

The OASIS Digital Signing Service and its Application to E-Invoicing in Europe

Nick Pope – Thales e-Security, UK
(nick.pope@thales-ecurity.com)

**Juan Carlos Cruellas - Universitat Politècnica de Catalunya,
Spain**
(cruellas@ac.upc.edu)

Nick and Juan Carlos co-chair the OASIS Digital Signature Services TC and have work together over a number of years on European Electronic Signature standards including most recently the ETSI specification on “Signatures for Digital Accounting”

Abstract

This paper presents two related activities, the first is the OASIS Digital Signature Services (DSS) standard, the second is the application of digital signatures to electronic invoicing as recognised under recent European legislation. DSS can be used to support a range of signature formats including the binary “cryptographic message syntax” and XML signatures, as well as related extended formats for “advanced electronic signatures” defined in European standards. The DSS standard is built around the general XML web based services structure and can be used with HTTP and SOAP transport protocols. The paper describes how DSS supports the needs of eInvoicing signature creation and verification, minimising the per user installation costs, improving security and reducing the need for revocation. It also describes how DSS verification greatly simplifies the complexity of user systems and facilitates centralised management of security within an organisation. Finally, the paper considers the requirements for maintaining the verifiability of signed invoices stored over a period of around 10 years and how this can be met by DSS verification services with time-stamping and / or archive services.

E-Invoicing in Europe

A directive was issued in 2001 with the aim of harmonising the requirements relating to “Value Added Tax” (VAT) in Europe [VATDirective]. This tax is a form purchase tax but is applicable to all sales including supplies of goods between companies to which value is added (hence the name value added tax). VAT legislation requires invoices be produced and recorded on all sales to which VAT is applicable and there are pan European rules on how this tax is itemised to facilitate auditing of the tax collection.

The recent directive on VAT harmonisation defines further rules for the form of VAT

invoices, including requirements for the security of electronic invoices. It states that:

“Invoices sent by electronic means shall be accepted by Member States provided that the authenticity of the origin and integrity of the contents are guaranteed ..”

The VAT directive then goes on to identify alternative solutions to providing such protection including protection using a form of digital signature based on a PKI (referred to in EU legislation as an “advanced electronic signature”).

Records of these signed e-invoices need to be kept for a number of years, varying from country to country, but can be up to 10 years or more. It

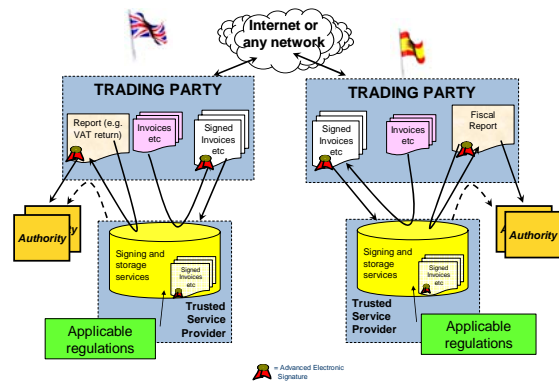
has been generally taken that the requirement for authentication and integrity extends for this period. So it can be necessary for signatures to be verifiable 10 years after the invoice was created, possibly long after any public key certificates involved in their creation have expired or have been revoked.

Recognising the need to establish techniques for maintaining the validity of signatures over the long term, a European based workshop operated by CEN (Comité Européen de Normalisation) has included as part of its CEN Workshop Agreement on E-Invoices and Digital Signatures [CWA 15579] guidance on the maintenance of signatures over the long term. This identifies the need for controls to ensure that the information needed to verify the signature at the time of signing is maintained. This can be through use of technical measures such as the preservation of relevant certificates and revocation information such as OCSP (Online Certificate Status Protocol [RFC 2560]) or CRL (Certificate Revocation List [X.509]), along with a signature time-stamp, augmented by archive time-stamps where the algorithm strength dictates cannot be guaranteed for the whole storage. Alternatively, this can be through use of organisational measures using, for example, trusted notaries to check signatures and maintain records. It is recognised that a range of solutions exist depending more or less on cryptographic technology, use of archive media such as WORM drives, and organisational controls. This requirement is discussed further below.

Similar requirements can be applied not only to the e-invoices, but other documentation for company accounting and auditing, such as the quarterly regular VAT reports required by the tax authorities, as well as other company reports required to support needs for secure accounting such as those imposed through the Sarbanes-Oxley Act in the U.S.

The work of CEN has been taken further by ETSI (European Telecommunications Standards Institute) in a specification to be published shortly on “policy requirements for trust service providers signing and/or storing data for digital accounting” [ETSI TS 102 573]. This identifies

best practice for third parties providing signing and storage of invoices and other accounting documents. It outlines the security controls that should be applied to ensure appropriate security on signing services and insure integrity of signed documents over the period of storage. It can be used as requirements external to an organisation, or internal services provides for use within large organisations. The model used in the ETSI standard is illustrated below:



Storage of Signed Invoices

The issue of particular concern when storing signed e-invoices is that when retrieved at a later date (say after 5 years) the signature may need to be verified by an auditor when looking back at old records. After such a period, it is likely that the certificates used in signing the invoice have expired and it is possible that one or more of the certificates used have been revoked. The auditor looking at an old signed document needs to be able to know that the signature was valid at the time the signature was applied.

Two basic solutions have been identified, The first is to use a trusted service that stores all signed documents along with a trusted statement that the signature was verified to be correct at the time when first placed in storage. Such a trusted service would require the use of secure databases or other forms of trusted storage and procedural controls to ensure that the appropriate checks are carried out when placing data in storage.

The second solution is to use technical measures to establish:

- a) The time when a valid signature existed,
- b) The certificates and revocation information (e.g. Certificate Revocation List or OCSP response) required to verify the correctness of the signature at that time.

This second solution allows an auditor to later verify the signature.

The time of when a valid signature is known to exist may be achieved by verifying a signature just before first storing and marking the signature with this time.

The most widely accepted solution to getting assurance of the time is to use time-stamping produced by a server such as defined in RFC 3161. If applied over the signature this can be used to demonstrate that the signature occurred before the time-stamp. Further assurance of the signing time can be achieved by including the signing time within the signed data and then apply a time-stamp afterwards. However, from recent work on profiles for “advanced electronic signatures” based on a survey of current practice [ETSI TS 102 704 and ETSI TS 102 904] indicates that a time-stamp applied after signing is generally considered sufficient. It is recognised that other mechanisms, such as secure audit logs, can be used to prove the time that the document was signed / stored.

Possibly the surest way of making the certificate and revocation information available is by storing it with the signed document. This, however, can be very inefficient requiring significant amount of storage with much common information repeated across documents. The alternative of depending on the certification authority (CA) to store all the historical information and make it readily available for access for any date for 10 years is beyond the capabilities of most CAs.

The solution adopted in European “advanced” electronic signature format standards ([ETSI TS 101 733], [ETSI TS 101 903]) is to recommend that signatures are time-stamped on receipt,

before placing in storage, and either the relevant certificates and revocation information is included with the signature by value or reference.

When storing documents for very long periods when the strength of the public key algorithm may not be assured (say longer than 10 years), additional protection needs to be applied. Over such periods the integrity of the signed document needs to be extended, for example, by additional signatures, signed time-stamps or secure storage mechanisms.

Since in Europe electronic documents are not generally required to be kept for longer than 10 years, this paper primarily considers the requirements for storage of documents in the 1 to 10 year time-scale. The mechanisms to protect documents for longer than ten years are not generally necessary for e-Invoicing.

Application of Conventional PKI to E-Invoicing

The application of conventional PKI techniques to signing e-invoices stored for a period of around say 10 years is illustrated in the following diagram:

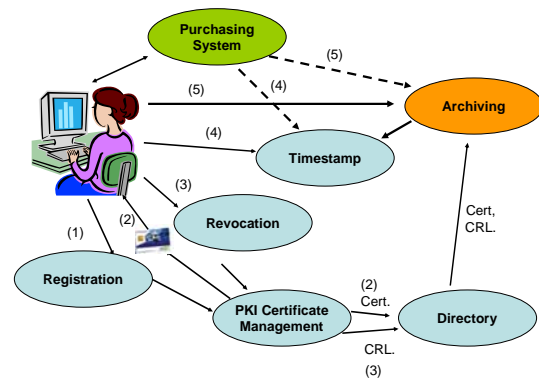


Fig 1: Conventional PKI solution for e-Invoicing

As illustrated each user needs to interact with several services to set up and apply digital signatures and maintain all the necessary records for e-invoicing documents produced by the purchasing system:

- 1) When first setting up the capability to create digital signatures, the user needs to interact with registration services which will carry out the necessary authentication and authorisation checks.
- 2) Some time later when the necessary checks have been completed the registration service interacts with the PKI management services to produce the necessary keys and certificates. The certificates are placed in a directory system and the key is passed back to the user, for example in a smart card device.
- 3) If after using the signing key the user changes role and is no longer authorised for signing, or the security of the key is compromised, for example due to loss of the smart card in a public place, the user needs to interact with revocation services to revoke use of the key.
- 4) When applying the signature in order to obtain a trusted indication of the time when the signature was applied the user (or purchasing system) timestamps the signature using a timestamp server.
- 5) In order to preserve the evidential value of the signed invoice the signed document is passed, either by the user or purchasing system, to the archiving system. The archiving system is required to maintain the integrity of the signature including the necessary CRLs and certificates which may be retrieved from the directory.

Some of the above steps may be simplified or handled by the purchasing application on behalf of the user (e.g. archiving and time-stamping). However, much of the complexities of the PKI system (registration, revocation handling) are inherent in the design of client based PKI.

In many European countries the need for digital (electronic) signatures is not limited to purchasing. Many of the accounting reports (for example quarterly tax returns summarising total VAT paid and collected, yearly corporate accounts) also have to be protected by signatures, widening the need for support for digital signatures.

DSS Based Solution

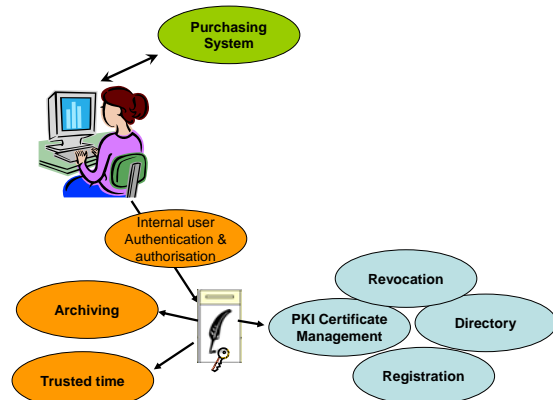


Fig 2: DSS Based Solution for e-Invoicing

An alternative solution to signing company documents, such as e-invoices, would be to employ a signing server which signs document for authorised users within the organisation.

Such a server based solution can build on the existing user authentication and authorisation system to control the use of the signing function and, if individual user signing keys are required, identify the appropriate signing key. All the complexities of the PKI Management are handled by the server without the need for any user involvement. The signing service can, in addition, be extended to provide the necessary archiving functions to maintain the signatures over the lifetime of the document. Also, trusted time functions can be used to provide the necessary evidence of the signing time.

The OASIS DSS Protocol

The basic aim of the OASIS Digital Signature Service (DSS) draft standard [OASIS DSS] is to define protocols for a networked web service to support digital signatures. It also supports a variety of variations on basic digital signature services such as time-stamping.

DSS is designed to support a range of signature formats. Not only does DSS support the World Wide Web consortium XML Signature [W3C XMLDSig], but also the widely used Cryptographic Message Syntax (CMS) binary signed data format [IETF CMS]. It can even be

extended to support other forms of signature such as PGP. The protocol is also designed to be easily extensible to enable support of advanced forms of CMS and XML based signatures such as defined by ETSI [ETSI TS 101 733] & [ETSI TS 101 903].

DSS supports two basic protocols one for the creation of digital signatures, the other for verification of signatures. The basic operation of a DSS sign and verify requests are illustrated below:

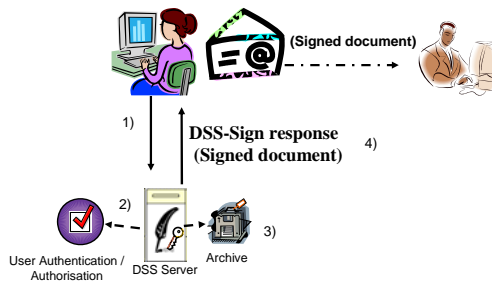


Fig 3: DSS Sign Protocol

- 1) The user sends the request for the document to be signed through a secure channel that authenticates the user (e.g. SSL + client authentication using one time password).
- 2) The server checks that the authenticated user is allowed to sign the document and if acceptable signs the document on behalf of the user with a corporate signing key or a key which the server holds on behalf of the user.
- 3) If required, the server can be extended to archive the document, signature and appropriate supporting information (CRLs, certificates, signing time).
- 4) The server returns the signed document to the user back through the same secure channel.

Having obtained the signed document from the DSS server the user can then pass it on to one or more recipients who may verify the signature themselves or use the DSS verify protocol.

The recipient may verify the signature himself or use the DSS verify protocol as indicated below:

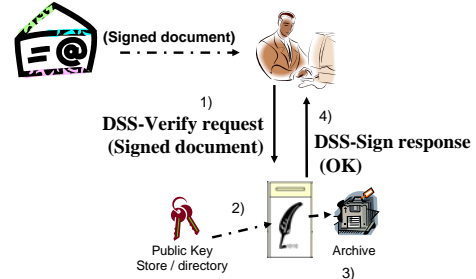


Fig 4 DSS Verify protocol

- 1) The user sends the request for the signed document to be verified through a secure channel (e.g. SSL).
- 2) The server verifies the validity of the signed document including checking the validity and revocation checks on any keys or certificates as necessary.
- 3) If required the verifying organisation may keep its own copy of the signed document and verification information (CRLs, Certificates, time at which document was verified to be correct).
- 4) The results of this verification is returned back to the user through the same secure channel.

The DSS protocol removes from the user all the burdens normally associated with digital signatures. There is no need for the management of large numbers of keys distributed throughout the organisation, and no special cryptographic code or keys are needed on the client system. Where it is necessary to authenticate the client existing mechanisms can be used. All the problems of maintaining the security of the keys and cryptographic functions associated with digital signatures can be managed by the organisation through centralised controls.

DSS servers can be used to maintain an audit record to confirm that signatures are verifiable at the time of receipt, and through use of time-

stamping ensure that the validity of archived signed documents can be assured long after the applicable keys have expired as described below.

DSS specification set structure

The DSS specification set is formed by the so-called core document (“Digital Signature Service Core Protocols, Elements and Bindings”) and a number of additional documents defining specific profiles of the aforementioned core protocols.

The core document defines the (XML-based) syntax and semantics for the basic services, namely: signature generation and signature verification. This includes:

- Definition of four basic messages: SignRequest, SignResponse, VerifyRequest and VerifyResponse. They are defined to easily manage the most common signatures formats, ie, [XMLSig] and [CMS].
- Definition of an extensibility mechanism that allows the clients to further qualify or even increase the extent of the requests through optional inputs. It also allows the servers to answer with extended responses through the corresponding optional outputs.
- Definition of a XML format for a time-stamp token, fully based on XML signatures as specified in [XMLSig].
- Definition of mechanisms for managing generation and verification of digital signatures carrying time-stamp tokens (both CMS-based as defined in [RFC 3161] and the XML-based specified in the core document itself) computed on the signatures themselves (signature time-stamps).
- Definition of bindings for transport and security. The first ones specify how DSS messages are encoded and carried over the most popular transport protocols (it defines bindings for HTTP –through HTTP POST exchanges- and SOAP 1.2). The security bindings establish rules for providing

confidentiality, authentication and integrity to the transport binding; TLS 1.0 support is mandatory and SSL 3.0 support is optional. In this way clients may use wide-spread tools that do not jeopardize their implementation.

The profile documents further develop the basic messages so that they may be easily tailored to meet the requirements of a specific application or use case. Profiles may restrict the values ranges of certain message elements, or, if required, extend the basic core protocols defining new optional inputs, outputs and/or bindings.

The final result is not only a set of protocols targeting a number of relevant scenarios but also a set of generic protocols which may be easily further profiled as new uncovered use cases are identified.

Variations and Profiling DSS

The DSS protocol supports a number of variations in this protocol. For example, the signature may be passed back to the user on its own, detached from the document to which it applies, or placed within the document to which it applies. Another variation is that the document is reduced to a simple hash fingerprint for sending to the server instead of the document for either signing or verification, thereby reducing bandwidth requirements and reducing the opportunity for the confidentiality of the document to be compromised.

When signing a document the DSS server may add additional attributes or properties to the signature such as the claimed signing time or a time-stamp against the content applied immediately before signing.

Due to the number of variations a specific set of options can be selected in the DSS protocol to support a particular mode of operation or application requirement. This selection from the DSS protocol is defined in separate DSS profile specification. The DSS protocol is also designed to facilitate extensions and so DSS Profiles may also extend the protocol, as well as

selecting specific options, defining its own profile specific input or outputs for profile specific attributes of a signature.

A number of profiles have been defined for DSS. This includes:

a) Time-stamp profile

As described above, including support for XML format time-stamps.

b) DSS Entity Seal Profile

This profile is a variation on a signed time-stamp, where the signed object includes not only the time but the identity of the authenticated user requesting the "entity seal". This provides further traceability and provides a form of "proxy" signature where the signature is produced on behalf of another identifiable party.

c) Advanced Electronic Signature Profile

This profile produces signatures that have the attributes needed for legally qualified and long-term signatures

d) Code signing Profile

This profile is designed to support the signing of code authorised for distribution with an organisational signature indicating its authenticity.

e) Electronic (Digital) Post Mark Profile

This profile is for providing an electronic post mark used confirm authenticity of email, as promoted by the Universal Postal Union [UPU-EPM].

f) Signature Gateway Profile

This profile supports the creation of signatures at a gateway from a form only recognised internally to a standard form which can be recognised externally.

Authentication and Authorisation for Signature Creation

The DSS services decouple the authentication / authorisation of the signing request from the authentication in the signature. This significantly simplifies the management of identities and authentication in the case of e-

invoicing, where the signature is generally applied on behalf of a company, either as a corporate signature or as the signature of an individual who signs as a person responsible for the company, such as a chief executive.

The authentication required to authorise a signature request within an organisation, can be based upon internal security controls. Internal user identities can be assigned as part of the normal internal user authentication and authorisation controls, there is no need to interact with external registration services to set up each individual user that may be authorised to sign. Furthermore, where more complex work flow processes are involved with authorisation of invoices this process can be controlled independent of the application of the signature. Finally, any changes in personnel or removal of access rights, need not affect external revocation. Any authorisations to sign documents can be removed immediately without any impact on external revocation services.

If required the method employed for user authentication to a DSS need not involve any installation of security devices on the user PC. For example, simple challenge response systems using hardware tokens may be used to request signing by the DSS server through a simple web interface without the need for special security installation. Thus the common difficulties with installing security devices such as smart card readers can be avoided.

The centralised management of corporate signing keys are also facilitated through the use a signing server. Strict organisational controls can be applied to the server. If necessary it can be held in a physically secure area. Dual control / split keys can be applied so that the signing key can be used under strict controls. Thus the probability of compromise, and hence the need for external revocation, is minimised.

This ability in DSS to centralise signing capability not only improves security but also can reduce costs by minimising the per user installation costs.

Signature Verification for Stored Signatures

As mentioned above, to assure that signatures are verifiable for the period they are to be stored, it is considered necessary to establish the time that they are known to be valid and the certificate and revocation information (e.g. Certificate Revocation List, OCSP response) used to confirm that validation.

The DSS verification service can take the burden of obtaining and maintaining the supporting evidence for “long term” signatures away from the user. Two basic solutions are envisaged. One is to extend the signature structure adding the signature time-stamp and references / values of the certificates and revocation information employed in validating the signature (as described in [ETSI TS 101 733] and [ETSI TS 101 903]). The other is to include a trusted time and relevant certificate and revocation information in a secure audit log. In either case all the complexities are taken from the user and handled by a trusted server.

A further advantage of using a DSS server for signature verification is that all the complexities of validating the certificate path are taken from the user. This can be particularly onerous where multiple certificate policies are involved or the trusted root certificate authority of the organisation where the signature was created is different from that where the signature is verified. By placing such functionality in the server the appropriate cross domain policy controls can be maintained and easily updated under central control.

In general the ability of DSS verification server to be placed under central control enables all the appropriate security measures to be applied and maintained. The security management authorities for an organisation can ensure that the procedures applied are secure and up to date. There is no need to depend on users to properly apply signature verification policy and there is no need to distribute up to date security software and information around the organisation.

DSS Within an eInvoicing Architecture

The use of servers for signing and verification of signatures fits naturally with the basic architecture of many e-invoicing systems. Generally, back office systems are used to handle invoices as part of the process flow. Whilst individuals may need to be accountable for the creation of invoices within the organisation, from the external viewpoint the signature belongs to the organisation, or in some countries a senior executive who represents the company.

As illustrated below in the case of invoices the creation of signatures may be initiated by an invoicing and accounting system which prepares and issues invoices under control of accounting clerks. The system is already trusted to properly maintain and control the creation of accounting information. The private key used in creating the invoice signatures can be managed centrally under clear security controls.

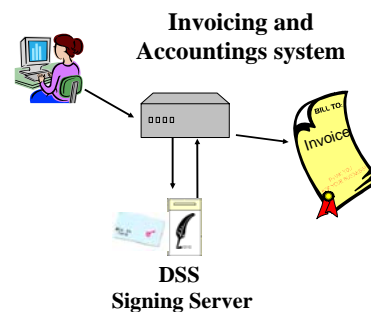


Fig 5 eInvoicing System with DSS Signing

Similarly, the verification of incoming invoices may be initiated by the accounting system. The information required for future verification of the stored invoice can be maintained in two ways. This can be done the use of a secure audit log maintained by the server containing the relevant validation information for later retrieval when subsequently re-verifying a stored document. Alternatively, by use of advanced electronic signature structures the document signature can be augmented with the information necessary to later re-verify the signature. In either case, the database used to store the

invoices do not need to be secure to ensure the integrity of the signatures as this is provided through the DSS verification server.

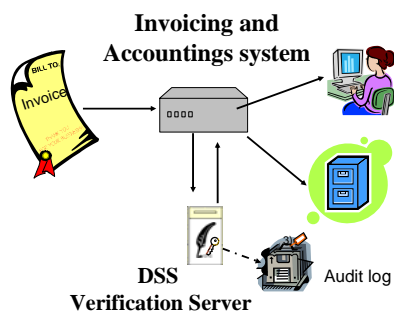


Fig 6 eInvoicing System with DSS Verification

DSS Implementations

The first version of the DSS core working draft dates back to October 2003. In 2004 and first half of 2005, the DSS Technical Committee developed a version of the core protocol incorporating most of the features of the current version, as well as the most important profiles. In 2006, the document went for public review. The TC received several comments that proved the attention attracted by his work. In parallel several members of the DSS TC have started an interoperability initiative for assessing the protocols under a practical perspective. At time of writing this paper specifications are in the final stage for ratification as OASIS specification early in 2007.

Over the last few years several systems have been deployed, which adopted DSS style of operation. As the specifications matured they attracted the attention an increasing number of manufactures of such a kind of systems. In the end, DSS specifications provide a standard way of operation for centralized services for electronic signatures generation and verification, which ensures interoperability.

2007 will likely start a period of extensive deployment of DSS-compliant applications. A number of organizations exist interested in providing centralized services for generation and verification of electronic signatures, which have decided to build a DSS-compliant application from the scratch. In addition, owners of

platforms based on proprietary protocols are evolving towards DSS-compliant implementations.

One of the first major deployments using DSS specifications is the PSIS [PSIS]: a platform for identification and signature services, conceptualized, deployed and run by the Agència Catalana de Certificació (CATCERT) [CATCERT]. CATCERT is the CA for public administration agencies in Catalunya, Spain. Along with provision of different types of certificates (among which the personal certificate for Catalan citizens), CATCERT also offers this platform to Catalan governmental agencies, local administrations and private companies that have to securely exchange electronic information with them. This platform offers centralized services of signature generation, signature verification, encryption, and decryption. In addition to that CATCERT also provides access control tools (that use Liberty Alliance protocols) based on unique authentication or identity federation, to those organizations that want to integrate these services in their own applications. As for the DSS, this platform implements the DSS-core, the management of XML time-stamps, the DSS-AdES profile and the DSS time-stamping profile. It is able to perform semantic validation of certificates, CMS, XML-Sig XAdES and CAdES signatures, indicating their validity and the security level associated to the signing certificate (this is important because each type of electronic transaction with Catalan public administrations requires that the signing certificate has a pre-determined level of security).

In Norway a consortium of banks and CAs offer an optional lightweight web based signing, of a style similar to DSS, to over 600,000 banking customers [BankID] [EEMA-Award] with the aim to extend this to 2.3 million.

The UPU EPM, adopted by several postal service organisations, has been working closely with OASIS to incorporate DSS verification services in its global digital post mark system [UPU DPM].

Also in Spain the “Ministerio de Trabajo y Asuntos Sociales” (Ministry of Labour and Social Affairs) [MTAS], runs a centralized system that verifies digitally signed labour accidents reports. Within the framework on the currently on going initiative for a Spanish electronic ID card [DNIE], the “Ministerio de Administraciones Públicas” (Ministry for Public Administration) [MAP] also runs a platform offering, among others, a centralized service for electronic signatures validation. These two platforms were firstly developed using a proprietary protocol. Without no doubt, all these platforms deployed in different governmental agencies will have to evolve and become DSS-compliant for the sake of interoperability.

By the time this paper is written, the authors know of several commercial systems DSS-compliant that are offered to both private sector and public administrations all over Europe, which demonstrates the timeliness of the effort done by the DSS TC.

Conclusions

The work of OASIS in developing the standard for Digital Signature Services has provided a fruitful alternative to conventional client based PKI systems. The approach has been demonstrated to significantly reduce the cost of the per user installation, whilst features inherent in this approach can improve security.

The use of DSS signing servers have significant advantages. By detaching the authentication of internal end users from security of external keys requirements for revocation can be minimised. Also, by placing the server under central control proper administrative control can be applied to ensure the security of signing keys.

The use DSS verification servers provides straightforward verification of signed documents both on receipt and when retrieved from storage several years later. It can be used to remove the burden of complex certificate path validation from users, and maintain information required

preservation of signatures over a period of up to around 10 years.

The features of DSS make it particularly suited to meeting the requirements of applications such as eInvoicing. DSS matches the need for invoice signing to be controlled on an organisation basis and handles the requirements for verification of stored signed documents.

The DSS specification is at its final stages of ratification. Interoperability trials have been run between separate implementations, and several major implementations are expected to appear over the next year.

Within Europe, and globally, there is significant interest in the use of web based and trusted third party services for the creation of digital signatures. Electronic invoicing is one of the major applications requiring digital signatures which is likely to be a major driver for a cost effective solution to digital signing.

By implementing DSS, the power of digital signatures can be provided without the headaches of installing PKI capabilities at every user system and ensuring signing keys and devices are managed securely.

Acknowledgement

The authors wish to acknowledge the significant contribution made to the members of the OASIS DSS Technical Committee and the ETSI Technical Committee on Electronic Signatures and Infrastructures in developing the ideas represented in this paper.

References

- [VAT Directive] Council Directive 2001/115/EC of 20 December 2001 amending Directive 77/388/EEC with a view to simplifying, modernising and harmonising the conditions laid down for invoicing in respect of value added tax.
http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_015/l_01520020117en00240028.pdf

[CWA 15579] CEN Workshop Agreement “E-Invoices and Digital Signatures”
<http://www.cenorm.be/CENORM/BusinessDomains/businessdomains/iss/cwa/electronic+business.asp>

[OASIS DSS] OASIS Digital Signature Services Technical Committee
http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=dss

[BankID] Bank ID
<http://www.bankid.no>

[EEMA-Award] The eema Award for Excellence in partnership with Infosecurity Today
<http://www.eema.org/static/isse/awards.htm>

[ETSI ESI] ETSI Electronic Signatures and Infrastructures public home page
<http://portal.etsi.org/esi/el-sign.asp>

[UPU-EPM] Electronic Post Mark
<http://www.globalepost.com/>

[W3C XMLDSig] XML-Signature Syntax and Processing, W3C Recommendation 12 February 2002
<http://www.w3.org/TR/xmlsig-core/>

[IETF CMS] Cryptographic Message Syntax (CMS) IETF RFC 3852, R. Housley, July 2004

[RFC 2560] “X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP”, M. Myers et al, June 1999.

[ETSI TS 101 733] Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAeS)

[ETSI TS 101 903]. XML Advanced Electronic Signatures (XAdES)

[ETSI TS 102 734] Profiles of CMS Advanced Electronic Signatures based on TS 101 733 (CAeS)

[ETSI TS 102 904] Profiles of XML Advanced Electronic Signatures based on TS 101 904 (CAeS)

[ETSI TS 102 573] policy requirements for trust service providers signing and/or storing data for digital accounting.

All ETSI documents are available from:
<http://pda.etsi.org/pda/queryform.asp>

[X.509] ITU-T Recommendation X.509: Information Technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks (Latest version 08-2005)

[CATCERT] Agència Catalana de Certificació
<http://www.catcert.cat>

[PSIS] Plataforma de serveis d'identificació i signatura
http://www.catcert.cat/web/cat/1_4_3_plataforma.jsp

[MTAS] Ministerio de Asuntos Sociales.
<http://www.mtas.es>

[MAP] Ministerio de Administraciones Públicas.
<http://www.map.es>

[DNIE] DNI Electronico
<http://www.dnielectronico.es/>
http://www.dnielectronico.es/seccion_aapp/cata.html