Open access • Proceedings Article • DOI:10.1109/CSAC.2002.1176311

Security architecture of the Austrian citizen card concept — Source link

Herbert Leitold, Arno Hollosi, Reinhard Posch

Published on: 09 Dec 2002 - Annual Computer Security Applications Conference

Topics: Security service, Cloud computing security, Enterprise information security architecture, Sherwood Applied Business Security Architecture and Security through obscurity

Security Architecture of the Austrian Citizen Card Concept

Herbert Leitold
Secure Information Technology Center – Austria A-SIT
Herbert.Leitold@a-sit.at

Arno Hollosi
Federal CIO Office Austria
Arno.Hollosi@cio.gv.at

Reinhard Posch
Federal Chief Information Officer Austria
Reinhard.Posch@cio.gv.at

Abstract

When admitting electronic media as a means for citizens to approach public authorities – i.e., when advancing official proceedings towards e-Government – security is an indispensable precondition for concerns of legal certainty and for achieving acceptance by the citizens. While the security-enabling technologies such as smart-cards, digital signatures, and PKI are mature, questions of scalability, technology-neutrality, and forward-compatibility arise when being deployed on the large scale, such as when being deployed nation-wide.
In this paper the security architecture followed with the Austrian citizen card is presented. This dedicated concept where smart-cards are going to be rolled out to every Austrian citizen will establish the citizen's security infrastructure to utilize emerging e-Government applications. We briefly present the legal provisions that enable e-Government. We than reflect on requirements to be fulfilled to achieve a lasting security architecture that provides swift deployment of applications, but provides the flexibility to not discriminate against service providers and technologies that will emerge in future. The concept called "security layer" is discussed as the core part of the security architecture, which basically is an open interface that hides the security-relevant functionality of the citizen card on a high abstraction level. A few e-Government applications that are being launched in the short-term are sketched to give a touch of the variety of requirements covered in the architecture.

1. Introduction

The omnipresence of modern communication media – in particular the Internet – is dramatically changing daily routine in both our work sphere and our private environment. We got used to 7 x 24 services when accessing our office networks, when doing bank transfers online, when ordering goods, or when selling stocks. In contrast to this, in official proceedings paper forms and personal appearance bound to authority's tenures of office in many cases continues to be routine.

e-Government – the interaction between state authorities and society with help of information and communication technology (ICT) – promises to improve the services for the citizen and at the same time tremendously reduces retention periods and costs such as by avoiding costly media transitions. Consider for instance the workflow of a tax form downloaded from the Internet, filled out at a personal computer (PC), printed out, signed and mailed by the individual, and finally re-converted to its electronic representation at the tax office. Compare that to simply entering the data to a Web form offered by the treasury.

Besides the work flow considerations, the tax form example already shows that security needs to be a major concern in order to avoid improper use, together with requiring a high-level security architecture applicable to the dissimilar proceedings. The individual needs to be identified and the filled tax form needs to be authentic. While the combination of a tax number or a social security number, together with a digital signature based on a public key infrastructure (PKI) e.g. provided by the treasury itself may serve that certain case, other departments may have different requirements. The variety of public proceedings asks for a sweeping security architecture that scales in two dimensions – the number of applications and the number of individuals that utilize e-Government. In addition, as the installation of e-Government is considered a long-term investment, the inclusion of future technologies needs to be considered in early design stages, as otherwise tailing applications for each new technology, as such technologies mature, may turn out a quite costly experience.

In a cabinet council in November 2000 the Austrian federal government unanimously decided to employ chip card technology to ease official proceedings for the citizens. This trend-setting decision will finally result in delivering an "e-Government-enabling" smart-card to each Austrian citizen in 2003/2004 – a concept we call the

"Austrian citizen card". In June 2001 a further cabinet council decided to reorganize the federal ICT coordination by installing a federal Chief Information Office (CIO) as a staff position which has among its main duties the establishment of an ICT and e-Government strategy that is concerted between the stakeholders involved, i.e. the CIOs of the federal ministries, the provincial governments, and the municipalities.

In this paper we discuss how these leading decisions have been implemented security-wise. A previous white paper discusses the security requirements of the so-called citizen card concept from a public authority's perspective [1]. We present a security architecture that addresses the requirements laid down in the paper in a scalable way as well as is open for the market in terms of easy inclusion of specific security solutions and emerging technologies.

In the remainder of the paper we discuss the security requirements that arise in e-Government environments in section 2. These are mainly identification and entity authentication, electronic signatures for data origin authentication, and confidentiality and data protection aspects. In section 3 the legal provisions that enable e-Government are sketched. These are the signature laws and rules regarding admissibility of electronic means of identification and delivery. The Austrian citizen card concept is introduced in section 4, where we describe how the security requirements and legal provisions are translated into a state-of-the-art technology. In section 5 the so-called 'Security Capsule' and 'Security Layer' are presented which are the core part of the security architecture in terms of technology-neutrality and forward-compatibility.

To give an outlook to the Austrian e-Government initiatives that will make use of this security architecture, section 6 describes a few e-Government applications that will be deployed shortly and that will utilize the concepts introduced in this paper. Finally, conclusions are drawn.

2. Requirements in e-Government

In a first rapprochement the security requirements arising in e-Government are:

- corroboration that the entity is the one claimed – entity authentication
- corroboration that the source of information is the one claimed – data origin authentication
- provision that the information is not disclosed to unauthorized entities – confidentiality
- provision against false denial of having carried out a transaction – non-repudiation

In official proceedings even a single case of abuse may carry high severity and may jeopardize civil rights. The consequence of such strict security constraints is that state-of-the-art technology needs to be used and that the security measures of the systems need to be proven.

A further fundamental requirement when aiming to roll out e-Government on the large scale is that no discriminatory situations shall arise. Providing solutions such as citizen smart-cards or portals to access services shall be open for the market. An intention is also to exploit synergies by aiming for an architecture where infrastructure deployed by the public authorities can also be used to improve the security of e-Commerce. In addition, e-Government may open business opportunities where in a public-private partnership civil services can focus on its core responsibilities where official competence is involved, while private business can offer value added services such as Web portals.

Figure 1 illustrates a scenario where the authorities identify standards and specify interfaces in a way that supports the different e-Government applications. The interfaces shall allow leading over conventional administrative channels with personal appearance to e-Government. Service providers can offer Web-portals that allow citizens access to the applications. In this scenario, it is of vital importance that the authority has full control on the interfaces to avoid vendor lock-ins, such as by proprietary solutions. Therefore the interfaces have been specified by the federal CIO office. These interfaced are described in more detail in section 5.

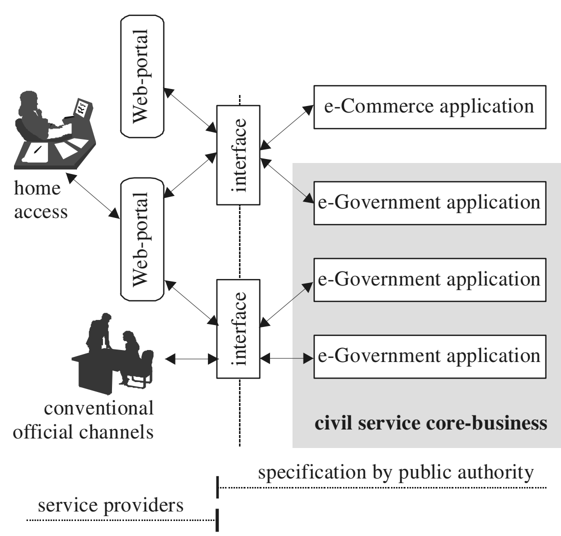

Figure 1: e-Government in public-private partnership

In paper-based official processes, the security requirements stated before may be accomplished by identifying the citizen or an authorized attorney by means of an identity card, deeds, or witnesses. Confidentiality is provided by envelopes or by classified records. Handwritten signatures, forms, stamps, and a notary public provide the integrity, data origin authentication, and the non-repudiation property.

The equivalences in electronic processes are well known: encryption, digital signatures and PKI. However, let us reflect a bit on the PKI case. By issuing a certificate a certification service provider (CSP) establishes the link between the physical identity and the virtual identity. The physical identity may for instance be indicated as the individual's name in the certificate and the virtual identity is usually a public key. However, even if the registration procedure includes personal appearance of the user and even if the identity link is established by showing an identity card during registration, the information provided with the certificate still is limited to data given in the certificate – the individual's name in our example. Official proceedings usually require to unequivocally identifying the individual. Even in a relatively small country such as Austria with eight million residents, and even if also giving the birth date – i.e. giving the first name, the last name and the date and year of birth to identify the individual, there are several hundreds of duplicates. To unequivocally establish the identity online, the CSP needs to give online access to the registration records, additional information such as a link to public registration records is needed, or the public authorities need to provide CSP services for its own.

Basing on the political decision of employing smart-cards as the security infrastructure of e-Government processes in Austria the procedure followed was to first define the general requirements arising from the public authority's perspective in a guiding document [1]. The further proceeding has been based on this consolidated view and is discussed in the remainder of this paper.

3. Legal provisions vs. technical concepts

Security-wise, public proceedings are in particular characterized by requirements of writing, handwritten signatures for authentication, as a declaration of will, or as a declaration of knowledge. Furthermore, requirements of identifying the individual and the delivery of decrees or notifications are evident. In the following sub-sections we discuss the legal provisions that enable modeling these requirements by electronic processes in an online world and compare the legal provisions to technical concepts.

3.1 Electronic signatures

Signature laws provide rules on the permissibility of electronic signatures as evidence. Usually digital signatures based an asymmetric cryptography are used. Its equivalence to handwritten signatures is a major aspect of signature laws. For the European Union (EU), the electronic signature directive [2] defines in its article 5.1 that electronic signatures create the same legal effect as handwritten signatures, if certain requirements are fulfilled. Such electronic signatures are commonly referred to as qualified signatures[1]. The requirements for a qualified signature are basically that:

- the qualified signature is created by a so-called secure signature-creation device (SSCD). The SSCD is the device getting in touch with the signer's private key – called signature-creation data (SCD) in the directive.
- the qualified signature is based on a so-called qualified certificate. A qualified certificate inter alia holds the signer's public key – signature verification data (SVD).
- the certification service provider (CSP) issuing qualified certificates needs to fulfill certain requirements, such as using trustworthy systems when creating qualified certificates.

The member states designate appropriate public or private bodies that assess the conformance of signature products such as smart-cards to the requirements laid down for SSCDs or for trustworthy systems used by CSPs. This also provides mutual recognition of the SSCDs within the EU. In order to establish a harmonized view on these security requirements, the European Commission can publish reference numbers to recognized standards. The European Electronic Signature Standardization Initiative (EESSI) [3] has been established therefore. The European Telecommunications Standards Institute (ETSI) and the European Committee for Standardization (CEN) have been entrusted to develop such standards. Among these is the list of algorithms eligible for qualified signatures [4]. Among the signature suites defined in [4] are Rivest, Shamir, Adleman (RSA) [5] or digital signature algorithm (DSA) [6] with 1020 bit keys, or DSA variants based on elliptic curves [7] with 160 bit keys. Moreover, Common Criteria (CC) [8] protection profiles for SSCDs [9] or hardware security modules (HSM) used by CSPs [10] have been developed [2].

The directive had to be implemented by the EU member states by July 2001, i.e. national signature laws had to be put in force by that date. Although the directive gives a common framework, national implementations in Europe show a few refinements. The Austrian signature law [11] and the signature order [12] e.g. lay down that the security-relevant components involved in the

[1] The term 'qualified signature' has been introduced by EESSI. Although it is not used in the directive [2], some EU member states have adopted the term, such as the German signature law. Other national laws use different terms, such as 'secure electronic signatures' in the Austrian signature law. To avoid confusion, we use 'qualified signature' throughout this document.

[2] At time of generation of this paper, the standards developed by EESSI have not yet been published as official reference numbers by the European Commission.

signature-creation process need to be assessed by a confirmation body – a designated body in directive terms.

The security-relevant components to be assessed include the SSCD that implements the SCD (the private key). The components to trigger the signature-creation process are security-relevant, e.g. the components to enter a personal identification number (PIN), as the PIN may not be intercepted. Moreover, the components to be assessed include the viewer component ensuring that the data to be signed (DTBS) is correctly displayed to the signer without any dynamic or hidden information. Finally, the hash function, if provided outside the SSCD, and the communication link delivering the DTBS (the hash value) to the SSCD are security-relevant.

A rationale for the Austrian signature law requiring assessment of the SSCD environment although the directive limits the conformity assessment to the SSCD itself origins from technical considerations[3]: to ensure that qualified signature may not be forged the PIN in transfer may not be intercepted as an impostor getting hold of the SSCD may create a signature. Interception of the PIN and tampering with the DTBS by trojan horses has e.g. been demonstrated for smart-card solutions available in the market in [13], countermeasures based on trusted computing platforms are proposed in [13], respectively. The problem of trustworthily displaying the document is discussed in [14].

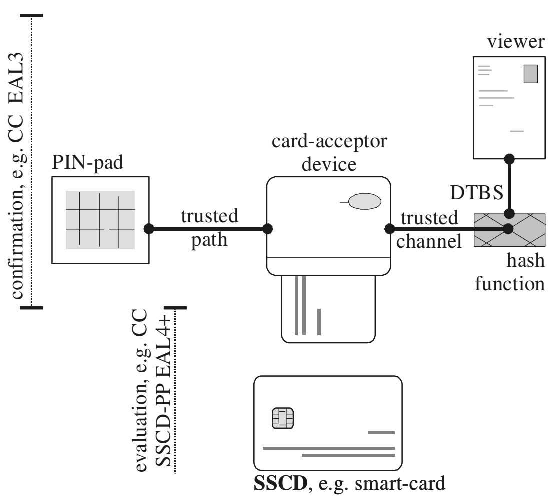

Figure 2: Signature-creation system

Figure 2 illustrates a signature-creation system. The SSCD is shown as a smart-card – a technology of choice to fulfill the security requirements, in particular due to the good physical protection that ensures SCD secrecy. The figure also shows the CC evaluation assurance levels (EAL) appropriate for fulfilling the security requirements which are EAL4 augmented for the SSCD [9], EAL3 for other security-relevant functions [12], respectively.

To counter the threats on the SSCD environment, the communication channels between the SSCD and the PIN-pad, and for communicating the DTBS to the SSCD are shown as trusted paths and trusted channels. I.e. the trusted path for PIN entry needs to maintain confidentiality and integrity, the trusted channel for the DTBS needs to maintain integrity. This shall ensure that an attacker can not tamper with these channels and also follows the approach taken with the SSCD protection profiles developed by EESSI [9]. Further requirements on the SSCD environment that have been developed by EESSI are given in [15]. An in-depth discussion on the requirements for SSCDs and implementation guidelines for different SSCD-technologies are discussed in [16].

3.2 Identification and delivery

It has been discussed in section 2 that identification solely on the basis of a certificate, such as a X.509 certificate, usually does not provide the identification of an individual in the online-quality required for e-Government applications. The reason is that the CSP registration information is usually not accessible online.

Under the Austrian registration laws, a unique central registration number is assigned to each citizen – called a ZMR number [17]. We developed a process called 'persona binding' [18] where an extensible markup language (XML) record is generated that is signed by the authority. For physical persons, the persona binding contains the ZMR number, the name of the individual, his date of birth, and the SVD (the public key) of the person. This data structure is signed using the XML digital signature standard (XMLDSIG) [19]. Comparable bindings for legal persons such as for associations are similarly constructed, but use alternatives to the ZMR, e.g. an official association number.

While the persona binding can provide the online identification quality required for e-Government, data protection aspects do not allow for unrestricted use of the ZMR number as identification of the citizen. A further step is required to inhibit prohibited inference between independent administrative procedures, e.g. between applying for a driver's license and a tax declaration. The provisions made in amendments to public procedures laws [20] are to define that a number termed VPK that is encrypted and procedure-specifically derived from the ZMR may be used for identification purposes and may be stored, while the ZMR may not be kept with the procedure's records. The implementation is basically, that the person-specific ZMR derived from the persona

[3] An approach of also requiring assessment of the SSCD environment is e.g. also followed in the German signature law, whereas some member states require evaluation just for the SSCD.

binding under control of the citizen is merged with an ID of the administrative process and a cryptographic hash function is applied. This is illustrated in figure 3.

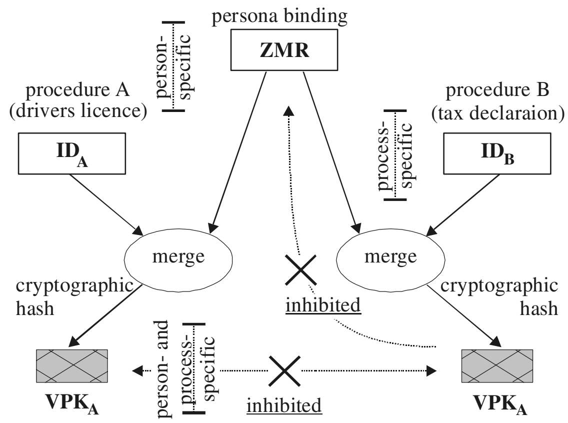

Figure 3: Process- and person-specific ID (VPK)

What comes for free with the process described in figure 3 is that each time a citizen accesses an administrative body, by combining the ZMR number under control of the citizen with the administrative body's ID identifying the particular process, the same unique number can be generated. This allows for process state tracking as e.g. common with packet delivery services, but under more stringent data protection provisions, as the individual permitted to track the state is identified by his persona binding under his control.

The final legal provision to enable e-Government is the conclusion of a process, i.e. the delivery of notification. This in many cases requires evident delivery, such as with registered letters. To enable electronic delivery, the notification of delivery law [21] has been amended. The technical process that can be followed is basically that the authority can deposit the notification on a delivery server. This server attempts to electronically deliver an indication that a notification can be downloaded from the server. Such an indication can be send by various media, as by email, fax, or cell phone short message service (SMS). The addressee can than download the notification and the process ends with an acknowledgement of receipt that is electronically signed by the citizen. In case the electronic indication does not reach the citizen – e-mail addresses or cell phone numbers may have been changed – or the citizen does not carry out the download for other reasons, the delivery server cranks back to conventional methods such as registered letters. In case the delivery server is not operated by the public authority itself, for data protection reasons the notification needs to be encrypted by the authority under a citizen's public key. In that case, the fallback to conventional delivery needs to be carried out by the public authority which is in possession of the plaintext notification.

4. Austrian citizen card concept

With the EU initiatives towards an information society, in particular the eEurope action plans [22] having usage and deployment of smart-cards as one major action line, as well as with the EU signature directive, a number of smart-card initiatives showed up in Europe. Among these are the "eEurope smartcard charter" elaborating ways to accelerate and harmonize the use of smart-cards across Europe. Moreover, several national initiatives such as citizen ID cards have been launched[4].

Having discussed the requirements for e-Government in section 2 and the underlying legal provisions that enable e-Government in section 3, we continue with the presentation of Austria's technological implementation of its security infrastructure – the Austrian citizen card.

Given the name 'citizen card' one might assume a single class of smart-card like devices which is specified in a high grade of details. This in fact is not the case: for concerns of technology independence and openness for solutions provided by the market, the Austrian citizen card is rather a concept that will show a variety of appearances. The health insurance card which roll-out to each Austrian citizen shall be completed in 2004 is one of these appearances. The public identity card that will be available as a smart-card in 2002 is another one. Further citizen cards will be a member card of the Austrian computer society, or SSCDs shipped by CSPs that issue qualified certificates. It is also expected that bank cards for automated teller machines will follow the citizen card concepts in 2004.

What the different solutions that have been sketched above have in common is, that in order to be 'Austrian citizen cards' they need to follow a set of general requirements. These requirements have been specified by the Austrian CIO office [23] and consist of mandatory functions and recommendations, as follows:

- **Qualified signature**: The qualified signature (called 'secure electronic signature' in the Austrian signature law), i.e. an electronic signature that fulfills the requirements to be considered equivalent to a handwritten signature, must be supported. While any signature suite eligible according to the Austrian signature order can be implemented, DSA variants based on elliptic curve cryptography (ECC) are recommended.

[4] For an overview of e-Government or public smart-card initiatives in Europe see the eEurope national progress reports at http://www.europa.eu.int/information_society/eeurope/action_plan/index_en.htm

- **Additional key pairs**: At least one additional key pair shall be implemented, that can be used for content encryption or for electronic signatures that are not considered qualified signatures, e.g. in cases where the equivalence to handwritten signatures is not required. Again ECC is recommended.
- **Info-boxes**: So called info-boxes must be accessible. Info-boxes are memory for storing data such as certificates, or the persona binding.
- **Access control**: Access to the info-boxes must be controlled. It must be possible to assign access rights for each info-box separately. Read access and write access needs to be assigned separately. The access rights must include
  - access after confirmation: the citizen confirms an indication given in the environment of the card
  - access after identification: access is granted, after the citizen has been identified, such as by entering a PIN or by using biometrics
  - unconditional access
- **Specific info-boxes**: A set of info-boxes has been specified that are required by e-Government applications and therefore must be implemented:
  - certificates for the key pairs
  - the persona binding (cf. section 3.2)
  - mandates: powers of attorney can be stored with the citizen card
  - links: although all info-boxes should be stored on the citizen card for concerns of convenience, this might exhaust the memory capacity. Therefore, links to data stored in the environment of the citizen card may be provided.
- **Session key negotiation**: The citizen card must implement a Diffie-Hellman session key exchange.

Given these basic requirements the concept that has been developed by the authors was to combine their actual implementation to a single entity which we call the 'Security Capsule' and to define an open interface to this entity which is called the 'Security Layer'. This concept is discussed in the following section.

5. Security capsule and security layer

From an architectural perspective, the openness towards different technological implementations that has been highlighted in the previous section and that already has led to a significant number of actual instantiations of the concept 'Austrian citizen card' has two major pitfalls: on the one hand, if various solutions enable various combinations of the security-relevant components to be assessed under the signature law (cf. section 3.1, figure 2), responsibility and liability becomes inscrutable. On the other hand, e-Government can not effort to keep that openness, if each application needs to be tailored to any specific solution that fulfils the general requirements of a citizen card as discussed in section 4, but with slight deviations regarding the signature suites, interfaces, etc. These aspects are discussed in the following sub-sections.

5.1 Security capsule

The idea behind the security capsule is that the responsibility for the security-relevant function blocks shall be separated from the application and shall be encapsulated. For the qualified signature, the Austrian signature law already lays down a certain liability of the CSP. However, in addition to the security-relevant functions for qualified signatures that have been sketched in section 3.1, the citizen card concept adds further security features which are per se not under the primary responsibility of the CSP. Examples are the info-boxes or the Diffie-Hellman exchange.

In order to achieve a straight-forward architecture, the security capsule is a requirement that the qualified signature functions, together with the additional citizen card requirements, need to be implemented in a self-contained component – the security capsule. This component may consist of a smart-card together with its IT environment, such as the card acceptor device, provisions for secure PIN entry, and even programs and hard-disk memory of the PC for storing info-boxes that do not reside on the smart-card or for implementing the key exchange functions. Even key pairs – except those for qualified signatures – may be stored in PC memory, although obviously a smart-card would also be the place desired to store such information. Note, that with developments such as the trusted computer platform alliance (TCPA) it is not fictitious to expect solutions showing up in the market where such sensitive information may also be securely stored on-board the PC, such as with a trusted platform module (TPM) [24].

Figure 4 illustrates a scenario where the security capsule stores information in both the smart-card and in the PC. The security capsule holds two SCDs (private keys), one for qualified electronic signatures and one for the second key pair. In that certain example, the smart-card holds just a set of data requiring a high level of protection against disclosure, i.e. the private keys (SCDs) and the info-box holding the persona binding. The corresponding certificates are given by links to the environment – the PC's memory. In addition, figure 4 depicts an info-box holding a mandate, e.g. a XML record signed by the person delegating the powers of attorney. The security capsule further implements those functions that need to be confirmed by a designated body under the signature law. This is sketched by a PIN pad and a viewer component (cf. figure 2).

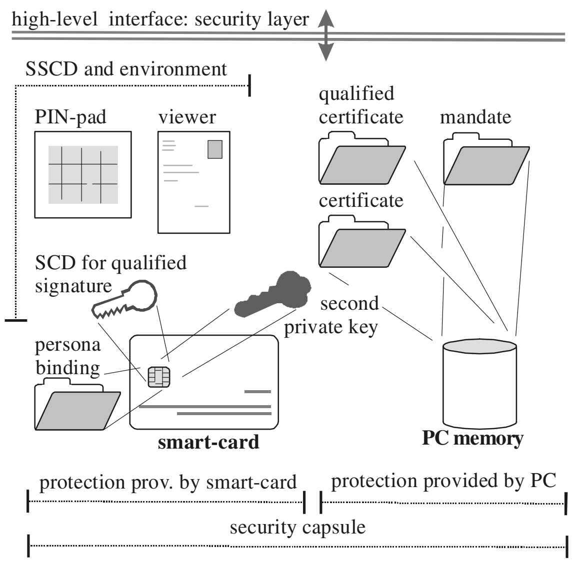

Figure 4: Security capsule

Note that from a security perspective, gluing together the security-relevant components to one logical entity – the security capsule – does not eliminate the problems addressed in section 3.1. Still the communication path between the PIN-pad and the SSCD needs to be secured, the DTBS (the hash value) may not be tampered with in transit, or a trusted viewer is needed. I.e. countermeasures to these threats still need to be in place, such as card acceptor devices including a PIN pad and which e.g. is capable of secure messaging as defined in [25]. What is gained in the concept is that these aspects are transparent to the application. For the application accessing the security capsule it is invisible whether data structures are kept in the smart-card, whether complex structures divide the functions between the smart-card and the PC, or no smart-card is used at all, but e.g. a HSM holds critical data. We call this transparent behavior of the security capsule a 'logical view' to the citizen card. The interface that implements that logical view is called security layer and is discussed in the following sub-section.

5.2 Security layer

From the perspective of an e-Government application the security-functions can be delegated to the security capsule. The application does not be aware of implementation details, such as which signature suite is used, the interfaces to the smart-card, and alike. The application needs a few basic security–related functions, as follows:

- **Signature-creation**: Once a document has been created, the application can request to create a signature. The application selects a signature format such as cryptographic message syntax (CMS) [26] or XMLDSIG [19], and passes the document to the security capsule. The whole signature-creation process – including document viewing and PIN-entry – is carried out by the capsule which returns the signed data, an indication that the signatory did not sign or that the signature-creation process failed, respectively.
- **Signature-verification**: Given a signed document, the application passes the signed data to the security capsule. The signature-verification which includes retrieving certificate status information – e.g. provided by a certificate revocation list (CRL) or online certificate status protocol (OCSP) – is carried out by the security capsule and the result is returned.
- **Info-box access:** The application can read and write info-boxes. Again the security functions, i.e. enforcing the access control policy, are delegated to the security capsule.
- **Session certificates**: The security layer offers functions to create session keys and to create session certificates. This allows securing the client-server communication such as by using transport layer security (TLS) [27].
- **Status information**: Status information, such as the smart-card status, lists of implemented info-boxes, or the functions that are supported by the capsule.

The security layer which has been specified [28] is an interface that implements a request-response scheme where the data representation is encoded in XML. For concerns of maximum flexibility, a variety of protocols have been specified communicating these XML structures between the application and the security capsule. We refer to these protocols as 'transport layer bindings'. The transport layer bindings include transmission control protocol; internet protocol (TCP/IP) where the security layer acts as TCP server and the XML data is communicated via TCP sockets. Moreover secure socket layer (SSL) and TLS, hypertext transfer protocol (HTTP), and HTTP over SSL (HTTPS) have been defined. In the latter two, the security layer acts as a rudimentary Web-server that can be accessed by Web browsers. This allows that besides the security layer no active components are required with the client application, which usually is a conventional Web browser. Techniques such as hypertext markup language (HTML) forms and HTML redirects are employed, as will be discussed in section 6.

The main advantages of the concept of a security capsule implementing the security relevant functions and a security layer as an open interface using open protocols is, that security-wise the trust required is focused to a single component. With the evaluation and confirmation requirements laid down in the signature order for qualified signatures, together with quality seals for security capsule implementations, the citizens get a high degree of confidence regarding the quality of the security measures offered. A further important aspect is forward compatibility. If technology advancements need to be integrated, this is done in a single component.

We have specified the security layer as a common interface to the Austrian citizen card concept. In addition we have implemented a prototype of the security capsule that acts as test and development platform for e-Government applications and as a reference implementation for the interface specification – the security layer – in order to assist developers in implementing the security using specific smart-cards and smart-card environments. For the prototype we implemented a software emulation of the cryptographic functions that substitute the smart-card in order to support various signature algorithms such as RSA and ECC in parallel, or to support several hash functions. For concerns of platform independence of the prototype that acts as a test suite, the prototype security capsule has been implemented in JAVA.

6. Applications and timeline

We finally discuss how e-Government applications make use of the security architecture. Two aspects are worth considering with respect to scalability:

- The citizens shall access the e-Government application with the applications of choice, i.e. the Web browser the citizen is used to. This shall result in higher acceptance, as no specific software besides the security capsule, which e.g. comes with the smart-card shipped by the CSP, needs to be installed.
- The applications shall be controlled centrally in order to make enhancements or modifications manageable.

A further aspect is that the transition to the security architecture needs to be smoothly with respect to existing applications, as integrating new concepts into an operational and in many cases proprietary environment can turn out a costly experience, if at all possible. Concepts on how the security architecture can be transparently integrated need to be developed.

In a typical e-Government application, the user accesses the application via the Web. The first step required is to secure the communication link. As different applications have different security requirements, the strategy followed is to define three classes, as follows:

I. **Normal use**: This class employs the TLS (HTTPS) capabilities of state-of-the-art Web-browsers and Web-servers. The security capsule is not employed, as no identification of electronic signatures is required. The class is usually employed just for information retrieval such as form archives.

II. **Trustworthy infrastructure**: This class employs the security capsule for identification and electronic signatures, but relies on the HTTPS implementation of the browser and the server. Thus, the Web-browser and the Web-server is assumed the trustworthy infrastructure.

III. **Technical end-to-end security**: The highest security level is given, if the security capsule replaces the session certificate establishment of the browser. The drawback is that this requires changes in the Web-browser, such as additional plug ins.

Re-using the workflow example we gave for tax forms in the introduction, we continue with discussing how this works with the security layer. We use this simple example, as tax declarations are limited to a single administrative domain – the tax office – and usually do not require successive communication steps back and forth. Thus, we avoid discussing delegations and we avoid considering file enclosures subsequently to entering the administrative process. We also neglect the case of Web-portals sketched in figure 1, as these anyhow shall not enter into the security-relationship between the citizen and the public authority.

The citizen first accesses the tax office's Web server. We assume a security class II as listed above. The citizen then needs to identify himself. In a process termed 'automatic authentication', we assume that at both ends – the citizen's PC and the tax office's Web server – a security layer is running. In addition, an active component (a servlet) has been implemented at the Web server. For automatic authentication the citizen activates a link to the active component that initiates the VPK-based identification process discussed in section 3.2. In a handshake process, the active component redirects an HTTP request to the security layer asking for releasing the persona binding, which the citizen needs to permit (cf. info-box access in section 4). The ZMR is combined with the identification of the tax declaration ID (cf. figure 3) and the VPK is constructed and signed with a timestamp and a nonce to avoid replays. The whole procedure is controlled by redirects implemented with the Web-server where an active component performed the necessary computations, and the security capsule ensures the security functions. The unique VPK can than be transformed to a conventional authentication scheme, such as a username/password scheme to access existing applications. For instance, tax consultants already access the tax offices online and thus smooth transition to existing applications is needed.

Once the citizen is identified, the Web-server offers a Web-form. Smart forms can be employed, e.g. the name and date of birth can be derived from the persona binding or data known to the tax office can be entered automatically. These forms are, once filled out by the citizen, converted to a XML representation which is redirected to the security layer for being signed. The conversion between a Web-form and XML is not a great deal which either can be done in java-script or the form itself may be described in XML. The whole process concludes with signature–verification carried out at the server-side security capsule and with forwarding the tax-declaration to the treasury's back-end serves. The client/server infrastructure for this sample case is sketched in figure 5.

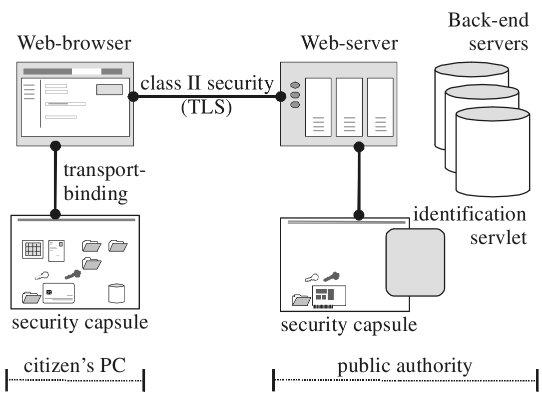

Figure 5: Application environment

Basing on the concepts described, numerous e-Government application are being developed and in the process of being launched. Already operational are filing applications to the social insurance system, or registration of a business in the city of Vienna, the latter not yet using electronic signatures. Petitions to the federal ministries that do not have form requirements will be launched in fall 2002. Calls for penal record reports will be possible to be carried out electronically in fall 2002. Our sample case discussed in this section – i.e. admitting access to tax offices online for all citizens – is to be launched beginning of 2003.

The selection also shows that the approach of an concerted e-Government strategy with an sweeping security architecture works out well: different federal and municipal agencies adopted the approach and thus a coherent access is possible for the citizens.

To give an example of the private-public-partnership, the banking sector has adopted the approach and will launch electronically signed acknowledgements of money orders in fall/winter 2002. Thus, the citizen can pay process fees via online banking and can instantaneously attach to the proceeding the signed payment conformation that has been received from the bank.

Conclusions

The paper has discussed the security architecture employed with Austrian e-Government initiatives. General requirements of e-Government have been discussed and the legal provisions that allow for carrying out public administrations online have been sketched.

The core part of the security infrastructure is the so-called citizen card which is a flexible concept that allows for technological variants, as long as a minimal set of general requirements is supported. These requirements are basically the capability of creating electronic signatures and to store additional data such as certificates. With the roll out of the health security card to each citizen, the personal identity card, and numerous other smart-cards that support the concept, a large scale security infrastructure will be established.

For concerns of flexibility and forward-compatibility, an approach of combining the security-relevant functions to a so-called security capsule has been followed. This security capsule is accessed by means of an open interface, the so-called security layer. With this approach of an interface at a high abstraction level, applications have a logical view to the citizen card. This shall allow for easy integration of upcoming security technologies without the need of tailoring the e-Government application to each upcoming technology.

The paper has discussed the process of accessing applications with a simple example. This has been complemented by an outlook to the actual applications that are being developed.

References

[1] Posch R., Leitold H.: "Weissbuch Bürgerkarte", Federal Ministry for Public Services and Sports, Federal IT-Coordination, June 2001. (in German)

[2] Directive 1999/93/EC of the European Parliament and of the Council of 13. December 1999 on a community framework for electronic signatures.

[3] European Electronic Signature Standardization Initiative: "EESSI explanatory document: Description of deliverables", EESSI Steering Group, 2000.

[4] European Electronic Signature Standardization Initiative: "Algorithms and Parameters for Secure Electronic Signatures, v2.1", EESSI algorithm group, 2001.

[5] RSA Laboratories: "RSA Cryptography Standard", PKCS #1 v2.1 draft 2, 2001.

[6] National Institute of Standards and Technology: "Digital Signature Standard (DSS)", NIST FIPS Publication 186-2, 2000.
[7] American National Standards Institute: "Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)", ANSI X9.62-1998, 1998.
[8] International Organization for Standardization: "Information technology - Security techniques - Evaluation criteria for IT security", ISO/IEC 15408-1 to 15408-3, 1999.
[9] European Committee for Standardization: "Security Requirements of Secure Signature Creation Devices (SSCD-PP)", CWA 14169, 2002.
[10] European Committee for Standardization: "Cryptographic Module for CSP Signing Operations – Protection Profile (CMCSO-PP)" , CWA 14167-2, 2002.
[11] Austrian signature law: "Bundesgesetz über elektronische Signaturen (Signaturgesetz - SigG)", BGBl. I Nr. 190/1999, BGBl. I Nr. 137/2000, BGBl. I Nr. 32/2001. (in German[5])
[12] Austrian signature order: "Verordnung des Bundeskanzlers über elektronische Signaturen (Signaturverordnung - SigV)", StF: BGBl. II Nr. 30/2000. (in German[6])
[13] Cremers, A.B., Spalka, A., Langweg, H.: "Protecting the Creation of Digital Signatures with Trusted Computing Platform Technology Against Attacks by Trojan Horse Programs", Proceedings of IFIP/SEC'01, 2001.
[14] Scheibelhofer K.: "What You See Is What You Sign – Trustworthy Display of XML Documents for Signing and Verification", Proceedings of IFIP Communications and Multimedia Security CMS, 2001.
[15] European Committee for Standardization: "Security Requirements for Signature Creation Applications", CWA 14170, 2001.
[16] European Committee for Standardization: "Guideleines for the implementation of Secure Signature-Creation Devices", CWA 14355, 2002.
[17] Austrian registration implementation regulation: "Verordnung des Bundesministers für Inneres über die Durchführung des Meldegesetzes (Meldegesetz-Durchführungsverordnung - MeldeV)", StF: BGBl. II Nr. 66/2002. (in German)
[18] Holossi A.: "XML-Definition der Personenbindung, Spezifikation Version 1.1.0", Chief Information Office Austria, 2002. (in German)
[19] Eastlake D., Reagle J., and Solo D.: "XML-Signature Syntax and Processing", W3C Recommendation, 2002.
[20] Administration reform law: "Verwaltungsreform Gesetz", 2001 amending "Allgemeines Verwaltungs-verfahrensgesetz (AVG)" BGBl. Nr. 51/1991.
[21] Notification delivery law: "Bundesgesetz vom 1. April 1982 über die Zustellung behördlicher Schriftstücke", BGBl. I Nr. 137/2001. (in German)
[22] Council of the European Union, Commission of the European Communities: „eEurope2002: An Information Society for all", 2000.
[23] Karlinger G.: " Anforderungen an die Bürgerkarten-Umgebung nach dem Konzept Bürgerkarte, Spezifikation Version 1.0.0", Chief Information Office Austria, 2002. (in German)
[24] Trusted Computing Platform Alliance: "Trusted Platform Module Protection Profile Version 1.9.4" TCPA Membership, 2002.
[25] International Organization for Standardization "Identification cards – Integrated circuit cards with contacts – Part 4: Interindustry commands for interchange and Part 8: Security related interindustry commands", ISO/IEC 7816-4:1995, 7816-8:1999.
[26] Hously, R.: "Cryptographic Message Syntax (CMS)", IETF Request For Comment RFC 2630, 1999.
[27] Dierks T., Allen C.: "The Transport Layer Security (TLS) Protocol, Version 1.0", IETF Request For Comment RFC 2246, 1999.
[28] Holossi A., Karlinger G.: "Schnittstellen-spezifikation des Security-Layers der Bürgerkarte, Version 1.0.0", Chief Information Office Austria, 2002. (in German)

[5, 6] English translation availablele at http://www.a-sit.at/informationen/gesetzlich/gesetzlich.htm