## Contents

1 Security Threats to E-Government and E-Health Systems ........................................... 1
   1.1 Introduction ................................................................................................................. 1
   1.2 Why Security Is crucial to E-Government and E-Health Systems ......................... 1
   1.3 Threats to E-Government and E-Health ................................................................. 3
      1.3.1 General Security Threats ...................................................................................... 3
      1.3.2 Identification of Peers, Digital Signatures and PKI’s ......................................... 4
      1.3.3 Identity Theft ....................................................................................................... 6
      1.3.4 Privacy Issues ...................................................................................................... 6
      1.3.5 Security Standards ............................................................................................ 7

2 Overview of E-Government Security Standards in Switzerland .................................... 8
   2.0.6 General Security Strategy ...................................................................................... 9
   2.0.7 Identity Management, PKI ..................................................................................... 9
   2.0.8 SAGA.ch ............................................................................................................... 10
   2.1 Conclusion ............................................................................................................... 14
Chapter 1

Security Threats to E-Government and E-Health Systems

1.1 Introduction

E-Government and E-Health systems are undisputedly on the rise. Various nations and healthcare providers have done first steps and undergone experiments in that field. Certainly, E-Health and E-Government are going to change the way how citizens and public administration, or patients and healthcare providers interact. However, with their rising popularity, E-Gov and E-Health might not only introduce new ways of interaction, but also new threats to their users and to their providers. Those threats shall be discussed in this paper in the first chapter. The second chapter will then present the current state of security standards in the E-Government projects of Switzerland.

1.2 Why Security Is crucial to E-Government and E-Health Systems

In the world of Information Security, the state of absolute security is treated as an unreachable goal. Always quicker evolving technologies make it im-
possible to foresee all risks involved when implementing or developing new products. Thus, information security is not supposed to be a single product but much more an ever on going process of securing one’s infrastructure against possible threats. (Maiwald, 2003)

While computer systems are well established in the daily life of millions of people, information security awareness lacks behind, leaving many systems open to attacks due to misconfiguration or inappropriate handling of sensitive information. Surveys show that though many people have become suspicious of threats like viruses, spam, phishing, credit card frauds and more, a great majority still lack the ability to appropriately protect themselves from the different kinds of attacks occurring throughout the internet.

E-Government or E-Health however, are fairly new topics. Many risks associated to the entry of public administration and healthcare sectors into the digital age, namely the arising of electronic government or health portals and systems, might therefore be unknown by the broad public. Other threats to E-Gov/E-Health which are similar to the general security problems of information and computer security might render the citizens sceptical towards adopting new E-Government services or to give away personal information to public administration or healthcare electronically.

In both, E-Government as well as in E-Health, the information to be handled is often of highly sensitive nature. Gathered data may include information about income, tax, credit card numbers, bank accounts, but also very personal information like religion, information about previous diseases or medical treatments etc. Security breaches and privacy issues might therefore turn out to affect a citizen more than in usual information systems usage. Even more so, taking into consideration that many E-Government or E-Health solutions intend to store data centralised.

Also, when taking E-Voting or E-Election mechanisms into account, information can affect a whole nation. Once political decisions are based on electronic elections or voting, the prevention of a successful attack on such systems will be of importance to national security.

Concluding, security failures in E-Government/E-Health may have a great impact on citizens or patients day to day life, in the case of E-Government even be of national importance.
1.3 Threats to E-Government and E-Health

1.3.1 General Security Threats

In information security, one often distinguishes between four basic types of attack (Maiwald, 2003). Those attack types certainly apply to E-Government and E-Health systems as well. Therefore, each of the four attack types is going to be illustrated by a short example in the E-Gov/E-Health context. The examples are, unless otherwise stated, purely hypothetical.

Access

An access attack is an attempt to gain information that the attacker is not authorized to see. [...] This type of attack is an attack against the confidentiality of the information. (Maiwald, 2003)

Put into the context of E-Government, an attacker might use a vulnerable system to extract sensitive information. This could include general personal information like address, age, religion and such, but also go as far as to tax information, bank accounts or credit card numbers. An example would be the reported security breach of the Rhode Island E-Government portal in 2005 (Business Wire, 2006).

Modification

A modification attack is an attempt to modify information that an attacker is not authorised to modify. [...] This type of attack is an attack against the integrity of the information. (Maiwald, 2003)

Modification attacks include the changing, insertion and deletion of information. An attacker who gains entry to an electronically accessible crime records database might remove his entries and get away from prosecution. Tax information might be altered in order to avoid paying high taxes. Election or vote results could be altered in order to change the outcome.
Denial of Service

Denial-of-service (DoS) attacks are attacks that deny the use of resources to legitimate users of the system, information, or capabilities. (Maiwald, 2003)

This type of attack is an attack against the availability of information. Voting mechanisms might be attacked, impeding citizens to take part in an election and possibly causing unbalanced results.

Repudiation

Repudiation is an attack against the accountability of the information. In other words, repudiation is an attempt to give false information or to deny that a real event or transaction should have occurred. (Maiwald, 2003)

Attackers might pretend to be someone else and give false votes on elections, or receive medical treatment in the name of a stolen identity.

1.3.2 Identification of Peers, Digital Signatures and PKI’s

One of the main problems concerning security in E-Government and E-Health systems is the issue of verifying the peers identity: An E-Government portal granting access to a citizen needs to verify that the citizen really is the person he pretends to be. In the physical world, one would be asked for a valid identity card. On the opposite, before a citizen submits sensitive information to a government portal, it wants to make sure the information is really sent to a trustworthy institution and not to a malicious fake site. Also, when treating official documents, information should somehow be signed and declared valid by the government as with stamps and signatures in the physical world. The common solution to those problems in large scale E-Government or E-Health projects are a Public Key Infrastructure and digital signatures.

Explaining Asymmetric Encryption and PKI’s in detail would be beyond the scope of this paper. However, a short overview of those techniques in relation to E-Health and E-Government should be given. Briefly explained,
a user may have a public and a secret key. The secret key is to be kept safely by the user and in some cases saved on a smart card. It allows the user to digitally sign documents or information. The validity of the document can then be checked by comparing the signature on the document to the public key of the signing user.

In a PKI, a so called Certificate Authority (CA) or Trusted Third Party (TTP) binds a specific public key to a single user identity. Users can then sign documents with their respective secret key. Signed documents may thereafter be verified by others through the CA, which will confirm whether a signature on a document is valid or not. The CA holds a register of public keys and matching user identities and checks signatures for validity on demand.

![PKI Infrastructure](image)

Figure 1.1: PKI Infrastructure

Digital signatures and a PKI hence allow a citizen or patient to digitally sign documents. Similarly, a citizen receiving information or documents from public administration can verify if the documents are authentic or not: Like each citizen, every e-governmental instance may have a public key verifiable through the CA.

As already stated, PKI’s are often seen as the main authentication
method in E-Gov/E-Health systems (UK online, 2002). Where the different implementations and standards differ is in the question of who constitutes the certificate authority: Some countries see it as an advantage to have total control over CA. Other countries like norway prefer not to intervene directly, rather publishing regulatory and policy frameworks for PKI’s and leaving the implementation to companies and already established certification agencies (OECD E-Government studies, 2007).

Implementing a central PKI for a country, in which one user identity can be used to access different systems, may make the adoption of E-Gov/E-Health systems easier. User would benefit from being able to access different E-Government, E-Health and even various Business sites and E-Shops and use their public key in order to identify themselves. However, federated identity, as such a system is called, can also raise more scepticism towards E-Gov/E-Health systems, as issues like identity theft and privacy become more important. (Sturgeon, 2006)

1.3.3 Identity Theft

The fraudulent acquisition and use of a person’s private identifying information, usually for financial gain. (Oxford University Press, 2007)

Identity theft can already be of greater annoyance to users without E-Gov/E-Health systems. Highjacked e-mail accounts or social networking sites may have serious consequences. Even worse are incidents involving credit card data. E-Government and E-Health systems finally, make identity theft an even more attracting activity for criminals, as the electronic storage of much more personal information increases the possible gains of identity thieves.

1.3.4 Privacy Issues

Privacy is often discussed together with E-Government/E-Health security for similar reasons as identity theft. Governments and institutions tend to accumulate and centralise citizen or patient data in E-Gov/E-health systems. Different peers will require access to different parts of user identities
or data. Therefore, a security strategy for E-Gov/E-Health systems should address how access to certain information will be regulated in order to avoid abuse. Revealing who will have access to exactly which information can also increase trust between service providers and users. Finally, some strategies may even define a controlling authority that monitors data access and reports privacy infringement.

1.3.5 Security Standards

The before mentioned threats make it important for E-Government and E-Health providers to properly protect themselves and their users/clients. How these issues are addressed are usually defined in the general E-Government/E-Health strategy or in a separate security standards or strategy document. Security standards are there to define what common measures are to be taken in order to secure and protect the respective system.
Chapter 2

Overview of E-Government Security Standards in Switzerland

General issues of E-Gov/E-Health security have been discussed. An overview of the current E-Government Security Standards in Switzerland shall demonstrate whether and how beforehand mentioned issues are addressed.

Switzerland’s E-Government projects are of a federative nature. The "Informatikstrategieorgan Bund ISB" presides over the projects and gives the general direction of development in form of frameworks, policies and strategies. Also, the ISB is charged with furnishing the fundamental infrastructure and fulfilling the basic requirements of the different E-Government projects.

The ISB has published a reference model for E-Gov architectures under the name E-GovCH, upon which the current E-Government Strategy of Switzerland is based. Additionally, the registered society eCH was founded. It’s objective is to promote E-Gov related standards. While the E-Government strategies coming directly from the ISB are quite vague at some points, eCH projects may go deeper into details and offer a better insight into the different E-Gov projects. This applies to the security standards as well.
2.0.6 General Security Strategy

One of the basic services demanded from the governmental side in "E-Government-Strategie Schweiz: Katalog priorisierter Vorhaben" is security in general (Steuerungsausschuss E-Gov Schweiz, 2007). However, the E-Government strategy papers do not give too much detail about what this may include. More information about security in general can be found in the "IKT-Strategie der Bundesverwaltung" strategy paper, which defines the overall goals of the ISB (Informatikstrategieorgan Bund ISB, 2006). Here, section 6.5 reveals that ensuring appropriate security in all governmental systems is an objective of the ISB.

Appropriate security is then defined as guaranteed information confidentiality, integrity, availability and non-repudiation. Further security measures guided by the ISB include the risk management of ICT projects, enforcing the use of an interoperable, standards compliant security architecture and to prioritise products certified with renowned security certificates at acquisition.

The same section also states that the E-Government service providers (namely the instances of the ISB) only furnish a basic security level. Further security requirements are then to be defined by E-Government service providers for individual projects. These additional requirements are then agreed upon by the service providers and clients.

2.0.7 Identity Management, PKI

The "E-Government-Strategie Schweiz: Katalog priorisierter Vorhaben" also states the need for a governmentally controlled public key infrastructure:

B2.06

Dienst für die Identifikation und Berechtigungsverwaltung Identifikationsdienste versehen die am elektronischen Behördenverkehr beteiligten Partner (wo nötig auch Maschinen) mit unverwechselbaren elektronisch bermittelbaren Identifikatoren. Mit Hilfe dieser Identifikatoren können die Partner zuverlässig erkennen, mit wem sie kommunizieren. Autorisierungsdienste definieren, welche
Rechte die so identifizierten Partner haben und stellen sicher, dass ein Teilnehmer am elektronischen Behördenverkehr nur Daten einsehen und Leistungen beziehen kann, wenn er dazu berechtigt ist. (Steuerungsausschuss E-Gov Schweiz, 2007)

B2.07

Infrastruktur für die Ausgabe von elektronischen Zertifikaten Elektronische Zertifikate sind ein wirkungsvolles Mittel, um Transaktionen ber das Inter- net sicher abzuwickeln. Wo das Gesetz Schriftlichkeit verlangt, können Geschäfte ohne sie nicht elektronisch abgewickelt werden. Spezielle Ausgabestellen stellen die Zertifikate aus und ziehen sie bei Kompromittierung wieder zurück. (Steuerungsausschuss E-Gov Schweiz, 2007)

Those requirements do not explicitly demand a PKI and this term is never mentioned in the whole paper nor other strategy documents of the ISB. However, the above features seem to correspond to what a PKI would be able to deliver.

2.0.8 SAGA.ch

One of the key publications of eCH is SAGA.ch. SAGA.ch understands itself as a guideline to standardised E-Government systems (Verein eCH, 2007). Section 8 of SAGA.ch defines the current security standards and gives an overview of what architecture and technology should be used. Contrary to the previously mentioned papers, SAGA.ch discusses technology and architecture in detail, giving concrete examples on how E-Government systems should be implemented. The security standards are divided into 11 subsections which shall be presented and briefly discussed now:

Architectural Model of Data Security (8.1)

The architectural model gives an overview of the different security aspects of the SAGA.ch standard. Those different aspects are put into relation with each other and then presented later in their respective subsections.
Security Objectives (8.2)

The security objective part defines the different fundamental requirements of a secured E-Government system. They include the before mentioned availability, confidentiality, integrity and non-repudiation of data.

Security Requirements (8.3)

Different levels of security requirements are fundamental to the SAGA.ch security standards. Data, services and applications are classified in different categories reflecting the damage caused should such it be compromised. The categories range from "no requirements" for e.g data where no harm is caused once compromised, to "very high" for services that, if compromised, could lead to catastrophic consequences. Between those two extremes, assets can also be classified as "medium" or "high".

Those levels of security requirements are to be mapped to the different security objectives from the previous section and the item in question accord-
ingly protected. E.g., a service with very high requirements on availability will have to be very well protected against DoS attacks.

Additionally, the security requirement levels have to be determined according to different aspects: Material and immaterial damage caused when compromised, regulatory law’s, as well as acceptance, costs and feasibility of protective measures. Immaterial damage of data refers to possible infringement of privacy when compromised.

Once security requirement level’s are defined for a certain object, appropriate defensive measures have to be determined.

**Cryptography (8.4)**

Recommended and depreciated cryptography systems and algorithms are denoted in this section. SAGA.ch lists RSA, IDEA, 3DES 168 Bit Key, AES 256 and SHA1 as highly recommended, while DES 56 Bit encryption is marked as not recommended.

**Security Measures (8.5)**

This section discusses 3 different security measures used in E-Gov systems in detail. That is online authentication, long-term signatures and online session key negotiation. For those different measures, various technologies are presented and again, recommended or noted as depreciated. The recommendations reflect state of the art security practises already in use in the private sector. SSL encryption for online authentication, as well as RSA or elliptic curve cryptography for digital signatures are promoted among other.

Biometric systems and long-term digital signatures however, are marked as "in observation", which means that those techniques are still new and have yet to prove their effectiveness.

**Authenticated and Sensitive Data Connections (8.6)**

Authenticated and sensitive data connections refer to either encrypted data or communication channels. A PKI is mentioned as an appropriate system to grant and manage data encryption and secure connections in general.
Security Technologies (8.7)

Different security technologies are generally recommended according to section 8.7. The list of the technologies which are presented and briefly explained includes:

- SSL/TLS
- WTLS
- SSH
- IPSEC
- S/MIME
- XML Security
- PGP
- Web Services Security
- Time Stamping Protocols
- Transaction Security

General Data Security Standards (8.8)

General Data Security Standards defines security systems which do not only apply to single applications or use cases but tend to be part of or interconnected with several other systems. Here, architectures like Smart Card implementation or certificate management are discussed. Different standards used by the mentioned architectures are evaluated.

Digital Signature Verification (8.9)

Section 8.9 lists the minimum requirements in order to accept a digital signature. Reasons for rejecting a signature are, among others:

- Public Key can not be verified
- Sender address does not correspond to registered address of certificate
• Digital signature is not certified by a trustworthy CA

• Signature has been revoked or is expired

**Key Management (8.10)**

SAGA.ch also defines the proper management of keys within any given E-Government PKI. This includes guidelines on how keys should be created and stored, as well as how keys can be accessed and used. Also, the recommended way of changing expired or revoked keys is discussed.

**Coordination (8.11)**

The last section of the SAGA.ch security standards gives the final remark that proper co-ordination of naming conventions and implementations of security measures are necessary. This, in order to have a seamless network of services which are consistently secured.

### 2.1 Conclusion

The threats and issues surrounding E-Government and E-Health Systems have been shown and, though only in a condensed form, been illustrated. The basic concepts of the current E-Gov security standards in Switzerland have been discussed.

The ISB follows a policy of providing only fundamental infrastructure guidelines and relying on eCH to deliver detailed standards and recommendations. This allows for gradual development and implementations of E-Government systems, piece by piece, where they are most needed. From a security point of view, the granularity of such a strategy may make it difficult to oversee all E-Government risks and security issues. Also, the lack of a overall security standard directly from governmental authorities might keep possible participants away and make a homogeneous, seamlessly secured E-Government environment harder to achieve.

The society eCH and it’s SAGA.ch paper however, fill the gap of a lacking security standard. The fact that the society is open to public and has members of the Swiss IT sector certainly help the released standards to be
up to date and to reflect state of the art in technology. As participation is encouraged, anyone concerned in E-Government security and privacy may get involved and change the outcome of future papers. This also enables the authorities to establish trust between themselves, the citizens and the companies which are all potential customers of E-Government systems.

In terms of completeness, the SAGA.ch security standards certainly deal with most problems discussed in the first chapter and demonstrate that security is being taken seriously. However, whether, when and to what extent the eCH standards are finally going to be implemented and respected remains to be seen by the course of time.
Bibliography


Verein eCH, eCH-0014 SAGA.ch Version 4.01, 2007

OECD E-Government studies, Norway Assessment, Executive Summary, 13.11.2007


Business Wire, NIC Says Rhode Island Security Breach Discovered and Vulnerability Corrected Same Day It Occurred, via:
http://findarticles.com/p/articles/mi_m0EIN/is_2006_Jan_30/ai_n16033211
January 30, 2006

Will Sturgeon, Federated identity ‘can transform e-government’
http://software.silicon.com/security/0,39024655,39156692,00.
List of Figures

1.1 PKI Infrastructure ........................................ 5

2.1 Security Standards Overview (Verein eCH, 2007) ........ 11