Digital Signatures Workflows in Alfresco

Patrícia R. Sousa, Pedro Faria, Manuel E. Correia, João S. Resende, and Luís Antunes

Department of Computer Science, Faculty of Science, University of Porto

Abstract. There are some obstacles, towards a paperless office. One of them is the collection of signatures, since nearly half of all documents are printed for the sole purpose of collecting them. Digital signatures can have the same legal evidential validity as handwritten signatures, provided they are based on certificates issued by accredited certification authorities and the associated private keys are stored on tamper proof token security devices like smart cards. In this article, we propose a platform for secure digital signature workflow management that integrates secure token based digital signatures with the Enterprise Content Management *Alfresco*, where each user can associate a set of smart cards to his account. The documents can then be signed with the citizen card or other smart card that has digital signatures capabilities. We have implemented an *Alfresco* module that allows us to explore several workflow techniques to implement real task secure digital signatures workflows, as people for example do when they pass a paper document between various departments to be signed. Since all users can see the current state of the documents being signed during the entire signage process, important security properties like system trust are preserved. We also describe an external validation web service, that provides a way for users to validate signed documents. The validation service then shows to the user important document security properties like timestamps, certificates attributes and highlights the document integrity in face of the digital signatures that have been collected in the workflows defined by our module in *Alfresco*.

Keywords: Digital Signatures, Workflow Management, Digital Citizen Card, Business Process Management, Alfresco

1 Introduction

Documents which are in printed format have been used for many years, such as books, papers, forms, contracts and any related materials [1]. Nowadays, there are a lot of reasons why people might choose to paperless environments, including reduction of the environmental harm of paper consumption and the economic cost of paper production, print, transfer and storage. Digital environments release people or companies of the location and physical constraints of paper and provide better support for updating, archiving, and searching of documents [2].

With the evolution of Information technology and computer systems, the documents have been managed by computer-based document management systems. A Document Management System (DMS) can be defined as a computer system that is used to store, manage, and retrieve electronic/digital documents on a closed client/server architecture network [3]. However, DMS were interested in the file and storage/indexing/retrieval mechanisms to allow the user to classify and retrieve documents. They were initially concerned only with the file as a container. But, as market needs changed, the DMS focus shifted from file management to content management. For example, if we have a Web site, it is composed of HTML, XML, or ASP pages that need to be managed. So, the name of the system was changed to Enterprise Content Management (ECM) [4].

According to the authors of [5] [6] going paperless is convicted to failure soon. Despite of many efforts which have been done to consume less paper, companies still use large amounts of paper. There are some obstacles towards a paperless office such as: read on screen is difficult for some people especially mid aged people it was not that easy to adapt to computer and Internet, who don't like to read on monitors and prefer to read in paper; the risk of losing data and document due to software or hardware failure; the people has fear because despite electronic storage be safer than having data on paper, some people do not trust the authenticity or security of online tools. Signatures is another obstacle towards a paperless office and according to the authors of [7] nearly half of all documents are printed for the sole purpose of adding signatures, so, we want to focus on a solution to this.

There are two methods of transforming a company into paperless office. One of the methods is by automating the processes that normally use paper as an essential tool. There are several technologies to make this: enterprise data automation software, used to integrate forms and data with systems that processes them; form technology, used to design various types of forms; databases device used to replace the function of a filing cabinet, i.e., data is made into digital form and then stored in a database with sufficient security technology; digital signature allow evidence of signature in digital form. Papers are generally used as business evidences. This is required in business transactions to generate legal binding between two or more parties and workflow platforms technology that is a processes flow of an office. Normally, paper documents are used to transfer a data to other departments so that it can continue doing what is needed next (for example, one document is transferred to other department to be signed). This flow of work can be documented and transferred in digital form, using the workflow platforms. The second method of transforming a company into paperless office is data storage transformation. In a general office, the data is normally stored and protected in a filing cabinet. This turns out to fill offices full of useless paper. Using the "Paperless Office" technology, all this data can be transformed to a digital form very easily. Some of the tools available to support this process: Scanners, book copiers, photo scanners, fax to Portable Document Format (PDF) converter and more. One of the most important tools are ECM systems [8]. This two methods of transforming a company into paperless office

leads us to a solution that could combine the technologies to automate processes that typically use the paper an essential tool, with a tool to store digital information, for example a ECM system as stated above.

The work detailed in this paper aims to provide companies a way to be able to automate their processes signatures to avoid transferring a printed data between departments. This type of transferring can result in loss of important documents or falsification of documents/signatures using printed paper. We want that companies to be able to involve several people in the automated process of signatures, safely in a ECM system. This leads companies to also benefit from a printed paper reduction and reduction of the loss of important documents because documents are online, this way. We will focus in integrating a digital signatures systems with a ECM system. This allows users to sign documents in a document manager, so users can also save their documents online, digitally. We take advantage of the workflow feature that some ECM systems have. Thus, we provide users a way to create a workflow signatures in a ECM system, so, multiple users can sign the same document for example, and all can see the state of the document. We provide a secure way to users sign documents, through a smart card (citizen card, for example).

The next chapters of the paper are organized as it follows: Related Work, Electronic Signature vs Digital Signature, Cryptography Concepts, Smart Cards, Alfresco and workflows, Implementation and Conclusions.

2 Related Work

In the following sections we present an overview of a set of systems comparing their features. As our goal is to integrate these two systems, we also present an overview what there is in that direction that is, digital signature systems (with or without workflows) integrated with an ECM and an overview of the features. To compare the different ECM systems analysed and choose the best ECM system to use, we decided to do a comparative table with the main features that we need in the system. Based on [9] [10] [11], we construct the following table:

Table 1. Comparison of DMS/ECM systems - (E-Enterprise Version, C-Community Version)

	Alfresco C	*Alfresco E*	*Nuxeo*	*DocuWare*	*eFileCabinet*
Open Source	LGPLv3	-	LGPLv2.1	-	-
Add-ons	✓	✓	✓	✓	✓
Workflows	✓	✓	✓	✓	✓
PDF Support	✓	✓	✓	✓	✓
Txt/binary support	✓	✓	✓	✓	✓
Users/Groups support	✓	✓	✓	✓	✓
Digital Signatures	-	-	-	-	-
Electronic Signatures	-	-	-	✓	✓
Record management	-	✓	✓	✓	-

	LogicalDOC C	*LogicalDOC E*
Open Source	LGPLv2.1	-
Add-ons	✓	✓
Workflows	-	✓
PDF Support	✓	✓
Txt/binary support	✓	✓
Users/Groups support	✓	✓
Digital Signatures	-	✓
Electronic Signatures	-	-
Record management	-	✓

We analyse some systems that are the most popular ECM. We're interested in open-source systems as well as we can have full control over the system and can create free add-ons, we also have security guarantees seeing the system code and adapt it to all our needs [12]. We also analysed some non open source because they could have some features that we want, so, we must consider whether we are adding something new to the market or if already exists. Within the non open source, we try to see those in which there have signatures or workflows, that are our principal focus. To select the open-source ECM, we look for systems that have workflows, so *LogicalDOC community* is not an option. Among others, *Alfresco community* and *Nuxeo community* the choice was more complicated, but beyond Alfresco has more users, it also has much more online communities, more tutorials and help documents.

To compare the different digital signature workflow systems analysed and see features that can be added to improve what already exists in the market, we decided to do a comparative table with the some features:

Table 2. Comparison of digital signature workflow systems

	SecuredSigning	*SigningHub*	*DocuSign*
Open Source	-	-	-
Cryptography technology	X.509	X.509	X.509
Physical technology	-	Smart Card and Mobile	Smart Card
Individual workflow	✓	✓	✓
Parallel workflow	✓	✓	✓
Sequential workflow	-	✓	✓
Group workflow	-	-	-
Validation of all signatures	✓	✓	✓

It is important to know if this type of software has support to physical technology like USB tokens, smart cards or mobile for example. There are some type of workflow: Individual Workflow (only one person), Sequential Workflow (follows a defined order), Parallel Workflow (any order allowed) or Group Workflow

(the system allow the creation of groups of registered users). The validation of all signatures is a feature of the system that validates a document with multiple signatures and gives information about them.

In this table we can see the principal features of the independent systems that can be integrated in the *Alfresco* and of the add-ons of *Alfresco*. We can compare the principal features that we need in our system. The difference of independent system and add-ons is that the add-ons are designed for work within *Alfresco* only, however, independent systems works without *Alfresco* providing the signature functionality and can be integrated into *Alfresco*.

We now proceed to compare some these systems by the following tables:

Table 3. Independent digital signature systems for *Alfresco*

	CoSign	*DocuSign*
Open Source	-	-
Crypt. technology	X.509	X.509
Psychical technology	-	Smart Card
Workflow ready/independent	✓	✓
Workflow *Alfresco*	-	-
One signature	✓	✓
Multiple signatures	✓	✓
Validation	-	-

Table 4. Add-ons for *Alfresco*

	Zylk	*E.Roux*	*Toolkit*	*CounterSign*	*Sinekarta*	*Dig. Legale*
Open Source	✓	✓	✓	✓	✓	-
Crypt. technology	X.509	X.509	X.509	X.509	X.509	X.509
Psychical technology	✓	-	-	✓	✓	-
Workflow signatures	-	✓	-	✓	-	-
One signature	✓	✓	✓	✓	✓	✓
Multiple signatures	✓	-	-	✓	-	✓
Validation	✓	-	-	✓	✓	-

With this investigation, we can see that the most popular independent systems / add-ons have most of the features that interest to us and can help us to see what we can improve on the market and that does not exist in the market to we can introduce a new idea.

3 Electronic Signature vs Digital Signature

These two concepts are often confused by people in general. However, a digital signature is an electronic signature but the reverse is not the case. Electronic signature is easy to implement, because a simply typed name can serve as one. Therefore, this type of signature has many problems to maintaining integrity and security, as there is nothing to prevent one person from typing another persons name. Due to this reality, electronic signatures is an insecure way of signing documentation. Electronic signatures are vulnerable to copying and tampering, making forgery easy. There are some examples of electronic signature such as, the scanned image of the person ink signature, the signature with a digital pen, a typed name, a signature at the bottom of an email, a biometric hand-signature, a video signature or a click in an "I agree" check box. The main point is that an electronic signature is any "mark" made by the person to confirm their review/approval of the document [13].

In the case of the digital signature, this is a mathematical scheme for demonstrating the authenticity of a document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender and the message was not altered during the transport. Therefore, this sender cannot deny having sent the message, that ensures authentication, non-repudiation and integrity. Digital signatures comply laws and regulations. This helps organisations ensure signer authenticity, data integrity, and the verifiability of signed electronic documents. Any changes made after the document has been signed invalidate the signature, thereby protecting against signature forgery and information tampering [14]. According to Portuguese law [15], electronic signatures have the same evidential validity as handwritten signatures, provided they are based on certificates issued by accredited certification entities. They are called digital signatures.

Nonetheless, electronic signature can be combined with a digital signature and gain legal value. It is important, today, generate a digital signature by deriving a signature key from human biometrics. Biometrics is the science of using digital technologies to identify a human being based on the individuals unique measurable biological characteristics [16]. With an electronic biometric signature, users can see his handwritten signature in the document and this is an important feature for usability. It is important to have this complement in a signature system because users have a connection in past with the signatures on the paper and users are more comfortable if they can see his usual handwritten signature on the document.

Thus, we now proceed to describe some sections about a digital signatures: cryptography concepts related to digital signatures, digital signature scheme and the different types of digital signatures.

3.1 Cryptography Concepts

Digital signatures use a public and private key pair that are usually purchased by a sender and issued by a Certificate Authority (CA). A key pair are math-

ematically related because a message encrypted with a private key can only be decrypted with a public key. So, a sender uses his private key to sign a document and the recipient uses the senders public key and the signature to confirm the authenticity of the document. The private key is received by a person and remains secret. This key is not to be distributed to anyone other than the private key owner. The public key, can be made available for anyone and can be found by accessing a CA public database. CA is a trusted third party who verifies the identity of the person requesting the key pair and can be created through a PKI [17]. According to the authors of [18], "a PKI is a set of hardware, software, people, policies and procedures needed to create, manage, store, distribute and revoke digital certificates (also called public key certificate) based on public-key cryptography. PKI is an arrangement that binds public keys with respective user identities by means of a CA".

3.2 Digital Signature Scheme

A digital signature scheme provides a cryptographic analogue of handwritten signatures that provides much strong security guarantees. In many countries, digital signatures is a powerful tool and are accepted as legally binding. This scheme is used by a signer and a set of verifiers. A signature scheme consists of three probabilistic, polynomial-time algorithms (*Gen*, *Sign*, *Vrfy*) along with an associated message space M=M_k. The signer starts by running some randomised key-generation algorithm *Gen* to produce a pair of keys (pk,sk), where pk is the signers public key and sk is the singers private key (also called secret key). The security parameter k is implicit in both pk and sk. For security parameter k, the signing algorithm *Sign* (possible randomised) takes as input a private key sk and a message $m \in M_k$ and takes as output a signature $\sigma \leftarrow Sign_{sk}(m)$. If $m \notin M_k$, the signature algorithm outputs $\perp$. For security parameter k, the verification algorithm *Vrfy* takes an input a public key pk, a message $m \in M_k$ and a signature σ. The output produces a bit, with $b = 1$ that means "accepted" and $b = 0$ that means "reject". This is written as b:= $Vrfy_{pk}(m, \sigma)$. If $m \notin M_k$, the verification algorithm return "reject" [19].

In summary, a digital signature is composed of a unique digital certificate for each signer; a private key which only the signer can use to sign and a public key which allows anyone to validate the signature. Signers can include, in digital signatures, for example their name, date, time stamp, their reasons for signing and also can include graphical signatures.

3.3 Types of Digital Signatures

Public Key Cryptography Standards (PKCS#7) is a standard defined by RSA (Rivest-Shamir-Adleman cryptosystem) describing a general syntax for data to which cryptography may be applied, such as digital signatures. PKCS#7 supports some different content types: data, signed data, enveloped data, signed-and-enveloped data, digested data, and encrypted data. Beyond PKCS#7, there

are other formats to encode the cryptographic messages, that are been proposed to improve security and interoperability [20]. There are some types of digital signatures. Comparing two standards, XML Advanced Electronic Signatures (XAdES) and CMS Advanced Electronic Signatures (CAdES), that serve the purpose of digitally signing any type of data using qualified certificates. Both of the standards allow the storage of attributes such as the Multipurpose Internet Mail Extensions (MIME) type of the data to be signed, signing time, for example [21]. XAdES is based on CAdES but required the syntax of eXtensible Markup Language (XML). XAdES introduces the attribute DataObjectFormat to describe the encoding format of the signed data. PDF Advanced Electronic Signature (PAdES) is a proprietary format for digital signatures in a PDF documents where a PDF can be seen as two compartments house. The first contains the PDF document to be signed and the second contains the information required by digital signatures, like, user's certificate, the encrypted digest (Digital Signature Algorithm (DSA) and RSA are supported). In PAdES, it's possible to sign more than just the document such as, time stamp obtained from a trusted server, a graphical signature, the system and the software application the user. This kind of signature has some strong advantage in terms of resistance to ambiguous-presentation attacks [20].

4 Smart Cards

Security solutions based only in software are not safe and are very vulnerable to some attacks. The reason for this lack in security is the conventional storage media use to store certificate and private key are not secure.

Hardware security modules (HSM) are an important security issue of the modern computer networks. Their principal purposes consists on increasing the overall system security and accelerating cryptographic functions. Smart cards can be seen as an example of an HSM that provides a secure and portable way to securely manage cryptographic keys and corresponding X.509 digital certificates, in a PKI context. Smart cards enhances the PKI security through an extra authentication level ("something you have") and with fact that cryptographic keys generated on the card never leave the card. PKI smart cards can provide most main security functions in modern information systems: authentication (X.509 digital certificate), confidentiality (based on asymmetric private key), data integrity (digital signature) and non-repudiation (digital signature by asymmetric key generated and stored on the card) [22].

5 *Alfresco* and workflows

An example of an open source ECM system is *Alfresco*. This system incorporates the major applications of ECM: documents, images, Web contents, records, and digital assets management. *Alfresco* system stands out in its services and controls that manage the content and features. The most important features of this system are the workflows, versions control, metadata management and search.

For a business, for example, this system has the most important features to support the content requirements of a number of business critical processes and uses. Office work, search and discover is supported by the document management tools. The businesses also needs workflow management capabilities that includes case management, review and approval. The creation and refinement of content and documents are supported by the collaboration applications. The scalable Web content management services support the delivery and deployment of content from the enterprise to its customers. One of the most benefits of this system is the capability of record management, that provides an affordable means to capture and preserve records based upon government-approved standards. The standards-based platform also provides access to applications that use these standards, such as publishing, image, and email management [9].

For a developer, the system has a benefit, the add-ons. They can develop an *Alfresco* add-on to improve the capabilities of an *Alfresco* product. The developers can make, for example, integrations with external systems, package customisations and system administration tools.

For creation of a business process more efficient, adaptive and effective to accomplish business tasks, Business Process Management (BPM) provides methods and techniques for this [23]. One of the biggest tools of the ECM *Alfresco* are the support to the Business Process Model and Notation (BPMN) and workflows. BPMN is used to modelling notations for designing business processes, consists of to represent the business workflow. BPMN solutions are framework used to develop, deploy, monitor and optimise multiple types of process automation applications, including processes that involve both systems and people like workflows.

Workflow can be seen as a task that has a initial and final state. An workflow handles approvals and prioritises the order documents are presented. The decisions of workflow are based on predefined rules developed by system owners [4].

6 Implementation

In this section, we describe the technical implementation of the proposed integration of digital signature with an ECM, in this case, *Alfresco*. We took the fact that this ECM has support for BPM and workflows to integrate digital signatures in a workflow where people could define who signs a specific document.

We focus on the signatures in PDF documents. We implement the signature in this type of a document because, as we can see in the Types of Digital Signatures subsection, this kind of signature is more resistant to attacks. One interested property is the time stamps. Timestamping is the process of securely keeping track of the creation and modification time of a document. No one, not even owner of the document, should be able to change it once has been recorded. That way, integrity is ensured. The timestamp is obtained from a trusted external server to have the guarantee that the service we are using is not changing the timestamps [24]. This can be considered as the stamps made by a notary in a paper.

We used smart cards to provide a way to users sign safely, quickly and provide mobility, as described in Smart Cards section.

As *Alfresco* allows add-ons, we took advantage of this feature and we integrate all the process to signing a document as one module/add-on that can be integrated in the *Alfresco*.

In the figure 1, we can see an example of our workflow process:

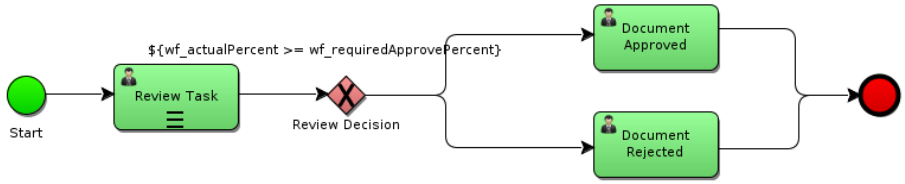

Fig. 1. BPMN

In this diagram, we can see that we have a circle that represent the state that indicates the start of your business process. Then, we have a user task that should be used when human interaction is required for the business process, for example, when details are to be filled or verified by a human. The review decision is represented by an exclusive gateway, that is used when we want to proceed with one path from the multiple paths defined. So, we can compare the exclusive gateway to an if-else statement of the programming concept. In this review decision, we can define a condition, that if it's true, the document is approved through the user task, otherwise the document is rejected trough other user task. In the two cases, we advance for the final state that represents the end of the business process.

We have three types of workflows as talked in the Related Work section. One of the workflows, users can sign in parallel, i.e., can sign in any order. The other workflow, users have to sign with a specific order, for example, first signs employed X, and only when X signs, employed Y can sign and in the final the director of the company accepts the task. The last workflow, a group of users can sign in parallel. Alfresco has a feature that allows the creation of user groups, so, we can associate a group to the workflow, without the need to associate one person at a time.

This diagram represents the BPMN that we create for this work. In the initial state, we have a form that we can choose the title of the workflow ($bpm\_workflowDescription$), a due date ($bpm\_workflowDueDate$), a priority ($bpm\_workflowPriority$), the reviewers ($bpm\_assignees$) that we want to sign a specific document (or more than one document $packageItems$) and the required approval percentage ($wf\_requiredApprovePercent$), i.e., the percentage of people that have to sign the document for workflow can be approved by the owner of that workflow. We have a possibility of send an email to the reviewers that are attached to the workflow with the link of the task to review and with the link(s) of

the document(s) attached to the workflow too (*bpm_sendEMailNotifications*). When the workflow is started, is created in the document(s) attached to the workflow, one signature field for each reviewer attached to the workflow. Each field has the corresponding user name of the reviewer who will sign this field. After the initial state, the review task consists in send a task, to each reviewer attached to the workflow, for the reviewer sign and therefore accept the task. If the user reject the task, then it does not agree with the document, therefore, does not sign. To review the task, a form is displayed to the reviewers, with the info of the task: title/description (*message*), owner (*taskOwner*), priority (*bpm_priority*), due date (*bpm_duedate*) and identifier (*bpm_taskId*); progress with the status of the task (*bpm_status*): not yet started, in progress, on hold, cancelled or completed; the items attached to the task (*packageItems*) and a comment (*bpm_comment*) that if it is written, is put in the digital signature reason. The result of the review task is identified by *wf_reviewOutcome*. The signature is made through the citizen card. When the user hit the button "Accept and Sign" is shown a pinpad to insert the signature PIN. When the signature is placed in the document, in addition to the signature of the reason it is placed in the same field the name of the person who signed the document and the date and time.

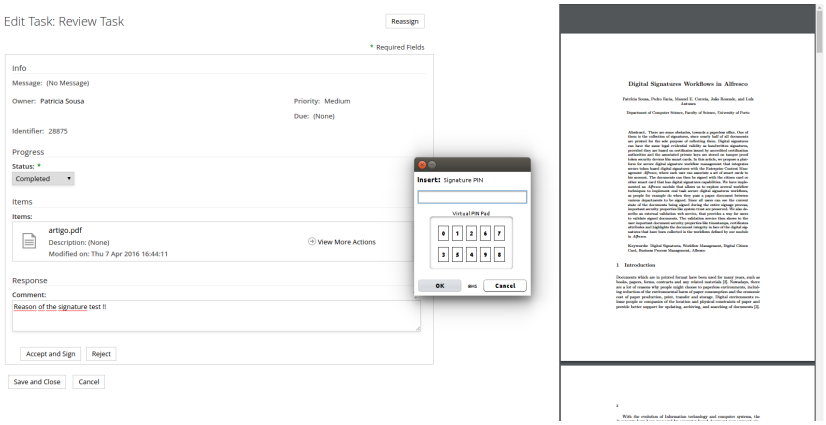

Fig. 2. Example of a signature page

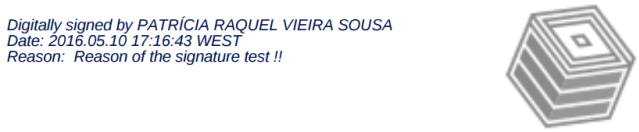

Fig. 3. Example of a signature

After this, the condition $\$wf\_actualPercent >= wf\_requiredApprovePercent$ is tested for the review decision. The $wf\_actualPercent$ is the percentage of reviewers that sign and accept the document and the $wf\_requiredApprovePercent$ is the required approval percent, filled on the form, previously described in this section. If the condition is true, then the document(s) can be approved by the workflow owner.

Algorithm 1 Count percentage of reviewers that approve the document

1: **if** $task.getVariableLocal('wf\_reviewOutcome') ==' Approve'$ **then**
2: $newApprovedCount := wf\_approveCount + 1;$
3: $newApprovedPercentage := (newApprovedCount/wf\_reviewerCount) * 100;$
4: $execution.setVariable('wf\_approveCount', newApprovedCount);$
5: $execution.setVariable('wf\_actualPercent', newApprovedPercentage);$
6: **end if**

The Algorithm 1 is called whenever a user approves a task. After this, the owner ends the workflow through a form, even if it is approved or rejected and can do a comment to the workflow. The form has info of the workflow: title/description, owner, priority, due date and identifier; progress with the status of the task: with the same choose status then the task review form; the information of outcome: number of reviewers, reviewers who approved, required approval percentage and actual approval percentage; the items attached to the task and a comment that owner can put in the workflow.

As the signatures are made with the citizen card, each user has to associate the card to their user profile. The system makes a check if that card already belongs to someone else profile, for security reasons. If the user has no smart card in the profile, when the user tries to sign a document through a workflow, it's required to associate the citizen card to their profile. To facilitate the use of the service, we have another way of association of the card to the profile. The users can associate the card without leaving the current workflow task through a button that makes the direct association of the smart card to the user profile.

In addition to the citizen card, we decided to also give the possibility of users associate other smart cards to their profile, instead of only citizen card. If the users work in a hospital, they can associate their hospital card profile. So they can, for example, sign hospital internal documents with the hospital card and human resources documents with the citizen card. It gives the possibility of the person to choose which card you want to use to sign the documents.

One of the other biggest capacity of our system is the provision of information about the signature fields for each document. Through an action button, which is one of Alfresco capabilities, that calls an external web service we offer the user the possibility to validate the document and which fields that are already signed and if the signatures are valid.

We decide to make a external web service to validate the signatures because, for example, if we have a customer, Alfresco and the validation service, the

customer wants to ensure that the document signing is being properly assessed on your product. To make sure that the validation is done correctly, the validation service has to includes a signature in your answer that the customer can validate and have the security that Alfresco is not changing any validation response.

The information that web service returns is the number of revisions, the number of fields, the status (empty, partial or full) and the number of signed fields. For each field the information is the name of the field, if it is signed. If it is signed we have the information if the signature cover all the document, if it has been revised, date, the certificate of the citizen card, the integrity of the signature and the response that web service gives (valid or not) is stored on the validation variable, then in the client side, we test the conditions again and we compare this variable, so, we can see if the result by the server is correct.

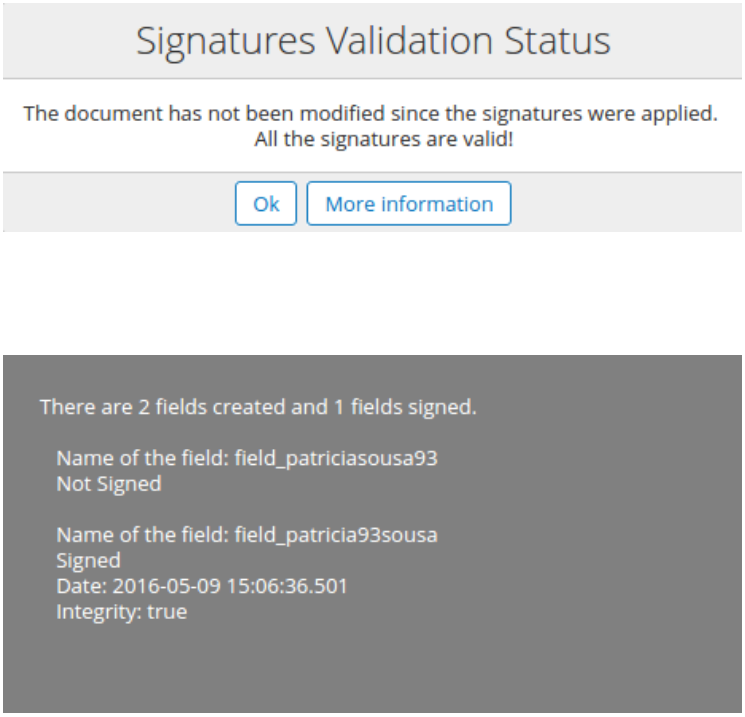

Fig. 4. Pop-ups example with signatures validation status and more information of validation

We can see in the Figure 4 the pop-ups that we use to show the information to the client. The first pop-up is showed when the user clicks on the "Verify Document" in a specific document, if the document has been modified since the signatures were applied and therefore, if the signatures are valid or not. With "More information" button, we can see an example, on the second pop-up, of

the information that is showed. We give the information of the number of fields that exists on the document, how many fields are signed, the name of the fields and if each field are signed. For the signed fields, we show which is the date/time and the integrity of the field.

7 Conclusions

When a paper document passes between multiple departments, the document can be falsified or tampered with. With this system, as already mentioned, import security properties are preserved, like system trust, since all users can see the current state of the documents being signed during the entire signage process, it's possible to verify the document at any time and see the modifications in real time. The digital signatures perverse too the security properties integrity, authenticity and non-repudiation. This all together, is an advance in paperless technology, since the signatures in addition to being integrated into a workflow, the signatures workflow are integrated in an enterprise content management, in this case, *Alfresco*. Thus, everyone can access the documents at any time and anywhere. This system will avoid the print of the paper for the purpose of the signatures and will contribute for the environment. This will be important not only to avoid the paper as well as to prevent damage to the paper using pens for example, but also avoid the use of printers and scanners to print and scan the papers that have the signatures.

8 Future Work

This investigation will enable to integrate, in the future, other forms of signatures beyond the smart cards, such as an yubikeys with a certificate to be using to sign, for example.

This system only allows digital signatures in a PDF file therefore, as a future work, we plan to add electronic signatures and biometric signatures and give the user option to choose between different types of signatures. It is also desirable to implement the signatures for other types of document that not only PDF such as XML, for example.

References

1. Asili, Harika and Tanriover, Omer Ozgur: Comparison of document management systems by meta modelling and workforce centric tuning measures. arXiv preprint arXiv:1403.3131. (2014) 1-2
2. Plimmer, Beryl and Apperley, Mark. Making Paperless Work 2007. Proceedings of the 8th ACM SIGCHI New Zealand chapter's international conference on Computer-human interaction: design centered HCI. ACM. (2007) 1-2
3. Zantout, Hind and Marir, Farhi. Document management systems from current capabilities towards intelligent information retrieval: an overview. International Journal of Information Management. Elsevier. Volume 19. Number 6. (1999) 1-2

4. Intergraph. Enterprise Content Management (ECM) Overview. Copyright Intergraph Corporation. (2010) 4-5
5. Majid Vesali. Paperless Office. Business Consulting Master. Hochschule Furtwangen University. (2012) 1-7
6. Harper, Richard and Sellen, Abigail J. The myth of the paperless office. MIT Press. (2001) 17-18
7. ALA's Legal Management: www.arx.com/files/uploads/2014/11/CoSign_ALA_Legal%20Management.jpg (Accessed March 13, 2016)
8. Nye, James. Issues and Disadvantages of moving to a paperless office. Issues. (2009) 4-6
9. Caruana, David and Newton, John and Farman, Michael and Uzquiano, Michael and Roast, Kevin. Professional Alfresco - Practical Solutions for Enterprise Content Management. John Wiley and Sons. (2010) 39-42
10. Maass, Wolfgang and Kowatsch, Tobias. Semantic Technologies in Content Management Systems - Trends, Applications and Evaluations. Springer Science & Business Media. (2012) 154-192
11. LogicalDOC - Product features: www.logicaldoc.com/product/features.html (Accessed March 13, 2016)
12. Nikoi, Ephraim and Boateng, Kwasi. Collaborative Communication Processes and Decision Making in Organisations (Advances in Human Resources Management and Organisational Development). IGI Global. (2013) 51-54
13. Aalberts, Babette P and Van Der Hof, Simone. Digital signature blindness analysis of legislative approaches to electronic authentication. EDI L. Rev. HeinOnline. Volume 7. (2000) 7-8
14. Luppicini, Rocci. Evolving Issues Surrounding Technoethics and Society in the Digital Age. IGI Global. (2014) 186-187
15. Decreto-Lei n. 290-D/99, de 2 de Agosto: dre.pt/application/dir/pdf1sdip/1999/08/178A01/00020011.pdf (Accessed March 13, 2016)
16. Jo, Je-Gyeong and Seo, Jong-Won and Lee, Hyung-Woo. Biometric digital signature key generation and cryptography communication based on fingerprint. Frontiers in Algorithmics. Springer. (2007) 1-2
17. Stern, Jonathan E. The Electronic Signatures in Global and National Commerce Act. Berkeley Technology Law Journal. JSTOR. Volume 16. (2001) 394-396
18. Xenitellis, Symeon. The Open-source PKI Book. Open CA Team. (2000) 34-35
19. Katz, Jonathan. Digital Signatures. Springer. (2010) 22-23
20. Gorelik, Samuil and Lyaper, Vitaly and Bershadskaya, Lyudmila and Buccafurri, Francesco. Breaking the Barriers of e-Participation: The Experience of Russian Digital Office Development. Electronic Government and the Information Systems Perspective. Springer. (2014) 175-176
21. João Pedro Bernardo Gonçalves. Cartão de Cidadão: Autenticação de Papéis do Cidadão. Lisbon Technical University. (2010)
22. Marković, Milan and Savić, Zoran and Kovačević, Branko. Secure mobile health systems: Principles and solutions. M-Health. Springer. (2006) 15-16
23. Laliwala, Zakir and Mansuri, Irshad. Activiti 5. x Business Process Management Beginner's Guide. Packt Publishing Ltd. (2014) 26-27
24. Boonmee, Choompol and Chatchumsai, Rattapol and Boonmee, Sunet. Development of Electronic Correspondence Letter Time-Stamping Service Using Oasis Digital Signature Services. The Proceedings of the 11th European Conference on EGovernment: Faculty of Administration, University of Ljubljana, Ljubljana, Slovenia. Academic Conferences Limited. (2011) 3-4