem; rather, it can be analyzed from various viewpoints, raising several questions; for instance, will the intensive use of IT increase not only democracy, but also the "digital divide"?

Developed countries have long observed the emergence of their inherent e-States and have set clear guidelines and established coordinating and directing offices with sufficient funds. Examples of such countries include the United Kingdom and the United States [51] [52].

In Estonia, the creation of an e-State has often been considered from a practical, but narrow, information technology viewpoint, the focus of which has been on developing only the infrastructure (communication channels, computer workstations, and PKI). The Tiger Leap Foundation, a national specific programme launched by the Estonian government with an aim to increase Estonian school education quality utilizing modern information and communication technology, has successfully educated the general public about IT in the late 1990s and early 2000s.

Researchers ([53], [54]) have identified three partially overlapping areas of e-State: e-Democracy, e-Citizen/e-Services, and e-Administration.

e-Democracy is defined as the direct participation of people in the decision-making process. Technology analysts see the Internet as the savior of democracy and a means by which to bring people back to the governing of the State. This area also includes the subject of e-Voting. Of the three overlapping areas, this is the most complex and difficult to put into practice.

The concept of e-Citizen or e-Services is understood as enabling citizens to interact electronically with the state. In practice, it is the creation of Internet portals which allow the citizen to exchange data and conduct business with the state. It is the most visible part of the e-State.

Finally, e-Administration is understood to be the use of IT to make internal government processes, faster, cheaper, and more manageable and efficient. It is the basis for the former two areas and is often hidden from the public.

For a few years already, e-Administration [40] and e-Citizen [47] systems have been under active development. e-Democracy (mainly e-Voting) is being discussed by lawmakers and the general public, but technically, it is still unfeasible [50]. The largest e-State project underway *[in 2001 –ed.]* in Estonia is X-Road, a Department of State Information Systems program for modernizing public administration databases. The primary objective of the program is to develop a means of electronic communication between state agencies and public administration databases in line with current legislation and to make public services available over the Internet.

As the existence of e-Administration is fundamental to the development of other, more visible parts of the e-State, this paper focuses on analyzing the problems of e-Administration. In Estonia, the data that are vital to the state is stored in public administration databases; therefore, the concept of the e-State is analyzed from the public administration database viewpoint.

The first part of the paper presents the principles that in the author's opinion should be applied when developing the changes to support the emerging e-State.

The main body analyzes a significant problem resulting from the creation of an e-State; that is, how to guarantee the security of data in public administration databases when the communication between citizens and the state becomes digital. The results of the analysis are presented as an architectural model of the e-State.

The main objective behind the new Internet-based architecture is to minimize the number of centralized services. Due to the nature of the services, the coordination of and supervision over the proposed data exchange system must be centralized. The upcoming monitoring service should be centralized for economical and security reasons, while all other services should be decentralized. On one hand, a decentralized architecture improves the availability of the system, since communication between two agencies relies only on the information systems of both agencies and on the communication channel between these agencies. On the other hand, decentralization helps to ensure the integrity and confidentiality of data, because data do not pass through third-party information systems.

2 THE BASIS FOR CHANGES

2.1 State and Enterprise

In some aspects, a state, or government, is similar to an enterprise. It has a structure, a budget, business processes, and so on. However, there are also significant differences between the activities of a state and those of an enterprise. Here, we will look at the risks that a state or a business can cause a third party with its activities, and the countermeasures available for risk mitigation.

For a business, third-party risks are limited to the extent of their investment. For example, customers of a bank risk only the money they have deposited. The bank could go out of business or deploy an insufficiently secure IT solution that could allow an attacker to hack into the accounts; still, the losses are limited to the funds that customers have in their accounts.

For a state, third-party risks are less limited. If the state deploys a poorly devised IT solution to perform its functions, an attacker could:

- Transfer another party's companies and real estate to *bona fide* buyers (see [44])
- Slander, libel, or otherwise damage another party's reputation
- Manipulate election results for political gain

There are also differences in risk reduction. If a business is no longer considered trustworthy, one could simply turn to a competitor to receive the same services. A state, however, has no competitors, and moving to another country is, for most people and for various reasons, out of the question. Moreover, the presence of competition motivates businesses to act reasonably for its customers and work to keep current customers and win new ones, but a state does not have such motivation.

More differences can be seen in how the activities of a business' subordinate units reflect the goals of the larger organization, the strategies used to achieve its goals, and the efficiency of coordination between its various units. A business is usually uniform, and the goals and strategies serve as the basis for all management decisions. In contrast, a state is diffuse. Every part of it has individual goals and strategies that should be developed in accordance with those of other units, but often aren't.

Finally, a business has much more freedom, in that there are no limitations on how it can motivate its employees, and neither is it particularly difficult for a business to penalize those who do harm to or work against it. For example, a customer could be blacklisted and never serviced again. When large and powerful businesses exhibit such behavior, a disciplinary effect is produced on small communities. In contrast, a state has limited resources to motivate public servants and punish those who commit crimes against it. Even criminal punishments eventually expire.

The types of risks incurred by a business and a state can be summarized as follows:

▨	**State**	**Business**
Risks	Unlimited	Limited
Alternatives	None	Some
Management/Government	Decentralized	Centralized
Methods of influence	Limited	Unlimited

As unpleasant as these facts are, they are important because the ultimate goal of data security is to reduce the risk of having the data compromised. To achieve this goal, risk assessment is performed and the results are compared to the costs of necessary security measures; this is done to find the optimal level of security with a minimum total cost. If the calculated risk exceeds acceptable risk, analysis is performed to determine which information assets to protect and which security measures to use. It may be necessary to discard security-critical but unimportant information assets to save on costs.

Compared to a business, a state faces somewhat different risks and can use different countermeasures to combat them, so neither the results of the risk analysis nor off-the-shelf security solutions can be used interchangeably. However, this doesn't mean that everything pertaining to security should be created from scratch, as there are numerous security solutions that a state could use, provided that the purpose and methods of their use is understood.

2.2 e-Kingdom or e-Republic?

When talking about states in general, it's important to know the form of government that is being referred to. This paper assumes a democratic country where the separation of powers (that is, legislative, executive, and judiciary) is respected [14].

Several assumptions made about an e-State in the previous section hold no validity for other forms of government. In a kingdom or dictatorship, for example, a lack of control methods or the diffusion of government are not problems. On the contrary, it would probably be easier and cheaper to establish an e-Kingdom than a democratic e-State.

In order for a democratic form of government to exist, it is important that it avoid an excessive concentration of power (either physical or intellectual); this ensures the separation of certain functions, and the creation of redundancy which avoids single spots of failure. The persistence of a state's strength and stability is ensured by a complex system of laws and regulations created over the course of time; the system establishes rules for lawful living, is the basis for bureaucracy, and creates the necessary redundancy.

New IT and communications technologies can make a government more efficient. However, optimization must be carried out carefully, as over-optimization removes the necessary redundancy that ensures stability. Also, not all bureaucracy is bad; some is essential to help preserve stability.

Furthermore, some security solutions would work well in a kingdom, but not in a democratic country. Since businesses more or less resemble kingdoms, few security solutions suited for a business environment are directly adaptable to a state environment.

2.3 Principles of State Development Process

Systems development is a relatively old discipline [22]. Over the course of time, several methodologies have been tried and researched, several grave errors have been made [5], and in response, numerous tools and paradigms have been invented to achieve results more efficiently. We've learned several simple truths, such as “The earlier a mistake is made, the higher its cost down the line” [32].

A state, too, is a system, and a very complex one at that, so the same principle holds true for state development. The most accountable, dangerous, and intangible phase is analysis, in which all possible inputs, such as needs, requirements, restrictions, principles, and goals, are collected. The inputs are analyzed, and from the inputs potential system architectures are derived. The architectures are then compared, and either the best architecture is chosen and developed further, or the entire project is discarded as unfeasible.

The development of a state rests on three bases: the laws, the advantages of new technologies, and the problems and hopes of the general public. These bases serve as the input into the analysis process, which could ultimately produce a model of the future e-State. Since existing laws are certain to conflict with newer technical solutions, the model must allow for compromise and resolution of conflict.

When planning the changes, assumptions should be as conservative as possible in an effort to maintain stability. Invariably, any new technology is (1) understandable only to a small group of specialists, (2) driven by powerful business interests, and (3) likely to change over the course of time.

Finally, there are not only technical aspects to analysis, but also legal and political. The results of the analysis can significantly affect the outcome of a state’s development; therefore, the process must be public, understandable to non-specialists, and properly managed to ensure efficiency and the attainment of goals.

2.4 Idealistic and Realistic Approach to Changes

If the aim is to establish an e-State, what should and could be the extent of changes, and how should they be introduced?

An idealistic approach would be to chart all the state's business processes, create a model (scheme) of state, optimize the model, and then create an electronic information system that corresponds to the model. One would then introduce changes in legislature and reorganize the operation of state agencies. In essence, this would mean a complete public administration reform, resulting in a state that operates with more efficiency than before.

Due to its gigantic scale, such a plan is hardly feasible, even if only the IT viewpoint is considered. The size of the model could be estimated by taking all existing government databases and counting the number of different data fields from the combined databases. The enormity of the resulting model makes it not only expensive, but also difficult to understand as a whole; hence, the main value of the model, i.e., providing an overview, would be lost. Another downside of the so-called "Big Bang" method of state reform is that in its inception phase, it could seriously destabilize the state.

A more realistic approach would be to first describe all typical state agencies; these should differ by size (that is, the number of employees or the amount of money budgeted) and by the monetary value of information assets managed. Next, a detailed model of each state agency would be created. To see if the models are realistic enough, they would be verified against a number of existing agencies.

Prospective new models must consider the following usage scenarios:

- Everyday work (communicating with citizens, decision-making, reporting)
- Personnel work (employment, dismissal, change of official duties)
- Support activities (maintenance and backup of the information system)
- Emergency activities (restoring the information system after a disaster, handling of security incidents, working when online systems are unavailable)

When creating the models, national infrastructure should be modeled alongside state agencies. Each new model must be in accordance with other new models and consider their requirements and services provided so that contingency measures and solutions can be developed to handle common problems; interfaces between systems can be defined, and operating standards can be determined. A good example of operating standards is the Recommendations for Standard Safeguard developed by Germany's Federal Office for Information Security [28].

After the development of new models, the most feasible or appropriate model can be selected, and building the corresponding infrastructure and related information systems can commence. It is likely that during development (and even in its later stages), corrections to the model, as well as to the standards and specifications that are based upon it, may be made. The coordination that this requires should be taken into account when planning the project.

While such a large project requires the intensive cooperation of businesses and numerous specialists from various areas, it can still be carried out feasibly, provided strong development methodologies, competent project management, and sufficient financial resources exist. The project should result in a number of standard "building blocks," or their detailed specifications, that can be used to build interoperable information systems. From a security standpoint, it is crucial to thoroughly analyze the security measures, determine their interoperability, and compile them into a standard set. These steps make it easier to certify a large number of information systems and provide a more secure integration of Estonia's many state information systems.

For the above reasons, the information system renewal project has to be disclosed to the public and include specialists such as lawyers and IT specialists from various areas.

Considering the extent of the project, it would be unrealistic for this paper to examine all the aforementioned topics. Hence, the paper examines only one problem out of the many that arise when building an e-State. Additionally, the threats that arise when opening electronic access to government databases to the public, and possible countermeasures to minimize the possibility of such threats materializing, will be examined.

3 ANALYSIS OF PROBLEMS CAUSED BY THE OPENING OF DATABASES

The following analysis aims to identify the principles that, technically, would allow the establishment of a secure e-State. Here, "security" [20:13], refers to the improvement of database availability and ensuring the traceability of data without damaging its integrity or confidentiality.

In addition, these terms are used and defined as follows:

- Availability: users have unrestricted access to the data
- Confidentiality: data are available only to certain specially authorized users
- Integrity: only certain authorized users can change the data
- Traceability: users who have modified the data can be identified

To analyze the problems inherent in a given system, it is best to start by creating a model of the system to be analyzed. First, a basic communication act is modeled and examined, followed by an analysis of more complex systems with multiple participants.

The problems which occur as a result of allowing public electronic access to databases can be solved using several methods. The following example clarifies the differences between various systems.

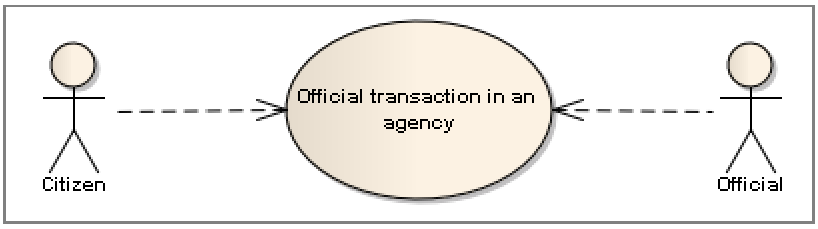

Figure 1. The use case to be analyzed and its participants.

Let us assume a citizen wishes to perform a transaction in state agency *A* that requires presenting a ***token*** (a legally binding document) issued by state agency *B* (see Figure 1). In the absence of an e-State, the citizen would first need to visit agency *B* and apply for the token, which takes time to process, either free of charge or for a fee. Only when the citizen has finally received the token can he can take it to agency *A* and present it together with an application to perform the transaction.

A comparable electronic system that could carry out the transaction and associated tasks could be developed based on the following examples:

1. Transfer the principles of an existing, paper-based system to the Internet environment. The citizen would make an electronic query to one state agency, receive a token, and

present it to the second agency together with another electronic query to perform the transaction.

2. Establish direct communication between state agencies, allowing one agency to query another agency's database directly and receive information that was previously transmitted via the physical token issued to the citizen.
3. Use any alternative possibilities, such as consolidating separate databases into one central database, which officials could access using secure remote access tools.

Next, we examine the first two options from above. While the third option is technically no less feasible, it remains outside the scope of this work, since its implementation would require significant changes in legislature and the work of public offices, yet would not solve the problem of establishing private-body databases and accessing the data therein.

During system analysis, a realistic assumption was made that non-electronic communication with state agencies should remain as an option. Thus, this paper separately examines the communication between state agencies and a state agency and citizens. This is because assumptions regarding an information system for citizens are different from those of an information system for officials. If the differences were to be overlooked, the result would be an inefficient system at best and insecure at worst. It can also be assumed that an information system, defined as an ensemble of hardware and software able to communicate with other information systems in equal terms, would be provided for officials for performing their duties.

3.1 Tokens

The following sections refer frequently to electronic tokens, or certificates (in the meaning of electronic documents that provide legally acceptable evidence, not cryptographic certificates), and in several cases, tokens are weighed against the results of a simple query. The difference between a token and the result of a simple query (henceforth referred to as *simple query*) is the existence of a defined evidentiary value.

After a token has been issued, the issuer no longer has control over its validity. The recipient of the token can, at any time, prove the identity of the issuer, and the contents of the token at the moment of issuing. Simple queries lack this quality, in that the creator of the result of the query can, at any time, deny giving that particular result.

The easiest way to implement electronic tokens is to use digital signature mechanisms [19:217] to sign documents that possess a well-defined structure and meaning. The existence of evidentiary value is important, since it allows the objective resolution of disputes which may arise over the course of communications between users.

3.2 A System Using Electronic Tokens

This usage scenario involves three participants, each of whom can use an information system to communicate with each other.

1) A citizen who wants an official transaction to be performed
2) Official *A* from the agency that manages the database

3) Official *B* from the agency that actually performs the transaction

As official *B* can't perform the required transaction before receiving a token from the database, the procedure should proceed as follows.

1. The citizen asks their information system to perform a transaction.
2. The information system requests a token from the agency that manages the database.
3. Official *A* is notified of the token query.
4. Official *A* decides to issue a token.
5. The system creates the token, registers the facts of issuing, and sends the token to the citizen.
6. The citizen's information system queries the second agency, adding to this query the token from the first agency.
7. The second information system notifies official *B*, who reviews the query and makes a decision to resolve the query.
8. If the decision is positive, the information system performs the requested transaction, logs it, creates a token that proves the occurrence of the official transaction, and returns the token to the citizen's information system. The latter stores the token for later disputes and notifies the citizen that the query was successful.

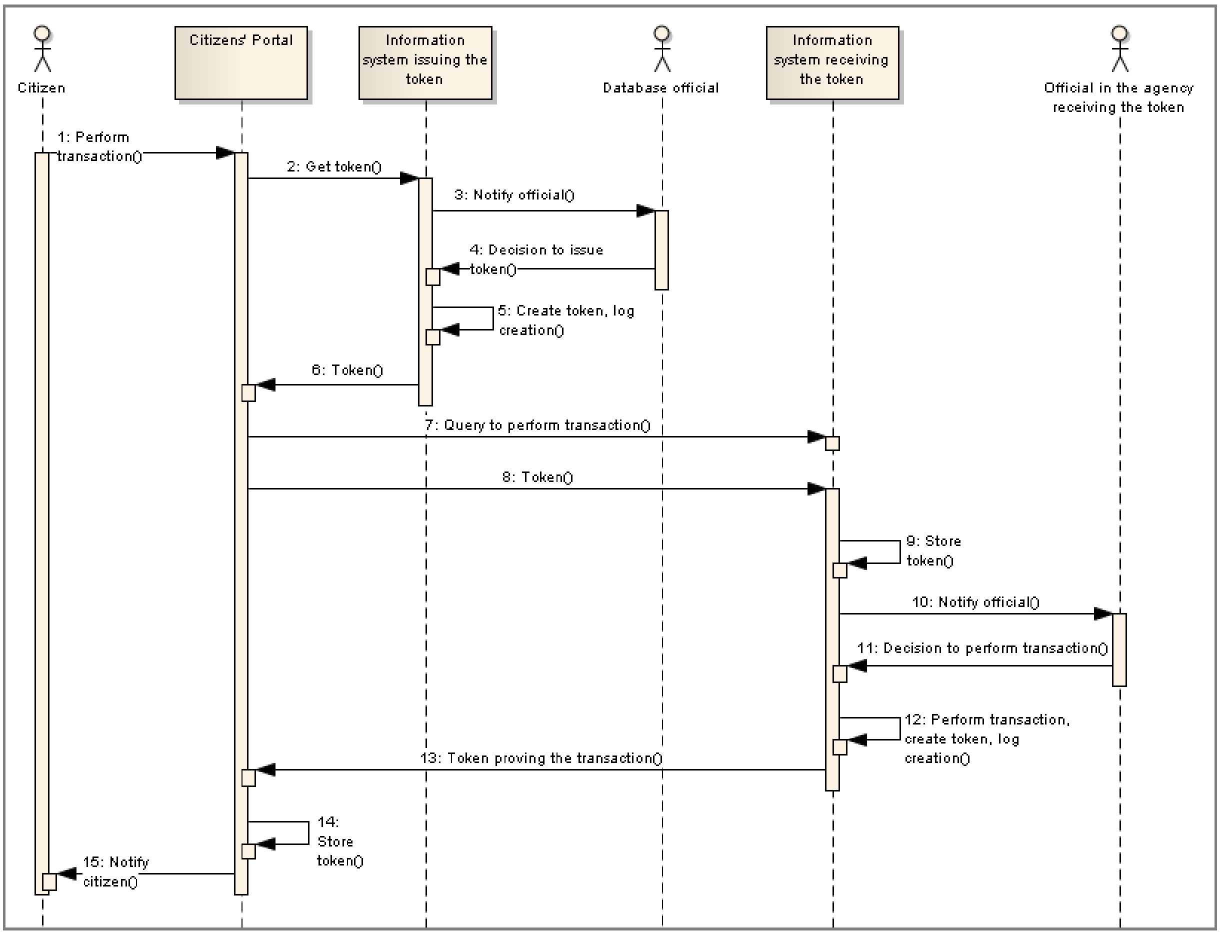
Citizen
Citizens' Portal
Information system issuing the token
Database official
Information system receiving the token
Official in the agency receiving the token
1: Perform transaction()
2: Get token()
3: Notify official()
4: Decision to issue token()
5: Create token, log creation()
6: Token()
7: Query to perform transaction()
8: Token()
9: Store token()
10: Notify official()
11: Decision to perform transaction()
12: Perform transaction, create token, log creation()
13: Token proving the transaction()
14: Store token()
15: Notify citizen()

Figure 2. Usage scenario for electronic tokens

This scenario is an exact representation of an existing government system that requires the citizen to present paper documents to a state agency in person. Hence, implementing the system should not raise conflicts with existing laws, except when queries are allowed to be performed only on paper.

There are two notable factors in this scheme:

1. Both acts of communication are actually the same. If we consider the token transmitted with message 8 as a parameter to the query transmitted with message 7, then steps 2-6 and 7-13 depicted on the above scheme are truly equal. Hence, it is sufficient to analyze only one of them.
2. The database official (official *A*) does no actual work. In the current system, official *A*'s duties are to verify the identity of a citizen (e.g., looking at the passport) and to create, register, and issue a token. The electronic system does all of this (including authorization) automatically; therefore, no duties remain for the official, who can be eliminated from the usage scenario. However, if it is necessary to verify the contents of the query and the verification of contents cannot be automated, then the presence of an official remains necessary.

However, it's not always possible to similarly eliminate the physical presence of the official from the second agency (official *B*). While transactions not requiring decision-making can be automated completely, transactions that include subjective decision-making still need a human participant. The following analysis, presented in Figure 3, examines a complex system that, includes the presence of an official.

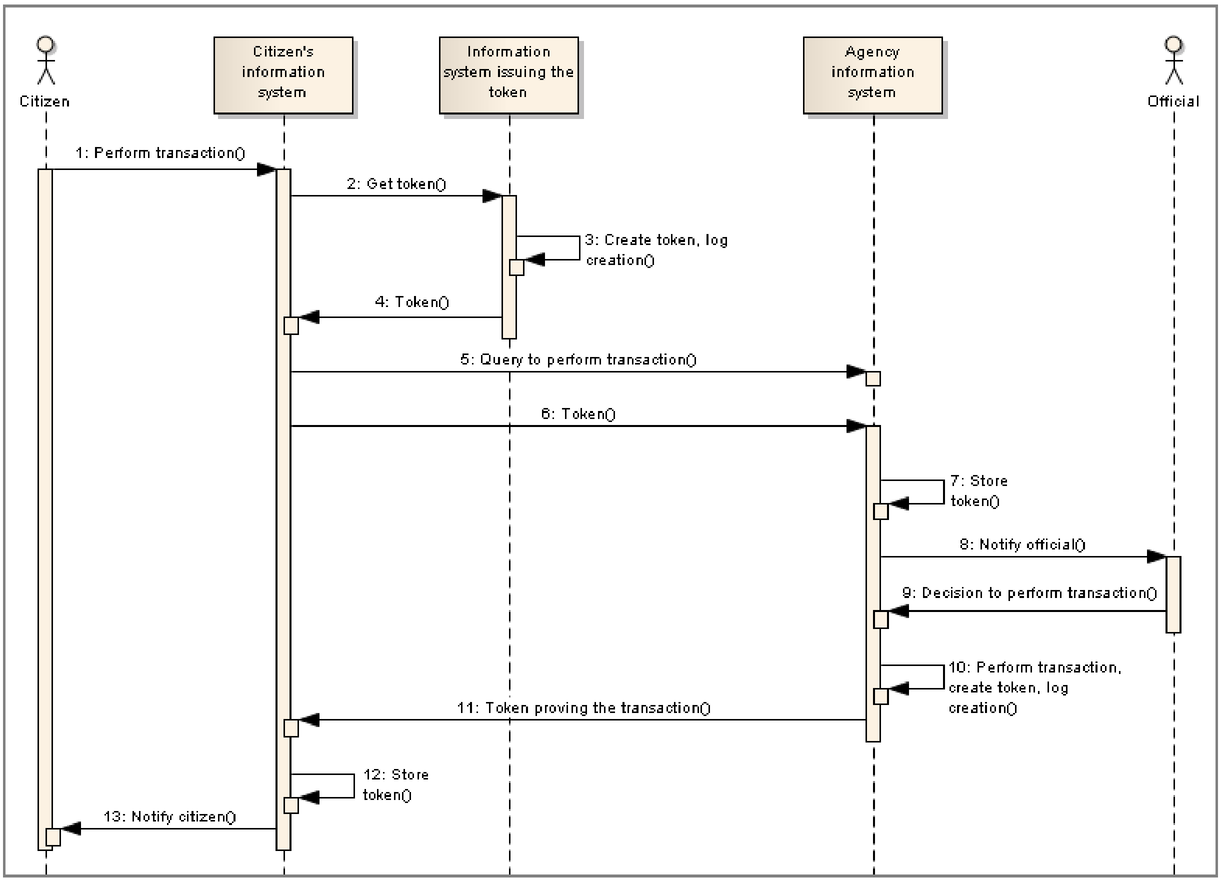
Citizen
Citizen's information system
Information system issuing the token
Agency information system
Official
1: Perform transaction()
2: Get token()
3: Create token, log creation()
4: Token()
5: Query to perform transaction()
6: Token()
7: Store token()
8: Notify official()
9: Decision to perform transaction()
10: Perform transaction, create token, log creation()
11: Token proving the transaction()
12: Store token()
13: Notify citizen()

Figure 3. A simplified usage scenario for electronic token use

While this model might not be in full accordance with existing laws, it is not reasonable to employ an official whose sole purpose is to ensure compliance with legal requirements. If the automatic issuing of tokens conflicts with existing laws, the laws should be changed accordingly.

A major benefit of the above schemes, compared to ones that follow, is that officials don't need more authority than they already have. The system can be built so that officials can't make queries about other people on their own initiative; they can only perform a query when a citizen presents the necessary token.

A major disadvantage of the scheme in Figure 3 is that it won't make non-electronic communication more efficient. If a citizen visits an official in person to request the performance of a transaction that requires a token from another agency, the official wouldn't have the permission to request the token. If the official had such a right, the scheme illustrated in Figure 4 would be used, whereby agencies exchange tokens directly through electronic channels. A downside is that strict compliance with existing laws would be lost, and the officials would need their limits of authority increased.

Further analysis is needed for cases in which officials can query another agency about a citizen without the citizen's cooperation. This functionality could be implemented with one of the following schemes, but then it would serve no purpose in implementing the above model.

Another aspect includes the fact that, in order to implement the above model, both agencies should be able to create and verify digital signatures to issue and receive tokens. The citizen's information system should only be able to create and verify digital signatures. All this would greatly help the implementation of systems that issue tokens.

3.3 Exchanging Electronic Tokens Between State Agencies

In this case, a citizen who wants an official transaction to be performed will delegate the requisition of a token to the state agency that performs the transacion (see Figure 4).

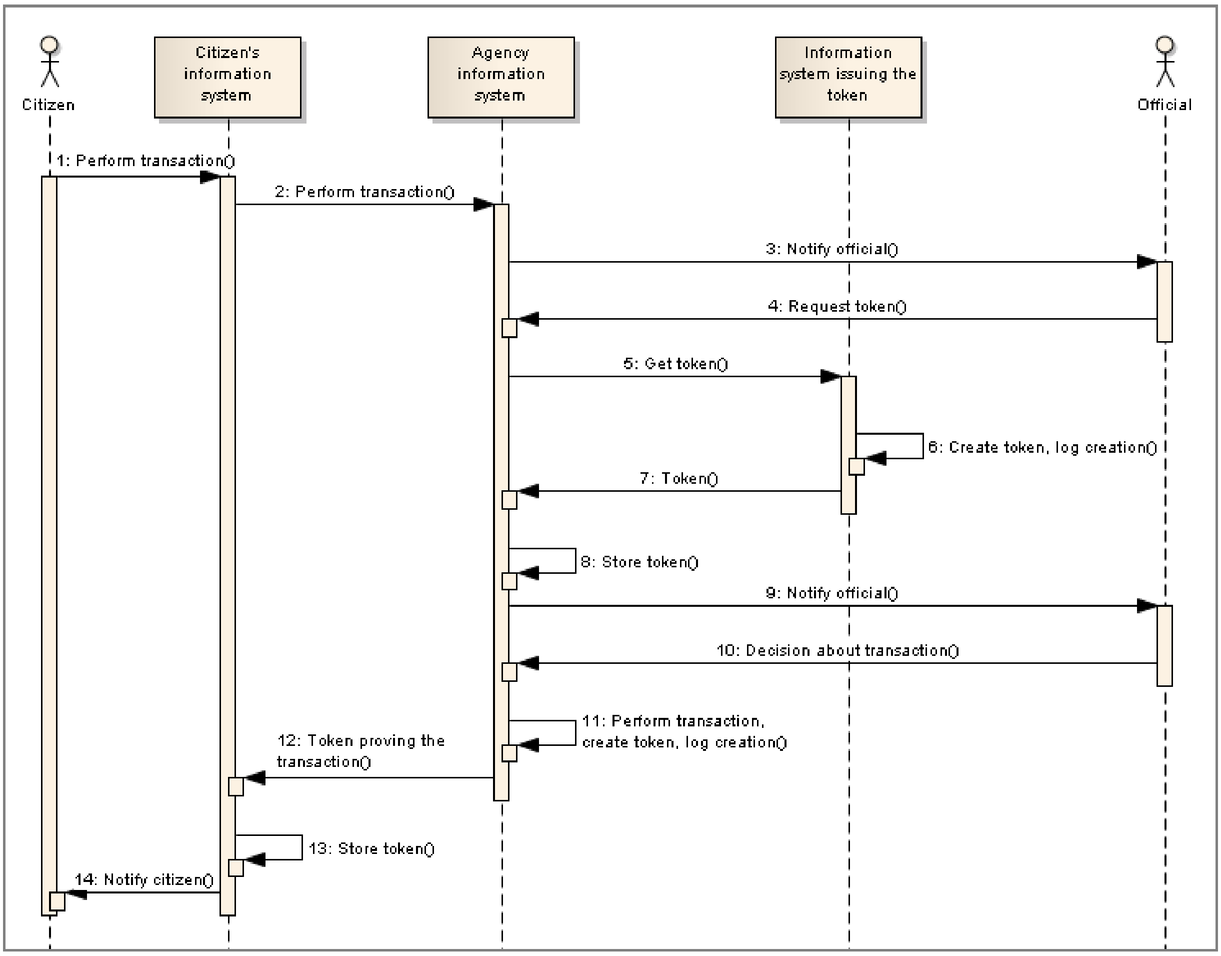
Citizen
Citizen's information system
Agency information system
Information system issuing the token
Official
1: Perform transaction()
2: Perform transaction()
3: Notify official()
4: Request token()
5: Get token()
6: Create token, log creation()
7: Token()
8: Store token()
9: Notify official()
10: Decision about transaction()
11: Perform transaction, create token, log creation()
12: Token proving the transaction()
13: Store token()
14: Notify citizen()

Figure 4. Direct exchange of electronic tokens between state agencies

1. The citizen orders his information system to perform an official transaction.
2. The information system queries the agency's information system.
3. The agency's information system informs the official of the request.
4. The official orders the requisition of a token.
5. The information system accesses the database and performs the query.
6. The database registers the query, creates a token, and returns it to the information system.
7. The information system notifies the official of the acceptance of the token.
8. The official makes a decision to allow the transaction to complete, upon which the information system fulfills the decision, registers it, creates a token, and returns it to the citizen's information system.
9. The citizen's information system saves the token and notifies the citizen of the successful completion of the task.

The official, who previously had to collect information across a variety of documents submitted by the citizen, now receives the information directly from the related database. The citizen no longer has direct control over this process. On one hand, it is assumed that officials must have the permission to perform any queries that fall within their duties, but this assumption might not be within the scope of current laws. On the other hand, officials are provided with additional means to abuse their authority; they can perform queries that are not necessary for the performance of their duties, and thus they can use the collected information for their own agenda.

While it is possible, by appropriately engineering the official's information system, to make it difficult to perform malicious queries, a certain risk still remains. To reduce the risk, abuse detection mechanisms should be created with an option to reprimand the official for abuse. Abuse detection assumes that the official's information system logs a query in a way that prevents the official from erasing or changing the fact afterwards. To instill a sense of discipline, officials should be informed about such measures from the beginning. Note that whatever the countermeasures are, it would still be impossible to "put the genie back into bottle" — that is, to revoke unlawfully issued information.

The advantage of this scheme is that it significantly reduces the complexity of the citizens' information system, which, considering the large number of such information systems, is a clear victory. Additionally, the system can be used to more efficiently service citizens who visit an official in person, since the necessary tokens can be acquired over the Internet. The system can also be used to exchange information without the citizen's participation.

3.4 Simple Queries to Databases

The scheme shown in Figure 5 is similar to the previous scheme, except that, for the sake of technical simplicity, state agencies don't exchange tokens and can perform only simple queries.

Compared to the previous scheme, there is no possibility to prove whether a state agency has queried another state agency, whether the state agency received a response, or what the contents of the response had been.

If an unsanctioned query was performed that might have caused an actual loss (for instance, by revealing disclosed information to unauthorized users), it would be difficult to later determine the actual culprit. Depending on the security of the sender's or receiver's information system, an official can, either on his or her own or in cooperation with their system administrator, delete or change the operation logs and thus significantly complicate the investigation.

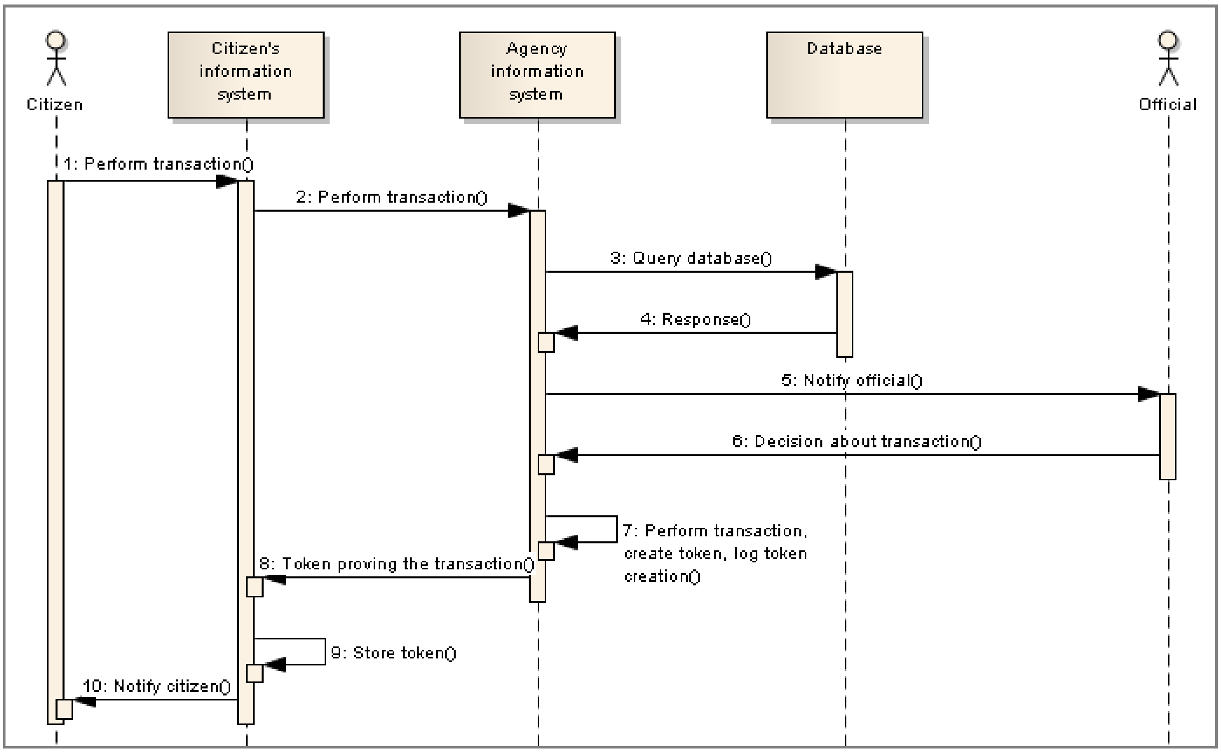
Citizen
Citizen's information system
Agency information system
Database
Official
1: Perform transaction()
2: Perform transaction()
3: Query database()
4: Response()
5: Notify official()
6: Decision about transaction()
7: Perform transaction, create token, log token creation()
8: Token proving the transaction()
9: Store token()
10: Notify citizen()

Figure 5. Usage scenario for direct queries

3.5 Conclusion of the Preliminary Analysis

- Implementing a system that uses only electronic tokens does not address all usage scenarios.
- In case of abuse, a system that uses simple queries is likely to not provide objective evidence to determine the culprits.

Considering these facts, **a solution based on direct exchange of tokens** should be used. The following sections analyze a sample model in detail.

4 OFFICE-TO-OFFICE INFORMATION EXCHANGE

As stated in the introduction, the communications between state agencies and those between a state agency and citizen require separate examination. The results of the present examination have been generalized and consolidated into a single model, seen at the end of the analysis.

The analysis does not presume that an "agency" and a "database" are government entities; they could as well be private enterprises. What matters is that the organization has legal basis for receiving the requested data, and the organization's information system has been audited.

In a simple case, two agencies participate in the data exchange (see Figure 6). The first (data provider *A*) manages his or her database, the second (data user *B*) works with the data, i.e., uses the database. The analysis examines the usage scenarios and associated threats.

While there are external factors affecting communications, such as legislation and best practices, these factors are currently not examined. Instead, it is assumed that there exist a document that explains best practices and serves as a basis for granting access to the database.

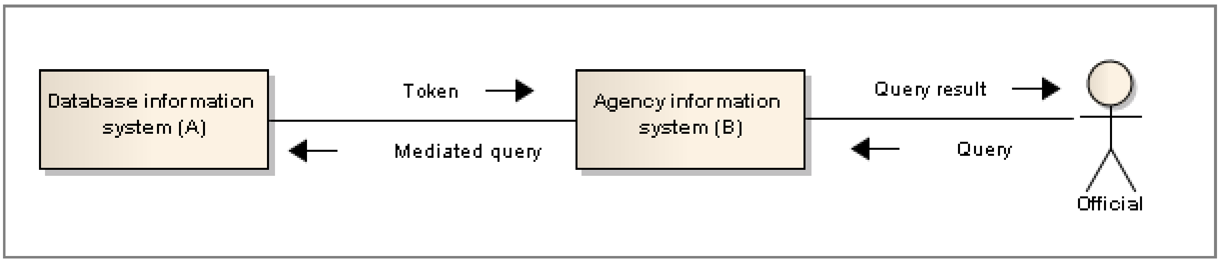
Database information system (A)
Token
Mediated query
Agency information system (B)
Query result
Query
Official

Figure 6. Simple database use between authorities

4.1 Assumptions

The first assumption is that a state agency possesses an information system, as defined above, that allows officials to perform their duties. The exact implementation of the information system is irrelevant, but there are a few assumptions regarding its functionality.

The agency's information system must differentiate users, which in practice means that an official must log in to the system to use it. The exact technical details of it may vary; it may entail logging in to their workstation (Single Sign-On solutions [46]), password-based authentication, or electronic authentication tokens using digital signatures [19:217]. It could even be implemented with physical access controls.

Any information system directly or indirectly used for activities that produce an action outside that information system must be able to differentiate users in order to objectively resolve (at least in theory) potential disputes, and to find the culprit in case of abuse. However, the ability to differentiate users alone is insufficient.

The second assumption is that once officials are logged in to the system, they can perform all activities necessary to fulfill their duties. In practice, it means that they have certain rights arising from their job descriptions and other documents. Those rights are represented in the information system in a machine-processed form, and the official who fulfills the role of the agency's system administrator is responsible for delegating the rights an official might have in using the system. The roles are assigned by the agency's manager or head of department, but again, the precise job titles and descriptions depend on responsibility distribution in the agency.

There are several ways to implement the rights system. For example, rights can be associated with a certain role or user group, including roles such as Backup Operator, Printer Operator, and others in Windows NT. In a state agency, there could be roles such as Customer Service Representative and Head of Department. All users get their rights either indirectly (through their role) or directly and personally from their system administrators or supervisors.

4.2 Authentication and Authorization

If an agency requires data from an external database, simply asking for it isn't usually an option. System administrators or IT developers working for the agencies are not allowed to make agreements between themselves regarding the use of an external database. Such agreements can be made only on behalf of, and between, the heads of the respective agencies—one that manages the database and the other who needs to use it.

An agreement to exchange data should state the conditions upon which one organization grants database access to another. While the agreement will usually establish the necessary technical requirements, the most important aspect of the agreement is that the head of the data-using organization takes responsibility for the diligent and purposeful use of its data. It is not necessary to state in the agreement, which employees are permitted to make which database queries. For the institution managing the database, this is irrelevant since it will respond to all legitimate, valid queries from other institutions. Setting per-user restrictions is the duty of the data-using organization, whose information system must support such restrictions, including differentiating users and setting their rights.

It is easy to demonstrate why it's not meaningful to authenticate and authorize external users on per-user basis at the service provider. Consider that to perform their duties, which include querying databases, officials use the information system of their organization. All activities, which may include authentication, are carried out through the organization's information system. The security of such activities depends explicitly on the security of the information system. If someone has tampered with the system and installed a network sniffer, a keyboard logger, or a backdoor, then that someone can silently act on part of the user without the user knowing it.

On the other hand, it isn't always clear to the user which queries the local information system makes to other databases in order to reply to their requests. Hence, the user must implicitly trust their organization's information system.

As the security of the authentication performed at the database depends explicitly on, and is limited to, the security of the information system querying the database, such authentication adds nothing to the overall system security. The organization's information system, if it's not tampered with, correctly registers the identity of the user performing the query; indeed, this is a prerequisite of accreditation. However, if the information system has been compromised and an unauthorized user performs illegal queries under another user's name, then the database will also log the wrong name, preventing the unauthorized user from being identified. It is possible to demonstrate that authentication at the database might even *reduce* the security of the system, as the management of users and their rights becomes more difficult.

Regarding user management, at minimum, the procedures including employment, dismissal, and changing of duties must be analyzed. These three procedures are internal to the organization. If the procedures were to be coordinated between multiple organizations, a number of problems would arise.

- When an employee leaves or his or her duties change, the owner of the database might not be notified immediately; hence, we have a subject without liabilities who can still access the database. [29]
- As the authentication of another organization's employees always involves communication between the organizations, it is possible that insecure user management practices such as phone transactions, which are vulnerable to many social engineering techniques, become widespread. [1]
- Another argument against double authentication of the official; i.e., at the local information system and at the database, is that it increases the number of authentication procedures required to perform a task. After logging in to the local

information system, the official would still have to enter additional passwords or use other means of authentication to perform a query. This reduces the availability of the system and encourages negligent password storage, and by extension, a short lifespan of passwords).

Thus, it is more sensible to employ a two-level authentication system.

Officials authenticate themselves to the local information system, using any method that is easy to implement and prevents, with enough certainty, system abuse by unauthorized users ("enough certainty" is defined by general laws to which the system supplier must conform; the conformity is verified with an audit or a certification of the system). The organization's information system also performs authorization and allows officials to make only those queries to which they are legally entitled and that are necessary to perform their official duties; the two requirements are complimentary.

Information systems use standard methods for mutual authentication. An appropriate authentication method must be developed and standardized in conjunction with another system that enables interoperability between the information systems. Additionally, at this level, the querying party undergoes authorization, but in this case he or she is not an official, but an institution, and the authorization is performed according to the agreement of information exchange between the institutions. The agreement states what types of data the institution is allowed to access from the database, and the database information system verifies that every query conforms to their agreement.

However, there is the possibility that over the course of the conformation to various laws and in creating evidentiary material, the information system making the query may transmit the name or personal identification code (e.g. the Social Security Number) to the database information system; this can't be regarded as legitimate authentication. [20:100]

Another advantage of a system employing two-level authentication is that the official can make queries only through the local information system, which is secure and logs the official's activities. If the queries were performed through the official's personal computer or a public computer, the institution would have no control over the information system used. Various viruses present a threat, the existence or non-existence of which the official cannot accurately assess. [35] The physical security (for example, access restrictions) of such computers is usually lacking or nonexistent, compounding the threat.

If remote access from other computers, including personal computers, is required, it must be arranged by following IT industry's best practices. For instance, an Intranet portal or web application could be created in which users authenticate themselves as usual. The portal would be protected with a firewall, and access over the Internet would be protected with remote access security methods, for example, by using Virtual Private Networking (VPN) software.

4.3 Ensuring Confidentiality

Most databases contain data with restrictions on access. If the databases are used within a single organization, access restrictions are ensured through organizational and physical measures, and IT measures to some extent. However, where remote access over public communication networks is provided, IT measures prevail, so for example, data encryption becomes a must.

In principle, there are several standards-compliant products that can be used to ensure confidentiality. That considered, we recommend that a transport-level protocol, [48] such as Transport Layer Security (TLS), [11] a successor to the well-known Secure Sockets Layer (SSL) protocol, or the Secure Shell protocol (SSH) [42] be used. These protocols make it remarkably easier to create and maintain a heterogeneous, distributed management network than it is with a network-level protocol [26] such as the Internet Protocol Security (IPSec) suite [27].

An advantage of transport-level protocols is that they ensure better separation between communicating parties and help them to avoid potential Intranet address space conflicts. As far as functionality, the differences between SSH and SSL are negligible, but it's easier to manage SSL-based applications as the number of users (i.e., organizations) grows. Furthermore, the SSL protocol is integrated with several application protocols such as HTTP [39], IMAP [37], SMTP [23], and CORBA [9] servers.

4.4 Integrity, Traceability, and Evidentiary Value

For most databases, maintaining integrity is more important than restricting access. An example would be the Commercial Registry in Estonia, which contains information about the signatories in a company. If someone made unauthorized changes and added to the list of signatories a person without liabilities, then it would become possible to cause irreparable damage to the company; for instance, by selling all its real estate a few times over, until the buyer is considered *bona fide* by law. [44]

Even non-electronic registries have problems with illegal entries and procedures. There are threats to a conventional registry; i.e., those utilizing a paper or a local, closed information system, that almost never materialize, but if the registry is opened to a larger audience, the threats become significant enough to warrant a separate threat analysis.

A closed registry is protected by a number of organizational, physical, and IT security measures. For example:

- Only authorized employees who repeatedly and successfully undergo background screening can access the registry. Security personnel and systems log authorized employees' activities.
- The registry maintains a history of all activities. For example, data are never changed or deleted; instead, a change in an entity's status is represented by adding a new record to the database that identifies the change, as well as the person who made the change.
- There are periodic audits which verify the integrity of the registry.
- There are documented and tested backup procedures, the compliance of which is monitored.

If the registry were to be opened, the same procedures would have to be applied to all users. Moreover, since a query can come from outside an organization, it should be possible to identify external and internal enquiries the same way. Reviewing a surveillance camera recording to see which employee used which computer when the query was made, wouldn't help in this case. While the other organization must have all the necessary security measures in place, the owner of the database still needs objective evidence that would make it possible to claim that a query originated from the outside. Such evidence could be provided in query logs that can fulfill either an identifying function for internal use, or an evidentiary function.

Since conventional, text-based log files can be changed easily without leaving traces, they can only fulfill the identification function. Performance of the evidentiary function is not possible without a cryptographic protection, which can be either a digital signature to identify the source of entries, or a one-way linking function with a central audit server to determine *post facto* changes; this, however, might not prove the author of an entry [30].

In the present case, it is imperative to ensure both the identification of the author of an entry and the detection of any *post facto* changes, so both of the above measures must be adopted.

A log file that has evidentiary value allows a large degree of certainty in determining whether a query originated from the inside or outside, and if from the outside, from which agency. It is then the duty of that agency to use conventional security measures to ascertain which official actually performed the query. Note that as a self-defense mechanism, the evidentiary function is necessary for the organization even when read-only network access to the database is all that is available; in other words, only queries and responses are exchanged.

To understand this concept better, let's consider the initial example and assume that a Land Registry official wants to verify if a person is allowed to provide signatures on behalf of a company. Typically, the official would query the Commercial Registry to determine whether the person is a legitimate signatory; if the response is positive, the requested official transaction would be performed.

Conversely, what would happen if the Land Registry official allied with an unauthorized user? Assume the Commercial Registry gave a negative response (the person in question was not a signatory), but the Land Registry official still carried out the transaction, arguing that the response from the Commercial Registry had actually been positive. Since the Commercial Registry cannot objectively prove what kind of response was sent to the Land Registry, the official can claim to have received a positive answer, even if the actual answer was negative. What's more, the official can now accuse Commercial Registry employees of fraud. Because of the lack of objective evidence, the ensuing investigation would be complicated.

However, when the mechanisms for creating objective evidence are established and well-known to everyone involved, then the fact itself works as an effective deterrent. Most officials, knowing that their activities leave a trail with evidentiary value, would not attempt to perform illegal queries.

As stated before, all messages exchanged between the two organizations must be digitally signed. Let's assume the official has the necessary means for that; i.e., a cryptographic key and a certificate. It would not be useful for the official to sign the entire original query since the local information system splits it into sub-queries, some of which are used locally, while others are sent to a database within the domain of another department within the same organization, and still others are sent to other organizations entirely. Since the original query doesn't reach the database in question, the data provider cannot verify the original signature. In some cases, such as if the query concerns an ongoing criminal investigation or is made by a criminal investigative agency (e.g. the FBI or its equivalent in other countries), it is imperative that the original query and signature never leave the local information system.

The alternative, whereby officials would sign all the sub-queries, would still not solve the problem because they wouldn't understand the contents of the low-level protocol messages to be signed. Also, such an approach would significantly reduce the availability of the system. Additionally, even if the official signed all the queries, it would not create evidentiary material.

Furthermore, splitting the query puts the official who makes the query, at risk, because an innocent query could be transformed into several sensitive (and thereby incriminating) queries to databases, even though the official didn't have such intent, and the responses could be collected by an "interpreter";i.e., the server that splits queries for its own use. The further away in an organizational sense the interpreter is from the official, the smaller the chance that the official can affect the splitting, and the higher the chance of such attacks materializing. Splitting the query is often not transparent to the user since the information used as the basis for splitting is known only to the interpreter.

In conclusion, without signed queries, log files have no practical evidentiary value. In addition, the integrity of logs should be maintained, for example, by using a central time-stamping or audit server [6], [7], [8] and a secure logging system. The logs must be stored and preserved in a way that guarantees that those concerned (i.e., the employees, the database owner, system administrators on both sides, and a possible intermediary) cannot alter or delete them. This can be achieved by publishing the logs, but this would significantly reduce confidentiality. Another option is to audit the servers regularly. To provide proof in log files that a query was performed and a response received, all queries should be signed, using server certificates, not personal ones. Signature-based authentication between servers considerably increases the security of the system on both sides.

4.5 Threats to System Availability

A system consists of three components: a database information system, an organization's information system, and a communication channel between the two.

Major threats to an information system include human error, various natural threats (such as floods and fires), power cuts, vandalism, and attacks (internal and external).

Communication lines are susceptible to additional threats including insufficient channel throughput, interruption of communication, and denial-of-service attacks.

Possible countermeasures depend on how important the database is to the functionality of the state. The following sections examine countermeasures against these threats [20].

4.5.1 Natural Threats

There must be separate copies of important registries in geographically diverse areas, since this is the only measure that allows the operation of the system to quickly resume. Furthermore, the systems must be continuously synchronized to avoid the loss of integrity of a database should a natural threat materialize. However, long-distance synchronization has distinctive security requirements requiring further discussion, which lies outside the scope of this paper.

For less important registries, the following measures are sufficient:

- Frequent routine backup with the geographical separation of backup copies
- The existence of a recovery plan and necessary preliminary contracts; e.g. for the delivery of replacement hardware
- The existence of an alternative, paper-based system that permits response to more important queries until the electronic system is restored

4.5.2 Power Cuts

Uninterruptible power supplies (UPSs) can be used during brief power cuts. To survive longer power cuts, diesel generators can be used, although they might not be feasible for registries with less vital information. It is important to protect all devices, including network devices.

4.5.3 Vandalism

To protect against vandalism, various physical security measures can be used, whereas serious vandalism is comparable to a natural threat (See Section 4.5.1).

4.5.4 Human Error

Human error comprises a large variety of possibilities which can debilitate the system. To address the consequences of human error, it is useful to have as recent a backup copy as possible.

4.5.5 Attacks

Attacks are directed against security holes in the information system. Modern information systems are very complex and consist of numerous subsystems, the interoperability of which is almost impossible to test due to the complexity involved. Therefore, new vulnerabilities are discovered in all systems, all the time. To counter vulnerabilities, the following activities can prove useful:

- Reducing the size of the system that is directly connected to the public network. A tried-and-true method is to use a firewall and disable unnecessary services running in public-network servers.
- Working continuously to keep all systems updated.
- Performing active monitoring and cooperating with Internet Service Providers (ISPs).
- Using effective access control at the physical, organizational, and information technology levels to avoid internal attacks.

4.5.6 Insufficient Channel Throughput

If there are a large number of queries or the throughput of the communication channel is insufficient, even valid queries might cause congestion. The following help to avert this:

- An analysis of system usage patterns that enables the prediction of the necessary throughput at peak hours
- Diffusion of traffic. Central servers that mediate and direct all the traffic in the system should be avoided because the communication channel between the server and the rest of the world could become overloaded.

4.5.7 Interruptions of Communication

Interruptions might be caused by human error, natural disasters, communication cable faults, communication equipment malfunctions, or power cuts in intermediate servers.

Since it is impossible to fight all the causes individually, a useful method is to duplicate communication channels to an important network node. The parallel communication channels up to that point must be completely independent of each other, and possibly be of different types.

4.5.8 Denial-of-Service (DoS) Attacks

This is a specific kind of attack originating from a public network; the source of the attack is often difficult or even impossible to pinpoint. To deal with DoS attacks, the best method is to create a semi-private network for the organizations that must communicate with each other, and to also reserve a certain band in *all* communication channels for the relevant traffic. This guarantees the operation of the system even at the time of the most dangerous attack. Survival of DoS attacks assumes tight cooperation with Internet service providers (ISPs) [31].

4.5.9 Availability - Conclusion

This chapter examined some of the more important and serious availability problems that can occur when two systems interact. When any type of mediator is added, the probability of faults significantly increases. For example, if a third party that mediates only queries is added to the system, the resulting system becomes almost twice as vulnerable as before since what is being added are an additional communication channel and information system. When the number of joined subsystems increases, the danger that the bandwidth of the channel connecting the central system with other systems becomes insufficient will increase.

4.6 Monitoring

No system can remain secure without continuous monitoring and incident response. On one hand, new vulnerabilities that need patching are discovered all the time. On the other hand, the discovery of vulnerability may not be publicly announced, but rather the knowledge will be used to plan an attack. Furthermore, there are always users who overstep their authority in one way or another. If they simply practice data mining instead of actively changing the data, then their activities can remain hidden for some time. The sooner such activities are discovered, the smaller the losses, and to minimize the possible losses, it's important to ensure continuous monitoring of the systems for optimal protection [41].

Since monitoring can be expensive, work-intensive, and requires specialized knowledge, it is probably not feasible for every database to have its own monitoring system or monitoring center. Central monitoring would not only be cheaper, but would also provide an independent view of communication. However, one should not rule out the possibility that the administrator of an especially important database does his or her own monitoring.

The purpose of monitoring is not to draw any conclusions based on the analysis of individual queries. Rather, its function is to identify trends such as a sudden increase in the number of queries compared to the previous period and abnormal usage patterns. Furthermore, the monitoring team should detect direct attacks, including DoS attacks, and identify their sources. In banking, for example, this type of monitoring has been implemented with some success. Methods and techniques utilized by banks could form the basis for the system analyzed in this work, but any precise feasibility estimations would require further study.

4.7 System Certification

The owner of a database *(A)* is also responsible for the database. If the owner enters into an agreement with another organization *(B)*, granting them the right to use the database, then it is the right and obligation of *A* to impose restrictions and conditions on *B* to ensure the protection of the information system of *A*. Among them could be restrictions on query type, requirements on the security level of *B*'s information system, and more.

However, *A* might not have the competence to design such requirements, especially if *B* has a higher position in the hierarchy of organizations. Therefore, to improve the actual availability of government databases, the requirements and restrictions on user systems must be determined on the national level [3]. Consequently, all user systems wishing to exchange information with government databases must be certified on the national level. The certification may include such aspects as the design and management of the information system, and in more sensitive cases, the screening of users. The need to certify user systems increases significantly when *A*, in addition to read-only access, grants database write access to *B*.

Even a read-only information system can contain vulnerabilities that can be exploited to acquire write access. Therefore, *A* is obliged to be ready to restore data up to the point where unauthorized changes occurred. Furthermore, the need for restore procedures increases with the number of users with write access to the system.

4.8 Implementing the Results of the Analysis for Special Types of Information Systems

The first part of the paper suggested modeling typical agencies, then classifying all agencies according to the model. As of 2001, there are no concrete models that address actual needs; hence, the security measures described earlier are suitable mostly for mid- to large-size institutions. This section demonstrates that the same concepts can be applied to smaller information systems as well.

Even one desktop computer constitutes an information system. In the context of this paper, the boundaries of an information system are set by the administrative domain. All computers managed by the same organization form a single information system. The justifications for such an approach are that the system is analyzed from the security aspect and given physical access to a computer, all the data therein (applications included) can be read and modified without the user leaving a trace of use. Consequently, it is not sensible to analyze a system, a part of which one can't control.

If there's an information system being developed and the organization wants to outsource thee development of part of the service [2], it is important to pay attention to contracts between the organization and the application service provider (ASP). The contracts must clearly state the duties and responsibilities of the service provider. As the ASP's information system forms an important part of the information system being analyzed, it must pass the same rigorous auditing and accreditation procedures as the new system, and be at least as secure.

Every information system needs complete protection against attacks. No countermeasure, taken individually, is effective; instead, it is the combination of countermeasures (physical, organizational, and informational security) that allows all possible attack routes to be protected. Of course, it is impossible to defend everything with absolute certainty. The required level of security can be determined after a risk analysis and a subsequent cost-benefit analysis by comparing the cost of information assets with that of the countermeasures [20:82].

The features required of an information system can be realized in many ways. In an organization with one employee and one computer, that one computer comprises the information system, and the employee would be responsible for all queries made from the information system. To acquire a permit to use this information system (i.e., undergo certification), a method for preventing unauthorized access must be demonstrated. The computer should be located in a room that only the authorized employee can access; also, the room must be equipped with a security alarm system which should be checked periodically. In the event of a security incident such as burglary, all software must be reinstalled in the computer, all passwords changed and certificates reissued. No confidential data should be stored in a stand-alone computer such as this.

In a large office with many employees who use the resources of a central server, the safeguards may be significantly different. For one, supervision over system administrators must be arranged. The creation of system administrator accounts with unlimited access privileges in all servers should be avoided. The system administrators' activities should also be logged such that they would be prevented from altering the log files. To reinforce personal responsibility in employees, the administration of workstations should be well-regulated and monitored. The use of tools that give absolute control to system administrators should be avoided. However, this again may create the dilemma of finding a balance between security and availability, such as simpler administration.

4.8.1 Example: Security Measures in the Information System of the Estonian National Registry of Certification Service Providers

The application of security measures can be illustrated by the information system for the Estonian National Registry of Certification Service Providers (NR-CSP), in the design stage of which the author of this paper participated. The NR-CSP is created pursuant to the Estonian Digital Signature Act [12].

The operation of the registry is organized according to the statutes for establishment and maintenance of a registry [43]. Some of the functions of the NR-CSP are to issue certificates to CSPs and TSPs, to keep a registry of the certificates, and to publish validity information regarding CSPs and TSPs. Therefore, very high confidentiality, reliability, and availability requirements are imposed on the NR-CSP information system.

Following is an overview of security measures applied, which together ensure the fulfillment of the above requirements.

4.8.1.1 Electronic Security Measures

- **Logging on to the system with a smart card.** To successfully log on to the operator's workstation, the person must present a valid smart card and PIN.
- **Lack of an administrator account.** The administrator (root) account is not just disabled, but removed altogether. All system components, including the firewall, servers, and operator's workstation are designed to not need basic maintenance such as log file rolling. If the need for common maintenance arises, it is considered a deviation from the specification and the system will be revised to eliminate the need. The lack of administrator account prevents many security problems that are inherent to typical information systems.
- **Easy backup procedure.** The backup procedure is designed to be easy, so the operator should not feel reluctant to perform backups. Therefore, if the system crashes, it would be more likely that a recent backup copy exists.
- **Fast restore procedure.** Restoring any component of the system after a crash is fast. For a firewall, it's about 5 minutes; for a server, about 10 minutes; and for the operator's workstation, about 15-20 minutes.
- **Mirrored databases.** Multiple secondary databases ensure that if one or more system components fail, the data in the servers as of the last backup are preserved.
- **Firewall.** Sensitive areas of the system are placed behind a firewall that protects them against certain simpler attacks from the Internet.
- **Minimum required functionality.** To reduce the probability of errors and security holes, the system provides only the minimum functionality necessary. In the entire system, there are no services or servers that aren't crucial to the operation of the system. The existing servers are selected and configured with potentially dangerous functions turned off; for example, the web server used to publish the registry would not allow the execution of CGI scripts, and even the underlying functionality would be removed completely from the server.
- **Individual backup power supplies.** Every server containing important data has its own UPS. The computers are automatically switched off before the UPS's battery is drained.
- **Active monitoring.** All system components monitor their own activity and that of their neighbors, and send error notifications if a critical error occurs. The system administrator can specify the e-mail addresses or cell phone numbers to where notifications should be sent.
- **Logging.** The system logs all activities of the system administrator to a file that he or she can't change. This allows the work of the system administrators to be audited.
- **Signed backups.** The backup copies of the system are digitally signed. When the system is installed, the public key necessary for the verification of backups is saved to an external medium that remains in the possession of an official committee present in the installation and restoration. The signing of backup copies avoids their unauthorized changing by a system administrator or a third party.

4.8.1.2 Physical Security Measures

- **Computer safe.** All security-sensitive components of the system are stored in a special computer safe, accessible only in the presence of the official committee. The safe contains all computers, UPSs, Intranet concentrators, and the console switch. The monitor, keyboard, mouse, CD writer for backups, smartcard reader, and printer remain outside the safe.

- **Restricted access.** Access to the room containing the information system is restricted according to the rules prescribed by the chief processor. These rules also regulate matters regarding fire safety, etc.

4.8.1.3 Organizational Security Measures

Administrative functions of the system are divided between three groups of people so that everyone's responsibilities are clearly delineated. The necessary regulation is established with the rules of the registry. It is important to note that no single person can manipulate the system without leaving proof of his or her access.

The following are the user groups and their functions:

- **The official committee** is present every time the safe is opened. It monitors and documents all administrative activities that the system administrator or technical support personnel perform in the system. The committee handles the external medium that stores the public key for the verification of backup copies. Every time a system administrator's workstation is installed or reinstalled, the committee verifies the signature of the restored data.
- **The "minister"** (e.g. Minister of Internal Affairs) creates operator accounts. It is important that the "minister" be certain of the person whose account is being created, and that the message digest of the operator's public key reaches, without alteration, the legal act that establishes the key.
- **The system administrator** is the person actually responsible for the administration of the registry. The system administrator accepts and archives documents; issues acknowledgements of documents received, decisions made, and the status of the registry; monitors the operation of the system, and produces backups. The activities of the system administrator leave an auditable trail in the information system. The system administrator has no physical access to the information system computers and cannot modify backup copies without leaving evidence that he or she had accessed the registry.

4.8.2 Example: Personal Security Environment

A PSE is a certain piece of equipment with the following features:

- It contains all the necessary functionality for secure message exchange including a user interface, cryptographic processor, key store, and communication interface.
- It is physically secure, having a monolithic, well-shielded, non-openable protective case. It also protects cryptographic against physical attacks.
- It is small and light enough to be easily portable.
- It can authenticate its owner.

PSEs allow for solutions wherein its user does not have to trust anybody else in their line of duty. For example, in an information system based on desktop computers, the user must trust people who have access to their computer, including the system administrator and colleagues. For PSEs, the only participant that needs to be trusted is the manufacturer.

A PSE is an independent information system that is especially suitable for users requiring mobility, in which classic physical and organizational security measures can't be used. System security is often compared to a chain in that a chain is as strong as its weakest link. For a PSE, the number of links is reduced to a minimum; hence, constructing a strong chain is cheaper than other solutions.

A good overview of PSEs is given in the MSc thesis of Margus Freudenthal [18] (available only in the Estonian language).

4.9 Scalability of Solutions

This paper, up to this point, has examined communications between only two agencies. There are additional factors to consider when more than two institutions are joined with the proposed data exchange system, and while all the security assumptions remain, new problems specific to this scenario will appear:

- There will be more business agreements between organizations, further stressing the importance of certification and the existence of standard solutions.
- The number of certificates in the organizations' information systems will increase. The situation should be improved by centralizing the issuing and management of certificates.
- Managing duplicated systems will become more difficult because of the large number of duplications. The situation should be improved by creating a central database of services.

Implementing the given solutions to items 2 and 3 above creates new databases and makes the whole system dependent on the databases' availability. The databases should have multiple mirrors, and there should be duplicated communication channels between the database and larger network nodes.

The solution described in item 3 above is, in fact, a directory service. In the Internet, this special directory service is implemented using the Domain Name System (DNS) protocol [36]. Assuming that the database allows the user to look up the URL of a service on the basis of its name the DNS service should be used before making the actual query to translate the hostname in the URL to an IP address. However, the purpose of the directory service would be two-fold. It would be better for the two directory services to use the same technical means and protocols, as this would reduce the number of components needing protection, and make the system cheaper to secure.

Another advantage of DNS is that it effectively solves problems with server mirroring and query response buffering; also, DNS has security extensions [13] that make it impossible to forge the information being broadcast.

A central monitoring system may also be feasible when the number of organizational information systems is large. Otherwise, it is easier for each organization to perform the monitoring individually.

4.10 Conclusions for Office-to-Office Information Exchange

1. It is not feasible to use digital signatures at the employee level to prove the occurrence of queries. The local authentication of a person and the tracing of their activities works well without the help of digital signatures; furthermore, the evidence collected doesn't need to be usable for external legal procedures.
2. There is no need for a central authentication and authorization service for officials.
3. It is sensible to use digital signatures for communication between information systems if the signers are the participating organizations; signatures are issued by the organization's server.

4. Using logs as evidence of system access requires both digital signatures and regular auditing.
5. To ensure the confidentiality of data exchanged between organizations, it is sensible to use transport protocol solutions such as SSL or SSH.
6. In addition to common standards, it is sensible to create a few central services for the information systems to be joined, including services for certification, domain name, monitoring, and auditing.
7. Using replication to ensure the availability of servers should be considered.
8. The information systems joining the proposed data exchange system must be certified, because when agency *B* is on the organizational level granted access to agency *A*'s information system, the security of *A* will depend on the security of the information system of *B*. Since *A* might not be able to investigate, let alone enforce, the level of security in *B*, a central certification service should be created if there are a large number of organizations communicating.

5 AGENCY-TO-CITIZEN INFORMATION EXCHANGE

A citizen receives various services from the state that can be categorized into three groups:

- Anonymous public services for which the authentication of the user is not necessary. Such services are not intended for citizens only, but for all interested parties.
- Authenticated public services; for example, the ability to view someone's tax declaration could be placed into this category. However, the most important aspect is that while the information is public, the citizen is notified of every occurrence in which someone accesses their data.
- Reflective queries requiring especially trustworthy authentication on the user level. In addition, the citizen should be given information regarding when and who, including themselves, have showed interest in their data. The latter would help to detect and reduce unauthorized access. Conversely, the query log displayed cannot be complete as it may contain evidence of queries from a certain privileged official or group of officials such as the Security Police.

From an authentication standpoint, the second and third options are equal. Therefore, the following types of services are examined: those that need authentication, and those that don't.

How will the user communicate with the e-State? If we consider the large number of users and the diversity of available software platforms, as well as the fast development of projects targeted to the public, then in the initial phase of the project, a solution requiring no additional software to be installed on the user's computer should be used. It is sensible to assume that one or more Internet portals will be created through which the citizen can communicate with the state using a Web browser.

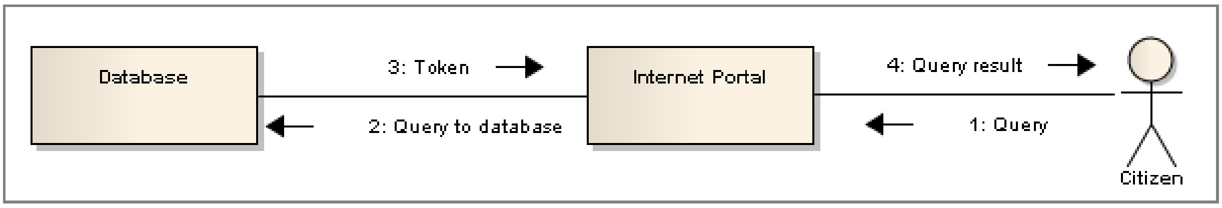

Figure 7. Communication between citizen and state

Figure 7 describes communication between agencies, in which officials authenticate themselves to the local information system and the agency's information system, in turn, will authenticate itself to the databases. In this case, however, there's a citizen instead of an official, and instead of the agency's information system, there is a portal.

The portal is managed by a government office to which the same rules used by other agencies apply; otherwise it would create a security hole, and funds used for securing the rest of the system would be wasted.

The analysis of interaction between the citizen and the portal raises the following questions:

- How does the citizen grant to the portal the right to make queries in their name? In comparison, an official grants that right to the agency's information system when he or she enters into a contract of employment and agrees to follow the internal work procedure rules.
- How is the citizen authenticated for the services that require authentication?
- How is the confidentiality of the communication between the citizen and the portal ensured?

5.1 Using External Authentication Provider

There are approximately one million authorized private individuals in Estonia, and the portal must be able to authenticate them all; however, managing authentication information for a million users is an enormous and expensive task. Creating and operating a portal would be significantly cheaper if the authentication service could be outsourced; for example, to a bank or another organization with a significant customer base, provided that the organization offers such a service.

If an external authentication provider is used (see Figure 8), the users' authentication information would not be managed by the portal. Instead, the portal would receive a confirmation from a third party, such as the authentication provider, about the identity of the person performing the query.

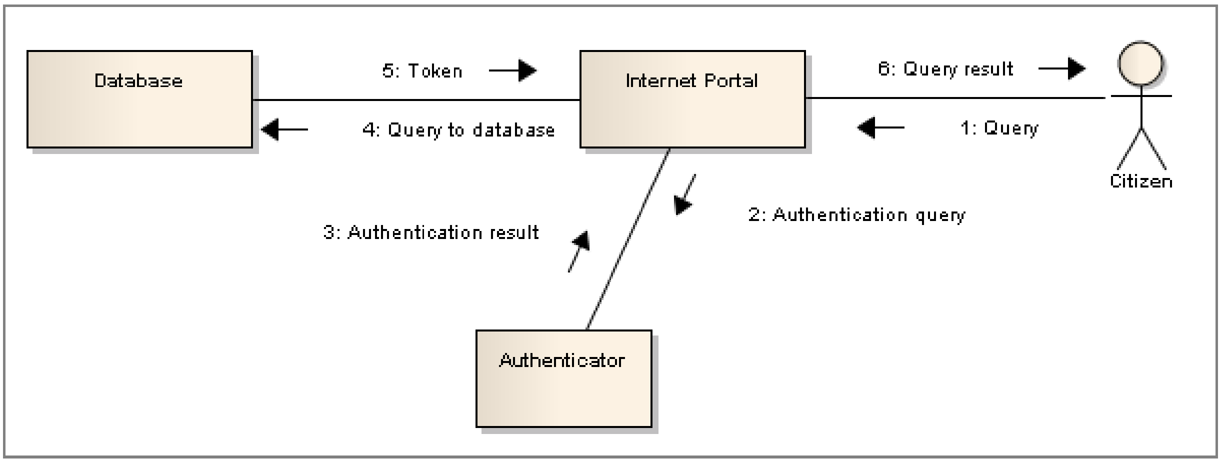

Figure 8. Authenticating the citizen through an external authentication provider

The above scheme could be modified, for example, to let the user interact with the authenticator directly and transmit an authentication token, electronically signed by the authenticator, to the portal.

An external authenticator may bring new security threats. For instance, the portal accepts the authenticator's claim about the user's identity, allowing the authenticator to perform unauthorized queries about anyone's personal data.

There are two possible types of attack. The first attack assumes that the user is authenticated using a password or another type of authentication scheme based on a shared secret which, by definition, is known to the authenticator. The authenticator connects to the portal and claims to be the citizen whose information he or she needs to look up. Since it knows the citizen's passwords, it can present the correct password. The attack will leave no suspicious traces in logs.

The second attack works even if the user is authenticated using public key cryptography, but the authenticator cannot perform a direct impersonation attack without leaving evidence of access. In this case, the authenticator connects to the portal and claims to be the citizen whose information he or she needs to look up. The portal makes an authentication query to the authenticator. Even though the query is incorrect, the authenticator responds with a positive reply, whereupon the portal allows the query to be processed. If the portal logs all authentication queries and responses, it would be possible to later detect the abuse committed by the authenticator.

It follows that an external authenticator can perform arbitrary queries about arbitrary persons. In other words, the authenticator has an illegal, but real opportunity to perform arbitrary queries in government databases. The analysis of potential external authenticators shows that the data exist, which up to now had only been known to citizens, but would be certainly useful for the authenticators in their other areas of business. Therefore, this danger should not be ignored.

5.2 Authentication with Public Key Cryptography Systems

Implementing an authentication scheme based on public key cryptography assumes that every user has a private key and a certificate. To use ID card authentication, the user needs a smart card reader; however, this requirement is not exclusive to this project, since the ID card is introduced also in other areas. The portal must be able to verify the validity of certificates, which is a service offered by the certification service provider who issues the certificates on the ID cards [12:22]. There are no other assumptions for the portal.

If we assume that the client is authenticated on the level of the SSL connection that secures the HTTPS [39] protocol[1], then to authenticate the client on the portal side, it will suffice to have an HTTPS server that can query certification service providers about the validity of users' certificates. Using public key cryptography authentication completely eliminates the need for an external authenticator. A disadvantage of this method is that it will take a few years for it to become widespread. During that time, either an alternative authentication method must be used, or the provision of personal services must be put on hold.

[1] The authentication of a client, performed upon establishing an SSL connection, is a standard feature of the SSL protocol supported by all browsers.

5.2.1 Authentication Using Shared Secrets

It is clear from the above example that this authentication method has serious flaws. No matter who manages the authentication information database, that person wields significant power. Furthermore, managing shared secrets is a work-intensive and security-critical process.

The following solutions could be considered.

1. Create a national infrastructure. The disadvantages of this approach include enormous costs and, considering the imminent *[as of 2001 – ed.]* implementation of the Estonian ID card, a very short period of use. From the financial aspect, it would be wasteful. From the security aspect, when the risk of existing authenticators making unauthorized queries is compared to the risk of fatal errors made in the creating and managing of the new infrastructure, it can be presumed that the latter risks outweigh the former; hence, the solution is not feasible security-wise either.
2. Use the services of existing authenticators. Financially, it would be feasible. If some authorization mechanisms, as discussed later in this paper, were to be added to this scheme, the solution would also provide an acceptable level of security.
3. Do not create a system with authentication based on a shared secret, and postpone personal services until the distribution of ID cards has commenced. This is the best solution from a security standpoint, and authentication requiring only the ID card would drive its acceptance.

Feasibly, the second and third options are the most realistic, and the decision to utilize one over the other is mostly political. It should be taken into account that the implementation of the citizens' portal depends on the rest of the infrastructure being in place beforehand. Since it takes at least a year to create an infrastructure that satisfies all security requirements, and by which time the ID cards are being issued, the third option becomes the most attractive: **the citizens' portal must not be opened before the distribution of ID cards has commenced.**

5.2.2 Adding Authorization Mechanisms to the External Authenticator Scheme

Some citizens consider an external authenticator, who might attempt to access someone else’s personal data, poses an unacceptable risk. Conversely, no authenticator has a database large enough to authenticate all citizens. An external authenticator should not be able to return an unauthorized, positive authentication result about another person.

It can therefore be concluded that the portal should have an authorizations database containing information about which authenticator (if any) is permitted to authenticate which citizens. The database cannot be managed by any one authenticator since it's meant to minimize the risks associated with them. More important than the contents of the database is the integrity of the database, for example, updating the database should be possible only upon the receipt of a citizen's application. When the system is launched, there should be no records in the database. All users should declare in writing the external authenticator they wish to use, if any.

This requirement may seem excessive. For instance, if it is possible to declare taxes through online banking [15], why couldn't the bank also manage other services, currently exclusive to the government? However, a bank would possess an accurate overview of the earnings and expenses of its customers, so the tax declaration contains little new information for the bank. It is a completely different matter when the customer's medical history or criminal record is considered. Even though this information might be useful to the bank, current legislation does not give banks any authority to use such information. **Hence, the tax declaration system cannot be extended to transmit arbitrary queries.**

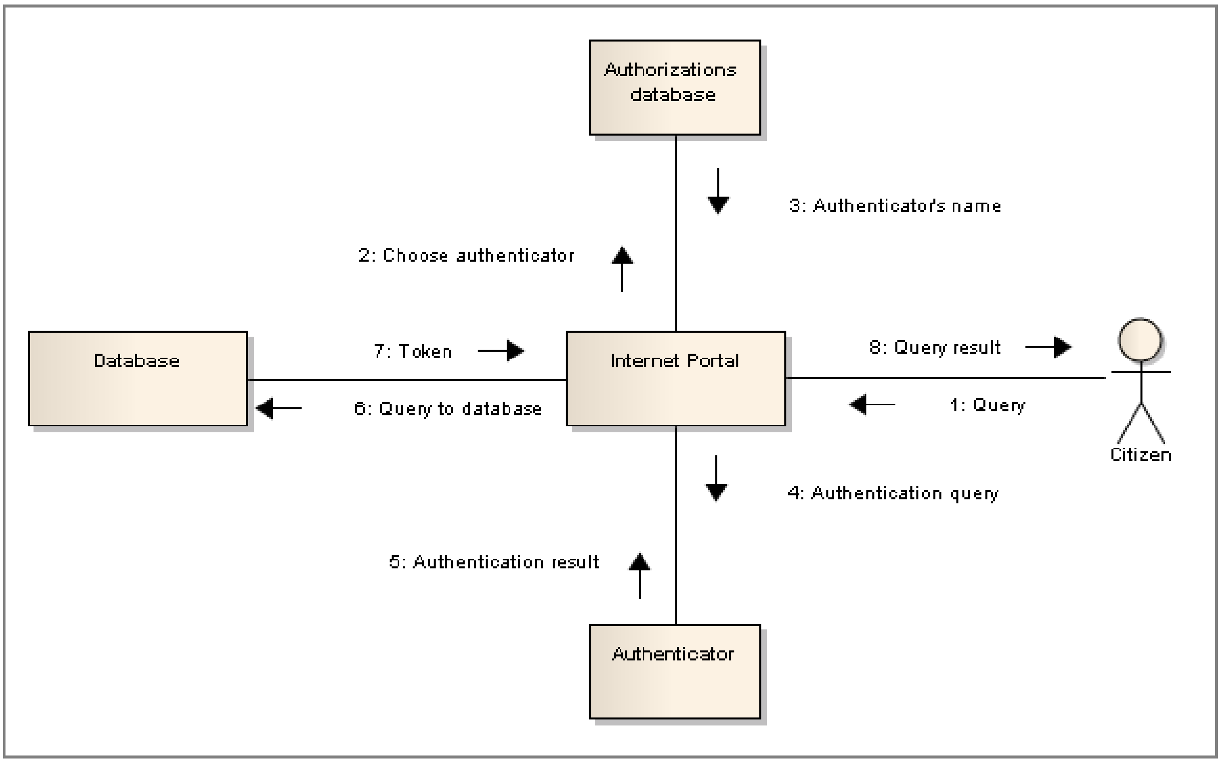

Figure 9. Using an authorizations database

If an authorizations database exists, a citizen's query is processed as follows (see Figure 9):

1. The citizen makes a query.
2. The portal requests the authenticator from the authorizations database.
3. The portal forwards the authentication query to the chosen authenticator.
4. The authenticator returns the result of authentication.
5. The portal makes a query to the government database.
6. The database returns a token, which is sent to the citizen.

For this system to work, it must be assumed that the citizen has submitted a written application to the authorizations database regarding the preferred external authenticator (see Figure 10), and that the citizen is a customer of the chosen authenticator.

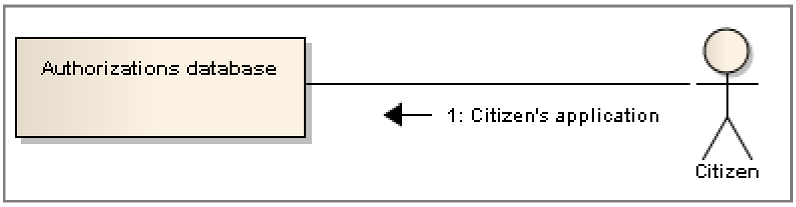

Figure 10. Inserting a record to the authorizations database

5.3 Compliance with the Estonian Databases Act

When creating the citizens' portal, attention should be paid to legal aspects of the project. According to the Estonian Databases Act [4], the authorized processor of a database is authorized to issue information only when it has identified the person making the query and has ensured that the person is entitled to see the data that they applied for. The authorized processor must prove that it has issued the data to an authorized recipient, whom it has identified, and that the person had access to the data in question.

The analysis of inter-agency interaction concluded that relevant agreements must be used so that the burden of proof rests with the agency/organization using the data. The agency, in turn, must choose between two alternatives:

- Authenticate officials who use the information system in a way that creates evidentiary material; that is, use the digital signature mechanism to authenticate all queries.
- Enter into a contract with the official that would free the agency from the burden of proof, or more specifically, take away from the official the right to challenge the agency's claims about queries performed.

The same situation occurs when citizens query the citizens' portal. When ID cards are used to sign queries, enough proof will be created for the portal, but authentication with shared secrets does not create evidentiary material. To ensure due legal process, the citizen must therefore free the portal from the burden of proof; that is, the citizen must abandon the right to challenge queries. It is possible and reasonable that the citizen uses the same application for the task that they submit to the authorizations database (i.e., the registry).

The portal must also ensure that the citizen can access only the data that he or she is entitled to. While some may be in a position to receive considerably more data, it is not feasible to make access rights management in the citizens' portal more complicated and less secure by implementing such queries there. The most sensible solution is to implement in the portal only the queries that all users are allowed to make. If one parameter of the query is the enquirer's personal code, which is known from the authentication procedure, it is possible to implement an easy, unified method for querying that returns the data that only the citizen in question has access to.

For the portal, the citizen acts only as a private person. The queries necessary for the role of an official, including an access rights control mechanism, will be implemented in the agency's information system. This is the easiest approach for bringing the citizens' portal into compliance with other requirements of the Estonian Databases Act, since the portal will implement only available queries.

6 SYSTEM ARCHITECTURE

This section consolidates the results of preceding discussions into a common model. The model describes the architecture of an e-State that is created in the spirit of the principles of a democratic state and, given the appropriate legal framework, enables the fulfillment of necessary security goals.

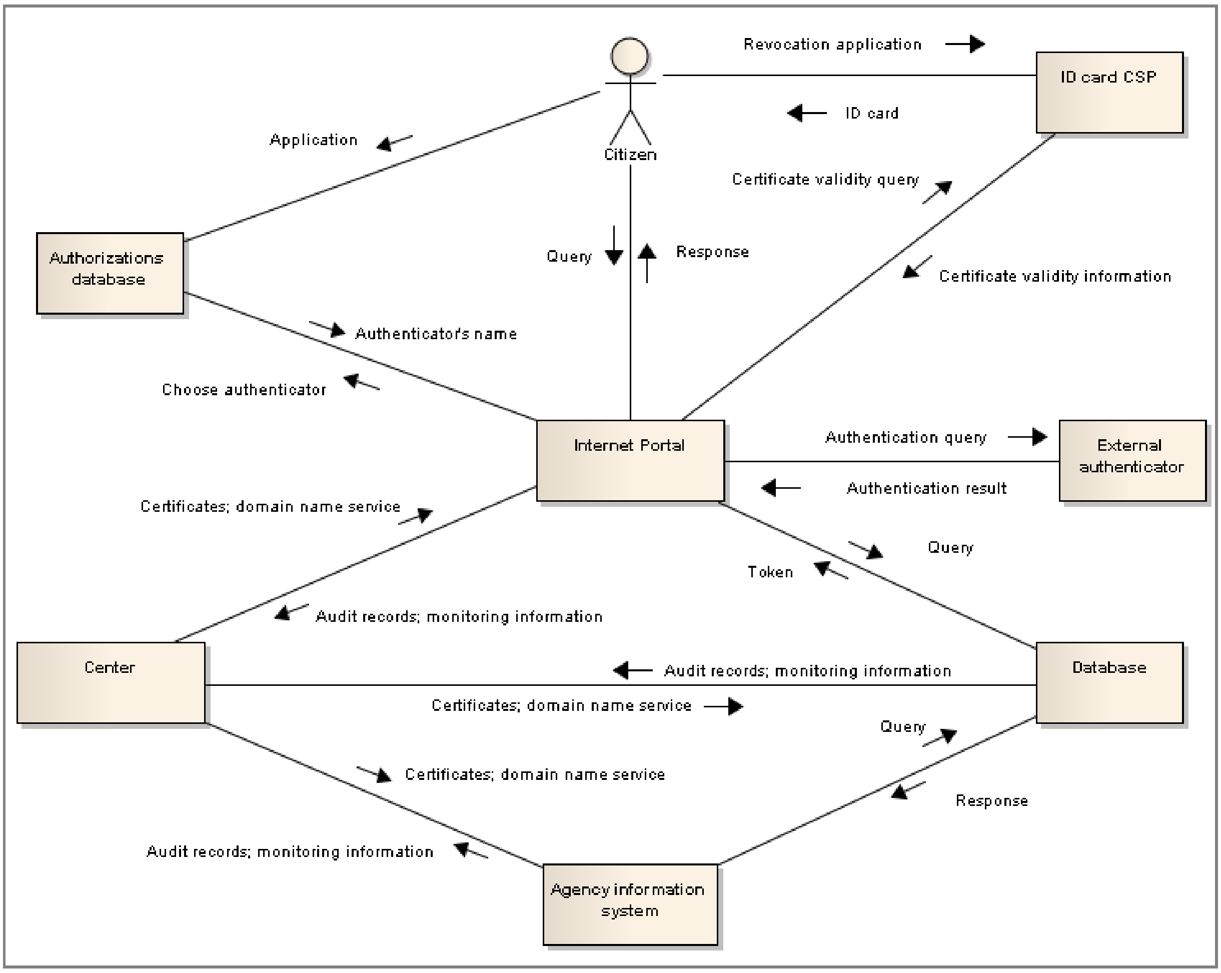
Revocation application
ID card CSP
ID card
Application
Citizen
Certificate validity query
Authorizations database
Query
Response
Certificate validity information
Authenticator's name
Choose authenticator
Internet Portal
Authentication query
External authenticator
Authentication result
Certificates; domain name service
Query
Token
Audit records; monitoring information
Center
Database
Audit records; monitoring information
Certificates; domain name service
Query
Certificates; domain name service
Response
Audit records; monitoring information
Agency information system

Figure 11. One possible system architecture

The model (see Figure 11) can be divided into three parts: a part that enables communication between institutions, a part that allows citizens to communicate with the e-State using the ID card, and a part that allows citizens to communicate with the e-State using passwords.

The first part forms the basis for the others; without implementing it, the communication between citizens and the e-State would not be possible. While the other two parts could be considered as alternatives, they can be implemented in parallel as well. They create a possibility for the citizen to communicate electronically with the e-State, using the services offered by the first part, which is why they can't be implemented individually.

The part enabling office-to-office communication contains three types of components: the center, the information system of the database, and the information system of the agency.

Additionally, a monitoring institution is required, which does not participate in the operation of the work directly and is therefore not depicted in Figure 11.

To enable communication between citizens and the e-State, it is necessary to have a citizens' portal that mediates citizens' queries to government information system. In addition, at least one of the two authentication methods must be implemented: authentication with the ID card and/or password-based authentication using an external authentication provider.

Implementing the first authentication method assumes that the ID card project succeeds and citizens will be issued smart cards. An additional component; namely, the ID card certification service provider, will be created externally of the project as per the requirements of the Estonian Digital Signature Act.

Implementing the second authentication method assumes that a special authorizations database will be created and that citizens will submit electronic applications to the database, granting existing external authentication service providers the right to authenticate themselves. The following sections describe the components and their functions in detail.

6.1 Center

The center fulfills the following functions:

- Certifying information systems connected to the system. The number of issued certificates will be small (equal to the number of connected systems); therefore, it would not be sensible to outsource the service or delay the project until the service emerges. Since the evidentiary value of data depends on the issued certificates, the precise procedures for certification must be established and monitored.
- Providing a domain name service. It becomes necessary from a certain size of a system on. For about ten subsystems, the name service is not yet necessary. The name service must support replication and guarantee the integrity of transmitted information.
- Offering monitoring service to all connected institutions.
- Auditing service, which is necessary to impart evidentiary value for the logs.

6.2 Agency Information System

There are as many subsystems of this type as there are institutions connected to the system.

The institution's subsystem:

- Certifies itself in the Estonian Data Protection Inspectorate.
- Enters into a subscription contract with the center and receives a certificate.
- Enters into a contract for use with the necessary databases.
- Authenticates its employees.
- Makes queries to databases.
- Logs the queries and the tokens received.
- Sends monitoring information to central server.
- Undergoes regular audits.

6.3 Database

There are as many subsystems of this type as there are databases connected to the system.

The database's subsystem:

- Certifies itself in the Estonian Data Protection Inspectorate.

- Enters into a subscription contract with the center, receives a certificate, and has its record written in the name server.
- Enters into a contract with institutions wishing to use the database.
- Responds to queries.
- Logs the queries and tokens issued.
- Sends monitoring information to the central server.
- Undergoes regular audits.

Important databases must ensure the existence of mirrored servers and redundant communication lines to important network nodes, such as to an Internet Exchange Point.

6.4 Data Protection Inspectorate

(does not participate in online activities; not depicted in the figure)

The function of the Estonian Data Protection Inspectorate is certification; that is, giving permission to information systems intending to connect with the system The Inspectorate already fulfills this function, but was mentioned for the sake of completeness of the information given on this paper.

6.5 Citizens' Portal

The citizens' portal is a non-essential subsystem which provides citizens with a means of communicating with the state. The portal is similar to the agency's information system and must undergo the same procedures. In addition, the portal:

- Enters into contract with external authenticators
- Authorizes authenticators using the authorizations database
- Submits online certificate validation queries to the ID card certification service provider
- Authenticates citizens using an external authenticator or the ID card.

The portal must ensure the existence of mirrored servers and redundant communication lines to important network nodes such as an Internet Exchange Point.

6.6 Authorizations Registry

A non-essential subsystem that becomes necessary when the citizens' portal is opened. It is not completely clear who should maintain this database. In any case, the existence of this registry is crucial when external authenticators are used. Since its functions are tightly coupled with those of only the portal, a reasonable solution would be to have the same institution manage the authorizations registry and the portal.

The authorizations registry registers citizens' applications regarding the chosen external authenticator, and responds to portal queries regarding the authenticators that are allowed to authenticate the user in question. The availability requirements are the same as for the portal.

6.7 External Authenticator

A non-essential subsystem that becomes necessary when the citizens' portal is opened and when other authentication methods besides the ID card are required.

The external authenticator:

- Enters into a contract with the portal.
- Enters into contracts with citizens.
- Certifies itself in the Data Protection Inspectorate.
- Responds to authentication queries received from the portal.
- Logs the received queries and the issued tokens.
- Sends monitoring information to the center.
- Undergoes regular audits.

6.8 ID Card Certification Service Provider (CSP)

A non-essential subsystem that becomes necessary when the citizens' portal is opened and when ID cards are used for authentication.

The ID card CSP:

- Issues to citizens the certificate in the ID card.
- Receives certificate revocation applications from citizens.
- Provides validity confirmations to the portal.

7 CONCLUSION

This paper presented the principles that should guide the implementation of the changes to a state's form of government, analyzed security problems arising from the opening of government databases for electronic communication, and described a secure architectural model of one of the base structures of an e-State.

The paper identified a crucial problem impeding the establishment of an e-State: a conflict between the founding principles of a democratic state, represented by existing laws, and the utilization of technological solutions for an enterprise environment, that resembles a kingdom.

To resolve the conflict, it was suggested that improvements of the modern system development be used as a guide, and that the development process that would be made public, well-managed and well-equipped involves a variety of specialists, and would result in a conflict-free model of an e-State that would be the unified foundation for further development work and law-making.

The paper expanded on the above ideas and analyzed one of the main concepts of an e-State: the additional threats arising from a widespread electronic use of the state's databases. The results of the analysis were compiled into the general architectural model.

In conclusion, there is no single piece of technology or a solution that would guarantee the success of the e-State implementation project. However, there exist a number of technologies that, when *not* used, guarantee the failure of the project.

8 FURTHER RESEARCH

This paper can be considered a proof-of-concept work. The analysis is by no means final, since the accurate analysis of even minor problems assumes the intense cooperation of a variety of specialists from many areas.

To put the e-State idea in practice, a well-managed and well-equipped development project must be started. The project must be public and involve the best specialists from various disciplines such as information technology specialists, lawyers, politicians, and economists in order to create a conflict-free model defining the e-State.

The resulting model is the basis for further law-making as well as for system development projects that will implement the various subsystems of the e-State.

9 LIST OF REFERENCES

All Web references were last accessed in May 2001.

[1] Abreu, E., Hurts So Good // The Standard http://www.thestandard.com/article/0,1902,20472,00.html?nl=nr

[2] An Introduction To Microsoft .NET // Microsoft Corporation http://www.microsoft.com/net/intro.asp

[3] Andmekaitse Inspektsioon http://www.dp.gov.ee/

[4] Andmekogude seadus // Riigi Teataja I osa (2001) nr 17 http://seadus.ibs.ee/aktid/rk.s.19970312.108.20000101.html

[5] ARIANE 5 Flight 501 Failure // European Space Agency http://www.esa.int/htdocs/tidc/Press/Press96/ariane5rep.html

[6] Buldas, A., Laud, P., Lipmaa, H., Accountable Certificate Management using Undeniable Attestations // 7th ACM Conference on Computer and Communications Security. ACM Press, 2000, pp 9-18

[7] Buldas, A., Laud, P., Lipmaa, H., Villemson, J., Time-stamping with binary linking schemes // Advances on Cryptology -- CRYPTO '98, LNCS v. 1462. Springer- Verlag, 1998, pp 486-501

[8] Buldas, A., Lipmaa, H., Schoenmakers, B., Optimally Efficient Accountable Time-Stamping // Public Key Cryptography '2000, LNCS v. 1751. Springer-Verlag, 2000, pp 293-305

[9] Common Secure Interoperability V2 Specification // Object Management Group http://www.omg.org/cgi-bin/doc?ptc/2001-03-02

[10] Consumer Privacy Attitudes and Behaviors // Privacy Leadership Initiative http://www.understandingprivacy.org/content/library/research.cfm

[11] Dierks, T., Allen, C., The TLS Protocol Version 1.0, RFC 2246 // Internet Engineering Task Force http://www.ietf.org/rfc/rfc2246.txt

[12] Digitaalallkirja seadus // Riigi Teataja I osa (2000) nr 26 http://seadus.ibs.ee/aktid/rk.s.20000308.22.20001215.html

[13] Eastlake, D., Domain Name System Security Extensions, RFC2535 // Internet Engineering Task Force http://www.ietf.org/rfc/rfc2535.txt

[14] Eesti Vabariigi põhiseadus // Riigi Teataja (1992) nr 26 http://seadus.ibs.ee/aktid/rh.s.19920628.1.19920703.html

[15] e-Maksuamet, Kuidas kasutada? // Maksuamet http://www.ma.ee/ema/kasutamine.shtml

[16] e-riik // Eesti riigivõrgu keskus http://www.riik.ee/et/

[17] Freier, A. O., Karlton, P., Kocher, P. C., The SSL Protocol Version 3.0 // Netscape Communications http://home.netscape.com/eng/ssl3/draft302.txt

[18] Freudenthal, M., Personaalsed turvakeskkonnad. Magistritöö, Tallinna Tehnikaülikool, 2001

[19] Hanson, V., Buldas, A., Lipmaa, H., Infosüsteemide turve 2: turbetehnoloogia. Tallinn: Küberneetika AS, 1998. 371 pp.

[20] Hanson, V., Infosüsteemide turve 1: turvarisk. Tallinn: Küberneetika AS, 1997. 125 pp

[21] Herbert, D., E-innovation, Estonian-style // Cable News Network LP, LLLP http://europe.cnn.com/2001/WORLD/europe/03/30/estonia.technology/

[22] History of Software Engineering // Schloss Dagstuhl http://www.dagstuhl.de/DATA/Reports/9635/report.9635.html

[23] Hoffman, P., SMTP Service Extension for Secure SMTP over TLS, RFC 2487 // Internet Engineering Task Force http://www.ietf.org/rfc/rfc2487.txt

[24] ID.EE - Eesti ID-programm // ID-kaart http://www.id.ee/

[25] Internet muutub kättesaadavaks igale eestimaalasele // Hansapank http://www.hansa.ee/et/hp.9c09c905598456f1f279134ab2a13fb8.html

[26] Internet Protocol, RFC 791 // Internet Engineering Task Force http://www.ietf.org/rfc/rfc791.txt

[27] IP Security Protocol // Internet Engineering Task Force http://www.ietf.org/html.charters/ipsec-charter.html

[28] IT Baseline Protection Manual: Standard security safeguards // Saksamaa Infoturbeamet http://www.bsi.de/gshb/english/menue.htm

[29] Kanellos, M., Former Intel employee admits to computer fraud // CNET Networks, Inc. http://news.cnet.com/news/0-1003-200-2174535.html

[30] Kelsey, J., Schneier, Minimizing Bandwidth for Remote Access to Cryptographically Protected Audit Logs // Second International Workshop on the Recent Advances in Intrusion Detection (RAID '99) http://www.counterpane.com/auditlog2.html

[31] Kessler, G. C., Defenses Against Distributed Denial of Service Attacks // SANS Institute http://www.sans.org/infosecFAQ/threats/DDoS.htm

[32] Kruchten, P., The Rational Unified Process : an introduction. Addison Wesley Longman, 1998. 255 pp.

[33] Martens, T., Pildikesi tulevikust ehk ID–kaart tagataskus // Arvutimaailm (2000) nr 5 (WWW) http://www.am.ee/arhiiv/00-5/martens.htm

[34] Marvet, P., Miks peab taotlema digiallkirja kiiret kasutusele võttu? // Äripäev http://www.aripaev.ee/temp/seminar/29032001/marvet.pdf

[35] Microsoft's software secret source codes stolen by computer hackers // Evansville Courier & Press veeb (WWW) http://www.courierpress.com/cgibin/view.cgi?200010/27+micro102700_latestnews.html+20001027

[36] Mockapetris, P. V., Domain names - implementation and specification, RFC 1035 // Internet Engineering Task Force http://www.ietf.org/rfc/rfc1035.txt

[37] Newman, C., Using TLS with IMAP, POP3 and ACAP, RFC 2595 // Internet Engineering Task Force http://www.ietf.org/rfc/rfc2595.txt

[38] Pangalingi tehniline kirjeldus // Hansapank http://www.hansa.ee/et/hp.4e822eef3603eed72ea96da3dff01894.html

[39] Rescorla, E., HTTP Over TLS, RFC 2818 // Internet Engineering Task Force http://www.ietf.org/rfc/rfc2818.txt

[40] Riigi andmekogude moderniseerimise programm // Eesti riigivõrgu keskus http://www.riik.ee/ristmik/

[41] Schneier, B., Secrets and lies: digital security in a networked world. Wiley Computer Publishing, 2000. 412 pp.

[42] Secure Shell // Internet Engineering Task Force http://www.ietf.org/html.charters/secsh-charter.html

[43] Sertifitseerimise riikliku registri asutamine ja pidamise põhimäärus // Eesti riigivõrgu keskus http://www.riik.ee/riso/digiallkiri/sertreg.htm

[44] Süvari, A., Vedler, S. Krahviperekonnalt varastati maja // Eesti Ekspress (2000) 19. aprill. (E-ajakiri) http://www.ekspress.ee/arhiiv/2000/16/aosa/kuum3.html

[45] Tehniline spetsifikatsioon // Eesti Ühispank http://www.eyp.ee/pages.php3/0102140201

[46] Tervo, T., Single Sign-On Solutions in a Mixed Computing Environment // Helsingi Tehnoloogiaülikool http://www.hut.fi/~totervo/netsec98/sso.html

[47] The e-Citizen, Estonia // Eesti riigivõrgu keskus http://www.riik.ee/ekodanik/ecitizen.rtf

[48] Transmission Control Protocol, RFC 793 // Internet Engineering Task Force http://www.ietf.org/rfc/rfc793.txt

[49] Vallner, U., SGML formaadiperre lisandub XML - ja muudab maailma! // Eesti riigivõrgu keskus http://www.riik.ee/xml/xmlam.html

[50] Lipmaa, H., Mürk, O., E-valimiste realiseerimisvõimaluste analüüs http://www.just.ee/oldjust/JM/lipmaamyrk.pdf

[51] Office of the e-Envoy (WWW) http://www.citu.gov.uk/

[52] CIO's Federal Architecture Working Group http://www.itpolicy.gsa.gov/mke/archplus/group.htm

[53] Heeks, R., Understanding e-Governance for Development http://idpm.man.ac.uk/idpm/igov11.pdf

[54] Caldow, J., The Quest for Electronic Government: A Defining Vision http://www.ieg.ibm.com/thought_leadership/egovvision.pdf