Towards concrete application of electronic signature

Diana Berbecaru, Antonio Lioy, Fabio Maino, Daniele Mazzocchi, Gianluca Ramunno
Dip. Di Automatica e Informatica, Politecnico di Torino
Corso Duca degli Abruzzi 24, 10129 Torino, Italy
{ berbecar, lioy, maino, mazzocchi, ramunno }@polito.it

Abstract

Even though the theory behind digital signatures is fully understood and the related cryptographic methods have proved the efficiency in deploying security services, concrete application of digital signature to real electronic documents is still hindered by the lack of standards.
In particular, we lack standards for the format of the data to be signed, the format of the signature itself and the format of the electronic documents. This has led to the appearance of proprietary solutions and incompatible ad-hoc software applications, with dramatic effects on deployment in real business environments. Several ad-hoc solutions for digitally signing documents are available, but they don't ensure the compatibility with other formats and the validity of the signature over long periods.
This paper introduces the proposed European standard for long-term electronic signatures and describes on-going work towards a generalised architecture for the development of electronic signature applications. As a case study, the architecture of a system for management of electronically signed documents is described.

***Keywords*:** digital signature, electronic signature, electronic documents, security

1. Introduction

In today's commercial environment, establishing a framework for the authentication of computer-based information or a legal framework for electronic signature, signature products and certain certification services requires a familiarity with concepts and professional skills from both the legal and computer security fields. Combining these two disciplines is not an easy task. Concepts from the information security field often correspond only loosely to concepts from the legal field, even in situations where the terminology is similar. From the information security's point of view, *digital signature* means the result of applying to specific information certain specific technical processes but the historical legal concept of *signature* is broader, that is it recognizes any mark made with the intention of authenticating the marked document.

In a digital setting, today's broad legal concept of *signature* may well include markings as diverse as digitized images of paper signatures, typed notations or even addressing notations, such as electronic mail origination headers. In the same it is important to notice the difference between *digital signature* and *electronic signature*. Digital signature represents data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery. According to the European Directive on a community framework for electronic signature [EuD99] the electronic signature represents instead data in electronic form attached to, or logically associated with, other electronic data in order to provide authentication. Scanned hand-written signature or the name put at the end of an e-mail message are examples of electronic signature and belong to the least complex class of electronic signatures.

Other classes of electronic signatures are built on digital signature that guarantees authentication, integrity and non-repudiation. Thus, it is possible to say that digital signature is a mechanism based on cryptographic

and hashing techniques which guarantees authentication, integrity and non-repudiation, while electronic signature is a class of applications that can be implemented using digital signature.

Certain classes of electronic signatures applied on future formats of e-documents will represent the translation to digital world of handwritten signature applied on paper documents. Throughout the article we can assume that an e-document is an electronic representation of a paper document. The e-document can be in public (e.g. XML, PDF) or proprietary (e.g. MS-Word) format.

Presently real processes for e-document management that make use of the electronic signature are implemented by many proprietary technologies and monolithic applications, named also ad-hoc applications, that don't interact and lock in users. This means that the programmer has to face by himself all the problems for correct creation and verification of electronic signature and the application would be however incompatible with the other electronic signature applications.

Nowadays the mathematical aspects related to the calculation of digital signatures are well defined and the cryptographic methods, provided by public key cryptography, have demonstrated the effectiveness in achieving scalable confidentiality, integrity, authentication and non-repudiation services. Even though there have been defined so far general standards for defining rich formats of a digital signature applied on data objects, like PKCS#7 [PKCS7] or CMS [Hou99a], there still exist the need for a standard entirely defining the format of the data that is to be signed, the format of the signature and the format of the electronic documents. Only the existence of a widely accepted standard for the format of electronic signature that could remain valid over long periods could avoid the appearance of incompatible specifications and solutions for electronic signatures in different user communities.

Furthermore to permit the implementation of compatible software applications we need a modular framework for easy development of concrete electronic signature applications. In order to ensure interoperability between different countries and business, public or administrative communities this framework has to be based on a widely recognized electronic signature standard. With the implementation of specialized modules for performing electronic signature there will be eliminated also ad-hoc applications, that is it will be avoided the need to write proprietary procedures for creation and verification of electronic signatures.

Starting from this general approach we are particularly interested in designing and implementing a prototype system for the management of electronically signed e-documents, using the classes of electronic signatures constructed over digital signature. The documents handled can be of three types: static documents not inserted in various processes that would change their state (no workflow), documents suffering state variations in document-only processes (workflow) and finally documents presenting state variations in document-only processed and with exchange of data from/to various repositories (workflow and access to a database).

2. State-of-the-Art

It has been observed the lack of a standard for defining the format of the data that is to be signed, the format of the signature and the format of the electronic documents. While PKCS#7/CMS has described a general syntax for data objects (generally referred throughout the article as blobs) that may have cryptography applied to it, such as digital signatures and digital envelopes, so far there weren't defined standards for the formats of electronic signatures. Another requirement would be that the electronic signatures need to be applied on documents with public formats (e.g. XML or PDF) and not on formats for which the specification are not public (e.g. MS Word format). In the next paragraphs we will present shortly the technological standards for digital

signature over which it is possible to construct the electronic signature, namely the CMS standard and XML-Signature. It will be described also one proprietary/specific solution offered so far for the construction of digital signatures, namely the PDF public key digital signature.

We distinguish three types of digital signature formats: enveloped signatures (signatures within content being signed), enveloping signature (content being signed is within signature) and detached signatures (signature object is detached from the content being signed). These terms will be generally referred several times throughout the article.

2.1 PKCS#7 / CMS

One of the most important cryptographic standards is PKCS#7 proposed by RSA Data Security. This standard has gained wide acceptance becoming the basis for various mechanisms such as the de-facto standard for electronic mail security S/MIME [Ram99], the Secure Electronic Specification Transaction (SET) specifications for credit card payments or the PKCS#12 standard [PKCS12] for secure transport of private key and certificate.

The evolution of this standard is the Cryptographic Message Syntax (CMS) standard [Hou99a] proposed by the SMIME working group of IETF to digitally sign, digest, authenticate, or encrypt arbitrary messages. Basically PKCS#7/CMS introduces various formats useful when there is the need to add cryptographic enhancements to data like digital signatures or encryption. The syntax allows arbitrary attributes, such as signing time, to be authenticated along with the content of a message, and provides for other attributes such as countersignatures to be associated with a signature. The standard has been designed to support various certificate based architectures such as the one which is currently defined by the PKIX working group [PKIX], that is X.509-based PKI. All the data types are clearly defined by mean of ASN.1 syntax and the encoding rules (e.g. where and when use DER and/or BER encoding) are also fully specified.

A full description of the PKCS#7/CMS standard is out of the scope of this article, so only a brief summary of a specific data type is presented, namely the *signed-data* content type, component of the *enhanced* class of content types. Any number of signers in parallel uses the *signed-data* content type when there exists the exigency to add a digital signature to an arbitrary data content. Format for data to be signed is blob. So PKCS#7/CMS doesn't support digital signatures over document's fragment. It's important to notice that the message can carry inside itself all or none of the certificates and the CRL [Hou99b] required for the verification of the signatures. The syntax has also a degenerate case that provides a means for disseminating certificates and CRLs, in which there are no signers on the content. Moreover there is the possibility to have detached signatures that is the data and the corresponding signatures are not grouped together in a whole message of *signed-data* content type; in the last case the mechanism for the verification of the signatures is application dependent. For instance the two formats for signed messages defined for S/MIME are application/pkcs7-mime with SignedData, and multipart/signed. Consequently someone can either construct detached signatures using the multipart/signed MIME content type [Gal95] or can construct a single CMS object of type signedData using the application/pkcs7-mime with signed data type [Ram99].

2.2 XML Signature

XML with *related languages* clearly has great potential as a standard for data interchange among just any files or documents or data collections due to its ability not only to identify and define info structure but also to specify presentation/layout for any type of document. By *related languages* we understand those languages

written also in XML 1.0 [XML1.098], needed for defining a complete document. Examples of *related languages* are XML Schema [XMLSch] for definition of a structure of a document using a XML based language instead of DTD, XSLt [XSLT99] for transformation and XSL [XSL00] (previously referred by XSL WG as XSLfo) for expressing stylesheets. However the XSL working draft is only in its second revision and given the crucial role that XSL plays in presentation of XML documents, this leaves a lot of XML formatting capabilities up in the air. XML Signature [XMLSig] is an application of XML 1.0 meta-language and can be applied to any digital content (data object), including XML, via an indirection and it may be applied to the content of one or more resources. Data objects are digested, the resulting value is placed in an element along with other information and that element is then digested and cryptographically signed. *Enveloped* signatures or *enveloping* signatures are over data within the same XML document as the signature; *detached* signatures are over data external to the signature document and are related to external data objects via URIs [URI]. XML Signature supports also digital signature of local fragment identifiers if data to be signed is written in XML.

FORMATS	Can be used as format for the data to be signed?	Can be used as format for the digital signature?	Can be used as format over which to construct the electronic signature?	Over which data format it is possible to apply the signature ?	Allows the signing of parts of the documents ?	Relations among the data to be signed and the digital signature
PDF 1.3	YES	YES	Yes, if it is used the PKCS#7 format (detached) for digital signature instead of the Raw Signature format	Only PDF	Yes, only on PDF: allows to affix many signatures on many parts	The signature(s) is/are embedded in the data. A single object: it is possible to construct only enveloped signature
XML Signature	NO	YES	YES	Blob	Yes, only on XML documents: allows to affix many signatures on many portions	Envelope containing the signature object and eventually the data: enveloping or detached signature
PKCS#7/ CMS	NO	YES	YES	Blob	NO	Envelope containing the signature object and eventually the data: enveloping or detached signature

Table 1. Current formats for data to be signed and digital signature object

Moreover, XML Signature has not become yet a standard, it's only a draft so even if is sufficiently stable as it's at its last call, it isn't yet appropriate for building a standard for electronic signature. Thus, it is premature to use it for designing and implementing non-experimental applications used by large communities.

2.3 PDF Public-key digital signature solution

The version 4.0 of Adobe Acrobat has introduced the possibility to add digital signatures to documents in Portable Document Format (PDF), because of evolution of PDF to version 1.3. This format has public specifications and it supports signatures embedded into data file (enveloped signature), thus it offers the

possibility to apply signature over a portion of the document and to have multiple signers. It supports also the "*signature significance"* attribute but unfortunately is not sufficient to completely define semantic of a signature.

There are two alternative formats for storing public key signatures in the signature data structure (named signature dictionary) of a PDF file, namely the Raw Signature format and the PKCS#7 Signature format, either of which presents advantages and disadvantages. The Raw Signature format stores certificates and the signed digest directly in the signature dictionary as attributes while the PKCS#7 format encapsulates the signature and the signed digest into a single PKCS#7 object that is stored in the dictionary

Raw Signature format is used by the specific prototype tool provided by Acrobat to permit the use of PDF 1.3 capabilities for the application of digital signatures. This Acrobat program allows the addition of so called "Self-Sign signatures", such that that every user can create his own profile. The user's profile comprises an RSA private key and a X.509 self-signed certificate that binds the public key to the identity of the user and it's included in the signed document for the verification of the signature.

When a user wants to add a signature to a document, he simply has to make a log-in operation, which is necessary to authenticate himself and to unlock the private key in his own profile. After that he opens the document to be signed and he makes a drag and drop operation to add a signature. Before adding the signature Acrobat asks the user for a series of parameters like a reason for signing a document (e.g. "I have reviewed this document", "Document is certified", etc.), a locality and password to add the signature.

A person receiving a signed document in PDF format can easily verify the signature because the necessary certificate is attached to the document. Usually this isn't sufficient because there is also the need to validate the signature but this could be done by comparing the fingerprint of the certificate with a fingerprint obtained in a secure out-of-band way from the sender of the document. If the comparison gives a positive result the recipient of the document can add the sender's certificate to his own personal address book for the validation of successive documents received from the same sender.

The trust model behind the tool is suitable only for small groups of people and isn't for sure the best solution for corporate use when the number of people exchanging electronic documents is high. Moreover, additional support for PKI (e.g. trusted CA, revocation of certificates) has to be developed separately as a plug-in, with the specific Adobe SDK. These plug-ins can construct digital signature using both RawSignature format and PKCS#7 format. Finally only files which may be transformed into PDF may be signed. Acrobat digital signature doesn't support digital signature over blob (a generic file or document). The signature is embedded in PDF file and enveloping or detached signatures are not supported. So even if PDF has support for digital signature, we think that it is recommended to use it only as a format for data to be signed.

The above considerations are summarized in Table 1.

3. Modular framework for concrete application of electronic signatures

3.1 Functional requirements

So far the "paperless office" has failed to move from theory to reality because of cultural reticence, unequal access to technology, and the lack of an adequate legal and service infrastructure to support such a paradigm shift.

All legally binding communications or transactions, whether electronic or paper-based, must meet the following fundamental requirements:

- the need for a *common way* to define and understand electronic signature, as it is the case of paper

documents signed with hand-written signature which is widely understandable

- the message has to provide sender authenticity to enable the recipient (or relying party) to determine who really sent the message and if that individual is, in fact, authorized to commit the transaction
- there must exist some means to ascertain that the message has integrity. The recipient must be able to determine whether or not the message received has been altered "en route" or is incomplete
- the ability to "prove up" the message in court. Referred to as non-repudiation, this requires some way to ensure that the sender cannot falsely deny having sent the message, nor falsely deny the contents of the message

In order to define a standard architecture for static electronic document management we identify the following particular requirements:

- support for different levels of legal values of the electronic signature depending on different context of the applications. For example in a real world it isn't necessary to use hand-written signature for buying a book, so translating this situation into e-commerce transactions it means the electronic signature does not require the same legal value as hand-written signature
- define and express the electronic signature semantic. This includes the possibility of managing the signature in accordance with the person's role(s) inside an organization, the possibility to apply multiple signatures (independent or embedded signatures) or the possibility for the validation of the electronic signature to be performed after a long period of time relative to its creation
- support for signing time with a reasonable and well defined approximation
- optional support for electronic signing of document's chunks

3.2 Design Requirements

3.2.1 Requirements for electronic signatures in applications for e-documents

In order to implement electronic signature applications respecting the functional requirements expressed in section 3.1 there have been identified a set of project requirements.

One of the primary design requirement refers to the use of a digital signature mechanism based on a public key infrastructure to guarantee the fullfillment of the authentication, integrity and non-repudiation functional requirements. Thus one of the project requirements directly referrs to the implementation of a PKI.

Another design requirement refers to the definition and use of standard formats widely recognized and adopted for the electronic signature object and for the data to be signed in order to ensure the *interoperability* characteristic, that is the possibility to recognize and interprete the electronic signature independently of the format of the data that is to be signed. Solutions proposed by specific technologies, like Adobe, capable of recognizing and interpreting only their own specific digital signatures are not satisfactory for building electronic signature. Among the main characteristics of the signature formats we can distinguish:

- support for the *enveloped* signatures, like in the case of Adobe PDF 1.3 format where the signature(s) is/are included into the data (PDF file), or for *enveloping* signature to obtain a single object containing both data and the signature (useful for example for the transmission of messages). Similarly *detached* signatures allowing separate maintaining of the signed data and respectively the signature could be particularly useful for archiving in a system for information retrieval that performs the indexing of the data to execute queries of type "full text".

- definition of data structures that permit the validation over a long period and of a set of formats increasingly complex with respect to the period of time for which it is desired to guarantee the possibility to validate the electronic signature. Consequently the data structures have to allow the insertion of CRL/OCSP response references and data and of multiple timestamps into the signature object.
- definition of data structures used to protect from hacking tentatives, for example a data structure where the digital signature depends on the public key certificate used for electronic signature creation / verification. In this case it is not possible to replace the certificate used for electronic signature creation with an untrusted certificate containing the same public key because the digital signature would become incorrect and thus the electronic signature verification would fail.
- support for multiple signatures (independent signatures or nested signatures).
- definition of data structures necessary to describe the semantics of the signature. These are data structures added to the basic structure of digital signature to express for example the signer's role or the signing time.

The definition and management of signature policies represent another important design requirement. A signature policy defines a set of rules that need to be respected by the electronic signature with respect to all areas like syntax and encoding formats, protocols, and other specific information applied in a given context and is voluntary chosen by the signer at the signing moment.

Other design requirements refer to the definition of Authorities involved in the signature/validation process as well as of the relative policies and Certificate Practice Statements (CPSs) or the definition of e-terms repositories, that is CPS/ Certificate repositories or Signature Policy repositories. Implicitly it is noticed also the need for the definition of standard protocols for interacting with the Authorities and for accessing the repositories.

Finally it is identified the requirement for the management of What You See Is What You Sign problem, that is the user must be aware of what he is going to sign and what the text specifies the signature has been verified for.

3.2.2 Generalized architecture for development of electronic signature applications

In order to implement electronic signature applications for document management a system has to be designed to comply with the project requirements for digital signature and additionally to the specific requirements for the electronic signature.

For the moment the modular infrastructure necessary for the implementation of the digital signature is well defined and consolidated and is composed of a public key infrastructure (PKI), eventually additional Trusted Third Party (TTP) authorities and Cryptographic Service Providers (CSPs). It is noticed however the lack of an architecture for the development of real electronic signature applications which imposes actually the appearance and usage of proprietary technologies and ad-hoc incompatible applications. Practically, to implement real electronic signature applications it is possible to use the consolidated architecture for digital signature to respect the requirements relative to digital signatures, while for responding to the requirements specific to the electronic signatures there have to be developed monolithic and proprietary applications (see the "Present" part of Figure 1).

To incourage the development of interoperable electronic signature applications it has to be defined a generalized, overall and modular framework, based on a widely recognized standard, covering the

infrastructure for the implementation of digital signature, the middleware and the application sub-areas (see the “Future” part of Figure 1).

The final goal is to design a multilayer architecture by defining a certain number of modules which give to developers the necessary levels of abstraction so that they are able to skip the electronic signature implementation details and to concentrate only onto the logic of the specific applications.

This framework will permit and simplify the development of real applications for electronic signature and will ease the management of electronically signed e-documents.

The diagram in Figure 1 illustrates our proposal for the generalized architecture whose characteristics have been described above. One part of the architecture is composed of the digital signature infrastructure, already consolidated, for which it is necessary to add some elements, like Time Stamp Authorities (TSAs) or Signature Policy repositories, to respond to the requirements expressed in section 3.2.1. Instead the part referring to the electronic signatures applications (see “Application of electronic signature” part from Figure 1) is left to be defined and is subject to our proposal. The concrete applications that would make use of this model could be constituted only of simple user interface applications to permit the access toward all the functionalities of the architecture or could be complex applications like electronic document management systems.

3.2.3 Design Requirements for a digital signature infrastructure

The digital signature mechanism is based both on public-key cryptography and hashing techniques. In order to use this kind of cryptography it is necessary to bind in a certified and unambiguous way the public-key with a well-defined entity.

The data structure used to guarantee this association is the public-key certificate. A public-key certificate contains a digital signature belonging to a Certification Authority (CA). This signature is used to validate the public-key trusting the CA as TTP. Usually the CA is only a part of a much more complex and hierarchical structure known as PKI (Public-Key Infrastructure). With respect to the definition in [Mai98], a PKI includes all hardware devices, software, users, policies and procedures necessary to create, manage, store, distribute and revoke public-key certificates.

Among the more relevant components of a PKI we distinguish the Certification Authority (CA), Registration Authority (RA), Attribute Authority (AA), repositories of E-terms that is of Certificate Practice Statements (CPS) and Certificate Policies, repositories of certificates and CRLs.

Other important components of a digital signature system are the Cryptographic Service Providers. This category includes both software (digital signature library and API) and hardware (smart cards and relative readers) tools which implement the mathematical algorithms used for signing data objects.

In order to implement electronic signature, the digital signature infrastructure has to be extended with at least the following two components: Time Stamp Authority (TSA) and repository of signature policies. The former is another TTP that is required to certify the signing time of an object, the latter is a place from where it is possible to retrieve the different policies under which is possible to add a signature.

3.2.4 Design requirements for the electronic signature applications area

As evidentiated in the introduction it is possible to recognize three types of applications of electronic documents:

- static documents not included in processes (no work-flow)
- dynamical documents with state variations connected to only documents processing (workflow)

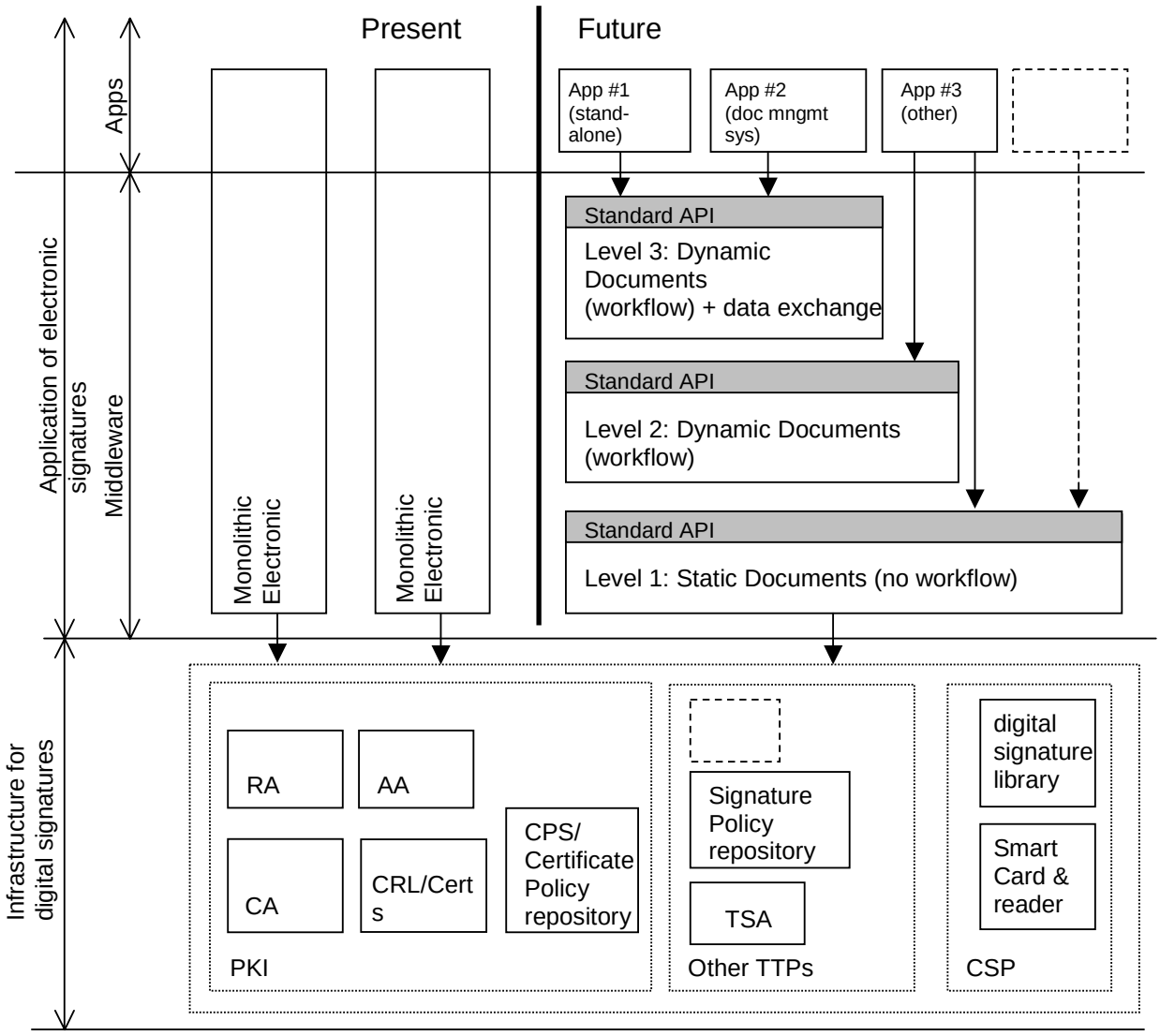

Figure 1. Generalized architecture for development of real electronic signature applications

- documents with state variations related to documents processing and with exchanging of information with different repositories (workflow + access to external databases)

For each type of e-documents cited above a specific module is defined in the middleware sub-area of the multilayer architecture illustrated in Figure 1. The implementation of the various modules implies, besides the problems related to the format for the signature, the definition of generation and verification/validation

processes of the electronic signature object, taking into consideration also various aspects like the choice of signer signature policy or the necessity to add a timestamp.
In this article we are going to make a proposal for implementing a prototype which is limited to the processing of static documents (level 1 module in Figure 1). Moreover, we have found that the ETSI standard for electronic signature formats satisfies most of the requirements cited in the previous paragraphs.

4. European Electronic Signature: EU Directive, EESSI and ETSI

4.1. EU Directive

In order to encourage the growth of electronic commerce the European Commission has proposed to the European Parliament and to the Council a Directive to provide a common framework for electronic signatures. This Directive has become a Common Position of the Commission and of the Council and finally has been approved by the European Parliament in 13 December 1999 [EuD99].

The Directive covers electronic signatures used for authentication like Electronic Signature and a class of Electronic Signatures with support for authentication, integrity and non-repudiation called Advanced Electronic Signature (AES), which may be implemented using digital signatures. It is defined also a particular type of "qualified" electronic signatures with legal equivalence to hand-written signatures, that are in fact AESs based on qualified certificates and are constructed using secure signing devices (see Figure 2).

The Directive also identifies requirements that have to be met by service providers supporting electronic signatures and requirements for signers and verifiers. These requirements need to be supported by detailed standards and open specifications which also meet the requirements of European business, so that products and services supporting electronic signatures can be known to provide legally valid signatures – thus furthering the competitiveness of European business in an international market.

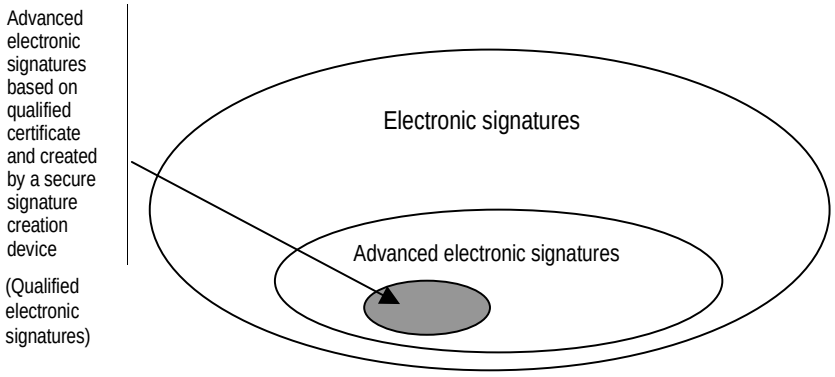

Figure 2. Illustration of Electronic Signature, AES, QES (from EESSI)

4.2. EESSI Initiative

Under the auspices of the Information and Communications Technologies Standards Board and under the monitoring of the European Commission, European industry and standardization bodies have launched the European Electronic Signature Standardization Initiative (EESSI) [EESSI]. EESSI has the objective of

analyzing the future needs for standardization activities in support of the European Directive on electronic signatures in a coherent manner, particularly in the business environment.

The activity of EESSI is split in three temporal phases. The first phase was of inventory type and has been concluded with the production of the "Final Report" [Nils99a]. There have been collected all the national initiatives or produced by particular entities (like the commerce chambers) in the area of electronic signature as well as the set of all technological standards produced or in course to be defined. There have been identified the areas where exist the necessity to define standards and there have been elaborated the first proposals. The approach used was of conservative and matching type, that is the intention was to use the existent industrial and technological standards, to profile or extend them where necessary and to define new standards into the areas presently not covered. Finally it has been decided the assignment of various area to standardization bodies and it has been established the time scheduling.

The standard developed by ETSI SEC ESI working group includes the specification of Security Management and Certificate Policies for TTPs, the definition of syntax and encoding of the signature formats and formats of Signature Policy, specification of qualified certificates based on X.509 certificates and specification of the Time Stamping protocol and timestamps format.

The standard developed by CEN/ISSS E-SIGN Workshop Security defines the security requirements for trustworthy systems used by TTPs issuing qualified certificates, the security requirements for signature creation devices, the specification of the user interface and the operating environment for electronic signature creation, the requirements for signature verification and the Guidelines for Conformity Assessment of Electronic Signature products and services.

The second phase is an operative phase when the members of ETSI and CEN produce their standard (under the monitoring of EESSI). This work is currently in progress. The standards produced in the second phase will be improved in the third phase in order to become European Norm (EN).

The first product of the second phase EESSI is in the area of signature formats and is composed of the ETSI standard approved at the end of March 2000 and has been finalized and published at the beginning of May 2000.

4.3. ETSI standard ES 201 733

ETSI Technical Committee on SECurity dealing with Electronic Signature working group (ETSI SEC ESI) is responsible for Electronic Signatures and Infrastructures standardization within ETSI (European Telecommunications Standards Institute).

In the first phase in the ETSI standard there have been selected to be standardized the format for various forms of electronic signatures and an experimental syntax for signature policies.

To describe the main aspects related to the format of an electronic signature ETSI has stated that the definition of electronic signature includes: "a commitment has been explicitly endorsed under a signature policy, at a given time, by a signer under an identifier, e.g. a name or a pseudonym, and optionally a role".

Among the characteristics of this standard we can distinguish:

- introduction in the signature object of ID and the hash of the public key certificate of the signer [Nils99b].
- this standard is constructed over CMS [Hou99a] and ESS [Hof99]. In the third phase EESSI will evaluate whether to rewrite it over XML Signature. Starting from the core syntax of the XML digital signature it is currently analyzed what can be made of it to get an equivalent functionality as the one obtained when

using electronic signature format constructed over basic CMS with some additional signed and unsigned attributes.

- the possibility to define the semantics of the signature by means of data structures added to the basic structure of the digital signature itself. In ASN.1 terminology these structures are called signature and signer attributes and can be signed or unsigned.
- format of the data to be signed is blob (it isn't managed the signature of document fragments). It provides support for *enveloping* signatures (more appropriate in message transmission, for example) or *detached* signatures (more appropriate for usage in systems for information retrieval).
- there exist different legal values defined in the directive: Electronic Signature, Advanced Electronic Signature (AES), Qualified Electronic Signature (QES). For the moment the ETSI standard addresses only the AES (with the enhancements like timestamping and others defined in the final report of EESSI). It is previewed an evolution of the standard to support QES.
- definition of a Signature Policy and of a Signature Policy ID as concepts as well as syntax proposal for machine-readable part of the Signature Policy.

It has been established that an electronic signature may exist in many forms. The basic form named Electronic Signature (ES) includes the digital signature and other basic information provided by the signer and ensures basic authentication and integrity protection and can be created without accessing on-line (timestamping) services. Another form called ES with Timestamp (ES-T) adds a timestamp to the Electronic Signature and takes the initial steps towards providing long term validity. ES with Complete validation data (ES-C) adds to the ES-T references to the complete set of data supporting the validity of the electronic signature, that is certificate reference and revocation status information by mean of references to CRL [Hou99b] and/or OCSP [Mye99] response.
An Electronic Signature, with the additional validation data forming the ES-T and ES-C is illustrated in Figure 3.

The values of signer's certificate, all the CA certificates that make up the full certification path and all the associated revocation status information may be added to the ES-C to form an ES with eXtended validation data (ES-X) if the verifier does not has access to this data, as referenced in the ES-C. Moreover, if there is a risk that any of the CA keys used in the certificate chain may be compromised, then it is necessary to additionally timestamp the validation data by timestamping all the validation data as held with the ES (that is timestamp ES-C). This eXtended validation data is called a Type 1 X-Timestamp. Another proposed solution is to timestamp only individual reference data as used for complete validation and this form of eXtended validation data is called a Type 2 X-Timestamp.

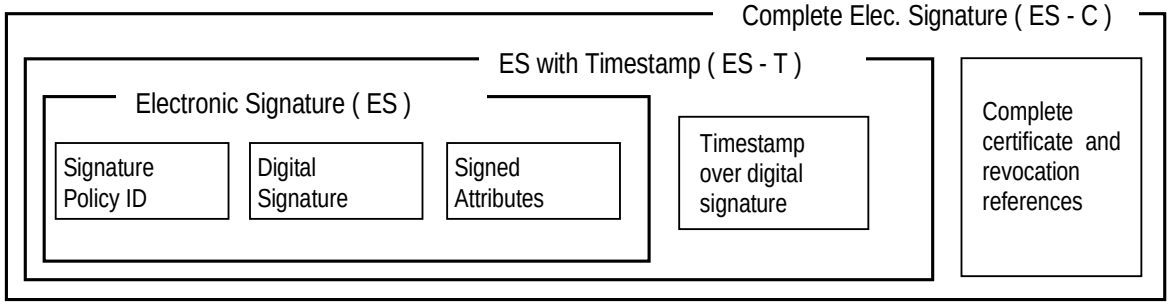

Figure 3. Illustration of ES, ES-T and ES-C (from ETSI)

The ES-A format ensures long term validation of the electronic signature. The additional data and timestamp added is called Archive Validation Data. For the definition of this format it has been has started from the following premise: before the algorithms, keys and other cryptographic data used at the time the ES-C was built become weak and the cryptographic functions become vulnerable, or the certificates supporting previous timestamps expire, the signed data, the ES-C and any additional information (ES-X) should be timestamped. If possible the timestamping process should use stronger algorithms (or longer key lengths) than in the original timestamp and it may be repeated every time the protection used to timestamp a previous ES-A become weak. Thus, an ES-A bears multiple embedded time stamps.

5. Practical applications

The use of electronic signatures in closed systems (e.g. a corporate Intranet) constitutes the premise for the customisation of a product for an electronic document management system used inside Politecnico di Torino that will allow in the end a concrete experimentation to be performed on e-signed real e-documents.
Among the three mentioned types of e-documents, we have been particularly interested in static documents, that is documents that don't present state variations and consequently are not included in a process. Our objective is the implementation of a complete experimental system for electronic signature creation and validation, taking into account the requirements of real documents like role management of the signer and the significance of the signature. The European electronic signature model EESSI/ETSI covers these areas.

The working groups from Politecnico di Torino involved in this project are: the Computer and Network Security Group of the Dipartimento di Automatica ed Informatica, that will be in charge of research and development the middleware sub-area, and Ce.S.I.T (i.e. the Computing Center) that will be in charge of the development in the application sub-area and will perform experiments in the Central Administration of the athenaeum.

In the same time the European Signature Guidelines, as well as digital laws in different countries, have begun to lay the foundations to issue electronic documents by public institutions such as administrative bodies, professional associations or universities, which - electronically signed - will be held equal to conventional paper documents. This will enable these institutions to issue innovative forms of conventional documents, such as electronic certificates of birth, electronic trade licences, electronic diplomas, that can be used instead of paper documents.

The previous objective is the target of an European project named AIDA (Advanced Interactive Digital Administrations) whose role is to deploy a technical platform and use it in order to demonstrate the feasibility of trustworthy electronic signatures in combination with enhanced electronic documents within a flexible and secure e-administration environment. The demonstrations focus on the needs of two major groups of service partners, namely the public bodies and the citizens. It is observed that the electronic signatures are used in this case for official communication with public institutions (e.g. calls for tender, exchange of application forms, identity documents, tax declarations, transmission of legal documents). In this area it is envisaged that the electronic signature is used with equivalent legal effect as a hand-written signature, that is the electronic signature format should belong to the QES category. For the moment the signature formats defined by the ETSI standard are belonging to the Advanced Electronic Signature (AES) category defined by the Directive, that is the electronic signature produced by our implementation will not have (for the moment) the legal equivalence of the hand-written signature. As soon as the specification for QES will be defined by the ETSI,

the current implementation of electronic signature formats could be improved to achieve the requirements of QES format.

5.1 Implementation in 'Digital signature infrastructure' area of the modular architecture

The modular architecture for the development of electronic signature application will benefit, at the digital signature infrastructure level, of the services of the public key infrastructure designed and developed by the EuroPKI [EuroPKI] project, eventually adding authorities like TSA and repositories for the Signature Policies. The EuroPKI is an European wide PKI that has been setup within the ICE-TEL and ICE-CAR projects with the goal of providing the necessary support for the deployment of secure applications for commerce, public administrations and research institutions. Regarding the Cryptographic Service Providers we are going to use modules and libraries, either software only (free libraries as Crypto++) or hardware (smart card and reader) and software, having different interfaces like PKCS#11 and MS-CryptoAPI.

5.2 Implementation in 'Application of electronic signature' area of the modular architecture

For the electronic signature application area of the modular architecture we'll concentrate both on the middleware and on the application sub-areas.

5.2.1 'Application of electronic signature' area: middleware sub-area

For the middleware part we are going to implement the level 1 module (see Figure 4) as objects (COM, CORBA, Java) for different platforms (Linux, Win32, Solaris) in order to be used both on client and server side in conjunction with stand-alone applications, web browsers, web servers, messaging systems, document management or information retrieval systems (open or proprietary, with or without web-based user interfaces).

For the development of the module we are going to use the existent CMS [Hou99a] and ESS [Hof99] libraries and over these libraries we are building a library that implements partly or entirely the ETSI ES 210 733 standard defining the electronic signature formats.

Additionally we'll use or implement libraries for the management and validation of X509v3 certificates, for access to the TSA, as well as for the formats and repositories for the Signature Policies. Finally we'll implement a library that makes use of the other modules to entirely manage the signing and validation processes. This library will provide APIs that will constitute the interface for user applications.

Implementation of generalised APIs, based on standard for access to the electronic signature services, like the IDUP-GSS-API [Ada98] specified by the ETSI standard is outside the objectives of the current project which is mostly oriented toward the interoperability of the formats and the development of the level 1 module.

5.2.2 'Application of electronic signature' area: application sub-area

For the application sub-area we intend to:

- develop a stand-alone program constituting the user interface towards all the functionalities offered by the libraries.
- use various mail systems (Eudora, Netscape or Microsoft Outlook) with messages signed according to the European standard and verify the interoperability among various formats.
- customise a product for document management and retrieval system with web-based interface, chosen by Politecnico di Torino, and to perform a concrete experimentation on real documents produced by Central Administration, managing the roles of the signer and the signature policies.

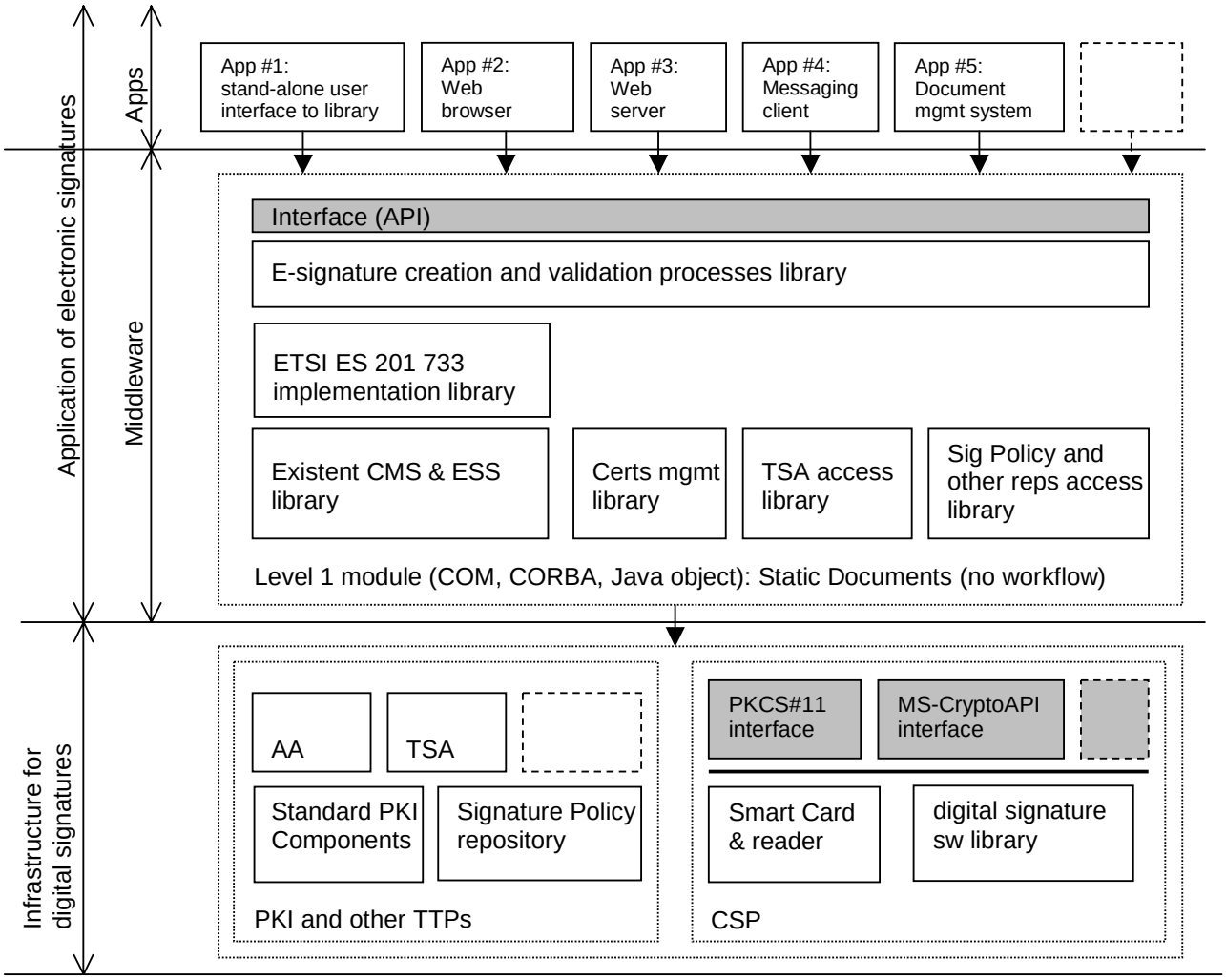

Figure 4. Diagram of the level 1 module of the architecture for the development of electronic signature applications

6. Conclusions

This paper presents a layered architecture for the development of electronic signature applications, build upon on a widely recognised standard to provide a flexible, dynamic and interoperable environment to business, administrative and public communities from different countries. We claim that the ETSI standard with its proposed formats for the electronic signatures satisfies most of the functional and design requirements for the implementation of such a generalised architecture.

Our efforts are concentrated towards developing both the middleware and the application sub-areas of the infrastructure, with special attention on requirements of signing/ verification of real static documents. We are

currently working on the customisation of a product system for document management and retrieval with Web-based interface to be used at Politecnico di Torino.

Acknowledgements

The authors would like to acknowledge Piero Bozza (director of Ce.S.I.T) for his contribution in defining the application aspects and his availability for the organisation and support of experiments in this area.

References

[PKCS7] B. Kaliski, "PKCS#7: Cryptographic Message Syntax Version 1.5", RFC-2315, 1998

[Hou99a] R. Housley, "Cryptographic Message Syntax", RFC-2630, 1999

[PKCS12] "PKCS #12 Technical Corrigendum 1", RSA Laboratories, 2000

[PKIX] http://www.ietf.org/html.charters/pkix-charter.html

[Gal95] J. Galvin, et al., "Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted", RFC-1847, 1995

[Ram99] B. Ramsdell, "S/MIME Version 3 Message Specification", RFC-2633, 1999

[Hou99b] R. Housley, et al., "Internet X. 509 Public Key Infrastructure Certificate and CRL Profile", RFC-2459, 1999

[XML1.098] T. Bray, et al., "Extensible Markup Language (XML) 1.0, W3C Recommendation", 10-February-1998, http://www.w3.org/TR/1998/REC-xml-19980210

[XMLSch] "XML Schema Part 1: Structures" and "XML Schema Part 2: Datatypes", W3C Working Drafts http://www.w3.org/TR/1999/WD-xmlschema-1-19991217/, http://www.w3.org/TR/1999/WD-xmlschema-2-19991217/

[XSLT99] "XSL Transformations (XSLT) Version 1.0", W3C Proposed Recommendation, October 1999. http://www.w3.org/TR/1999/PR-xslt-19991008

[XMLSig] D. Eastlake, J.Reagle, D. Solo, "XML Digital Signatures Working Group, *Internet Engineering Task Force & W3C* draft, 2000

[URI] T. Berners-Lee, et al., "Uniform Resource Identifiers (URI): Generic Syntax", RFC-2396, 1998

[XSL00] "Extensible Stylesheet Language (XSL) Version 1.0", W3C Working Draft, March 2000

[Mai98] Fabio Maino, "Definizione, implementazione e gestione di una infrastruttura di certificazione a chiave pubblica di dimensione europea", Ph.D. Thesis, Politecnico di Torino , 1998

[EuD99] "Directive 1999/93/EC of the European Parliament and of the Council on a common framework for electronic signatures", http://www.ict.etsi.org/eessi/e-sign-directive.pdf

[EESSI] http://www.ict.etsi.org/eessi/EESSI-homepage.htm

[Nils99a] http://www.ict.etsi.org/eessi/Final-Report.pdf

[Nils99b] Hans Nilsson, Denis Pinkas, "Validation of Electronic Signatures", White Paper, March 1999

[Hof99] P. Hoffman, "Enhanced Security Services for S/MIME", RFC-2634, 1999

[Mye99] M. Myers, et al., "X509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP", RFC-2560, 1999

[EuroPKI] http://www.europki.org

[Ada98] C. Adams, "Independent Data Unit Protection Generic Security Service Application Program Interface (IDUP-GSS-API)", RFC-2479, 1998