Certificate Policy Tool for Automated Cross-Certification

Athena Bourka[1], Despina Polemi[2], Dimitris Koutsouris[1]

[1] Department of Electrical and Computer Engineering
National Technical University of Athens (NTUA), 15773 Athens, Greece
Email: {abourka, dkoutsou}@biomed.ntua.gr
[2] EXPERTNET SA
244 Kifissias Ave. & 1 Achilleos Str, 15231, Athens, Greece
Email: despina.polemi@expertnet.net.gr

Abstract. One of the main PKI problems is currently the lack of interoperability at international level, which is greatly dependent on the automation of the cross-certification procedure using Certificate Policies (CP). This paper addresses the above-mentioned need by presenting an XML-based tool for the automated development and comparison of CPs, with main emphasis on healthcare environments. The CP tool is developed in JAVA and is characterized as flexible, standards-based and extendable, since all data representation is in XML. The implementation follows a prototype CP content standardization for healthcare using RFC2527 Standard, whereas the CP comparison algorithm is based on a multi-criteria decision support system. The final aim of the CP tool is to serve as a baseline for an on-line automated cross-certification service, thus enhancing PKI co-operation and interconnection for several business sectors.

1 Introduction

Over the last years, *Public Key Infrastructures (PKI)* based on *Trusted Third Parties (TTPs)* [10, 16] have been qualified as an appropriate framework for the provision of cryptographic security services (like data encryption, digital signature, time-stamping, etc) in several business sectors. These services are essential for the data confidentiality, integrity, availability and non-repudiation, which form the basic requirements for reliable electronic transactions [11].

Despite the broad PKI acceptance and deployment, there are currently open issues (technical and organizational) with regard to PKI interconnection and interoperability, especially at European and international level. A major PKI service for achieving interoperability is *cross-certification*, which is based on the mutual (one to one) acceptance and certification of *Certificate Authorities (CAs)*, independently of their position in the PKI hierarchy [6, 12].

However, there are still several problems in the technical implementation of cross-certification, mainly because of the inadequate standardization of the *Certificate Policies (CP)*, which form the basic comparison criteria for the mutual acceptance of CAs. A CP is actually a document describing the certificates' profile and the architectural structure of the underlying TTP and, thus, can be used as the main tool for compatibility assessment between different PKIs [5, 9].

Although the CP structure is defined in some of the existing standards [1, 5, 15], there is a significant gap in the *systemized development and assessment* of CPs both in general terms, as well as per specific business sector. This makes the *automated CP comparative analysis* a difficult task and obstructs the automation of the overall cross-certification procedure. This fact has serious impacts on the secure co-operation, information exchange and knowledge sharing in all business sectors and is even more increased due to the lack of the necessary legal/regulatory harmonization of the PKI operations at cross-national level [4, 8].

The current paper, addresses the above-mentioned problems, by presenting a tool for the systemization and automation of the CPs comparison in different PKIs. As an application domain for the work performed, we chose the healthcare sector, mainly due to its specific demands for attributes identification and roles' definition, as well as the multiple and different actors involved in the information exchange process. However, the results can easily be applied to several other domains, like e-commence and e-government, as long as a relevant CP content standardization procedure, as the one described in this paper, is followed.

The CP tool is based on a three-step development approach, including CP content standardization, decision support algorithms for CPs comparison, as well as XML representation formats [3]. The tool's development is in JAVA, using XML for data representation. Digital signature and encryption mechanisms are also embedded in the tool's functionality, in order to assure the confidentiality and integrity of CP private information.

The ultimate objective of the paper is to serve as a baseline for an on-line automated cross-certification service, thus enhancing PKI co-operation and interconnection for several business sectors.

The paper is organized as follows: Section 2 presents the methodology used for the development of the CP tool, whereas Section 3 describes its main use cases and functions. Section 4 presents the application design and S/W packages. Section 5 provides an overview of the main results, evaluates the work performed from a technical and business perspective, and draws the conclusions, as well as the open issues for further research.

2 Methodology for XML-Based Comparison of CPs

This Section describes the methodology for the CPs comparison, which was developed and implemented via the presented CP tool. As mentioned in the previous Section, the application domain for the work performed was healthcare, but the results can be extended in several other sectors as well.

More specifically, the basic methodological steps used for the CP tool development were the following [3]:

2.1 Step 1- CP Content Standardization

Following the RFC2527 structure [5], a list of possible content values (or content options) for each CP paragraph was defined. A distinction was made between general content values, which can be found in all CPs (independently of business sector) and healthcare specific content values, arising from dedicated requirements of the healthcare arena (since this was our specific application domain). These values can be used for a standardized development and assessment of CPs via decision support algorithms and XML, as mentioned in the next step.

2.2 Step 2 – Prototype CP Comparison Method

A specific method for CP comparison was developed, which lies on the mathematical area of *multi-criteria decision-making algorithms* with scoring techniques [3]. Following this method, the main criteria for the compatibility of two CPs are the:

- *Weights* (w_i), assigned to each CP paragraph, indicating the paragraph's importance within the overall CP.
- *Scorings* (s_i), given to all possible values of each paragraph according to the CP content standardization described in step 1.

In this way, the final result of the CPs assessment is extracted as a *weighted average* of all CP paragraphs scorings.

This prototype method turns the overall complex CP comparison to a simple addition of integers, which can be implemented in a structured S/W application. An important element is that the comparison criteria (weights and scorings) are set by the comparing organization according to its specific certification strategy. This fact makes the method very flexible and extendable to different needs and requirements, like for example, need for role based certificates extensions in healthcare.

2.3 Step 3 – XML Representation of CPs

Following the above-mentioned CP content standardization and comparison method, two different XML document types were defined [3]:

Extended CP: This is an XML document, including all CP paragraphs, the weights and existing values (options) per paragraph, as well as the scorings for all paragraphs' values. In other words, this document is actually defining the organization's certificate profile and is setting the criteria (weights, scorings), against which other organizations can be compared and evaluated. Following its definition, the Extended CP should be considered as a private document, which can be used internally within the organization for the compatibility assessment of external CPs .

Basic CP: This is an XML document, including all CP paragraphs with the values (options) selected as their content. Therefore, the Basic CP is the organization's "public" Certificate Policy as defined by RFC2527 (without the weights and scorings), which can be sent, for comparison, to external organizations. The Basic CP can be extracted from the Extended CP if for each CP paragraph the weights are excluded and only the highest scorings are kept.

2.4 Step 4 – Automated CP Comparison

Following the three above methodological steps, Fig. 1 presents the XML-based CP comparison process, which was defined.

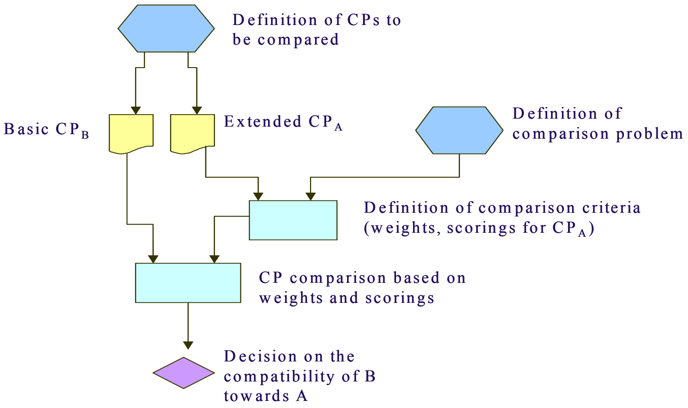
Definition of CPs to be compared
Basic CP_B
Extended CP_A
Definition of comparison problem
Definition of comparison criteria (weights, scorings for CP_A)
CP comparison based on weights and scorings
Decision on the compatibility of B towards A

Fig. 1. Flow chart for XML-based CP comparison

As shown in the Figure, given two organizations A and B (with Certificate Policies CP_A, CP_B respectively), the compatibility of B against A is assessed by evaluating the Basic CP_B against the Extended CP_A. The assessment is based on the criteria (weights, scorings) set by the comparing organization A, which are included in the Extended CP_A. When assessing A against B, the reverse procedure should be used, i.e. evaluation of the Basic CP_A against the Extended CP_B.

The overall methodology for XML-based CP comparison described in the Section, was implemented via the prototype CP tool, which, in this way, enables systemized CP development and automates the overall PKI cross-certification process.

3 CP Tool Use Cases and Functionality

This Section describes the main use cases and functionality of the CP tool, which implements the flow chart of Fig. 1 and automates the development and comparison of CPs. The CP tool was developed in JAVA, using XML as the only representation means of the (healthcare) CPs and their content. In this way, all the application's data are dynamically created from XML document formats, thus making the tool completely independent of the CP content standardization and enabling its further extension for different business sectors (besides healthcare).

As shown in the UML Use Case diagram of Fig. 2, the basic CP tool functions include:

- Development of a new Extended CP.
- Modification/View of an existing Extended CP.
- Extraction of Basic CP (in order to send it for comparison to other organizations).
- Comparison of different CPs.

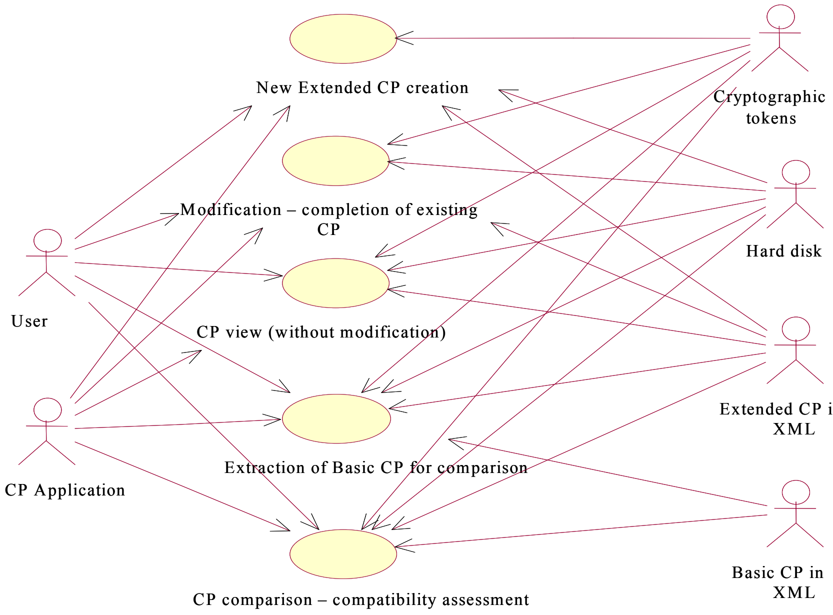
New Extended CP creation
Modification – completion of existing CP
CP view (without modification)
Extraction of Basic CP for comparison
CP comparison – compatibility assessment
User
CP Application
Cryptographic tokens
Hard disk
Extended CP in XML
Basic CP in XML

Fig. 2. Use cases of the CP application

It should be noted that the Extended CP, being private organizational information, must always be digitally signed and encrypted. This is the role of the "cryptographic tokens" actor in Fig. 2.

The next two paragraphs describe in more detail the CP development and comparison use cases of the CP tool.

3.1 Development of a New Extended CP

The development of a new Extended CP is divided in two parts: a) development of the CP document in XML, b) document evaluation, digital signature – encryption and storage on disk. The next two Figures present the UML sequence diagrams for the above processes.

As shown in Fig. 3, when the CP development process is initiated, a new XML document is created using the Extended CP format, as described in Section 2. After the CP title definition, the tool presents the overall CP structure to the user following RFC2527. Each time the user selects a specific CP paragraph, the CP tool automatically asks for the definition of this paragraph's weight. After the weight has been defined, the CP tool automatically presents all possible values (options), which can be used as content for the specific paragraph. The user must score all the values, in order to complete the session.

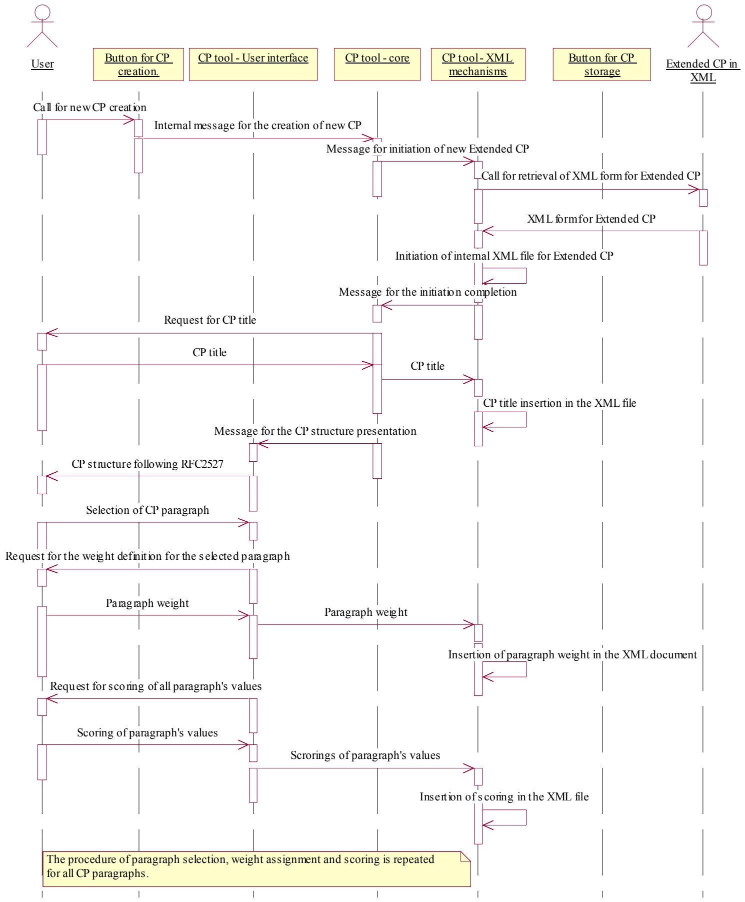
User
Button for CP creation
CP tool - User interface
CP tool - core
CP tool - XML mechanisms
Button for CP storage
Extended CP in XML
Call for new CP creation
Internal message for the creation of new CP
Message for initiation of new Extended CP
Call for retrieval of XML form for Extended CP
XML form for Extended CP
Initiation of internal XML file for Extended CP
Message for the initiation completion
Request for CP title
CP title
CP title
CP title insertion in the XML file
Message for the CP structure presentation
CP structure following RFC2527
Selection of CP paragraph
Request for the weight definition for the selected paragraph
Paragraph weight
Paragraph weight
Insertion of paragraph weight in the XML document
Request for scoring of all paragraph's values
Scoring of paragraph's values
Scrorings of paragraph's values
Insertion of scoring in the XML file
The procedure of paragraph selection, weight assignment and scoring is repeated for all CP paragraphs.

Fig. 3. UML sequence diagram for the development of a new CP

The above procedure is repeated for all the paragraphs of the CP and when it is completed, the CP tool automatically evaluates the completeness of the new created Extended CP document and initiates the digital signature and encryption process as shown in Fig. 4.

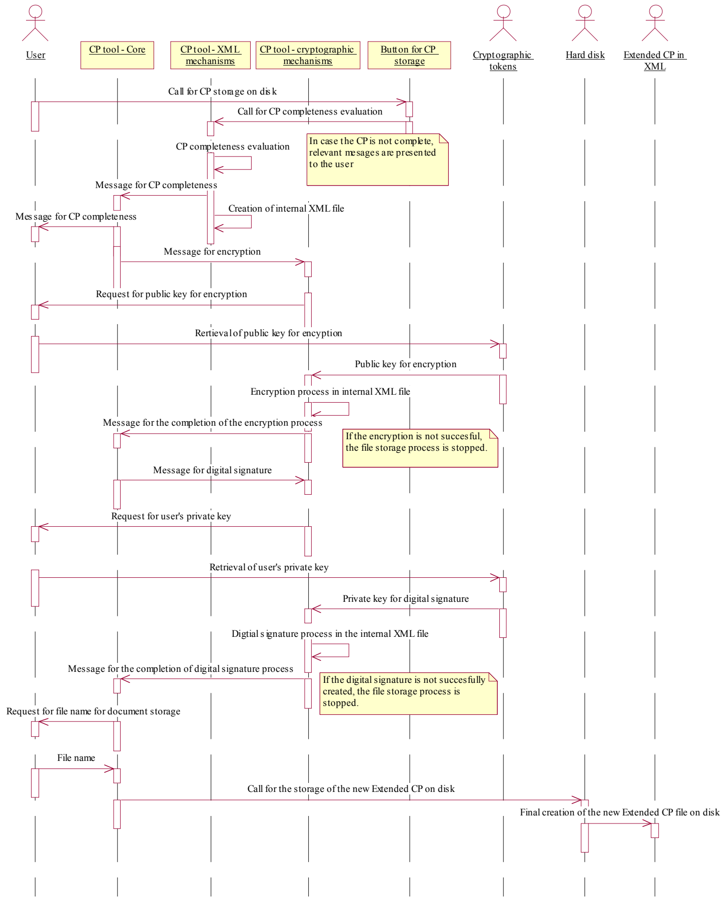
User
CP tool - Core
CP tool - XML mechanisms
CP tool - cryptographic mechanisms
Button for CP storage
Cryptographic tokens
Hard disk
Extended CP in XML
Call for CP storage on dis k
Call for CP completeness evaluation
CP completeness evaluation
In case the CP is not complete, relevant mesages are presented to the user
Message for CP completeness
Creation of internal XML file
Mes sage for CP completeness
Message for encryption
Request for public key for encryption
Rertieval of public key for encyption
Public key for encryption
Encryption process in internal XML file
Message for the completion of the encryption process
If the encryption is not succesful, the file storage process is stopped.
Message for digital signature
Request for user's private key
Retrieval of user's private key
Private key for digital signature
Digtial s ignature process in the internal XML file
Message for the completion of digital signature process
If the digital signature is not succesfully created, the file storage process is stopped.
Request for file name for document storage
File name
Call for the storage of the new Extended CP on disk
Final creation of the new Extended CP file on disk

Fig. 4. UML sequence diagram for the digital signature, encryption, evaluation and storage of a new CP

In the above Figure, the CP security mechanisms are performed at the XML level, with the W3C XML Digital Signature and Encryption Standards [7][17]. The algorithms used are RSA-SHA1 for Digital signature and RSA, Triple DES CBC for Encryption. In each case, the user must have at his/her possession the relevant cryptographic keys, which are available either on local keystores or on smart cards.

Automated CP Comparison.

The automated CP comparison is executed via the CP tool in two phases: a) Insertion of comparing organization's Extended CP and validation of the embedded cryptographic information (digital signature, decryption), b) Insertion of the external organization's Basic CP and comparison.

The second phase of the automated CP comparison is depicted in the UML sequence diagram of Fig. 5. As shown in the Figure, the Basic CP, which is under evaluation, is first inserted and then the comparison process starts using the methodology of Section 2. More specifically, the Basic CP is assessed against the Extended CP of the comparing organization, using criteria (weights, scorings) of the latter. When the assessment is completed, the CP tool presents the overall compatibility percentage of the CPs. The user is also able to see the assessment results per CP paragraph, by selecting specific paragraphs in the RFC2527 CP tree.

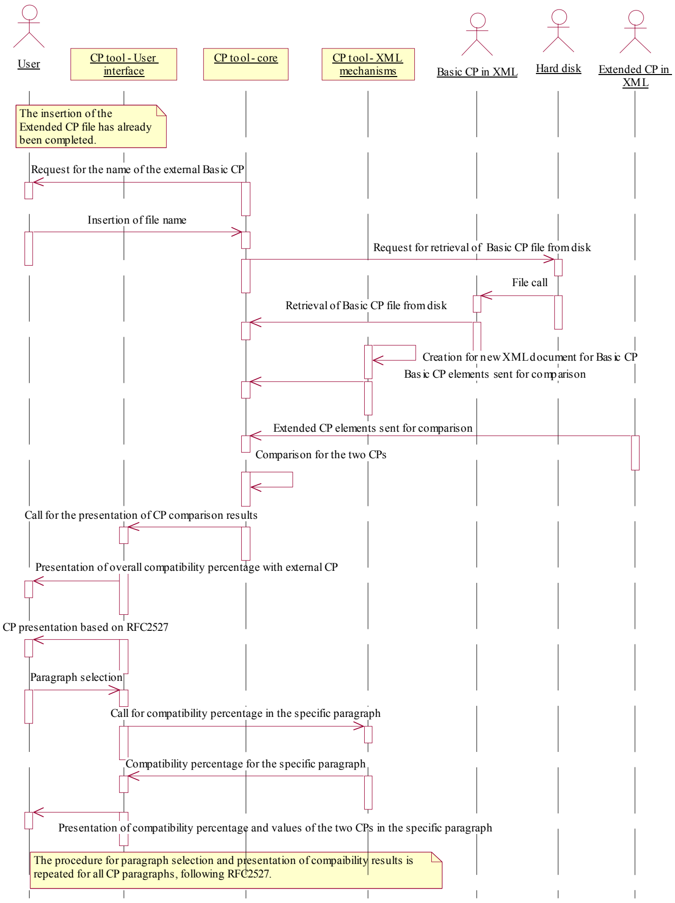
User
CP tool - User interface
CP tool - core
CP tool - XML mechanisms
Basic CP in XML
Hard disk
Extended CP in XML
The insertion of the Extended CP file has already been completed.
Request for the name of the external Basic CP
Insertion of file name
Request for retrieval of Basic CP file from disk
File call
Retrieval of Basic CP file from disk
Creation for new XML document for Basic CP
Basic CP elements sent for comparison
Extended CP elements sent for comparison
Comparison for the two CPs
Call for the presentation of CP comparison results
Presentation of overall compatibility percentage with external CP
CP presentation based on RFC2527
Paragraph selection
Call for compatibility percentage in the specific paragraph
Compatibility percentage for the specific paragraph
Presentation of compatibility percentage and values of the two CPs in the specific paragraph
The procedure for paragraph selection and presentation of compaibility results is repeated for all CP paragraphs, following RFC2527.

Fig. 5. UML sequence diagram for the automated comparison of two CPs

4 CP Tool Development and Implementation

With regard to the application structure, the main modules of the CP tool are shown in Fig. 6.

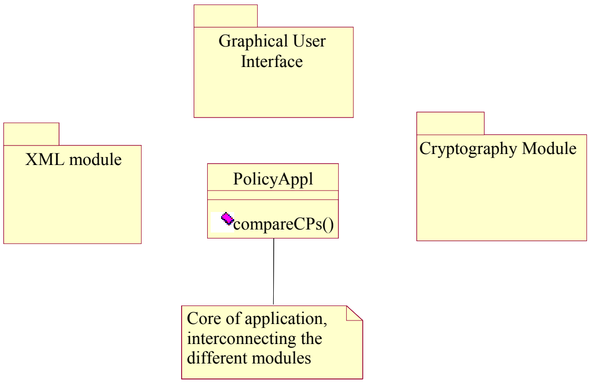

Fig. 6. Package diagram of the CP tool

The XML module is based on the Borland XML JAVA library [2], which enables the automated mapping between XML elements and JAVA objects, following the XML DTDs for Extended CP.

The Cryptography Module is implemented via the IBM XSS4J library using the SUN and IAIK Cryptographic Providers [13][14]. The next Figure shows the class diagram for this module.

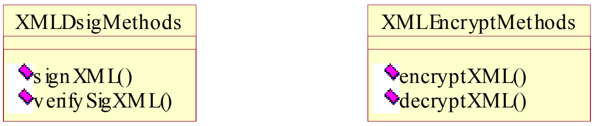

Fig. 7. Class diagram for the CP tool cryptographic module

The user interface module is designed using the Jbuilder 5 JAVA libraries (JDK 1.3) [2]. Last, the application's core (PolicyAppl) is responsible for connecting all the other packages and implementing basic functions, like the decision-making algorithm for CPs comparison.

he above-described CP tool simplifies the development and comparison of CPs, enabling in this way the automation of the overall cross-certification service.

5 Conclusions and Further Research

The paper presents a tool for the automated development and comparison of Certificate Policies, aiming at the automation of the overall cross-certification procedure in different PKIs. Although healthcare was chosen as an application domain, the tool can be used for automated CP comparison in several other domains, like e-commerce and e-government.

The CP tool is developed in JAVA using open technologies, whereas its design follows a certain methodology for CP compatibility assessment, addressing all the required intermediate steps for such an action (standardization, systemization, development and implementation).

In this respect, the main technical innovations of the work performed concern:

A) The methodology used for the CP development, which includes:

- CP content standardization, defining specific lists of values (options) per paragraph of the RFC 2527 Standard.
- The prototype CP comparison method, based on the dynamic assignment of weights and scorings for each CP paragraph.
- The XML formats for Extended and Basic Certificate Policies, which enable embedding of all the comparison criteria within the (XML) document of the CP.

B) The CP tool application itself, which aims at automating the cross-certification process. The technical particularities of the above application lie on the flexible, standards based, secure, open and extendable implementation via XML.

The above elements provide a possible solution on the automation of the CP comparison procedure that is currently the main barrier in the establishment of an automated cross-certification service at international level. Therefore, the basic business oriented benefits of the work described include:

- An extendable "model" for the development of Certificates Policies, based on specific and often dedicated needs and requirements in sectoral PKIs.
- A framework for comparison and compatibility assessment of different PKIs, following commonly accepted practices and standards.
- A basis for the implementation of a new service for automated cross-certification of TTPs for several sectors, like healthcare, e-government and e-commerce.

These results can greatly enhance the current paper-based and complex cross-certification procedure, simplifying the overall PKI interoperability and co-operation at international level.

Relevant open research fields that can be examined in the future include: embedding of functionality for the development of Certification Practice Statements (CPS), integration with broader Security Policy mechanisms (Vulnerability assessment, Risk assessment), as well as the provision of on-line cross-certification services (based on specified architectures).

It should be noted though, that besides the above-described technical dimension, there are still open issues at the PKI legal/regulatory level which need to be resolved, in order to provide a real interoperable and mutually accepted cross-certification service. In such an attempt, the involvement of international authorities and standards-development organizations is required, which can assure a broader acceptance of the results.

References

1. ASTM: Healthcare Certificate Policy. E31.20 Standard. ASTM (2000) Available at: http://www.cio.gov/fpkisc/healthcare, http://ncvhs.hhs.gov
2. BORLAND: JBUILDER 5 Documentation. BORLAND, Scotts Valey (2000) Available at: http://www.borland.com
3. Bourka A.: Advanced Public Key Infrastructure Services for Healthcare: Development of Secure Application for e-Healthcare Documents Communication – Implementation of Prototype Method for Automated Certificate Policies Compatibility Assessment. Ph.D. thesis. National Technical University of Athens, Athens (2002)
4. Bourka A., Polemi D., Koutsouris D.: An Overview in Healthcare Information Systems Security. *Proceedings MEDINFO Conference*, London (2001)
5. Chokhani S., Ford W.: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework. RFC 2527 Standard. IEFT (1999) Available at: http://www.ieft.org/rfc/rfc2527.txt
6. COSACC Project Consortium: The COSACC Solution for the Secure Interconnection of CoCs. Technical Deliverable D04.01. COSSAC (1999)
7. Eastlake D., Reagle J., Solo D.: XML-Signature Syntax and Processing. RFC 3075 Standard. IETF (2001) Available at: http://www.ietf.org/rfc/rfc3075.txt
8. European Commission: Directive 1999/93/EC of the European Parliament and of the Council of (13 Dec. 1999) on a Community framework for electronic signatures. Official Journal L 013 (2000) 12–20 Available at: http://europa.eu.int/ISPO/ecommerce/legal/digital.html
9. Federal PKI Task Force: Model Certificate Policy. Discussion Draft. USA Government Information Technology Services (1998) Available at: http://gits-sec.treas.gov
10. Ford W., Housley R., Polk W., Solo D.: Internet X.509 Public Key Infrastructure Certificate and CRL Profile. RFC 2459 Standard. IEFT (1999) Available at: http://www.ieft.org/rfc/ rfc2459.txt
11. France F.H.R., Gaunt P.N.: The Need for Security - a Clinical View. *International Journal of Bio-Medical Computing* 35 Suppl.1 (1994)
12. Government of Canada PKI: Cross Certification Methodology and Criteria. Technical Document. Government of Canada, Ottawa (2001) Available at: http://www.cio-dpi.gc.ca/pki-icp/crosscert/methodology/method00_e.asp
13. Graz Technical University: IAIK JCE 3.0. Graz (2003)
14. IBM: XML Security Suite. IBM, New York (2002) Available at: http://www.alphaworks.ibm.com
15. ISO: Healthcare Informatics – Public Key Infrastructure, Technical Specification ISO/DTS 17090 Parts 1-3. ISO TC 215/WG4 (2001)
16. ITU-T/ISO: Information Processing Systems – Open Systems Interconnection – Basic Reference Model Part 2: Security Architecture. ITU-T Rec X.800 | ISO/IEC 7498-2 (1989)
17. W3C: XML Encryption Syntax and Processing. Candidate Recommendation. W3C (2002) Available at: http://www.w3.org/TR/xmlenc-core/