WEB-SERVICE BASED TRANSFORMATION OF DIGITAL SIGNATURE FORMATS

Klaus Stranacher[1]
Bernd Zwattendorfer[2]

Electronic signatures are of great importance in electronic processes. Since the EU Signature Directive [14] was set up in the year 1999, many countries have implemented different types of signature formats. Due to that mixture of various signature types, interoperability in a cross-border context is an open issue. Currently, the recognition of electronically signed documents in cross-border processes is not yet thoroughly discussed between EU Member States. This may result in a situation where a certain eGovernment service in one Member State requires a specific signature format (e.g. CMS), while the document has a different signature format in the country of origin (e.g. XAdES). This hinders automatic processing. The impact of this issue can be also seen in discussions on electronic signatures in relation to the Services Directive [15] where Member State expert groups discuss minimum standards for signature formats. Within this paper we introduce a concept of a web-service based signature transformation that is able to convert different signature formats. Furthermore we have evaluated this concept by implementing a SOAP/WSDL web-service.

1. Introduction

Electronic documents have already started to replace traditional paper documents and hence they form an essential part in various communication processes. They carry import information relevant to all parties involved in these processes. Whether business or governmental communication, electronic documents build an easy and flexible way for information exchange.

During many communication processes, information and document exchange between participating parties form an essential part. In some cases, the integrity and authenticity of documents' contents must be assured. In paper-based processes these requirements are achieved by signing the documents by authorized persons' own hand. For electronic documents integrity and authenticity can be ensured by using digital signatures. Thus digital signatures enable a reliable and secure exchange of electronic documents.

Digital signatures can guarantee the integrity of an electronic document, any alteration of a digitally signed document breaks the signature and verification will fail. Authenticity of the signature can be

[1] Institute for Applied Information Processing and Communications, Graz - University Of Technology, 8010, Graz, Inffeldgasse 16a, klaus.stranacher@iaik.tugraz.at

[2] Institute for Applied Information Processing and Communications, Graz - University Of Technology, 8010, Graz, Inffeldgasse 16a, bernd.zwattendorfer@iaik.tugraz.at

achieved by using signing certificates based on an underlying PKI infrastructure. *Table 1* briefly overviews widely used and standardized signature formats.

Table 1: Signature Formats

Signature Format	Relevant Standards	Comment
CMS	[1]	Cryptographic Message Syntax
XMLDSIG	[2]	XML Signature
CAdES	[3]	CMS Advanced Electronic Signature
XAdES	[4]	XML Advanced Electronic Signature
PGP	[5], [6]	Pretty Good Privacy

Within the eGovernment domain, the most commonly used formats are CMS signature formats for arbitrary data and XML based signature formats for XML data. In electronic cross-border scenarios situations may arise where a certain service requires a specific signature format (e.g. CMS) whereas the signed document has a different signature format (e.g. XMLDSIG or XAdES). This would result in a situation that the receiving service cannot validate the signature and the document cannot be processed automatically. While the conversion of documents' contents between formats can be simply done by wrappers, such conversion invalidates the signature.

This paper introduces a concept to cover such situations within cross-border processes. Therefore, a web-service for the transformation of digital signature formats has been specified and developed. The main research activities on this subject have been carried out within the eGov-Bus project [13], an eGovernment project out of the Sixth Framework Programme funded by the European Commission.

2. Problem Description

EGovernment takes place in a very heterogeneous environment, where different file and signature formats come together. As stated in [7] (Page 124, chapter 5.3.3.6.1), such different signature formats exists among Member States eGovernment applications. Therefore, in cross-border processes situations will appear where documents with different file and signature formats must be exchanged. As an example, imagine the need of a digitally signed birth certificate during a cross-border or cross-domain scenario. In such a case, the receiving application may require the birth certificate in a different signature format than the original format from the delivering service for processing. Thereby the following problem exists: In case of any simple transformation on the birth certificate, the signature will get invalid. This is the situation where the need of an adequate transformation service arises. The signature transformation service can be used for such a conversion. During the transformation process the contents of the birth certificate will not be altered, only a different signature format will be applied. The contents will be signed again by a trustworthy body.

3. Related Work

Jan Piechalski and Andreas U. Schmidt presented a paper on how to carry out authorized document translations in a totally electronic environment. Their scientific work is based on the TransiDoc project [8]. TransiDoc examines a solution for a legally compliant transformation of electronic documents. On the one hand motivation for this project has been the realization of electronic business processes through the exchange of signed documents across borders or domains; on the other hand the long time archiving of signed documents to preserve the probative force has been a reason for this implementation. Within this project concepts and applications for electronic notarization of signed documents in the field of local governments, the public health sector and in notary's offices have been developed.

After transformation and translation, respectively, of a document's contents, the originally applied signature gets invalid. Thus a new digital signature must be applied. To overcome this problem the solution of TransiDoc relies on a so-called "transformation seal". This transformation seal attaches all relevant data that has been produced during a transformation process trustworthily and permanently to the target document. The transformation seal should guarantee the integrity of the transformed document, the correctness of the transformation process and the authenticity of the person who transformed and signed the document. The transformation seal is a piece of XML data containing relevant meta-data of the transformation process as well as an authorized translation signature [9].

Another eNotary service is for example cyberDOC [16]. It is a joint-venture of the Austrian Chamber of Civil Law Notaries and Siemens Austria AG. This service represents the Austrian Electronic Document Archive. To archive a certain document, following process steps are executed: After the document was created by the notary, the document is scanned to get an electronic document. Then the electronic document is digitally signed and encrypted by the notary. Finally, the document is sent to the archive. So cyberDOC guarantees the legal quality of a notarial document.

4. Description

The signature transformation service supports the conversion of widely-adopted signature formats. The most commonly used signature formats can be divided into two classes:

- CMS based signature formats
- XML based signature formats

CMS based formats such as CMS signatures [1] or advanced CMS signatures (CAdES) [3] provide digital signatures in a BER or DER encoded (thus binary) ASN.1 structure. This structure contains the signed content as well as an arbitrary number of signatures on that content, together with information about each signer.

XML based signature formats such as XMLDSIG [2] or XAdES [4] provide XML-encoded signatures on arbitrary but addressable content. The XML signature merely references the signed content (although the reference might be on local data). Like CMS signatures, an XML signature further contains information on the signer and the actual signature value. However, only one signer is allowed.

Both signature formats have in common that a message digest (by applying a cryptographic one-way function) is computed from the canonical form of the encoded content. The message digest is included in the signature format and the actual signature value is computed from this digest value. A direct transformation from XML to CMS signatures (and vice versa), by merely changing the format, is not possible because, as stated above, the signature value is calculated from the digest over the canonically encoded content. Due to the mathematical properties of cryptographic hashfunctions, any alteration of the content – even if this alteration only affects the encoding – leads to a different digest value, yielding a different signature value. Thus, the signature would no longer validate. A signature format conversion therefore necessitates the creation of a new signature on the extracted original signed content.

The signature transformation service includes this stated functionality, applying the signature format conversion from CMS to XML/XAdES and vice versa as well as the transformation from XAdES to different types of XAdES signatures. As a proof, the transformation service outputs a signed verification result of the original inputted signature (base64 encoded). Besides this, the original signature as well as the new signature applied to the content is returned by the service. The input needed for transformation by this service is the original signature and the original document or its contents respectively. In case the original document is in a specific schema of the issuing authority (state), the transformation to an XML schema of the receiving state needs to be carried out in advance and securely delivered to the transformation service (see *Figure 1*).

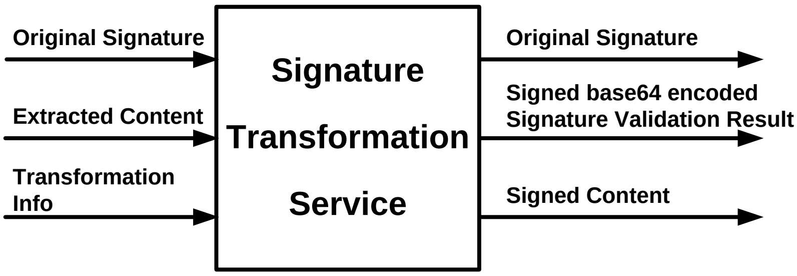

Figure 1: Signature Transformation Service

Summarizing, the signature transformation service has to interpret and verify the original signature and converts its contents according to the target signature's rules. The following three signature transformations are possible and provided by the signature transformation service:

- Transformation of CMS signatures to XML/XAdES signatures
- Transformation of XML/XAdES signatures to CMS signatures
- Transformation of XML/XAdES signatures to other types of XML/XAdES signatures

5. Architecture

5.1. Signature Transformation Service

Figure 2 shows a rough architecture of the signature transformation service. The signature transformation service is a SOAP/WSDL web-service using an appropriate request/response protocol for message exchange. A client calling the signature transformation service has to provide the service with the original signature, the content to sign which must be extracted before and additional information on how the signature transformation service should handle the internal processing. The signature transformation service itself invokes the signature creation and validation service for processing the signature transformations. The resulting output - containing the original signature, the signed result of the signature verification and the newly signed content - is sent back to the calling client. In case of an error during the transformation process an error response is generated which contains a special error code and a textual description of the occurred error.

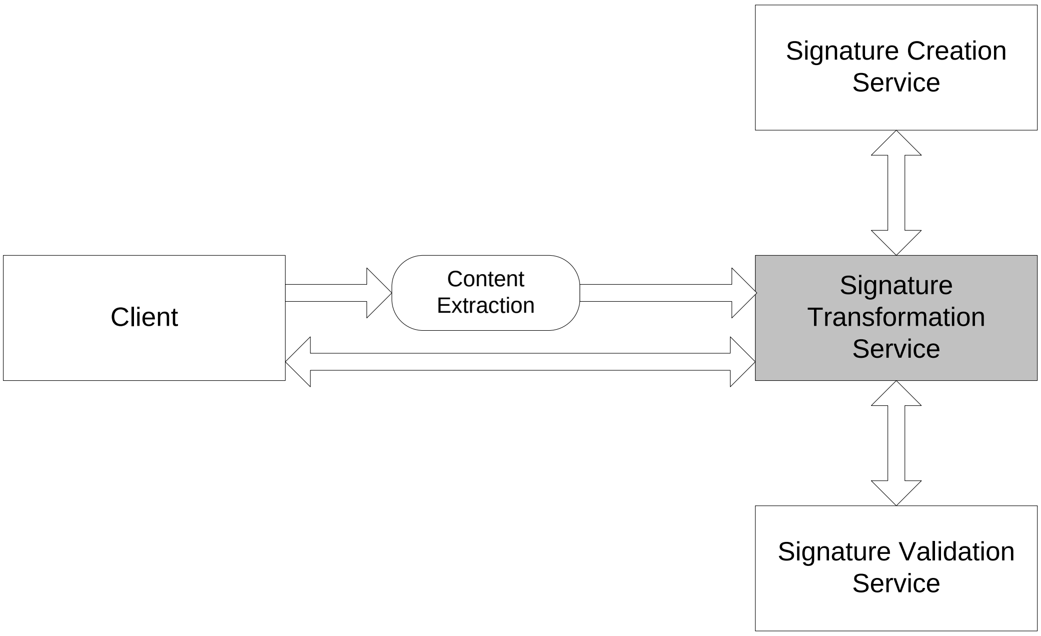
Signature Creation Service
Client
Content Extraction
Signature Transformation Service
Signature Validation Service

Figure 2: Architecture of the Signature Transformation Service

The transformation process consists of following steps (depending on the signature format to apply):

- Validation of the original signature
  Depending on the provided signature type, the original signature is verified accordingly. For this action, the signature validation service is invoked. The signature transformation service assembles a verification request message and sends it to the signature validation service (see section 5.2 for details).
- Creation of a signature over the verification result
  Assuring the calling client the integrity and non-repudiation of the original signature's verification result, the signature transformation service signs the result received from the signature validation service. Before signing, the result is base64 encoded. For signing processes, the signature transformation service invokes the signature creation service which is particular designed for the generation of digital signatures (see also section 5.2 for details).
- Creation of a new signature over the extracted content
  The transformation to a new signature format is achieved by signing the extracted content in the designated format. Again, the signature creation service is called for this operation.

According the specification of the signature creation and validation service, the following signature formats are supported by the signature transformation service:

- XMLDSIG signatures
- XAdES-BES signatures
- XAdES-T signatures
- XAdES-C signatures
- XAdES-X signatures
- CMS signatures

For signature verification within the transformation process, all above mentioned XAdES formats are supported. For signature creation only XAdES-BES and XAdES-T are available.

5.1.1 Architectural Details

The signature transformation service is based on web technologies and is used to convert different electronic signatures. The interface supports three types of transformations, the transformation of CMS signatures into XML compliant signatures and vice versa as well as the conversion of different XML/XAdES signatures into other types of XML/XAdES signatures. All transformation operations build upon request/response messages received and issued by the signature transformation service. For each kind of transformation separate messages are defined. In the following, details to these messages are listed.

CMS to XML/XAdES transformation

The TransformCMSToXadesRequest message contains:

- The CMS signature to transform in base64-encoded form
- The content to sign either encoded in XML or base64.
- An ID for selection of trustable root certificates for signature verification
- The type of the signature to be newly created
- An ID identifying a group of keys used for selecting a signature key

The TransformCMSToXadesResponse message contains:

- The original CMS signature value as stated in the request
- The XML signed result of the CMS signature verification
- The XML signed content
- An error response if any error has occurred during computation

XML/XAdES to CMS transformation

The TransformXadesToCMSRequest message contains:

- The XML signature to transform
- The data to be CMS signed
- An ID for selecting the appropriate certificates for signature verification
- Information on supplementary objects if used in the XML signature
- An ID representing a group of keys for CMS signing

The TransformXadesToCMSResponse message contains:

- The original XML signature as in the transformation request
- The CMS signed result of the XML/XAdES signature verification
- The CMS signed content
- An error response if any error has occurred during computation

XML/XAdES to XML/XAdES transformation

Since the structure of the request and response messages (TransformXadesToXadesRequest and TransformXadesToXadesResponse) is similar to the other two types of transformation possibilities, we skip a detailed analysis of these messages.

5.2. Signature Creation and Validation Service (SCVS)

The signature creation and validation service is based on modules of an Austrian eGovernment open source program and extends these basic modules by XAdES capabilities and CMS signature creation. The Austrian module is named MOA-SPSS and is specified in [10] and [11]. The combination of these specifications describes the overall module. The extensions to this module are based on well-established standards like CMS and XMLDSIG signatures. Furthermore, XAdES signatures and the XAdES profile for eGovernment according to [12] are used. The service is implemented as SOAP/WSDL web-service. The functionality of the extended service includes the creation and validation of CMS, XMLDSIG and XAdES signatures.

For the following description, the SCVS module is split into a signature validation and signature creation module. The sections comprise a short interface description of the SCVS module. The interface used by an application to access functions of the signature creation and validation module is described. The protocol consists of simple request/response messages. The application sends a request coded in XML to the web-service. The latter returns a corresponding XML-coded response to the application.

5.2.1. Signature Validation

The signature validation module comprises following requests and responses (see *Figure 3*):

- VerifyXMLSignatureRequest – VerifyXMLSignatureResponse
    - Used for validation of XMLDSIG, XAdES-BES, XAdES-T, XAdES-C and XAdES-X signatures
- VerifyCMSSignatureRequest – VerifyCMSSignatureResponse
    - Used for validation of CMS signatures

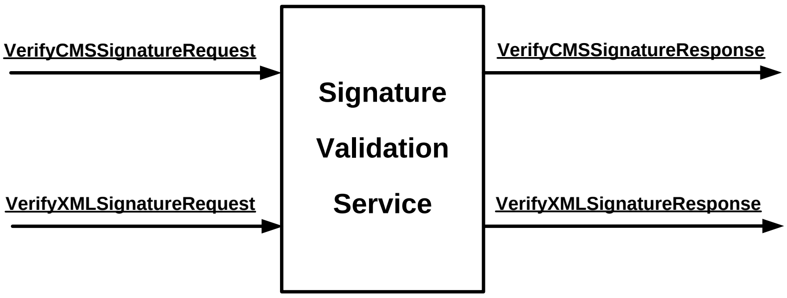
VerifyCMSSignatureRequest
VerifyCMSSignatureResponse
Signature
Validation
Service
VerifyXMLSignatureRequest
VerifyXMLSignatureResponse

Figure 3: Interface Signature Validation Service

XML Signature Validation

The XML signature validation is used to validate XMLDSIG signatures according to [2] and XAdES-BES, XAdES-T, XAdES-C, XAdES-X signatures according to [4]. The validation of an XMLDSIG signature comprises the following tasks:

- Core validation (reference and signature validation)
- Validation of the signing certificate.

The validation of XAdES signatures executes several validation steps depending on the type of the XAdES signature. *Table 2* lists the XAdES properties which will be validated for each signature type. Furthermore, the last column states which signature will be generated (generating means adding the appropriate ETSI properties) if the previous signature validation was successful.

Table 2: Validation Tasks

Signature	Checks	Generator
XMLDSIG	Core validation Certificate validation	-
XAdES-BES	+ SigningTime check + SigningCertificate check + DataObjectFormat check	XAdES-T[3]
XAdES-T	+ SignatureTimeStamp check	XAdES-X[3]
XAdES-C	+ CompleteCertificateRefs check + CompleteRevocationRefs check + AttributeCertificateRefs check + AttributeRevocationRefs check	XAdES-X[3]
XAdES-X	+ SigAndRefsTimeStamp check + RefsOnlyTimeStamp check	XAdES-X[3]

CMS Signature Validation

The signature validation service is able to validate CMS signatures according to [1].

5.2.2. Signature Creation

For the signature creation module the following requests and responses are defined (see *Figure 4*):

- CreateXMLSignatureRequest – CreateXMLSignatureResponse
  - Used for creation of XMLDSIG, XAdES-BES and XAdES-T signatures
- CreateCMSSignatureRequest – CreateCMSSignatureResponse
  - Used for creation of CMS signatures

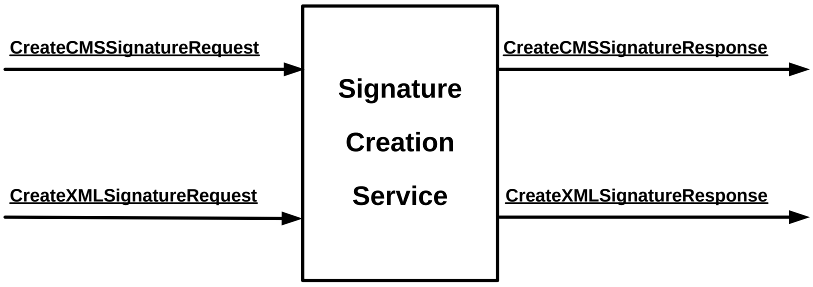
CreateCMSSignatureRequest
CreateCMSSignatureResponse
Signature
Creation
Service
CreateXMLSignatureRequest
CreateXMLSignatureResponse

Figure 4: Interface Signature Creation Service

XML Signature Creation

The signature creation module supports the creation of XMLDSIG signatures according to [2] and following XAdES signatures according to [4]:

- XAdES-BES
- XAdES-T

Furthermore, creating these XAdES signatures is based on the XAdES profile for eGovernment

[3] Generating these signatures is based on the XAdES profile for eGovernment according to [12].

according to [12].

CMS Signature Creation

The signature creation module supports the creation of CMS signatures according to [1].

6. Conclusions and Future Work

Electronic documents offer practicable means to easily distribute information electronically. Assuring authenticity and integrity, electronic documents can be signed by using digital signatures. Currently, several different digital signature formats exist.

Within the European eGovernment domain, not every Member State has implemented or is using the same signature format for official documents. Thus issues exist in exchanging electronic documents across borders. Some cross-border eGovernment channels cannot be processed automatically since any alteration on the documents' contents invalidates the signature. For these cases, a secure transformation of signature formats is needed.

In our work we have specified and developed a concept for a web-service that is capable of converting different signature formats. By using this service it is possible to transform CMS based signatures into XML/XAdES signatures and vice versa as well as to convert XML signatures into other types of XML signatures. For evaluation, this service has been implemented as SOAP/WSDL web-service.

As part of this implementation we have tested and evaluated different signature formats with variable content. For testing real documents, an official birth certificate issued by an Austrian public authority has been used. Such a certificate is structured in XML and its signature has been transformed into CMS format. Adopting the signature transformation service in the cross-border eGovernment context, automatic processing of signed documents using different signature formats becomes possible.

To guarantee confidentiality and integrity, the signature transformation service should be operated by an official eNotary service such as cyberDOC [16]. Furthermore the liability should be assumed by the eNotary service.

To improve our service, we have planned some future activities. Currently, a client needs to extract the signed content before using the signature transformation service. Thus we intend to add the content extraction directly to the transformation service. Additionally, the support of advanced CMS signatures (CAdES) is a further step in enhancing the service.

7. References

[1] Housley, RFC3852, *Cryptographic Message Syntax (CMS)*, http://www.ietf.org/rfc/rfc3852.txt, 2004
[2] W3C Recommendation: *XML-Signature Syntax and Processing (Second Edition)*, http://www.w3.org/TR/xmldsig- core/, 2008.
[3] ETSI TS 101 733, *Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)*, V1.7.4, 2008
[4] ETSI TS 101 903, *XML Advanced Electronic Signatures (XAdES)*, V1.3.2, 2006
[5] Callas, Donnerhacke, Finney and Thayer, RFC2440, *OpenPGP Message Format*, http://www.ietf.org/rfc/rfc2440.txt, 1998

[6] Elkins, Del Torto, Levien and Roessler, *RFC3156, MIME Security with OpenPGP*, http://www.ietf.org/rfc/rfc3156.txt, 2001

[7] IDABC Study – *Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications*, November 2007

[8] *TransiDoc* Website, http://www.transidoc.de/, 2008

[9] Fischer–Dieskau, Kunz, Schmidt and Viebeg, *Grundkonzepte rechtssicherer Transformation signierter Dokumente*, Workshop "Qualifizierte elektronische Signaturen in Theorie und Praxis" (QSIG2005) at the Conference Sicherheit 2005, 2. Jahrestagung des Fachbereichs Sicherheit der GI, University of Regensburg, 5. - 8. April 2005. In: Conference volume of "Sicherheit 2005", GI-Edition, Lecture Notes in Informatics (LNI), Vol. P-62, p. 401-412. (german), http://www.transidoc.de/website-transidoc/publications/Transidoc_QSIG2005.pdf

[10] *MOA-SS/SP Specification*, Version 1.3.0, 24.08.2005

[11] *The Austrian Citizen Card*, Overview of Version 1.2.0, 14 May 2004, http://www.buergerkarte.at/konzept/securitylayer/spezifikation/20040514/Index.en.html

[12] European Telecommunications Standards Institute: ETSI TS 102904: Electronic Signatures and Infrastructures; *Profiles of XML Advanced Electronic Signatures based on TS 101 903 (XAdES)*, v1.1.1. Technical Specification, February 2007

[13] EU Project *eGov-Bus*, http://www.egov-bus.org

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

[15] European Parliament and Council, *Directive 2006/123/EC on services in the internal market*, 12.12.2006

[16] *cyberDOC* – The Electronic Document Archive of Austrian Civil Law Notaries, http://www.notar.at/de/portal/einrichtungen/cyberdoc/