A Prototype System for Electronic Data Interchange among Registrar's Offices of Different States

Igor Metz[1], Adrian Blöchlinger[2], and Alexandros Varveris[3]

[1] GLUE Software Engineering AG, Zieglerstrasse 34, CH-3007 Bern, Switzerland
[2] Federal Office of Justice, Bundesrain 20, CH-3003 Bern, Switzerland
[3] University of Athens, Asklipiou 9 Street, 10679 Athens, Greece

Abstract. This work presents a prototype system that enables electronic integration of civil status records of the International Commission on Civil Status (ICCS) member states; the pursued issues are involving civil status matters for citizens of member states through their respective Registrars' Offices organization. Phase 1 of the prototype system is presented together with the technical feasibility securely to exchange messages among civil status offices as well as to assure message integrity, authenticity, confidentiality and non-repudiation.

Keywords: Civil Status, ICCS, CIEC, Electronic Data Interchange, Registrars' Office, e-government, e-participation, Civil Status certificates.

1 Introduction

Governmental initiatives on electronic information require a high-level set of standards in order to cover a large spectrum of services. It is also necessary to produce design parameters that will ensure data security, privacy, reduction of paperwork and free data access [1, 2].

Currently, messages between civil status offices have been exchanged on front and a back side paper forms, where the front side holds the labeled fields written in several languages, usually in the language of the sending country and in French, the latter being the official diplomatic language. The fields are numbered on the front of the message, having the translations and some explanatory articles of conventions [3] on the back side in order to facilitate the reader. Such a form is referred to as "formule plurilingue" by the International Commission on Civil Status (ICCS or Commission Internationale de l'État Civil) [4], an intergovernmental organization since 1948, aspiring the promotion of international cooperation on civil status matters while improving national authorities collaboration on the subject. The Commission concluded to address the arising needs with a computer system designed for the exchange of information on civil status matters in the various ICCS member countries and to resolve the resulting problems.

To date, each of the participating countries has designed individual forms. These forms differ in the language used on the front page, whereas some may include supplementary fields. Currently, the ICCS is working on a system of label codes, which allows searching the individual translations of a label within a multilingual dictionary

A.B. Sideridis and Ch. Z. Patrikakis (Eds.): e-Democracy 2009, LNICST 26, pp. 270–278, 2010.

which will render the translations on the back side useless. Also, it endeavours to limit the language of the system to French in addition to the language used by the sender.

In the present work, the term 'civil status' contains all the attributes assigned to an individual in accordance to civil law, namely citizenship, marriage, paternity, relations, name, residence, legal endowment, and sex. Consequently, the term 'civil status' includes the administrative mechanism for registering authentic personal records. Additionally, ICCS aims at establishing a platform for a world-wide secure electronic interchange of civil status messages in-between participating civil status offices. The following figure shows an overview of the final target architecture of the ICCS platform (Fig. 1).

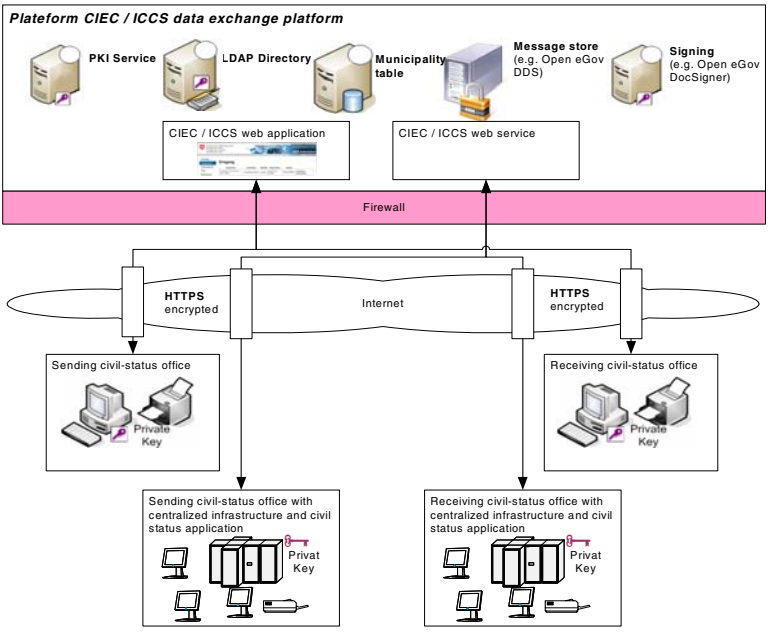


Fig. 1. Overview of the ICCS Platform Target Architecture

The proposed platform is planned to be realised in several phases which are:

Phase 1: A prototype [5], supporting Death and Free Text messages. The goal of this phase is to display the secure electronic interchange of messages, giving a special attention to the feature of authentication of users using digital certificates, and the signing and en-/decrypting of messages.

Phase 2: Introduction of the LDAP (Lightweight Directory Access Protocol) directory [6], municipality table, PKI (Public Key Infrastructure) [7]. Also, support of three to five additional ICCS forms and one or two additional languages.

Phase 3: Introduction of an online registration process and application. Also, support of five to seven additional ICCS forms and three or four additional languages.

Phase 4: Support of remaining ICCS forms and languages, optimisations, and transfer to operational environment.

This paper intends briefly to describe the system as already built in the context Phase 1. It employs a service-oriented architecture and emphasises on the reuse of pre-existing components provided by the Swiss Federal Administration [8].

2 Overview

Figure 2 presents an overall view of the ICCS Phase 1 platform. As envisaged, the final platform will be using a centralized architecture, where all the messages are exchanged via one central hub system, supported only by human users. In regard to the civil status applications worldwide, these will be integrated in later phases.

The ICCS platform is designed to be secure. Message authenticity, integrity, confidentiality and non-repudiation are technically enabled by the signing and encrypting all messages. However, the quality of the used certificates is crucial, and only certificates with sufficient quality can guarantee the above security requirements.

The ICCS Phase 1 platform uses its private OpenSSL installation to create the necessary public/private key pairs and certificates [9]. This is considered sufficient for the purpose of a prototype. For the succeeding phases a fully fledged PKI is foreseen.

The said system can be accessed by authorised users through personal digital certificates. The ICCS platform, in particular the ICCS web application, has to support all languages of the participating countries, and it is possible to extend the platform for additional languages just by providing the relevant textual resources.

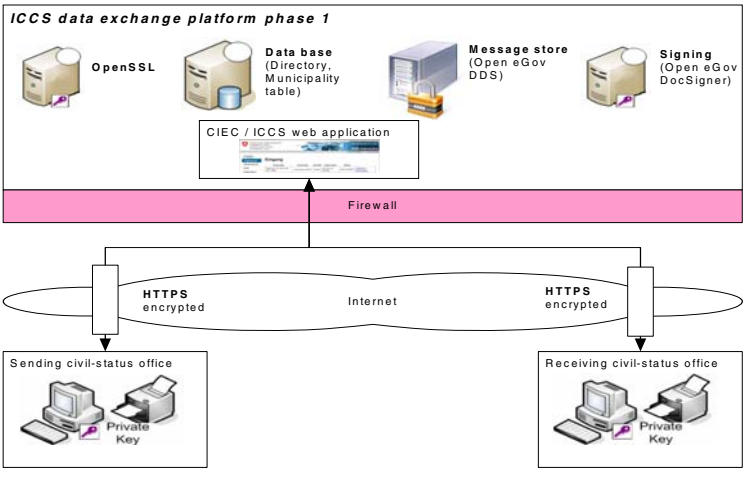


Fig. 2. Overview of the ICCS Phase1 platform

3 System Architecture

This section gives a more detailed view of the building part of the system architecture of the ICCS Phase 1 platform. Some of the components have been built to provide a minimal functionality as needed for this phase, while others are already fully functional. The components of the systems are based in Java enterprise applications, which run in a Java EE container.

The *ICCS Web Application*: This provides the user interface for human platform users, which are the clerks of the civil status offices. It is accessed via HTTPS using mutual authentication, i.e. both the server and the client are identified using digital certificates. For this purpose, the user certificates are stored on the server-side.

The *ICCS Core*: This contains the business logic of the ICCS platform. The core functionality has been isolated in a separate component in order to allow an easy integration with an ICCS Web Service in later phases.

The *Database:* The ICCS Phase 1 platform uses a central database for the following purposes:

- Storing user and office information as well as the certificates. Here, the users and offices are organised in the form of a tree having the following structure: ICCS/<country>/<office>/<user>, where the ICCS is the root node (Fig. 3). It has a sub-node for each participating country, the country nodes containing office nodes, which in turn contain the user nodes.
- Storing of process cards, inbox, sent and read box per office.
- Storing of the ICCS label codes and the label texts in all necessary languages. In Phase 1 we support four languages, namely, English, French, German, and Greek.
- Access to the database is always performed through abstract interfaces.
- The interface IDirectory provides the look-up interface for user and office certificates, in addition contact information, such as e-mail addresses of users and offices, etc.
- The interface IMunicipality provides the look-up interfaces for the civil status offices and the type of messages an office may send or receive. In Phase 1 this is simply another interface to the directory.
- The interface IFormTexts provides the label codes and the texts used within the PDF message documents in the necessary languages.

The *Document Delivery Service (DDS), Message Store*: This is used to store the messages in a secure manner. All messages are encrypted and may be decrypted and read only by the intended recipient. The DDS provides interfaces to supply and deliver messages and to notify the ICCS Core about any events concerning the stored messages (download, expiration, deletion).

Finally, the DDS notifies the recipient civil status office by e-mail, if there are new messages to be downloaded.

DDS is a generic service of the Open eGov platform [10] and is available as an open source component under GPL (General Public License).

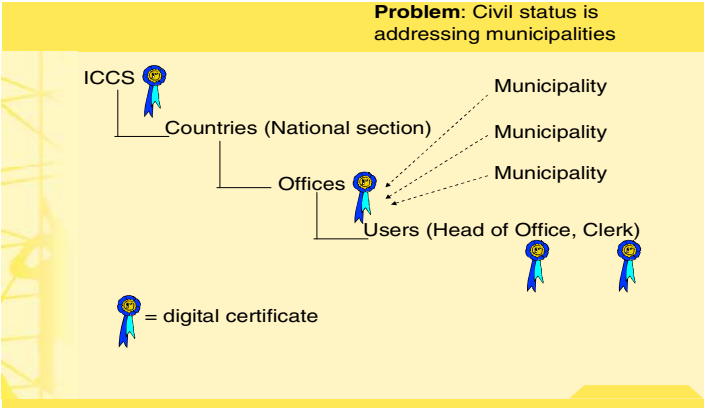


Fig. 3. Organisational structure of the ICCS Platform

The *Doc Signer*: This component provides the functionality to sign the PDF messages locally. For this purpose, a signed Java applet is downloaded to the clerk's local browser. The applet loads the document to be signed by the ICCS Web Application server to the local machine, searches the clerks to locally install the certificate and performs the signing process, including the query for the clerk's certificate PIN (Personal Identification Number).

The Doc Signer [11] is a generic component of the Open eGov platform. It is available as an open source component under GPL.

The *Content Management System (CMS)*: The ICCS Web Application is using a CMS from where all static pages, labels, texts, images, etc. are retrieved. In Phase 1 this integration has been kept very simple.

The *Application Container*: The Glassfish [12] open source application server is used as the runtime environment for the platform**.**

The *OpenSSL Public Key Infrastructure (PKI)*: The ICCS platform is using certificates for user and office authentication and authorisation, as well as for message encryption and message signing. The certificates are issued by a dedicated PKI. In Phase 1 this PKI is realised using an OpenSSL installation on the platform.

The ICCS platform uses PKCS#11 (Public Key Cryptography Standards) [13] hard and PKCS#12 [14] soft certificates for its purposes. Soft certificates are issued by the ICCS (ICCS Certification Authority)

Each clerk has a personal certificate for authentication. This can be a soft certificate provided by the ICCS CA (Certification Authority) or an already existing hard certificate, which is accepted by the ICCS platform.

Each participating civil status office has a soft certificate for addressing.

The ICCS platform itself uses a soft certificate to sign the messages in the XML (Extensible Markup Language) form.

4 Message Structure and Signing

Messages, whose, authenticity and integrity is ensured through several signatures, are transmitted as zip files. Fig. 4 shows the structure of such a zip file and how it is assembled.

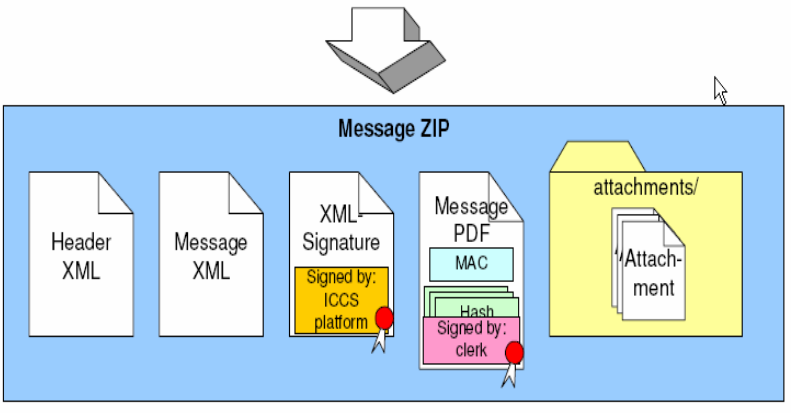
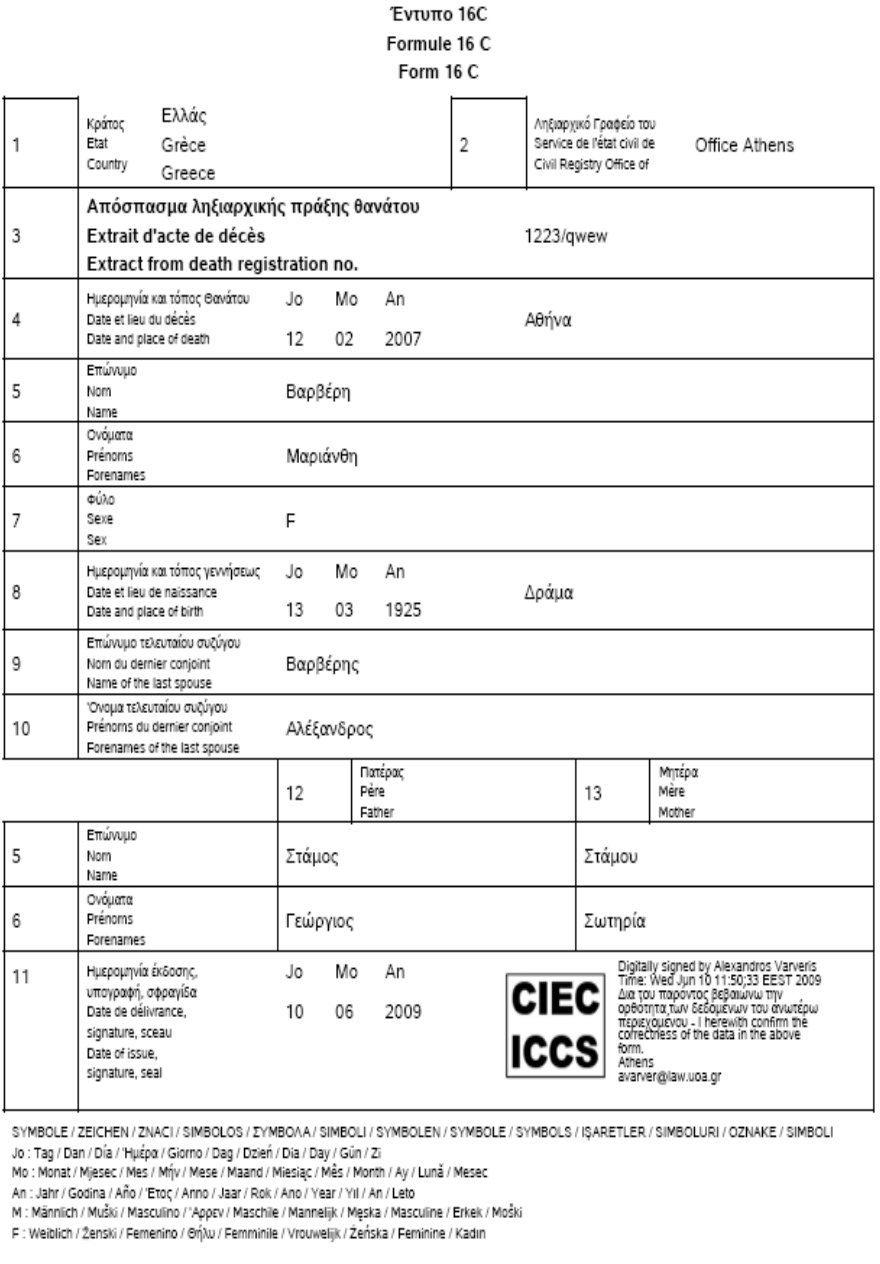


Fig. 4. ZIP Message structure

The base of a message is an XML document containing all the business case specific data entered by the clerk during data capturing (e.g. Fig. 5). Additionally, the clerk may also provide a set of attachment documents. The list of attachments and an optional comment per attachment is also part of the XML document.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns3:form16C xmlns="http://www.ciec1.org/xmlns/iccs-base/1" xmlns:ns2="http://ww
   <ns3:country iccs-code="2-1-1">CH</ns3:country>
   <ns3:civilRegistryOffice iccs-code="1-1-6">Zivilstandsamt des Kreises Bern</
   <ns3:deathRegistrationNo iccs-code="1-3-5-1">12345-abc</ns3:deathRegistratic
   <ns3:dateOfDeath iccs-code="9-9">2009-03-02+01:00</ns3:dateOfDeath>
   <ns3:placeOfDeath iccs-code="2-6">Bern</ns3:placeOfDeath>
   <ns3:surnameOfDeceased iccs-code="7-6">Onassis - Ωνάσης</ns3:surnameOfDeceas
   <ns3:forenamesOfDeceased iccs-code="8-6">František</ns3:forenamesOfDeceased>
   <ns3:sex iccs-code="3-4">M</ns3:sex>
   <ns3:dateOfBirth iccs-code="9-7">1919-04-23+01:00</ns3:dateOfBirth>
   <ns3:placeOfBirth iccs-code="2-4">Athens - Αθήνα</ns3:placeOfBirth>
```

Fig. 5. XML Message structure



Έντυπο 16C
Formule 16 C
Form 16 C

1	Κράτος Etat Country	Ελλάς Grèce Greece	2	Ληξιαρχικό Γραφείο του Service de l'état civil de Civil Registry Office of	Office Athens
3	**Απόσπασμα ληξιαρχικής πράξης θανάτου** **Extrait d'acte de décès** **Extract from death registration no.**			1223/qwew	
4	Ημερομηνία και τόπος θανάτου Date et lieu du décès Date and place of death	Jo Mo An 12 02 2007		Αθήνα	
5	Επώνυμο Nom Name	Βαρβέρη			
6	Ονόματα Prénoms Forenames	Μαριάνθη			
7	Φύλο Sexe Sex	F			
8	Ημερομηνία και τόπος γεννήσεως Date et lieu de naissance Date and place of birth	Jo Mo An 13 03 1925		Δράμα	
9	Επώνυμο τελευταίου συζύγου Nom du dernier conjoint Name of the last spouse	Βαρβέρης			
10	Όνομα τελευταίου συζύγου Prénoms du dernier conjoint Forenames of the last spouse	Αλέξανδρος			
		12 Πατέρας Père Father		13 Μητέρα Mère Mother	
5	Επώνυμο Nom Name	Στάμος		Στάμου	
6	Ονόματα Prénoms Forenames	Γεώργιος		Σωτηρία	
11	Ημερομηνία έκδοσης, υπογραφή, σφραγίδα Date de délivrance, signature, sceau Date of issue, signature, seal	Jo Mo An 10 06 2009	CIEC ICCS	Digitally signed by Alexandros Varveris Time: Wed Jun 10 11:50:33 EEST 2009 Δια του παρόντος βεβαιώνω την ορθότητα των δεδομένων του ανωτέρω περιεχομένου - I herewith confirm the correctness of the data in the above form. Athens avarver@law.uoa.gr	

SYMBOLE / ZEICHEN / ZNACI / SIMBOLOS / ΣΥΜΒΟΛΑ / SIMBOLI / SYMBOLEN / SYMBOLE / SYMBOLS / IŞARETLER / SIMBOLURI / OZNAKE / SIMBOLI
Jo : Tag / Dan / Día / Ἡμέρα / Giorno / Dag / Dzień / Dia / Day / Gün / Zi
Mo : Monat / Mjesec / Mes / Μήν / Mese / Maand / Miesiąc / Mês / Month / Ay / Lună / Mesec
An : Jahr / Godina / Año / Ἔτος / Anno / Jaar / Rok / Ano / Year / Yıl / An / Leto
M : Männlich / Muški / Masculino / Ἄρρεν / Maschile / Mannelijk / Męska / Masculine / Erkek / Moški
F : Weiblich / Ženski / Femenino / Θήλυ / Femminile / Vrouwelijk / Żeńska / Feminine / Kadın

Fig. 6. A signed PDF Message

For transmission, the ICCS platform generates an individual platform XML signature [15] for the XML message document using the platform certificate, and also calculates an individual hash value for each of the attachments. As for the next step,

the platform transforms the original XML document, the platform signature value and the attachment hash values into an equivalent PDF document. This document is presented to the clerk for validation. Once accepted by the clerk, the PDF document is signed with the clerk's personal certificate (Fig. 6).

In such described way, the PDF document can always be traced to the original XML document and to the clerk, who sent the message.

The XML document, the platform signature, the signed PDF document and the attachment documents are packed into a ZIP file. The attachments and their respective signatures are put into a subfolder named "attachments".

Finally, an XML header document is added. This document contains the following transport information:

Sender Id: ICCS participant identifier of the sending office.

Recipient Id: ICCS participant identifier of the recipient office.

Message type: The business case type, i.e. 1603 for death message, or 0 for free text.

Message identifier: ICCS platform Referenced message identifier for replies only.

Date of sending.

Unique identifier of the message (UUID).

Subject: e.g. the business case type and some kind of case id, such as the name of the person involved.

The header document is not signed; however, it is transmitted in an encrypted form, as the whole ZIP container is transmitted in an encrypted form.

5 Conclusion

The International Commission on Civil Status (ICCS) platform Phase 1 discussed above has successfully created a fully operational prototype system enabling electronic integration of civil status records in-between four member states. The next phases will include additional member states inporting supplementary civil status forms that will serve the community. The above mentioned work intends to provide easily accessible information and to lessen bureaucracy for the benefit of citizens.

Acknowledgment

The authors wish to express their appreciation to the Swiss Open eGov project team for their assistance.

References

1. Varveris, A.G.: Electronic data interchange among the Registrar's Offices of different countries. In: Proceedings of 2nd Conference entitled Electronic democracy - challenge of digital era, Scientific Council for the Information Society, Athens, pp. 191–204 (2006)

2. Varveris, A.G., Tsouca, Ch., Papatheodorou, Ch.: Electronic data interchange among the Registrar's Offices of different states: Technical standards and administrative consequences, Revue Hellenique de Droit International, Sakkoulas Editions, pp. 283–311 (2005)
3. Commission Internationale de l'Etat Civil (C.I.E.C.), http://web.lerelaisinternet.com/CIECSITE/ListeConventions.htm
4. International Commission on Civil Status (ICCS), http://www.ciec1.org/
5. CIEC Platforme - ICCS Platform Wiki, http://www.ciec-plateforme.org/wiki/display/platformpublic/Home
6. The OpenLDAP Project, http://www.openldap.org/
7. Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., Polk, W.: RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (2008), http://www.ietf.org/rfc/rfc5280.txt
8. Swiss Federal Administration, http://www.admin.ch/ch/index.en.html
9. The OpenSSL project, http://www.openssl.org/
10. The Open eGov Project, http://www.e-service.admin.ch/wiki/display/openegov/Home
11. Open eGov DocSignerService, http://www.e-service.admin.ch/wiki/display/suispublic/Open+eGov+DocSignerService
12. The GlassFish Community open source software, https://glassfish.dev.java.net/
13. RSA Laboratories Inc., PKCS #11 v2.20 Amendment 3 Revision 1 Additional PKCS#11 Mechanisms (2007), ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-11/v2-20/pkcs-11v2-20a3.pdf
14. RSA Laboratories Inc., PKCS 12 v1.0: Personal Information Exchange Syntax (1999), ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-12/pkcs-12v1.pdf
15. XML Signature Syntax and Processing (Second Edition) (2008), http://www.w3.org/TR/xmldsig-core/