Implementation of Digital Signature Solution

Nuno Filipe Jorge Guedes

Extended Abstract

April, 2008
1. Introduction

The scope of this study points to security area and has its own focus on digital signatures over documents.

In nowadays Portugal is giving the first steps towards the creation of an infrastructure of support to qualified digital certificates. The recent initiatives with the National Government Electronic Certification System (SCEE) or the latest Citizen Single Card as draw attention to digital signatures reflecting a window of opportunity for spreading its use and featuring generalization.

With the massive usage of personal digital certificates, obtained through the Citizen Card, seek to broaden the use of them not only to interact with the services of the state but also with other entities that need to guarantee the authenticity, integrity and non-repudiation of data exchanged with customers. Banks are a clear example of such entities.

2. Problem to Solve

Today, even with the use of digital certificates, there's not a single solution, widely known, that ensures the legal value of documents digitally signed. There exists some secure web applications, which allow the deal of state issues such as the declaration of IRS, but they are not using the potential of digital signatures on the documents and their receipt.

The Citizen Card has two certificates: one for authentication and another for the creation of digital signatures. Thus is eliminated a problem that came to see: the acquisition of qualified certificates for personal use. The focus of the problem now lies in the application of signing certificates because it doesn't exist, so far, a solution to achieve integration of digital signatures with various business contexts and that is considered a reference in the area.

This thesis seeks to identify the mechanisms and technologies to be used in the submission via the Internet of digitally signed documents that serve as substitutes of documents signed on paper. As a result, it is expected to reach a solution which manipulates digital signatures representing a kind of "middleware" between web applications from different business contexts and its users (Figure 1).

![Figure 1 - Solution as "middleware" between users and business](image-url)
The solution should be as generic as possible to facilitate integration with various applications of different business areas.

The solution must ensure the execution of basic digital signatures functionalities, sign and verify, and also the extraction of the original document from the signed version and the acquiring of signed document with only the signatures desired by the user. Any type of document can be signed (XML, text file, image, etc.).

Special attention should be paid to the architecture for ensure the use of the system in several scenarios and maximize safety. The creation and the verification of signatures and the association between the digitally signed document and the original document are crucial to ensure the properties inherent to digital signatures. Thus, in order to ensure greater security, the proceedings shall be executed as much as possible under the control of the user, preventing communication with external entities and reducing the threat of imminent capture and manipulation of messages.

The solution must be complied with latest standards, taking special attention to EU directives and national legislation. This requirement implies the use of XAdES (version 1.3.2) as format of digital signatures and the support for all levels of the same.

3. State of the art

3.1. Solutions

Some existing solutions that could solve the problem in question were analyzed:

- OpensTrust-SPI, OpenTrust (OpenTrust-SPI)
- WebSign Project (Cardon de Licthbuer)
- TrustedX, Safelayer (Safelayer)

The solutions for integration of digital signatures in web applications are reduced. Additionally if we eliminate those that don’t support XAdES we obtain an even lower number.

The solutions that were studied are a sample of the existent universe. After the examination of each one is clear that none responds effectively to the aimed objectives closest ones do not allow the addition of development.

Faced with this analysis is possible to conclude that none of the solutions presented is a valid option to resolve the issues proposed. Thus, it becomes evident the need to develop a customized solution. This option leads to the interest for analysis of libraries that manage XAdES signatures.

3.2. Libraries

There exist some libraries on the market for the manipulation of digital signatures. The follow ones were studied:

- OpenXAdES (OpenXAdES)
- IAIK XML Advanced Electronic Signatures (IAIK)
- DContract Core: Digital Contract Core Library (DContract)
- SecureBlackbox, EldoS (EldoS - SBB)
Although there are other libraries to support XAdES, these were the ones that seemed more appropriate to face the proposed problem.

Among analyzed libraries there are two that stand out clearly, the one provided by IAIK and the one supplied by EldoS. Despite the SecureBlackbox entail a greater effort to support the higher levels of XAdES, factors such as the possibility of obtaining the trial version without functional limitations or its low cost, in a potential purchase, compared with its rival, were instrumental in its choice. The effort referenced can be offset by the extensive documentation provided by EldoS.

4. Developed Solution

In the absence of a solution that met all the objectives proposed, it was developed, in this dissertation, a customized solution using a set of libraries of EldoS for XAdES support.

The picture that follows (Figure 2) presents the architecture of the developed solution. The implementation of the solution in various scenarios would only lead to the replacement of the module “Business” by the module corresponding to the desired scenario, without changing the surrounding architecture. Thus it’s guaranteed one of the objectives proposed: the solution must be as generic as possible to be integrated in several scenarios.

![Figure 2 - Architecture of the solution developed]

The module of the solution consists in four components: SignerUserControl, VerifierUserControl, AdvancedDigitalSignatureWS and StorageWS.
4.1. SignerUserControl

The SignerUserControl is a Windows Control Library that is materialized as a dynamic-link library (DLL). It is embedded in a web page and its main feature is the creation of signatures through interaction with the module SecureBlackbox of EldoS.

This component will run in the user’s machine and arises from the need to ensure that the creation of signatures takes place in a secure form.

The SignerUserControl presents an interface (Figure 3) that can be broken into four areas, which are highlighted in the figure and presented below:

1) Details of the document target of the signature;
2) Certificates available to create the signature;
3) Signature configuration showing the different levels of XAdES and ensuring the dependencies between the various levels;
4) Name of the target document in the form of link. The selection of the same provokes the contents display of the document to sign.

4.2. VerifierUserControl

The VerifierUserControl is very similar to SignerUserControl only differing in functionality. This component main functionality is the verification of signatures, but also allows the extraction of the original document from signed file and gets a document signed only with the signatures desired by the user.
The VerifierUserControl presents an interface (Figure 4) that can be decomposed into six areas, which are highlighted in the figure and presented below:

1) Details of the document target of the signature;
2) Signatures affixed to the document, for each signature appears the name of the subscriber, the name of the certification authority, the date on which the signature was created, a link to cause the verification of signatures and the state of signature validity;
3) Checkboxes for signatures selection. They are directly linked to the "Get File With Signatures" ("Obter Ficheiro Com Assinaturas") (4);
4) Link to get the signed file with the signatures previously selected (3);
5) Link to obtain the original document;
6) Details of the verification of a signature, provides information on the signature and its first counter-signature, if exists. They are actualized after being selected the link "Check" ("Verificar") (2) associated with a signature.

![Graphical interface of VerifierUserControl](image)

**4.3. AdvancedDigitalSignatureWS**

The AdvancedDigitalSignatureWS is a Web Service whose primary purpose is the handling of files containing signatures, in particular it’s responsible for validating and counter-signing signed documents. Meets the objectives proposed by interactions with the module SecureBlackbox of EldoS.
4.4. StorageWS

The StorageWS is a Web service that provides the basic functionality of a file repository (add, delete and get). This is a temporary repository because it stores only documents signed by a short period of time. This Web Service only exists as result of storage limitation regarding variables in javascript.

4.5. Signed Documents Format

As one of the requirements was the possibility of sign any type of file it has been established a format for the signed documents.

The developed format is based on XML document because the signatures XAdES are only applied to such documents. The structure starts with a root element with the name SignedBinaryFile under which it is created another element designated as BinaryData that has as value the contents of the document to sign on the base 64 binary format. This last element has an attribute "Id" filled with the name of the document target of signatures, allowing the extraction of the target document with its original name. Through the attributes of this element it could be stored more information about the original document, if necessary.

The signatures created on the document are added to the root element SignedBinaryFile because they are enveloped signatures.

5. Validation

The developed solution has fulfilled all the objectives that were set initially. However it has some limitations properly documented.

The created signatures were successfully validated, assuring a platform of understanding, the so-called policy of use.

The modules for create and validate signatures are executed on the user’s machine, thus ensuring greater security.

Any type of file can be target of signing thanks to the implemented format for signed documents.

The solution guarantees compliance with the standards and legislation in force, including technical specification for XAdES 1.3.2 (ETSI).

The solution was successfully applied for two different scenarios. First was implemented in eBanka, a system for home banking, and successfully validated by a set of use cases. Later it was integrated with eDoc, a document management system. The SharePoint and an application of workflow are the future testing scenarios.

The use of both applications, eBanka and eDoc, integrated with the developed solution, ensured the acceptance of the solution.
6. Conclusions

Over the work produced in conjunction with the results obtained there can be drawn some conclusions.

The library used to support XAdES, the SecureBlackbox, supports all levels of the format but for those above the XAdES-T requires some effort. This effort was facilitated by the extensive and diverse support information, through the specifications, tutorials or even the forum. However, the crucial point was the verification of signatures given the surrounding complexity. Is in this critical process that there is still a lack of information. I personally think that the existing information in the technical specification of XAdES is insufficient.

The two components developed for creating and verifying signatures, which will run on the user's machine, have major limitations because they are only supported by Internet Explorer and force a particular configuration in the environment system. Because of the technical impossibility to transfer the contents of the document signed by SignerUserControl for the business layer it was necessary to include a temporary repository and, consequently, additional security measures.

Through the practical use of the signature features on the two scenarios it was possible to withdraw some conclusions regarding the relation between the document size and the time taken to validate and counter-sign it. The documents in eBanka are usually transactions applications like wage payments translating into reduced size files and with a maximum of four signatures. The documents size in eDoc is relative, there may be documents with a few Kb and others with some Mb, adding the possibility of being signed numerous times. In the latter scenario was possible to identify situations where the validation of signatures for a document, with about 1 Mb and two signatures, and the addition of a counter-signature were extended by more than 3 minutes, which is not at all bearable by all users. Notice that in the scenario described the chains of certification only has two certificates and Certification Authority is in the internal network. In normal environment the time would increase. This is a negative point to be considered and that has the power to require a weighting to signing documents known as "heavy", threatening the common use of signatures as it was desired.

The area of digital signatures is still maturing and, as such, are expected major developments in short term. For the solution presented in this thesis it becomes interesting to pay attention to any new technological develop that may create an alternative to the components of creation and verification of signatures (Windows Control Library), solving existing limitations, and to any addition or modification of information associated with the process of verification of digital signatures.
7. References


ETSI. *ETSI TS 101 903 v1.3.2.*


