

Instituto Superior Técnico
Assinatura Electrónica Qualificada

Daniel Tiago Nave Prata de Almeida
daniel.almeida@ist.utl.pt

November 24, 2009

Resumo

À medida que os documentos vão sendo armazenados em suporte digital, a necessidade das organizações gerirem documentos assinados electronicamente é uma realidade eminente. Esta dissertação aborda este problema actual, identificando os problemas existentes, propondo uma solução e demonstrando a sua exequibilidade através da implementação da solução proposta, um sistema de assinatura electrónica de documentos.

As assinaturas electrónicas são usadas numa vasta área de contextos e aplicações, dando origem a novos requisitos de produtos e serviços relacionados com a assinatura electrónica. Surgiram da necessidade de transpor a tradicional assinatura manuscrita para os documentos electrónicos, colmatando as falhas de segurança existentes, uma vez que a tradicional assinatura manuscrita não é segura, pois é facilmente falsificável e consequentemente não se pode garantir a sua autenticidade nem a sua veracidade.

As organizações necessitam de assinaturas electrónicas seguras que permitam garantir a autenticidade, a temporalidade e o não repúdio dos documentos assinados electronicamente, assim como garantir que estes permaneçam válidos por longos períodos de tempo, mesmo que a segurança de uma assinatura electrónica seja futuramente comprometida.

A interoperabilidade das assinaturas electrónicas tem vindo a ser promovida pela União Europeia (e consequentemente pelo Estado Português), assim como a harmonização do critério legal das assinaturas electrónicas, originando uma *framework* legislativa coerente, promovida através da Directiva Europeia 1999/03/EC, de 13 de Dezembro de 1999, e de outras decisões da Comissão Europeia. Estas medidas pretendem contribuir para a aceitação geral dos métodos de autenticação electrónica, de forma a garantir que as assinaturas electrónicas constituam prova legal em todos os Estados Membros. O recente surgido documento de identificação electrónica português, Cartão de Cidadão, promove o desenvolvimento tecnológico e a modernização administrativa e organizacional. Na sua vertente digital, promove o desenvolvimento das transacções electrónicas dando-lhes a segurança necessária através da autenticação forte e da assinatura electrónica.

Os problemas relativos às assinaturas electrónicas existentes identificados nesta dissertação foram os seguintes:

- Os sistemas de assinatura electrónica tipicamente utilizados, são sistemas proprietários de-

pendentes do sistema operativo e do tipo de documento, oferecendo bastantes limitações quanto à validação da assinatura, pois o receptor da assinatura terá que dispor dos mesmos meios que o assinante de forma a que a possa validar. Esta validação é tipicamente realizada no sistema do utilizador, pelo que o processo de validação poderá ser maliciosamente subvertido, apresentando um estado erróneo de validade da assinatura, induzindo o utilizador em erro.

- Mesmo estando na posse de um certificado revogado ou expirado, é possível realizar uma assinatura forjada temporalmente, realizada no espaço de tempo em que o certificado se encontrava válido, subvertendo desta forma os mecanismos de validação da assinatura. Isto deve-se ao facto de a assinatura ser gerada usando o relógio do sistema operativo máquina local, cujo valor pode ser manipulado.
- Tipicamente uma organização não assina documentos, estes são assinados por um indivíduo pertencente à organização, de forma a que este tenha a responsabilidade inerente à sua concordância. Enquanto o nome do assinante é importante, o cargo do assinante dentro de uma empresa ou organização é tão ou mais importante. Alguns contratos poderão apenas ser válidos se o assinante tiver um determinado cargo dentro da organização (e.g. Director de Compras), ou se o assinante tiver autoridade para assinar determinado tipo de documento.
- Outro problema reflecte-se com a manifestação explícita do compromisso do assinante relativo ao documento que assina quando este não se encontra evidenciado no próprio documento. Uma assinatura deverá ser passível de inclusão do compromisso a que o indivíduo se compromete ao assinar o documento (e.g. aprovo o conteúdo do documento, tomei conhecimento, etc...), para que em caso de disputa não haja dúvidas da intenção do assinante.
- Um algoritmo criptográfico considerado seguro no presente, pode no futuro vir a ser comprometido através do aumento da capacidade de computação ou da descoberta de pontos de falha no algoritmo que permitam obter colisões num espaço mais pequeno. Este ponto é particularmente crítico nas funções de resumo (*cryptographic hash functions*), uma vez que as assinaturas (e.g. RSA) são realizadas sobre o resultado da função de resumo, o que permite a troca do documento por um diferente, mas manipulado, para que a função de resumo produza o mesmo resultado.

A análise destes problemas, permitiu conceber um sistema de assinatura electrónica de documentos, que tivesse em conta os problemas identificados e apresentasse soluções para os mesmos. Desta forma foi possível propor um sistema seguro de assinatura electrónica de documentos, cujas assinaturas garantam propriedades fundamentais como o não repúdio, a autenticidade, a validade a longo prazo e a sua veracidade temporal. A utilização do recente criado cartão de cidadão permitiu a utilização de certificados digitais qualificados na produção das assinaturas, o que confere às assinaturas validade legal em todos os Estados Membros da União Europeia.

Os requisitos a que o sistema proposto deverá obedecer são os seguintes:

- Fornecer ao utilizador um mecanismo simples de criação de assinaturas electrónicas, necessitando apenas de um *web browser*, e utilizando mecanismos seguros que possam ser mantidos sob o seu controlo.
- Permitir ao utilizador realizar uma assinatura electrónica qualificada de um documento electrónico, produzindo um documento num formato bem definido e normalizado que contenha o documento electrónico assinado e a assinatura, assim como permitir ao utilizador a sua validação (local e remota) e verificação WYSIWYS (*What you see is what you sign*) do conteúdo assinado antes da sua submissão ou partilha electrónica.
- No contexto de uma organização, permitir ao utilizador a submissão electrónica do documento assinado num sistema de notariado da organização, que atestará as propriedades qualificantes reclamadas pelo indivíduo, contra-assinando a assinatura inicial e as propriedades qualificantes, produzindo uma assinatura que possa ser facilmente validada por terceiros.
- Permitir à organização a validação temporal, o armazenamento, e a protecção a longo prazo da veracidade das assinaturas, recorrendo a carimbos temporais electrónicos (*Trusted Timestamping*).

Na solução proposta, o indivíduo titular de um certificado qualificado para assinatura electrónica qualificada de documentos, presente no seu cartão de cidadão, utiliza-o de forma a assinar electronicamente um documento mediante a sua vontade, utilizando o seu PIN pessoal da assinatura digital. Este processo é realizado numa aplicação segura de criação de assinatura que se executa no computador do indivíduo, onde este escolhe qual o documento a assinar,

podendo visualizar o seu conteúdo (WYSIWYS), escolhendo a qualidade (i.e. o cargo do indivíduo na organização) em que deseja assinar o documento e outras propriedades qualificantes, assinando-o. Opcionalmente poderá incluir na assinatura um carimbo temporal, de forma a atestar a temporalidade da mesma. Deverá opcionalmente, validar pelos seus meios o valor da assinatura do documento e do conteúdo assinado, e/ou poderá efectuar uma validação on-line. De seguida deverá submeter a assinatura para o sistema de notariado da organização, de forma a que esta possa atestar as suas qualidades.

O sistema de notariado da organização aceita documentos assinados electronicamente por indivíduos pertencentes à organização, e efectua a validação da assinatura e das suas propriedades, atestando a sua veracidade através da realização de uma contra-assinatura. Este sistema é responsável pela validação da assinatura, do certificado utilizado na assinatura e da sua hierarquia de certificação, pela validação temporal da assinatura validando a data na qual o assinante diz ter criado a assinatura, e pela validação das propriedades qualificantes reclamadas pelo assinante, como o cargo do indivíduo na organização e o seu compromisso relativamente ao documento assinado.

Este sistema de notariado recorre a um sistema de certificação temporal, de forma a acrescentar à assinatura um carimbo temporal, isto é, uma prova temporal não repudiável. A produção da contra-assinatura da organização poderá ser realizado através de um processo manual, dependendo dos requisitos existentes para o tipo de assinatura em questão.

O sistema de arquivamento tem como função arquivar os documentos e as suas assinaturas, protegendo-as a longo prazo contra algoritmos de segurança que no futuro se tornem fracos e contra pares de chaves criptográficas cuja segurança tenha sido comprometida. Este processo realiza-se através da adição de sucessivos carimbos temporais à assinatura, periodicamente ou sempre que seja necessário, de modo a proteger carimbos temporais anteriores. À semelhança do sistema de notariado recorre também a um sistema de certificação temporal.

Uma assinatura electrónica de um documento no contexto organização poderá ser considerada válida numa das seguintes situações, dependendo dos requisitos organizacionais:

- Quando o documento se encontra assinado por um indivíduo através de uma assinatura digital qualificada, e quando existe uma contra-assinatura da organização que ateste as propriedades qualificantes da assinatura inicial. Esta contra-assinatura da organização deverá

ser certificada por uma entidade externa confiável a terceiros que efectuem a validação, ou deverá ser estabelecida uma relação de confiança com a organização e consequentemente com o certificado utilizado pela mesma na realização da contra-assinatura. A aposição de pelo menos um carimbo temporal não repudiável é essencial para garantir a temporalidade da assinatura.

- Quando o documento se encontra assinado por um indivíduo através de uma assinatura digital qualificada, e quando existe na assinatura um carimbo temporal não repudiável (e da confiança da organização) que ateste a data de criação da assinatura. Em caso de litígio entre o assinante e a organização, as disputas sobre a validade ou não da assinatura terá que ser feita à posteriori, verificando se na data em que foi realizada a assinatura o assinante teria poderes para tal. Este tipo de assinatura simplifica o processo de assinatura na medida em que dispensa um serviço de notariado. É particularmente útil para assinaturas de documentos utilizados apenas dentro da organização, isto é, não partilhados com terceiros (i.e. entidades externas).

O sistema de assinatura electrónica qualificada de documentos descrito foi implementado, dando origem a um protótipo funcional baptizado de AEQ Docs. A utilização deste sistema requere apenas o uso de um *web browser* com suporte para Java SE 6 e da Aplicação do Cartão de Cidadão instalada (i.e. middleware do cartão de cidadão), sendo compatível com os sistemas operativos Windows, MacOSX e Linux. A utilização deste sistema necessita também de um leitor de *SmartCards* compatível com a norma ISO 7816. A implementação do sistema proposto foi realizada utilizando vários módulos *standalone*, sendo cada um deles responsável por uma parte das funcionalidades. Todos estes módulos, à excepção da Web Application foram implementados na linguagem de programação Java.

O sistema de assinatura proposto é uma *web application* independente do sistema operativo, oferecendo uma boa facilidade de integração e implantação num qualquer contexto organizacional. Este sistema foi implementado recorrendo única e exclusivamente a tecnologia *Open Source*. Este sistema permite a realização de assinaturas electrónicas qualificadas de qualquer tipo de documento passível de representação digital.

As assinaturas produzidas neste sistema incorporam outras propriedades qualificantes, como o compromisso do assinante relativamente ao documento assinado, ou o cargo (i.e a qualidade)

do assinante numa organização. As assinaturas incorporam também mecanismos de protecção da sua validade a longo prazo, no caso em que a segurança tenha sido comprometida, pelas mais diversas razões. O formato sugerido e adoptado para as assinaturas, é o formato XAdES uma extensão das assinaturas XMLDSig, que se encontra normalizado.

O protótipo AEQ Docs, atingiu todos os objectivos propostos e satisfez os requisitos enunciados, resultando num sistema de assinatura qualificada de documentos com aplicabilidade numa organização. Os seus componentes, fornecem também a possibilidade de realizar assinaturas fora de um contexto organizacional (i.e. pessoal), realizando assinaturas electrónicas qualificadas de qualquer tipo de documento utilizando o cartão de cidadão, tendo essas assinaturas valor legal em todos os estados membros da União Europeia.

Conclui-se que o formato XAdES, apesar de ser ainda pouco adoptado, reúne todas as condições necessárias à produção de assinaturas electrónicas que englobem um diversificado leque de propriedades qualificantes. A extensibilidade do XAdES é o seu ponto forte, podendo uma assinatura com determinado perfil ser actualizada. Os diversos perfis do formato XAdES permitem a protecção da validade das assinaturas a longo prazo, quer pela adição de sucessivos carimbos temporais e/ou de contra-assinaturas, e simplificam o processo de validação.

Apesar do RSA ser um algoritmo seguro para a realização de criptografia de chave pública, é necessário ter especial cuidado com as funções de resumo utilizadas e com a sua segurança. Isto deve-se ao facto de apenas o resumo do documento ser assinado, e não o documento em si, o que pode levar à criação de um documento diferente mas que produza um resumo igual. Este facto iria permitir a substituição do documento por um diferente, sem comprometer a validade da assinatura, o que não é de todo desejável.

Conclui-se que o sistema proposto é exequível, o que foi demonstrado através da implementação do protótipo AEQ Docs, mas que para ser colocado em produção necessita de algumas modificações, por exemplo, para contemplar a autenticação e a autorização dos seus utilizadores, e adicionalmente manter um registo seguro de todas as acções realizadas pelo sistema e qual o seu autor. Este sistema tenta transparecer todo o processo de produção e validação de assinaturas no formato XAdES, de forma a eliminar o conceito de *black box* existente no processo de assinatura de documentos, permitindo uma melhor compreensão de todo este processo.

Palavras Chave

Keywords

Palavras Chave

Assinatura Electrónica Qualificada

Cartão de Cidadão

Certificados X.509

Documento Electrónico

Não Repúdio

Segurança Electrónica

XAdES

Abstract

As documents are being stored in digital form, the need for organizations to manage documents electronically signed is an imminent reality. This thesis addresses this actual problem, proposing a solution and demonstrating its feasibility through implementation of the proposed solution, an electronic signature system for documents.

Electronic signatures are used in a wide area of contexts and applications, giving rise to new requirements for products and services related to electronic signatures. They arose from the need to implement the traditional handwritten signature for electronic documents, closing the existent security gaps, as the traditional handwritten signature is not secure because it is easily falsifiable, and therefore can not guarantee its authenticity or its accuracy.

Organizations need secure electronic signatures to guarantee authenticity, temporality and non-repudiation of electronically signed documents, as well as ensure that they remain valid for long periods of time, even if the security of an electronic signature is compromised in the future.

The interoperability of electronic signatures has been promoted by the European Union (and subsequently by the Portuguese State), as the harmonization of the validity criterion of electronic signatures, resulting in a coherent legislative framework, promoted by the European Directive 1999/03/EC, of 13 December 1999, and other decisions of the European Commission. These measures aim to contribute to the general acceptance of electronic authentication methods in order to ensure that electronic signatures constitutes a legal tender in all Member States. The recently emerged Portuguese electronic identification citizen card (Cartão de Cidadão), promotes technological development and the modernization of administrative and organizational contexts. In its digital form, the citizen card promotes the development of electronic transactions by giving them the necessary security through strong authentication and electronic signatures.

The problems with existing electronic signature identified in this thesis were:

- The electronic signature systems typically used, are proprietary systems dependent on the operating system and the type of document, providing many limitations on the validation of the signature because the signature receiver has to have the same means that the signer so that he may validate it. This validation is typically performed in the user's system, so the validation process can be maliciously subverted, showing a wrongful state of validity of the signature, inducing the user in error.

- Even being in possession of an expired or revoked certificate, it is possible to perform a forged signature temporarily held in the time where the certificate was valid, thereby subverting the mechanisms for signature validation. This is due to the fact that a signature is generated using the clock on the local host operating system, whose value can be manipulated.
- Typically an organization does not sign documents, these are signed by an individual in the organization, so that he has the responsibility inherent to his signature. While the signer's name is important, the position of the signer within a company or organization is as or more important. Some contracts may only be valid if the signer has a particular position within the organization (e.g. Purchasing Director), or if the signer has the authority to sign certain type of document.
- Another problem is reflected in the explicit expression of commitment of the signer who signs the document when it is not evidenced in the document itself. A signature should be open to inclusion of the commitment that the individual undertakes signing the document (e.g. I approve the contents of the document, I have readed, etc. ...), so that in case of dispute there is no doubt in the intention of the signer.
- A cryptographic algorithm considered safe today, may in future come to be compromised by increasing computing power or the discovery of points of failure in the algorithm which allow to obtain collisions in a smaller search space. This is particularly critical in the digest functions (cryptographic hash functions), since the signatures (e.g. RSA) are performed on the outcome of the digest function, which allows the document exchange for a different one, but manipulated so that the digest function produces the same result.

The analysis of these problems, allowed to design a system for electronic signature of documents, which takes into account the identified problems and provides solutions for them. This made it possible to propose a secure system of electronic signature of documents, whose signatures guarantee fundamental properties such as non-repudiation, authenticity, validity and long-term temporal validity. The use of the newly established citizen card allowed the usage of qualified digital certificates in the production of signatures, which renders the signatures legally valid in all Member States of the European Union.

The requirements that the proposed system must meet are:

- Provide the user a simple mechanism for creating electronic signatures, requiring only a web browser, and using secure mechanisms that can be kept under user control.
- Allow users to perform a qualified electronic signature of an electronic document, producing a document in a well-defined and standardized format which contains the signed electronic document and signature, as well as allow the user to validate the signature (local and remote) and to WYSIWYS (What you see is what you sign) verify the signed content before submission or electronic sharing.
- In the context of an organization, allow the user the electronic submission of the signed document in an organization notary to certify the qualifying properties claimed by the individual, counter-signing the signature and the qualifying properties, producing a signature that can be easily validated by third parties.
- Allow the organization to validate temporal veracity, the store, and the long-term protect the veracity of signatures, using electronic time stamps (Trusted Timestamping).

In the proposed solution, a person holding a certificate eligible for qualified electronic signature of documents present in his citizen card, uses it in order to electronically sign a document at his own will, using his digital signature personal PIN. This process is conducted in a safe signature creation application that runs on the individual's computer, where he chooses which document to sign and can view its content (WYSIWYS), choosing the quality (i.e. the role of the individual in the organization) in which he wants to sign the document and other qualifying properties, signing it. Optionally he can include a time-stamp in the signature in order to demonstrate the document temporality. Should optionally validate by his means the value of the document signature and the signed content, and / or may perform an on-line validation. Next he should submit the signature for the notary system of the organization so that it can attest his qualities.

The notary system of the organization accepts electronically signed documents by individuals belonging to the organization, and performs signature and their properties validation, attesting to its accuracy by performing a counter-signature. This system is responsible for validating the signature, the certificate used for signing, and its certification hierarchy, validating signature temporality by validating the date on which the signer claims to have created the signature and

the validation of qualifying properties claimed by the signer, as the role of the individual in the organization and its commitment to the signed document.

This notary system uses a temporal certification system, in order to add the signature time-stamp, that is, a temporal non repudiable evidence. The production of the organization counter-signature can be accomplished through a manual process, depending on the existing requirements for the type of signature in question.

The archiving system has the function of archive documents and their signatures, protecting them in the long-term against security algorithms that may become weak in the future and against pairs of keys whose security has been compromised. This process is carried out by adding successive time stamps to the signature, periodically or whenever necessary, to protect previous time stamps. Like the notary system, the archiving system also uses a system of temporary certification.

An electronic signature of a document in the context of an organization can be considered valid in the following situations, depending on the organizational requirements:

- When the document is signed by an individual through a qualified digital signature, and when there is a counter-signature of the organization certifying the qualifying properties of the initial signing. This counter-signature of the organization must be certified by an external trusted entity by third parties that need to carry out the validation, or there should be a trust relationship with the organization and therefore with the same certificate used to produce the counter-signature. The inclusion of at least one time stamp is essential to ensure the temporality of the signature.
- When the document is signed by a person through a qualified digital signature, and when there is a non refutable time stamp (of the organization's trust) stating the creation date of signature. In case of dispute between the signer and the organization, disputes about the validity of the signature must be made after by checking that the date on which the signing was held the signer would be able to do so. This type of signature simplifies the process of signing, as it dismisses a notary service. It is particularly useful for signatures on documents used only within the organization, that is, not shared with third parties (i.e. external entities).

The system of qualified electronic signature of documents described has been implemented,

resulting in a functional prototype dubbed AEQ Docs. The use of this system requires only the use of a web browser that supports Java SE 6 and the citizen card application installed (i.e. citizen card middleware) and is compatible with Windows, Mac OS X and Linux operating systems. The use of this system also needs a SmartCard reader compatible with ISO 7816. The implementation of the proposed system was performed using several stand-alone modules, which are each responsible for one of the features. All these modules, except the web application was implemented in the Java programming language.

The signature system proposed is a web application that can be used regardless of operating system, offering a good ease of integration and deployment in any organizational context. This system was implemented using solely Open Source technology. This system allows the creation of qualified electronic signatures of any document capable of digital representation.

The signatures produced in this system incorporate other qualifying properties as the commitment by the signer relative to the signed document, or the role of the signer in an organization. The signatures also incorporate mechanisms to protect their validity in the long term, in the case where security has been compromised, for any different reasons. The suggested format adopted for the signatures, is XAdES an extension of XMLDSIG signatures, which is standard.

The AEQ Docs prototype, achieved all the proposed objectives and satisfied the stated requirements, resulting in a system of qualified signature of documents with applicability in an organization. Its components also provide the possibility of producing signatures outside an organizational context (i.e. personal context), making qualified electronic signatures for any document using the citizen card, and producing signatures that are legally valid in all member states of the European Union.

It is concluded that the XAdES format, although still not widely adopted, meets all the conditions necessary for the production of electronic signatures that cover a diverse range of qualifying properties. XAdES extensibility is its strongest point, enabling a signature with a specific profile to be updated. The various profiles of the XAdES format allow to safeguard the validity of signatures in the long term, by the addition of successive time stamps and / or counter-signatures, and simplify the process of validation.

Although the RSA algorithm is a secure algorithm for the conduct of public key cryptography, it is necessary to take special care with the used digest functions and their safety. This is due to the fact that only the digest of the document is signed, not the document itself, which

can lead to the creation of a different document that will produce the same digest. This would allow the replacement of the document by a different one, without compromising the validity of the signature, which is not desirable at all.

It is also concluded that the proposed system is feasible, as demonstrated through the implementation of the AEQ Docs prototype, but to be put into production it requires some modifications, for example, to include authentication and authorization of users, plus keep a secure record of all actions performed by the system and its author. This system attempts to disclose the entire process of production and validation of signatures in the XAdES form in order to eliminate the black box concept that exists in the process of signing documents, allowing a better understanding of the process.

Keywords

Digital Qualified Signature

Cartão de Cidadão

X.509 Certificates

Electronic Document

Non repudiation

Electronic Security

XAdES