

Media-Break Resistant eSignatures in eGovernment: An Austrian Experience

Herbert Leitold¹, Reinhard Posch², and Thomas Rössler³

¹ Secure Information Technology Center – Austria (A-SIT)

Herbert.Leitold@a-sit.at

² Federal Chief Information Officer Austria

Reinhard.Posch@cio.gv.at

³ IAİK, Graz University of Technology

Thomas.Roessler@iaik.tugraz.at

Abstract. Governments and public administrations produce documents – laws, orders, permits, notifications, etc. With the transition from traditional paper-based administration to eGovernment that we have seen in the last decade, authentic electronic documents gain importance. Electronic signatures promise to be a tool of choice. However, given the choice of access channels – electronic or conventional – public administrations offer, eDocuments will have to co-exist with traditional paper documents for several years, if not for decades. In this paper we discuss the Austrian practical experience gained with eSignatures and eDocuments in eGovernment.

1 Introduction

Electronic government (eGovernment) is increasingly supplementing or even replacing traditional means of carrying out public administration. 7 x 24 availability, efficiency, accessibility, reduced red tape, better services for citizens and businesses, reduced costs, or accessibility are the promises. These promises are made for citizen to administration (C2A), business to administration (B2A), and intra-government (administration to administration A2A) communication. Cross-border eGovernment bridging different legislations increasingly gets on the agenda: In the EU policy initiatives such as within eEurope2005 [1] i2010 [2] showed impact and EU Member States—in addition to their existing national eGovernment programs—committed themselves to improve their services towards such cross-border services.

Austria has introduced electronic signature in eGovernment early, such as for official notifications or in 2003 even for official promulgation of laws [3]. The achievements made in Austria have been confirmed by an annual eGovernment benchmark carried out by the European Commission [4] reporting for Austria 100% online-availability of the twenty services that have been benchmarked.

In such an environment where sensitive personal data are processed or where misuse of data may severely impact citizens' or businesses' rights, information security and privacy is a clear must. Research has shown that privacy is among the main concerns in eGovernment, such as shown by an Oxford Internet Institute (et al.) research

that has included lack of trust and inadequate security and privacy safeguards in seven key barriers to eGovernment [5]. Citizens need to have certainty that their data is well protected. Public administrations need certainty that they are dealing with the citizen or the business claiming to have filed an application. Both citizens/businesses and public administrations need assurance that data are authentic. Last not least, the probative value of eDocuments as evidence in court proceedings needs to be ensured.

A number of technologies and tools are needed and are employed to support information security in eGovernment. In this paper we limit our-selves to the role of electronic signatures in eGovernment, i.e. to data-origin authentication. We refer to qualified electronic signatures as electronic signatures that yield legal equivalence to manual ones, i.e. “satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data”. This legal definition has been taken from in the EU Signature Directive [6]. The national implementations are domestic signature laws such as the Austrian Signature Act [7].

The technologies backing electronic signatures exist for a while, i.e. digital signature and public key infrastructure (PKI). While these technologies are widely deployed in commodity products such as email clients, or document viewers, deploying the technologies in eGovernment for nationwide or cross-border use may lead to some additional requirements.

We discuss such requirements, roads followed, solutions developed, and practical experiences in the Austrian case in the remainder of this paper: In section 2 challenges to eDocuments in eGovernment are discussed. While some of the challenges are found in other environments such as in the private sector, others may be considered specific to the public sector. An example of such specific situations are fairly long transition periods from paper to electronic processes that are caused due to the many actors on national, regional, and local level. In section 3 we discuss electronic signatures created by citizens, i.e. signing applications. While this seems to be easy at first sight, the relatively low frequency of a few government contacts per year asks for open solutions that search for synergies with private sector applications in order to increase take up and to make infrastructure investments economic. We continue in section 3 with discussing electronic signatures created by public administrations. The problem addressed here is that co-existence of conventional paper-based documents and electronic documents shall not lead to a duplication of infrastructure. This shall serve as an outlook how the experience made in Austria may serve as best practice. Finally, conclusions are given.

2 Challenges to eDocuments in eGovernment

Documents are the fundamental vehicles of public administration – we are used to show birth certificates as birth date confirmation and legal presence documents, we fill forms to apply for a driver license; we receive building permits from the authority, or show a proof of citizenship when applying for a passport.

Taking a birth certificate as an example, basic characteristics are that the document is needed for many years and it is used in many different processes with a variety of different authorities. Assume that birth certificates are issued as electronic documents where an electronic signature ensures authenticity: We than can state two desired

properties: (1) From a government's perspective, the signed eDocument should also be usable by authorities or in processes that are not yet online and not yet electronic. Thus, paper copies should be possible so that the citizen can print the electronic birth certificate and use it as an attachment to a conventional, paper-based application. This of course raises the question of how authenticity of the printed document can be ensured and how one can verify that the document has been created by an authority. (2) The second requirement stems from a citizen's perspective: If an official document is delivered electronically the citizen may not want to be burdened with keeping a reliable electronic archive for decades – think e.g. of the birth certificate example. Even though today computers are found in almost any household, life-situations may change or computers may break which shall not render essential official documents inaccessible. Again printing important documents on paper may be seen as a proven durable backup media.

The considerations made so far lead to the requirement that when migrating to official eDocuments printouts should remain a genuine representation. Authenticity of eDocuments should be ensured in a way that tolerates media breaks. To state a more stringent requirement, printouts of official eDocuments shall have legal probative value and the assumption of genuineness should apply to printed eDocuments – two requirements that have been included in the Austrian eGovernment Act [8]. We will describe in section 4 how this has been implemented technically in Austrian eGovernment based on electronic signatures.

3 Citizens' Signatures – The Mass-Deployment Challenge

An initiative to employ smartcards to facilitate citizens' access to public services has been launched in an Austrian Cabinet Council in 2000. In early stages of this citizen card project it became obvious, that two major challenges need to be solved [9]:

- The relatively low frequency of citizen contacts with public administrations asks for solutions that are not limited to the public sector, but search for synergies with the private sector. This applies to both government-issued citizen cards used in private sector applications needing adequate security levels (e.g. Internet banking) and enabling the private sector to issue own tokens (e.g. bank cards) as citizen cards that can be used as official electronic identities (eID) in eGovernment.
- Applications usually need to be signed by the applicant. Qualified electronic signatures give the legal basis to sign electronic forms [6] [7]. eGovernment user interfaces of choice – Web browsers – however give no standardized vendor-independent and platform-independent way to sign forms. Integration of smartcards is usually limited to client authentication using SSL/TLS [10].

To address these challenges, Austria has chosen to develop an open specification "Security Layer" between the Web browser and the citizen card [11]. The interface is based on the hypertext transport protocol (HTTP) and thus is accessible via any Web browser using standardized methods. The implementation of the interface is a middleware called "citizen card environment". Aside de-coupling the citizen card from the browser, the middleware integrates the different tokens, as various smartcards can be used. The concepts, the identity management model, and the security architecture of the citizen card are described in detail in [12].

The process of signing electronic data using the middleware bases on a simple XML based request-response protocol. To sign a document, an XML command “CreateXMLSignatureRequest” selecting the key pair and certificate for a qualified signature is sent by the application to the middleware. The data to be signed is referred by a so called “DataObjectInfo”-element. The result is an XMLDSIG signature [13] which is returned by the middleware as corresponding “CreateXMLSignatureResponse”. Using complex requests the data to be signed can be almost arbitrary XML data, can include transformations, or can contain supplements. As an alternative signature format cryptographic message syntax (CMS) [14] is supported.

4 Administrations’ Signatures – The Media-Break Challenge

In this section we discuss electronic signatures created by public authorities, such as on official notifications. We refer to such signatures as “official signatures”. We first describe the underlying concepts and then give two case studies of actual implementations in sub-sections 4.1 and 4.2.

With reference to the challenges for authentic eDocuments that have been discussed in section 2, the two underlying objectives to be addressed by official signatures are:

- Verifiability that the signer was a public authority or a public official
- Authenticity robust against media-breaks

To meet the goal of identifying a public authority an attribute to the signature certificate has been specified. An object identifier (OID) has been defined as an extension to the X.509 certificate and has been registered as “Austrian eGovernment OID”. Using OIDs to define attributes in certificates is a common approach in PKI [15]. It however requires that verification software interprets the OID and informs the relying party. For a domestic administration that e.g. receives an eDocument containing an official signature it is an easy task to identify the official signature, as the national OID is known. For citizens or foreign administrations the problem arises that standard signature verification software can verify the signature, but usually is not aware of an Austrian eGovernment OID. The problem however turns out minor as the eGovernment Act [8] asks the authority (i.e. the signer) to provide a link to information on how to validate an eDocument it issues. This is usually a validation service that does the signature validation and makes an attestation that the document has been issued by the authority based on the eGovernment OID.

The tricky problem is how the media breaks can be overcome. The chosen solution was to apply an electronic signature to the (electronic) document and to construct the eDocument in a way that all information needed to validate the electronic signature is visible on the document – thus printable and also visible on the printout. We define the following conditions:

1. Relevant information needs to be text based. The limitation is however minor for official documents that usually are text documents (for official signatures including images and other binary data, see the binary mode in section 4.2)
2. Text information that can lead to ambiguity on printouts, such as different hyphens, multiple blank spaces or tabs, or diacritics, need to be normalized to an unmistakable representation

3. All elements in the electronic signature are appended as visible text elements to the document as a visible signature block

XMLDSIG [13] has been chosen as signature format being a text-based format meeting condition (1) above. A normalization algorithm has been specified to meet (2). Figure 1 illustrates a signature block (3).

| | | |
|---|---|---|
| Signature Value | K5EY07C1XqArMBUv/AcGw1Zy8dk5fgFYmDMoR6A06mudhDtqIkiv7EU2KYQ5ImWJ | |
|  | Signatory | T=Dipl. Ing., serialNumber=865438804219, givenName=Herbert, SN=Leitold, CN=Herbert Leitold, C=AT |
| | Date/Time-UTC | 2009-01-18T16:39:58Z |
| | Issuer-Certificate | CN=a-sign-Premium-sig-02, OU=a-sign-Premium-sig-02, O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH, C=AT |
| | Serial-No. | 92575 |
| | Method | urn:pdfsigfilter:bka.gv.at:text:v1.1.0 |
| | Parameter | ets1-bka-1.0@1232296799-64918006@23101-9724-0-2175-20711 |
| Verification | validation service: https://www.buergerkarte.at/signature-verification/ | |

Fig. 1. Visual signature block over this paper

The signature block shown in figure 1 is a qualified electronic signature over this contribution to SEC2009 that you are currently reading. It is created in a “text-mode” using the PDF official signature tools described in sub-section 4.2. The electronic signature can be verified using the verification link either based on the electronic file (if available) or based on the typed text if just the printout is available (admittedly, the length of the paper makes typing without allowing a single typo troublesome. Compare however to the little amount of relevant data on your birth certificate which easily can be typed).

The signature block needed to validate the signature contains the following elements:

- A *logo*: The logo has no security value, but is used to allow citizens to visually identify an authority’s official signature.
- The *signature value*: That is the cryptographic result of the XMLDSIG [13] signature in base-64 encoding.
- *Signatory* is the person who signed the document. Either the distinguished name (DN) taken from the signature certificate is shown or a friendly name that can be freely chosen.
- *Date-Time/UTC*: The time when the signature has been created in coordinated universal time.
- *Issuer-Certificate* and *Serial-No.*: The issuer-field and the certificate serial number uniquely identify the certificate and, for qualified certificates or other sufficiently reliable CAs, the signatory. Provided that certificates are published in a directory service (e.g. LDAP [16]), the certificate can be retrieved using this data. This eliminates the need to include all certificate content in the signature block.
- *Method* refers to the text extraction, normalization and representation method used. This also identifies the form used. The form can be a single text block, or arbitrary complex XML structures. An example of official signatures used with complex forms is given in section 4.1.

- *Parameter*: Additional parameters used in the XMLDSIG signature-creation process are encoded in this string.
- *Verification* is a reference to the signature validation service that can be used to verify the document. In the example in figure 1 the URL of such a service provided by the official citizen card web page is given.

Validating the electronic signature using the electronic version of the eDocument has no difference with conventional XMLDSIG signature validation, as all data including the signature certificate is given in the eDocument. When reconstructing and verifying authenticity a few preparatory steps are needed: Let's assume that the relying party has used optical character recognition (OCR) to convert the printout to a text-stream. The next step is to carry out a text analysis to identify the signature block(s) that can be at arbitrary positions in the text stream. The next step is to identify the *method*, i.e. which document format has been used to convert XML. The XML form is retrieved and filled with the text from the OCR-stream. Finally, the certificate is retrieved from the CA's directory service. The result is an XMLDSIG structure and the signature can be verified.

The considerations made so far on official signatures are independent from the document format. Tools have been developed to sign raw text, complex XML structures, portable document format (PDF) documents, OpenOffice documents, or Microsoft Office Word 2007 documents. Taking two examples from this list, the following sub-sections describe how official signatures are used with XML data and PDF.

4.1 Case Study: XML Plus Stylesheet

The first case study of signed eDocuments is structured XML data. Having read the validation process from printouts described above, the reader might have wondered whether this actually will work in practice, such as typing long text from paper with conversion errors that still are frequent with OCR systems. Any mistyped character would render the electronic signature invalid and may be hard to find. Two aspects are however to be considered: On the one hand, reconstruction from paper is the scarce case – usually validation is done using the electronic version as an attachment to an application and even with paper the assumption of genuineness is challenged just in doubt. On the other hand, most official documents (forms) are highly regular and have just a few dynamic elements such as a reference number, the citizen's name, or a date as variable elements. Significant portions are static – permits or other content is often made of known text blocks with little variables. This allows to provide a Web-form that gives the look-and-feel of the paper-document. By filling a few dynamic elements the electronic original is reconstructed.

To give an example of how verifying authenticity of printed official signatures is used in practice, we use the criminal record certificate showing convictions of the applicant. Such certificates are frequently used, as in public procurement a fresh criminal record is to be provided by the bidder. In the majority of cases the certificate shows no convictions. Thus, a limited amount of data is dynamic. Figure 2 below is the Web form to validate a printed criminal record certificate. It requests for entering few data only.

BEZUG: SB INTERNET [REDACTED]
(REFERENCE NUMBER)

STRAFREGISTERBESCHEINIGUNG
(CRIMINAL RECORD CERTIFICATE)

Familiennam(e): [REDACTED]
(Family Name)

Geschlecht: male female
(Gender: MALE/FEMALE)

Vorname(n): [REDACTED]
(First Name)

Akad. Grad: [REDACTED]
(Academic Degree)

Geboren am: [REDACTED]
(Date of Birth: DD.MM.YYYY)


Geburtsort: [REDACTED]
(Place of Birth)

Im Strafregister der Republik Österreich – geführt von der Bundespolizeidirektion Wien – scheint keine Verurteilung auf.
(No convictions are listed in the criminal records database of the Republic of Austria, kept by the Federal Police Directorate of Vienna.)

DVR: 0003506

Tagesdatum: [REDACTED]
(Date)

Uhrzeit: [REDACTED]
(Time)

| | |
|---|--|
|  | Verfahren: urn:publicid:gv.at:for+erb-1.1 |
| | Datum: [REDACTED] |
| | Aussteller: CH+a-sign-corporate-light-02.OU+a-sign-corporate-light-02.O+A-Trust Ges.f. Sicherheitssysteme in el ektr. Datenverkehr GmbH,C+AT |
| | Seriennummer: 82210 |
| | Signaturwert: Base64-Signaturwert |

Dieser Bescheid ist gemäß §20 E-Government-Gesetz (E-GovG) rückführbar. Das Service für die Rückführung und Signaturprüfung kann unter folgender URL abgerufen werden:
https://apps.emiz.gv.at/strafregister/Verifiv.do?action=prepare_verifiv&tv=0&sv=1

Fig. 2. Reconstruction-form for signature validation from printouts

4.2 Case Study: Official Signatures and PDF

PDF is a desirable document format for official signatures, as it is frequently used and PCs are often shipped with PDF readers as pre-installed standard software. Even though PDF has electronic signature features since its version 1.6 [17], the official signature requirement to allow for reconstruction from the printout could not be fulfilled. Thus, separate tools have been developed in Austria. Two signature-modes are supported:

- A *binary mode* where the PDF document is considered a binary stream that is signed. That allows signing arbitrary data including images, but bit-identical reconstruction from printouts is not possible.
- A *text mode* where the raw visible text is signed. This mode does not include images or other binary data into the signed data, but allows for validating the signature from printouts [8].

Binary signatures on PDF documents are similar to PDF signatures defined in [17]. The main difference is that a visible signature block with data shown in figure 1 is created – which gives additional information compared to PDF signatures as known from Acrobat® products.

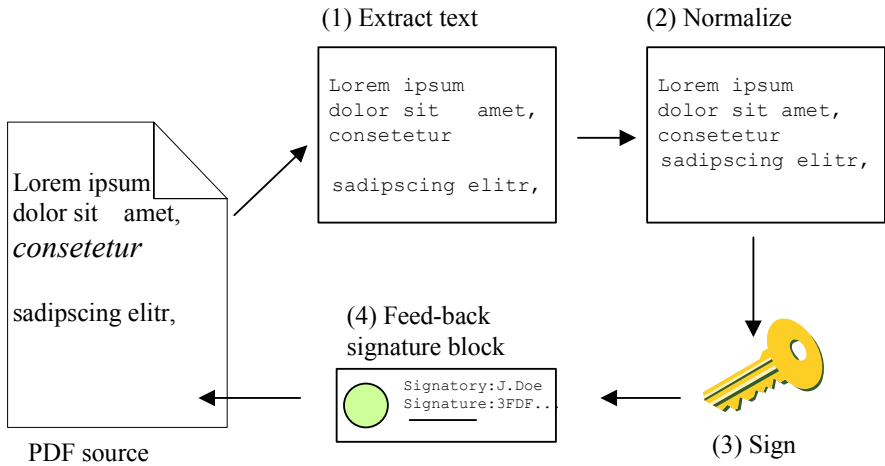


Fig. 3. Text mode signature-creation for PDF documents

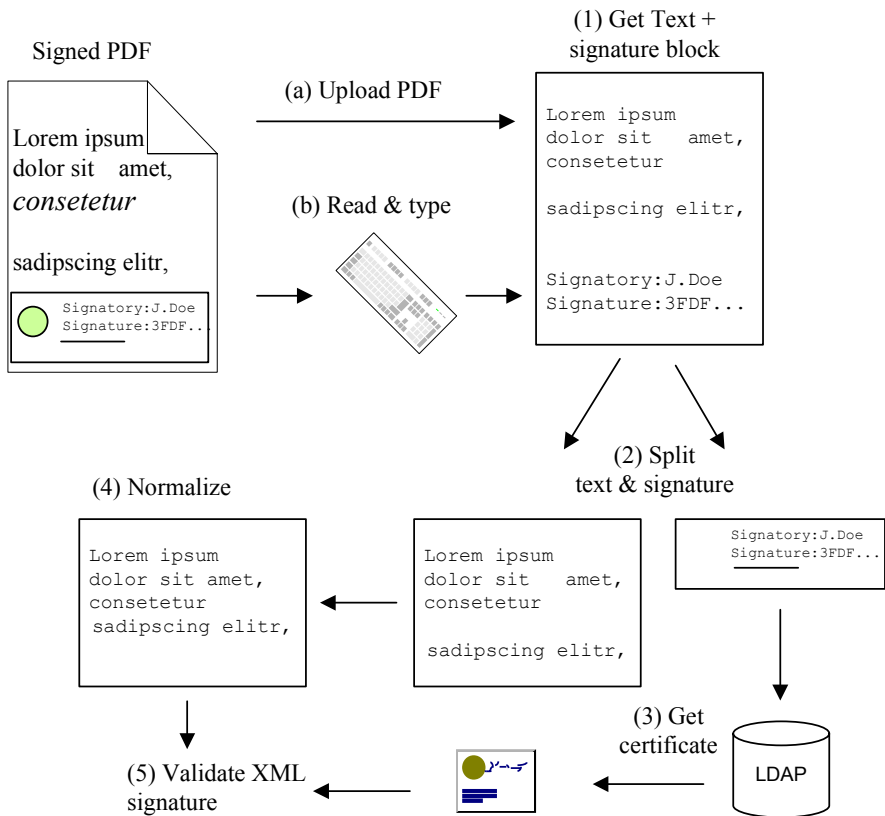


Fig. 4. Signature validation from the electronic document (a) or a printout (b)

We therefore focus on text mode signatures that allow validation from printouts. The tools carry out four steps during signature-creation, as illustrated in figure 3: (1) First the raw visible text is extracted from the PDF document as UTF-8 encoded stream. Formatting is ignored. A critical issue is that the text extraction needs to exactly represent the reading order “top left to bottom right”. This is needed for reconstructing the text from printouts in the same order. It turned out that most PDF tools perform well on extracting from standard text documents, but depending on the PDF creation tools used for the document to be signed tables, headers, footers, and footnotes can result in reading order errors. (2) The second step is a normalization step to eliminate ambiguous characters or text representations on printouts. The normalization specification defines how to handle characters that can be mistaken with similar characters, such as similar hyphens, dashes, or diacritics. Moreover multiple spaces and tabs need to be eliminated. (3) The third step is to sign the normalized text. XMLDSIG [13] is used. (4) Finally, the signature block as shown in figure 1 is created and fed back into to PDF document.

If using the validation link in the signature block and the PDF version of the paper, signature validation follows five successive steps, as illustrated in figure 4: (1) the original text together with the text of the signature block is extracted and converted to a UTF-8 stream. This is either done by (a) uploading the electronic version and employing PDF text extraction tools or (b) by reading the printout and manually typing the text, using OCR tools, respectively. (2) The signature block – or signature blocks in case of multiple signatures – is separated. As the signature-block is well defined, that is done by rather simple text analysis. (3) The certificate issuer and the certificate serial number are taken from the signature block to identify the CA and the certificate. In case the certificate is not embedded into the electronic PDF, it is retrieved from the CA’s directory service. (4) The text is normalized using the same algorithm as during signature creation. The methods used are identified by the *method* field in the signature block (cf. figure 1). (5) Conventional signature validation is done.

A set of tools has been developed to allow for creating and validating such *text mode* or *binary mode* PDF signatures using either the citizen card or server-based signature-creation devices for high volume operations. Among the most convenient ones is a plug-in for Acrobat® Standard or Acrobat® Professional. The signatory uses the plug-in to position the signature block using the mouse within the PDF document.

5 Conclusions

The paper has introduced Austrian electronic signature initiatives in eGovernment. Austria has started in 2001 with a comprehensive eGovernment program where electronic signatures play an important role as a security tool. Electronic signatures are however no end in itself, but the means to achieve authenticity with electronic documents. Thus, the main topic of the paper is how to achieve authentic eDocuments using electronic signatures as the vehicle to provide genuineness.

eDocuments can either be created by the citizen such as filling a form, or can be issued by the public authority as the electronic substitute of paper documents. On the former – applications of the citizens – the paper has briefly described the Austrian citizen card concept as the citizen’s tool to electronically sign forms. On the latter – official documents created by an authority – the paper has described the concept of

official signatures. Official signatures are electronic signatures created in a way that the relying party can verify that an eDocument originates from a public authority. A specific feature developed by Austria is that official signatures are robust against media breaks. That is that an electronic signature created using the concepts discussed can be validated even if printed on paper. This facilitates the introduction of eGovernment as the media preference or capabilities of the final receiver of a document – either the citizen or an authority receiving the document as an attachment – no longer determines on which media a document is issued.

References

1. European Commission, eEurope 2005: an Information Society for all, COM (2002)
2. European Commission, i2010 – A European Information Society for growth and employment, SEC (2005) 717
3. Republic of Austria, Austrian Federal Act on the Federal Law Gazette 2004 (Promulgation Act), Federal Law Gazette, part I, Nr. 100/2003 (2003)
4. CapGemini, The User Challenge Benchmarking The Supply Of Online Public Services, 7th measurement, Prepared by: Capgemini, For: European Commission Directorate General for Information Society and Media (2007)
5. Oxford Internet Institute, Breaking Barriers to eGovernment, MODINIS contract 29172, Deliverable 2, Prepared by: Oxford Internet Institute (and others) For: European Commission Directorate General for Information Society and Media (2007)
6. European Union, Directive 1999/93/EC of the European Parliament and of the Council of 13. December 1999 on a community framework for electronic signatures (1999)
7. Republic of Austria, Austrian Federal Act on Electronic Signatures, Federal Law Gazette, part I, Nr. 137/2000, last amended by Nr. 59/2008 (2000)
8. Republic of Austria, Austrian Federal Act on Provisions Facilitating Electronic Communications with Public Bodies; Federal Law Gazette, part I, Nr. 10/2004, last amended by Nr. 59/2008 (2004)
9. Posch, R., Leitold, H.: Weissbuch Bürgerkarte, Austrian Federal Ministry for Public Services and Sports, Federal IT-Coordination (2001) (in German)
10. Dierks, T., Rescorla, E.: The Transport Layer Security (TLS) Protocol, Version 1.1, IETF Request For Comment RFC 4346 (2006)
11. Hollosi, A., Karlinger, G.: The Austrian Citizen Card – Security Layer Application Interface, Version 1.2.2, Federal Staff Unit for ICT Strategy, Technology and Standards (2005)
12. Leitold, H., Hollosi, A., Posch, R.: Security Architecture of the Austrian Citizen Card Concept. In: Proceedings of 18th Annual Computer Security Applications Conference (ACSAC 2002), Las Vegas (2002)
13. Eastlake, D., Reagle, J., Solo, D.: XML-Signature Syntax and Processing, W3C Recommendation, 2002; RFC 3275 (2002)
14. Hously, R.: Cryptographic Message Syntax (CMS), IETF Request For Comment RFC 3852 (2004)
15. ITU-T, Information Technology – Open Systems Interconnection – Systems Management Overview – Procedures for the Operation of OSI Registration Authorities: General Procedures, ITU-T Recommendation X.660 (1992), ISO/IEC 9834-1 (1993)
16. Zeilenga, K.: Lightweight Directory Access Protocol version 2 (LDAPv2), RFC 3494 (2003)
17. Adobe Corporation, PDF Reference, fifth edition - Adobe Portable Document Format version 1.6 (2006)