Digital Signature Solution for Document Management Systems - The University of Trás-os-Montes and Alto Douro

Cláudio Pereira, Luís Barbosa, José Martins, Jorge Borges

Universidade de Trás-os-Montes e Alto Douro, Vila Real, Portugal
{cpereira, lfb, jmartins, jborges}@utad.pt

Abstract. The University of Trás-os-Montes e Alto Douro (UTAD), in an effort to streamline processes and reduce bureaucracy, decided to develop and use an in-house document management system to handle processes. However, this practice created additional needs such as the actual digital signing of documents associated with the institution business and administrative processes. This paper explores a solution proposal to this problem, documenting what are its functionalities and how it works. An initial application of the developed solution is also described and analyzed in order to demonstrate the overall adequacy of the proposed artefact and its overall impact to the institution administrative operations.

Keywords: Digital signature, Document management, Multi OS, UTAD

1 Introduction

The changes undergone by the paradigms adjacent to productive processes, especially during the last two decades, have significantly altered the way in which society and organizations view available information. The increasing use of Information Technologies, both professional and socially, was one of the greatest catalysts for these changes [1].

Documents often store important information, with existing literature stating that documents represent between 80 and 90% of an organizations' information [2]. Thus, managing such volumes of information is very important, and technologic Document Management Systems (DMS) are important tools to maximize the value of such huge amounts of information [3].

A considerable number of documents generated at the University of Trás-os-Montes e Alto Douro (UTAD) have origin on a DMS named GesDoc, developed in-house by the Informatics and Communications Services (SIC). This system is being improved over time, and is gradually replacing traditional document management. In the same way traditional documents can be easily authenticated with a signature on paper, benefitting from legal validity, it is critical to achieve the same result on digital documents. Digital signatures are one approach to this necessity, allowing for a trustworthy identification of the signer, integrity verification and non-repudiation

[4][5][6], as well as improving the efficiency and security of transactions, and enhancing collective approvals in a fraction of the time traditional signatures would take [7].

Both Portuguese law [8] and European Union regulations [9] define the conditions to be met for digital signatures to have any legal value, from the device used to create such signatures to the certificates used and their issuers. Signatures that satisfy the conditions imposed are referred to as "qualified digital signatures". Portuguese citizens bear an identification document able to create qualified signatures called Citizen Card (CC). The CC is a mandatory identification document with both traditional and electronic aspects, allowing its bearer to prove his identity by reading elements visible on the card, or electronically through electronic authentication and qualified digital signature [10].

Thus, to address the problem of authenticating digital documents on a technologic DMS, it is proposed a digital signature solution using the Portuguese CC, being then described and analyzed.

2 Literature review

There were identified some digital signature implementations, both with and without the CC. One of such implementations uses the CC to sign documents with the final grades of students of ISCTE – University Institute of Lisbon [11]. This solution substitutes the traditional signing with digital signing on an already established workflow. Another implementation, documented by the same author, uses digital signatures to sign account opening documents on a bank [11]. In this case, the documents are signed by the client on a tablet device with a stylus and, after that, signed by the system with a certificate. The last case refers to a solution for the exchange of invoice information between companies of the same organization, but with distinct Enterprise Resource Planning systems [12]. The author describes a system in which the companies submit the invoice information being, after that, generated signed XML and PDF documents to be accessed by a website.

UTAD also has the need to implement digital signature into its DMS. The adoption of one of the existing solutions is not viable due to their characteristics. The first presented solution is based on web browsers and the technology used to its implementation is not specified, neither whether browsers still support it. The second one could potentially subvert the validity of a digital signature, making its legal value unclear. Finally, the third does not sign documents with a device users already have, like the CC. Additionally, SIC usually develop and implement specialized information systems, such as a student management system [13][14] and a scholarship management system [15], among others.

Thus, UTAD chose to develop a custom solution. This paper proposes a solution to UTAD's problem using the Portuguese Citizen Card and the existing DMS.

3 Case Study

Over time, UTAD has generated a great number of paper documents, most of them signed by interested parties and people with decision power within the institution. From hiring of staff, signed by the rector, among others, to the acquisition of goods and services, signed by the Financial and Patrimonial Services, for example, every signature was made the traditional pen and paper way. However, factors such as the proliferation of digital information systems and their adaptability led to a gradual change in the way UTAD creates and consumes documents. Currently a considerable part of the generated documents has its origins in a DMS called GesDoc, designed and developed by the SIC.

Originally, GesDoc was only responsible for processes without expense, but the need to handle processes with expense digitally led to its implementation. However, the approval and authentication of documents on a digital system became a problem. Traditionally, a paper signature would legally authenticate a document, but that is not an option for digital documents. Considering the system's ability to store digital documents in the long term, it is required to be able to read and validate them over time. In addition, a traditional signature does not guarantee the integrity of a document, offering no protection against tampering. Such protection is very desirable on UTAD's system. These requirements are also transversal to the institution, and may exist not only in GesDoc but also in any current or future information system or DMS. An example of future systems that may benefit from digital signature in the UTAD would be the integration with the Public Administration Interoperability Platform. This is a service-oriented platform, with goals such as providing the Public Administration with tools to interconnect systems, process payments, send messages and other electronic services. Given this, the authentication, integrity validation and non-repudiation of electronic documents in the institution are challenges that the proposed solution seeks to overcome, the following requirements are identified: 1: Provide electronic documents with a legally binding authentication mechanism; 2: Guarantee a document's integrity after it has been created; 3: Offer a mechanism that allows the long-term validation of the authenticity and integrity of electronic documents; 4: Enable the use of these features from web platforms and through any of the more common operating systems (Windows, Linux and MacOS); 5: Provide a way to integrate the proposed solution with existing or later adopted information systems.

In addition to these requirements, a specific case exposed an additional problem regarding the performance evaluation of teachers. This evaluation is carried out on a platform developed for this purpose, and the documents resulting from these evaluations must be signed one by one by the rector. However, the volume of documents to sign up to can easily go up to a few hundreds. With that in mind, a further requirement arises: 6: Provide a functionality that allows a convenient way to sign many documents in series.

Given the requirements presented, and considering that the transition from traditional to electronic documents is already a reality in UTAD, it is urgent to provide a solution that can solve these problems.

4 Solution Proposal

To meet the needs of the University, considering the requirements documented previously, it was proposed a solution named "Assinatura Digital UTAD" (ADUTAD), or "Digital Signature UTAD". It is a desktop solution for Windows, macOS and Linux that can be integrated both with web and desktop platforms, and allows users to make qualified digital signatures on PDF documents with their Portuguese Citizen Card.

4.1 Architecture

Originally, the proposed solution was implemented as a Java applet on a browser. This allowed the application to benefit from a few advantages, like being possible to sign documents without installing the application, having the applet readily available after the webpage loads, triggering the execution of the applet's public functions using JavaScript or calling the host website's JavaScript code on demand. However, issues such as frequent Java configurations blocking applets and, more importantly, the cessation of support by browsers such as Google Chrome and Mozilla Firefox led to a change in the way the application is provided. Therefore, a change was made to the proposal, having it be a desktop application with an assigned custom protocol handle named "utadsign". With this handle, it is possible to set the desktop signing application as the default application to process URL addresses beginning with "utadsign:", allowing a website to launch the application and provide it with parameters relative to the signature.

Regarding the functional part of the proposed solution, the following diagram exemplifies the steps necessary to make a regular digital signature on GesDoc.

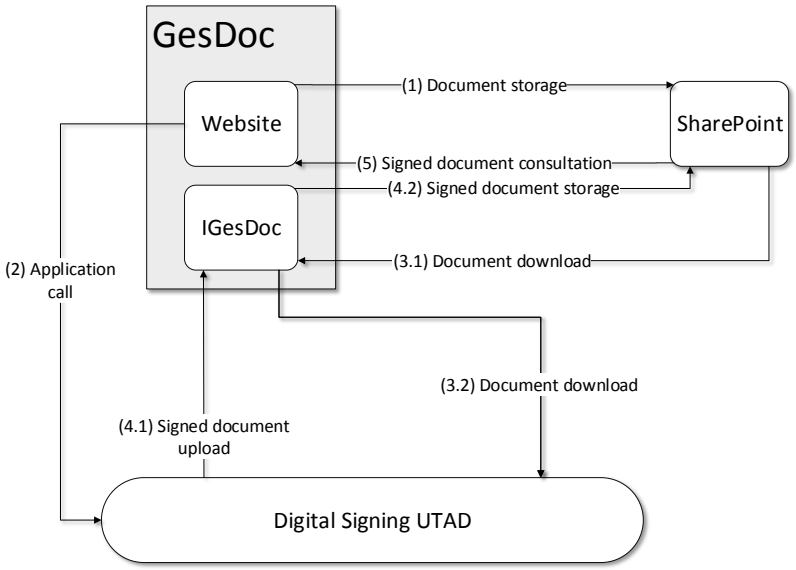

Fig. 1 – Workflow diagram of the solution proposal on GesDoc

The normal operation of a digital signature on GesDoc can thus be described as follow: (1) GesDoc generates the document in the PDF/A-3 archive format and stores it on the SharePoint server; (2) the website calls the signing application, providing parameters such as the download address to obtain the document, and the upload address that expects the signed document; (3) the application requests the document from IGesDoc, which in turn obtains it from the SharePoint server, signs it with the user's Citizen Card and attaches Long Term Verification (LTV) information to the signature; (4) the signed document is returned to the web service, being stored in SharePoint afterward; (5) with the file properly signed and stored, GesDoc makes it available on the relevant process.

Over time, it became apparent that it could be interesting in the future to allow the application to be used by systems other than GesDoc. The application was stripped from every specific GesDoc instruction, such as finalizing processes and a few minor others. The result was a simpler application, performing just the actions it was designed to. Such result allowed for a simplification of its launching parameters, not needing GesDoc specific parameters anymore. Removing these unnecessary parameters lets the application function with just the download and upload URL parameters to obtain and return the relevant file, an URL for version checking, and optional parameters such as the location of the signature. Therefore, any generic system can take advantage of the application with a few eventual adjustments.

Currently, GesDoc does not require the application to sign multiple documents in series. However, the teacher evaluation platform generates a large number of documents that need to be signed without inserting a PIN for every single one of them. The workflow is roughly similar to a regular signature, with a few key differences. The following diagram illustrates the process of signing multiple files in series on a generic system.

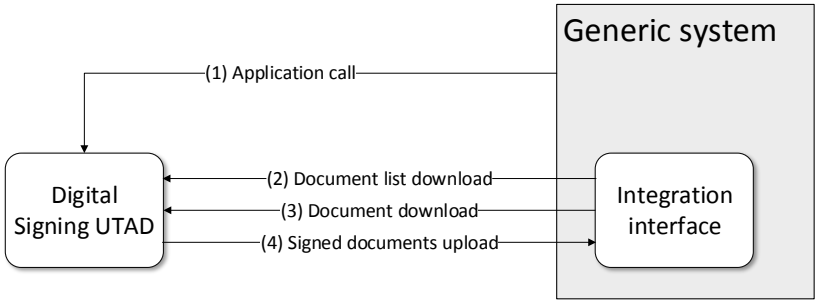

Fig. 2– Workflow diagram of the solution proposal on GesDoc

First, the application needs to know where to fetch the documents that are to be signed. This is accomplished by passing a web address as a parameter to the application. A request to this web address yields structured data with the download and upload addresses of the files to be signed. Because the number of files to sign in one go can ascend to a few hundreds, this approach circumvents any URL limit in place by passing the list as data from a web request. The rest of the workflow is similar, downloading, signing and uploading every file in the list.

4.2 Components Description

In order to better understand the workflow described above, it is useful to globally understand the components that constitute the different parts of the proposed artefact. The Digital Signature UTAD application represents the main deliverable of the project, and is responsible for digitally signing PDF documents. As documented before, the application is meant to be launched from a browser through a custom protocol handle. However, any program can attempt to launch an URL with the application's custom protocol handle, making it possible to use it without the browser as originally intended. This application also updates itself automatically, checking its version against the most updated one provided by a method in IGesDoc. Provided the application is outdated, it launches a helper program that downloads and updates the required files.

The GesDoc platform is a document and information management system developed by SIC. The platform aims to gradually replace paper processes throughout UTAD. Therefore, any process that legally requires a signature must be digitally signed. The hiring of staff, scholarship funding and the acquisition of goods and services are some examples of such processes.

The web service IGesDoc is also a part of the GesDoc platform, and facilitates the integration of applications with GesDoc. One such application, as the diagram illustrates, is Digital Signature UTAD. This web service supports operations such as downloading and uploading documents, finalizing and creating processes, and many others.

The last relevant piece of the solution proposal is the SharePoint server. This server was already used by some applications even before GesDoc was developed. The operations GesDoc and IGesDoc perform on this server are simple file operations, such as downloads and uploads.

5 Results

Overall, over 200 documents were successfully signed with the proposed solution. This allowed for a significant reduction of the time a process takes to be handled and signed. Traditionally, a process would have to go through the required people via an internal mail system. This means a process could take 15 days or even more to be concluded. With GesDoc and the digital signature functionality, processes usually do not take more than three days. These time estimates depend on the type of the process and the people it had to go through, and can vary. Additionally, users report that this solution allows them to work from wherever is more convenient. This allows users to process and sign documents faster and conveniently, giving them time to focus on other tasks.

An analysis of how the solution proposal addressed the problems regarding digital signatures identified in the section 3 is also offered. Fundamentally, the solution proposal needed to provide digital documents with legally valid authentication mechanisms, as well as assuring their integrity and allowing these properties to be long term verified. This could be achieved by creating an application that appends

qualified digital signatures to documents, guaranteeing their authenticity, integrity and non-repudiation, and the addition of LTV data to said signatures allows them to be verified in the long term. However, LTV data is verified against a timestamp signature on the document to reliably determine when the document was signed, and this timestamp can itself expire. A solution to this problem would be a periodic routine that would renew these timestamps, but UTAD does not have one implemented as of the writing of this paper. Overall, these problems were successfully solved. Although it is outside the scope of this solution, GesDoc creates PDF/A-3 documents for archival. This format is useful to store documents that can't have their appearance change over time because of different future fonts or even color spaces. Thus, using LTV-enabled signatures on PDF/A-3 satisfies UTAD's requirements.

Another requirement was the need to use the signing software from a web platform and on Windows, Linux and macOS. While the signing software itself started as a Java applet, the gradual lack of applet support from the most common browsers led to the development of a desktop application. This application is launched through a custom protocol, akin to how the HTTPS preceding an URL works, and the rest of the address is treated as the input parameters. Furthermore, the application was developed in Java and this functionality is possible to implement in Windows, Linux and macOS, covering the operating systems used by UTAD's staff. This approach was deemed very satisfactory.

As explored in the subsection 3.1, the Digital Signature UTAD application used to be launched with parameters specific to GesDoc. However, should the application need to be used from other system (such as the teacher evaluation platform), this would become a hindrance. By removing GesDoc specific operations and parameters, delegating them to GesDoc itself, the application can be used from other information systems, requiring only download and upload links as parameters, and other signing-specific optional parameters. By making small adjustments, if needed, the application can be used from existing or later adopted systems.

Signing various documents in series, with only one PIN entry, is the last identified requirement. By tweaking the way a signature is done, storing the user's PIN in memory, it is possible to sign multiple documents in series. This functionality had a few problems, as it was necessary to change some source code on an open source library to use the Citizen Card. While the functionality was implemented successfully, such changes made it impossible to update the library without performing the same changes and tests. Furthermore, there was no way to know the tests performed were comprehensive enough, as certainly there were many unconsidered variables. This led to the functionality's code being discarded and developed again, but without changing anything on the used libraries. This proved to be successful, as no functionality was lost, and the library can be updated as normal.

To simplify use of Digital Signature UTAD, it was developed an automatic update functionality. The motivation was that, due to the sensitive nature of the digital signatures, older versions of the application with potential unresolved bugs can't be used. However, while the users were provided clear instructions when an update was necessary, generally involving downloading and installing the new application, they would call Technical Support every time an update was necessary. The new update method requires no user input, as the application verifies its version against the last

version set on IGesDoc, downloads it and applies to update through a helper updater program. This greatly improved the experience of the users and the developer as well, as users can sign with the application with no interruption and new updates can be rolled out and applied immediately.

This solution was being used on about five workstations, but recently it was expanded to about eight other users, as GesDoc gradually supports processes that are to be signed by different people.

Overall, the present solution is deemed satisfactory by the University, although the need to develop a timestamp renewal system, for example, shows there is still room for improvement.

As for difficulties, developing a macOS installer was somewhat challenging, mostly because of the inexperience in AppleScript and how the operating system works overall. The application used to be delivered on a *.dmg* file for macOS. This required input that was not very clear to some users, so a straightforward *.pkg* installer was developed. This way, the installer leads the user, similarly to how most Windows applications are installed, and allows operations specific to this solution.

The application used to be installed into folders only accessible through administrator permissions. However, because the application itself didn't run as administrator in any operating system, automatically updating it was impossible. The devised solution was to install the application to a user's folder, such as *AppData* on Windows or to the user's home on Linux and macOS.

Beyond technical difficulties, human resource difficulties were also evident. The most prominent of which led to the automatic updater described above. However, the very nature of the CC poses a difficulty any entity will face when working with digital signatures. By law, the signature certificate on the card must be activated at the Civil Registry Office. This problem is easy to solve if the solution is used by the same, regular people. However, if students were to sign documents, for instance, an adequate communication to clarify the requirements to sign documents with the CC would need to take place. Other than that, this problem does not have a definitive solution, at least in the scope of UTAD.

6 Conclusions

This document starts by briefly exposing the signature-related problems inherent to the implementation of the digital information and document management system GesDoc. The documentation of these problems supported the specification of the architecture of the solution proposal, clarifying some of the design choices. One of those choices stemmed from the need to use the digital signature application from a web platform on Windows, Linux and macOS. While a Java applet would satisfy these conditions, the diminishing support from the most common web browsers motivated a change. Making a Java desktop application that can be launched through a custom protocol handle solves the problem, as well as providing some level of future proofing, as handling URL protocols is a basic feature on any operating system.

This specification aims to document how the application is integrated on both GesDoc and on any generic system, and offers a systematic description of how the

application performs both single and multiple document signatures. To further detail the solution proposal, a brief description of the individual components is offered, allowing for a better comprehension of the system.

However, a few technical and human difficulties made the implementation of this solution proposal more challenging. As for technical difficulties, the more relevant ones were documented on section 5, such as implementing the multiple signing logic, integrating the application with web platforms and adapting the software to work in macOS. Difficulties such as having users update their application, as well as having their signing certificates activated, constitute the biggest human difficulties faced. It is also identified one of the few limitations of the solution, which is the maintenance of signed documents with LTV data.

The proposed system has shown to have many benefits over the traditional processes. With over 200 documents digitally signed, traditional processes that could take beyond 15 days can be closed in no more than three days. Furthermore, users can benefit from this solution wherever is more convenient, allowing them to handle and forward processes outside UTAD.

Considering the problems this solution proposal is ought to solve, as well as an analysis of the signed processes and error logs, it is considered that this project is a success, as it answers every need of UTAD regarding the authentication of digital documents and their storage, while making the handling of processes significantly more efficient. This solution proposal successfully allows users to digitally sign documents on a web platform with their Portuguese Citizen Card, as well as archiving them and assuring their validity in the long term. These signatures are also legally valid as of European regulations and Portuguese law. It is also possible to easily perform these signatures on large volumes of documents, as well as adapt the solution to other information systems.

This paper exposes a viable solution to problems regarding digital document authentication and software integration with web-based systems on the three most used operating systems: Windows, Linux and macOS.

Acknowledgements

This work was developed and financed by Project SAMA Gateway (nº 012627), Programa COMPETE 2020, Portugal 2020.

References

1. Branco, F.: Uma proposta de arquitetura de sistema de informação para as empresas agroalimentares do setor de produção de cogumelos: o caso Grupo Sousacamp. Universidade de Trás-os-Montes e Alto Douro (2014).
2. Hausmann, V., Williams, S.P.: Social Business Documents. Procedia Comput. Sci. 64, 360–368 (2015).
3. Vico, H., Calegari, D.: Software Architecture for Document Anonymization. Electron. Notes Theor. Comput. Sci. 314, 83–100 (2015).
4. Alrehily, A.D., Alotaibi, A.F., Almutairy, S.B., Alqhtani, M.S.: Conventional and

Improved Digital Signature Scheme : A Comparative Study. J. Inf. Secur. 59–67 (2015).
5. Warasart, M., Kuacharoen, P.: Paper-based Document Authentication using Digital Signature and QR Code. Em: 4TH International Conference on Computer Engineering and Technology (2012).
6. Almeida, D.T.N.P.: Assinatura Electrónica Qualificada. Universidade Técnica de Lisboa (2009).
7. Hullavarad, S., O'Hare, R., Roy, A.: Digital Signatures Deciphered. Em: Internal Auditor. p. 35 (2015).
8. Decreto-Lei n.º 88/2009 de 9 de Abril da Presidência do Conselho de Ministros , Portugal (2009).
9. Council of the European Union: Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. Off. J. Eur. Union. 57, 73–114 (2014).
10. Lei n.º 7/2007 de 5 de Fevereiro (Versão à data de 16-07-2017) , Portugal (2017).
11. Gomes, C.: O impacto dos diferentes tipos de assinatura digital nas empresas do Séc. XXI, casos de estudo: ActivoBank e ISCTE-IUL. ISCTE - Instituto Universitário de Lisboa (2015).
12. Teixeira, A.A.S. de A.: Facturação electrónica entre empresas de um mesmo grupo empresarial com diversos sistemas ERP. Universidade do Porto (2008).
13. Barbosa, L.: Sistema de Informação de Apoio ao Ensino - um Estudo de Caso do portal SIDE da UTAD. Universidade de Trás-os-Montes e Alto Douro (2010).
14. Reis, A.: Modelo de Ecossistema de Sistemas de Informação em Instituições de Ensino Superior. Universidade de Trás-os-Montes e Alto Douro (2015).
15. Borges, J., Justino, E., Gonçalves, P., Barroso, J., Reis, A.: Scholarship Management at the University of Trás-os-Montes and Alto Douro: An Update to the Current Ecosystem. Em: Advances in Intelligent Systems and Computing. pp. 790–796 (2017).