Digital Signatures for Document Workflow and SharePoint

Dum requiescebat meditans
Praesens ecce! oculis cui
fera flamma micat, Ibat, et
horrendum burbuliabat
et tu brute su monde illus
nos fidelius cante di iens!

John Doe

John Doe

Dum requiescebat meditans
Praesens ecce! oculis cui
fera flamma micat, Ibat

John Doe

John Doe

John Doe

John Doe

Dum requiescebat meditans
Praesens ecce! oculis cui
fera flamma micat, Ibat, et
horrendum burbuliabat
et tu brute su monde illus
nos fidelius cante di iens!

John Doe

About the White Paper

As the non-profit association dedicated to nurturing, growing and supporting the ECM (Enterprise Content Management) community, AIIM is proud to provide this research at no charge. In this way the education, thought leadership and direction provided by our work can be leveraged by the entire community. Our objective is to present the "wisdom of the crowds" based on our 65,000 strong community.

We are happy to extend free use of the materials in this report to end-user companies and to independent consultants, but not to suppliers of ECM systems, products and services, other than ARX and its subsidiaries. Any use of this material must carry the attribution – "© AIIM 2010 www.aiim.org / © ARX 2010 www.arx.com"

Rather than redistribute a copy of this report to your colleagues, we would prefer that you direct them to www.aiim.org/research for a free download of their own.

Our ability to deliver such high-quality research is made possible by the financial support of our underwriting sponsor, without whom we would have to return to a paid subscription model. For that, we hope you will join us in thanking our underwriter for this support:

ARX
855 Folsom Street
Suite 939
San Francisco, CA 94107
Tel: (415) 839 8161
Fax: (415) 723 7110
Website: www.arx.com

Process used and survey demographics

The survey results quoted in this report are taken from a survey carried out between 5th and 15th January 2010, with 388 responses from individual members of the AIIM community surveyed using a Web-based tool. Invitations to take the survey were sent via e-mail to a selection of AIIM's 65,000 registered individuals. Respondents are predominantly from North America and cover a representative spread of industry and government sectors.

About AIIM

AIIM (www.aiim.org) is the community that provides education, research, and best practices to help organizations find, control and optimize their information. For more than 60 years, AIIM has been the leading non-profit organization focused on helping users to understand the challenges associated with managing documents, content, records and business processes. Today, AIIM is international in scope, independent and implementation-focused, acting as the intermediary between ECM (Enterprise Content Management) users, vendors, and the channel.

About the author

Doug Miles is Director of the AIIM Market Intelligence Division. He has over 25 years experience of working with users and vendors across a broad spectrum of IT applications. An early pioneer of document management systems, Doug has been involved in their evolution from technical solution to enterprise infrastructure platform. Most recently, Doug has produced a number of the AIIM survey reports on user issues and drivers for ECM, Email Management, Records Management, SharePoint and Enterprise 2.0. He has also worked closely with other enterprise-level IT systems such as ERP, CRM and BI, has an MSc in Communications Engineering and is a member in the UK of the Institute of Engineering and Technology.

Table of Contents

Introduction

For this report we have measured the potential productivity benefits of a modern digital signature system and the implementation issues that may arise. In particular, we have found that freeing electronic workflows from the interruptions and process delays incurred by physical signing on paper of otherwise electronic documents can produce considerable efficiency improvements.

Today's digital signature systems, with well designed user and certificate management, can be readily extended across the enterprise, and indeed to the extended enterprise of customers and partners. Benefits can be achieved in all the key areas – better customer service, improved staff productivity and reduced administration costs. Existing users report payback periods that are much better than expected and are mostly within a single budget cycle.

Based on our survey data, we look at the regulatory requirement for signature approvals across different industry sectors, the drivers and issues for selecting a solution, the barriers to adoption, and the business benefits reported by existing users.

We take a specific look at the increasing popularity of Microsoft SharePoint as a process workflow platform, and whether the prevalence of self-implemented installations could either compromise regulatory requirements or result in sub-optimum processes.

Key Findings

- Speeding up the approval process and saving staff time are considered to be the biggest benefits by those who have implemented a digital signature solution.

- 63% of digital signature users achieved ROI in 12 months or less.

- For 40% of non-users, half or more of their electronic document workflows are interrupted by the need for physical sign offs. For 23% of non-users, this results in a week or more of process delay on average.

- In 63% of organizations without digital signature systems, more than half of the printed process documents are printed just to add a signature.

- On average, 3.5 additional photocopies or fax copies of process documents are produced just to collect signatures.

- 60% of respondents consider authorization signatures to be essential in their regulatory environment, particularly in national government, healthcare and pharmaceutical.

- For 40% of organizations, over half of their main business processes and documents require formal signature.

- 43% of SharePoint users would like to apply digital signatures to SharePoint workflow processes.

- 24% of survey respondents are already using digital signatures. A further 21% plan to implement them in the next 12 months.

Digital Signature Primer

For those who are unfamiliar with the technology, we need to establish the difference between electronic signatures and digital signatures. Some standards bodies and government regulations use the term "electronic signature" interchangeably between, say, scanned or fax signature images (i.e., "digitized images") and public-key encryption-based digital signatures. In the US, usage and legal admissibility is fairly consistent. An "electronic signature" is likely to be a bit-map representation, either from a scanned image, a fax copy or a picture of someone's signature, or may even be a typed acknowledgement or acceptance. A digital signature is "extra data appended to a message which identifies and authenticates the sender and message data using public-key encryption"[1]. Some digital signature systems will combine the authenticated signature data with an associated bit-map image.

Many types of signature are acceptable in law, subject to the judgement that the process used to apply the signature to the document and subsequently to present the document, has authenticity, integrity, enforceability and non-refutability – i.e., that the right person applied the signature, that it can be recognized as their intent to endorse the document and that the document hasn't been subsequently tampered with. Establishing this in a court of law is obviously going to be somewhat easier with a digital signature than with a mere electronic one, although the legal admissibility of scanned documents is well covered in best practices and standards[2,3,4]. Indeed, the same considerations would apply to a paper document with a physical signature.

Some organizations go to elaborate lengths to password-protect scanned signatures, or to establish the authenticity of a check-box sign-off within a workflow process. Indeed, if this were contested, it would be the rigor and consistency of the process that would be challenged in the court, not the electronic-signature mechanism per se.

Digital signatures, on the other hand, provide a convenient mechanism whereby the unique application of the signature by the signee is established by the combination of applying their private signing key along with their personal ID certificate containing their public key. The subsequent verification of this signing process by any third party requires just the public key ID certificate. In addition, a checksum mechanism confirms that there have been no modifications to the content. The public-private key combination is generally self-generated but its associated certificate is issued (purchased) from a trusted Certificate Authority (CA). Self-certified public keys are possible, but require a "leap of faith" from others because they do not establish the verifiable identity of the signee. Digital signature standards are mature and converging internationally[5,6].

Confusion frequently arises between the usage of digital signatures and document encryption. Full document encryption ensures that only those co-operating persons who possess a shared secret key can read the contents of the document, thereby securing it against any third party access. Alternatively, especially for emails, both parties can agree to mutually trust one or more CAs who will underwrite a personal digital certificate for each party. Unless it is absolutely essential, full document encryption is often advised against for use within electronic records management systems as it prevents full-text indexing, and requires that the decryption keys (and application) are available for any future access. Furthermore, if the decryption key is lost or an employee leaves without passing it on, encrypted documents and records will in effect be electronically shredded as no one will be able to read them.

Correctly certified digital signatures do not prevent unauthorized persons reading a document nor are they intended to. They do confirm that the person who signed it is who they say they are, and that the document has not been altered since they signed it. Within a records management system a digital signature is often considered to be an important part of the metadata of a document, confirming both its heritage and its integrity.

Administering digital signatures in an ad-hoc way within a corporate environment can prove to be something of an overhead - enrolling and revoking users, obtaining certificates from a trusted certificate authority, providing user access licences to signature-supporting applications, administering password protection, and retiring the certificates of staff who have moved on. There are more systematic ways to manage certificates and signatures. This may involve a service agreement, or the outright purchase of a certification management product, which may be integrated with an ECM system, linked to the Active Directory service or administered as a stand-alone function. Ideally, the enterprise should have a root certificate that is trusted by all, and centrally issue certificates to all users.

Business Drivers

The business importance of signatures

Like hand-shakes, signatures pervade all parts of business. They may no longer be made with a fountain pen on velum paper, but they are still an important stamp of authority and approval. When we asked in our survey "How important are authorization signatures in your organization?" over 60% of respondents considered them to be "essential" with a further 22% considering them to be "very important". We qualified this against the industry sector, and as we see in Figure 1, the more heavily regulated areas - national government, healthcare, pharmaceuticals and finance - take the lead.

Figure 1: With regard to the regulatory environment or business practices in your industry, would you say that authorization signatures within your organization are "Essential"? (N=234, % answering "Essential", rather than "Very Important", "Somewhat Important", "Important" or "Not that important")
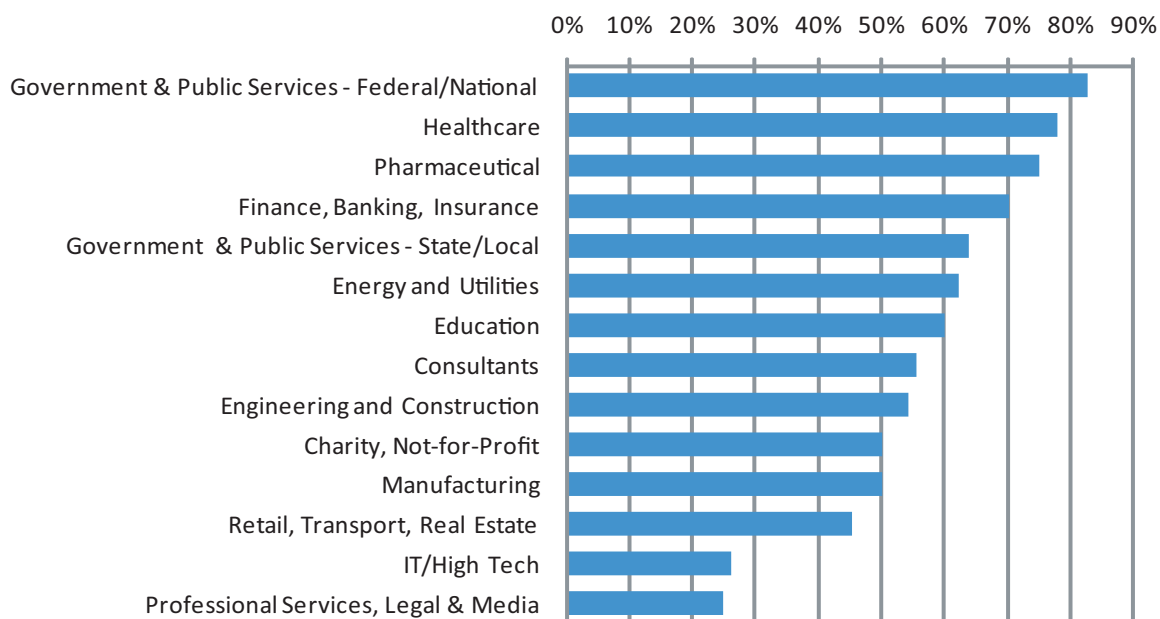
We then evaluated how prevalent formal signatures are in day-to-day business. Taking all sectors together, a surprising 40% of organizations consider more than half their main business processes and documents require formal signatures, with a further 32% opting for a fifth to a half of documents and processes.

When we look at this by industry sector we see a slightly different picture in that "Engineering & construction", and "Professional services & legal", have very signature-orientated business processes.

Figure 2: Would you say that more than 50% of the main business processes/documents in your organizational unit require formal signatures? (N=192, % answering "More than 50%" from a selection of bands up to 50%)
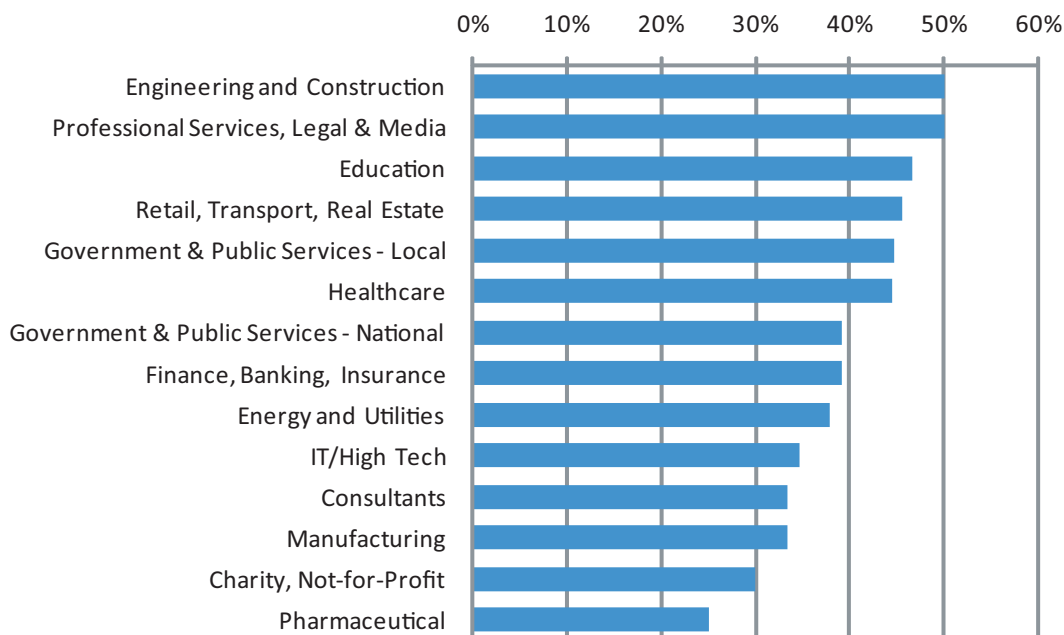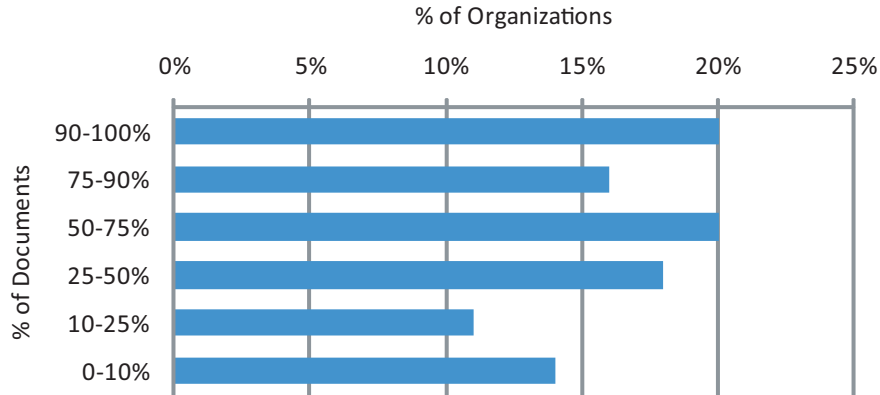

Signatures as part of the business process

We know that within modern business, the majority of documents are created digitally, and spend most of their lifecycle in digital form. This in itself enables business to be carried on in a much more geographically dispersed manner, both within businesses and between businesses. However, the requirement for a physical signature can frequently disrupt and hold up these processes. Senior executives travel more and more these days, but can still stay in close touch with the office. It can therefore be very frustrating when physical signatures are required on urgent processes or documents.

Figure 3: As part of your main business workflows, who of the following are required to sign and return documents or approve process steps? (N=385 all respondents)
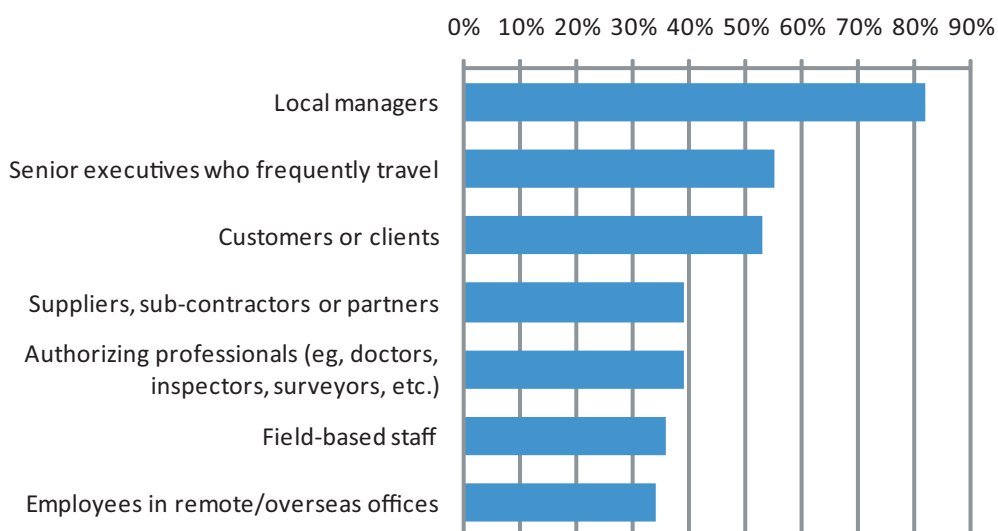
If documents have to be printed, posted, faxed, physically signed and rescanned, this adds costs, delays and staff inefficiencies. As we can see from Figure 4, in 42% of organizations without digital signature solutions, three-quarters or more of the printed process documents are being printed just to add a signature. Averaging the figure over all non-user organizations, 59% of all process documents would not need to be printed if a digital signature system was in place.

Figure 4: Considering the documents that are printed out as part of your formal approval processes, what proportion would you say are printed for the purpose of adding one or more signatures? (N=290 non-users)

In many established business processes, multiple signatures are required – and in 15% of organizations, contracts and agreements are initialled on every page, with a further 23% doing so in some geographies. We also found that on average, 3.5 additional photocopies or fax copies are needed in order to collect signatures. For an unfortunate 3% of organizations, the *average* is more than 20 copies.

We also asked non-users what proportion of their electronic or scanned document workflows are interrupted or prematurely completed by the necessity of physically signing off. For 40%, half or more of their workflows are impacted. In Figure 5 we see the result of this on process times, with at least a day added on average for 68%, and a whole week added on average for 23% - probably indicating that a postal exchange is involved.

Figure 5: On average, how much time would you say is added to the end-to-end process as a result of this physical sign-off? (N=196 non-users with no plans)
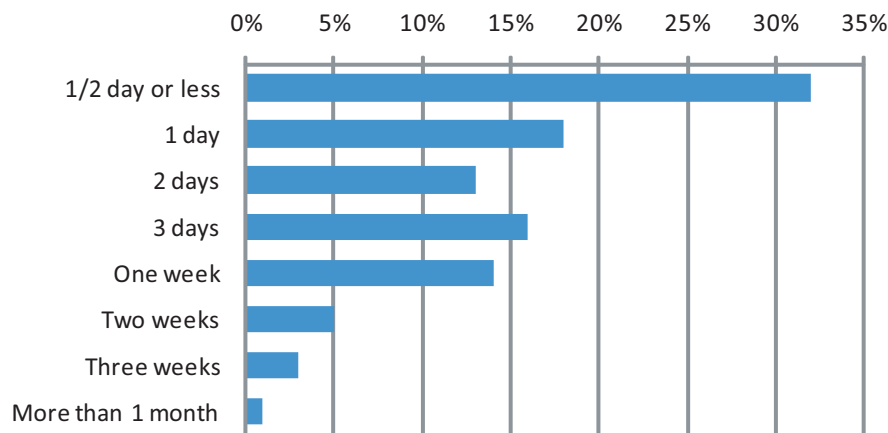

SharePoint requirements

SharePoint is a particularly interesting application as regards signature requirements. It is becoming ubiquitous, and is relatively straightforward to use for a whole host of workflow processes including staff claims, purchase requisitions, project reports, etc. Generally, a tick box is used, under password protection, to indicate approval. However, as applications become more business critical, processes which are part of a regulatory regime, or with legal implications, are increasingly likely to find their way onto SharePoint. At that point it is important to have a more rigorous sign-off mechanism. It is in the nature of SharePoint that local IT departments will likely create their own electronic or digital signature solution around SharePoint, but this may be found wanting in terms of both convenience and security.

Figure 6: Do you have any of the following requirements within SharePoint? (Check all that apply)
(N=231 SharePoint users)
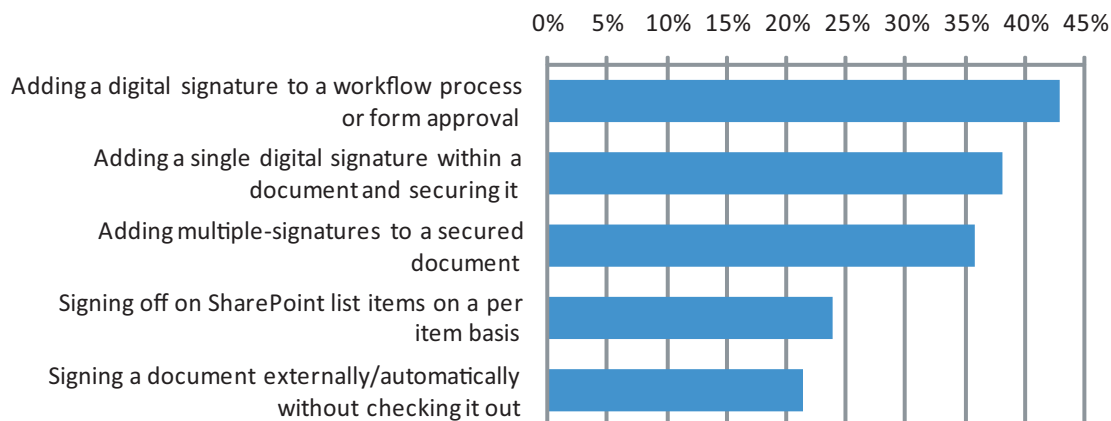
Digital Signature Adoption

Our survey response was self-elected, and so at 24%, it is likely to overestimate those already using digital signatures, and in particular those 21% planning to. Even so, this result points to a very high level of potential take up in the next 12 months.

Figure 7: How would you describe the use of digital signatures in your organizational unit?
*(N=385 all respondents)*
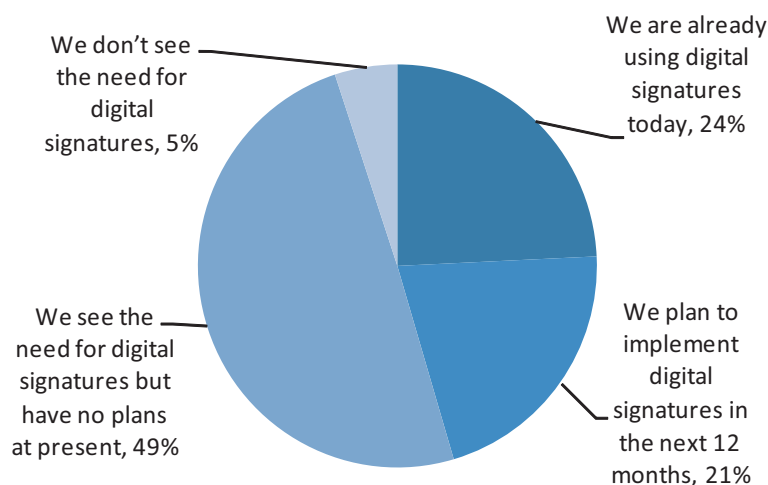
Barriers to adoption

For those not planning to buy a system, 42% have a requirement to sign off completions or approvals within their main business process, and 41% have a need to sign off within SharePoint. Despite this, 28% consider that their senior management do not consider digital signatures to be a worthwhile investment. However, ignoring IT priorities, lack of familiarity with the technology shows very highly as a barrier to adoption, endorsing our view that discussion in the past has been about the intricacies of how the two-key encryption system works rather than the benefits available. Convenience of use also plays a part in the reluctance of staff to move away from time-honored physical methods. It also seems likely that incorporating a scanned image of a physical signature within the digital signature mark would prove reassuring.

There is an understandable concern on extending signatures beyond the firewall, or persuading customers and partners to use them, although the acceptance and admissibility issues do at least seem to have been overcome. Cost and convenience of certificate management is not seen as a big issue by non-users.

Figure 8: What would you say are the most prevalent reasons that digital signatures are not used in your organizational unit — maximum THREE? (N=203 non-users)
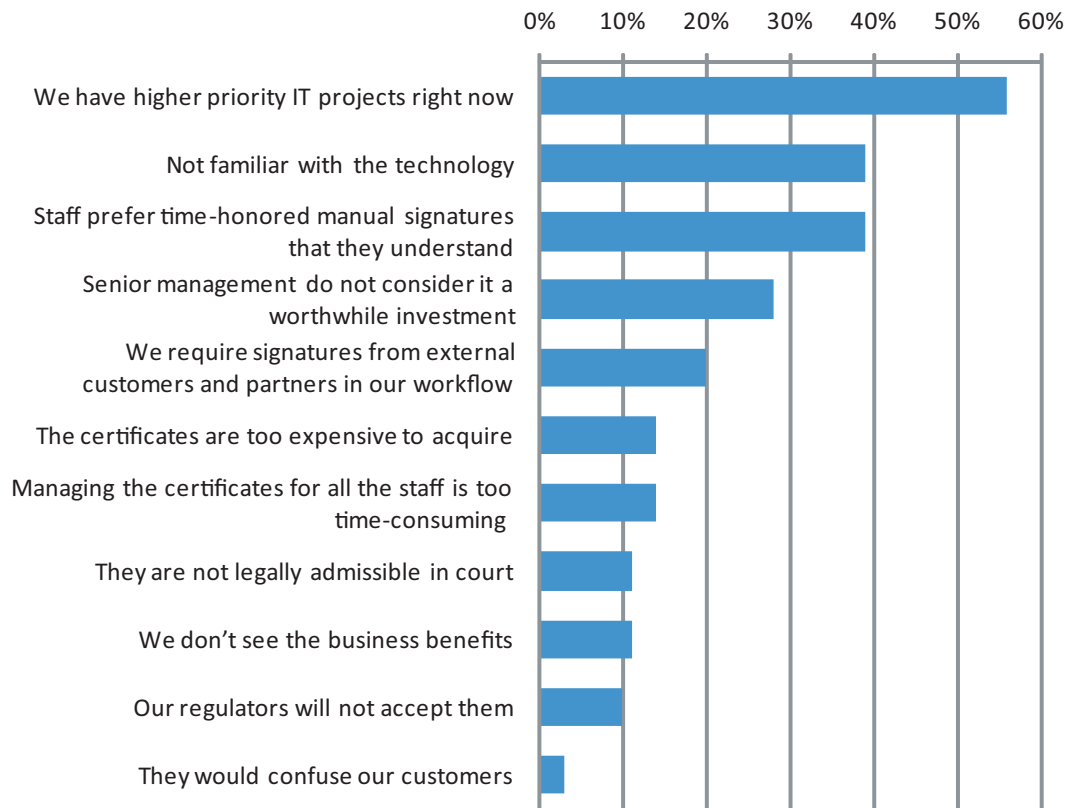
Return on Investment

Implementing a digital signature system can bring a number of hard dollar and soft dollar benefits. Based on the existing users in our survey, speeding up the approval process and saving of staff time in scanning, copying and routing documents are the most immediate benefits, followed by the costs of prints, photocopies, faxes and post. The reassurance of proven compliance for audit and archive counts as a significant benefit too. Ease of signing for staff who are not in the local office is an important factor, and would also have an influence on the number of lost documents.

Figure 9: Which THREE of the following would you describe as the biggest benefits of your digital signatures system? (N=84 users)
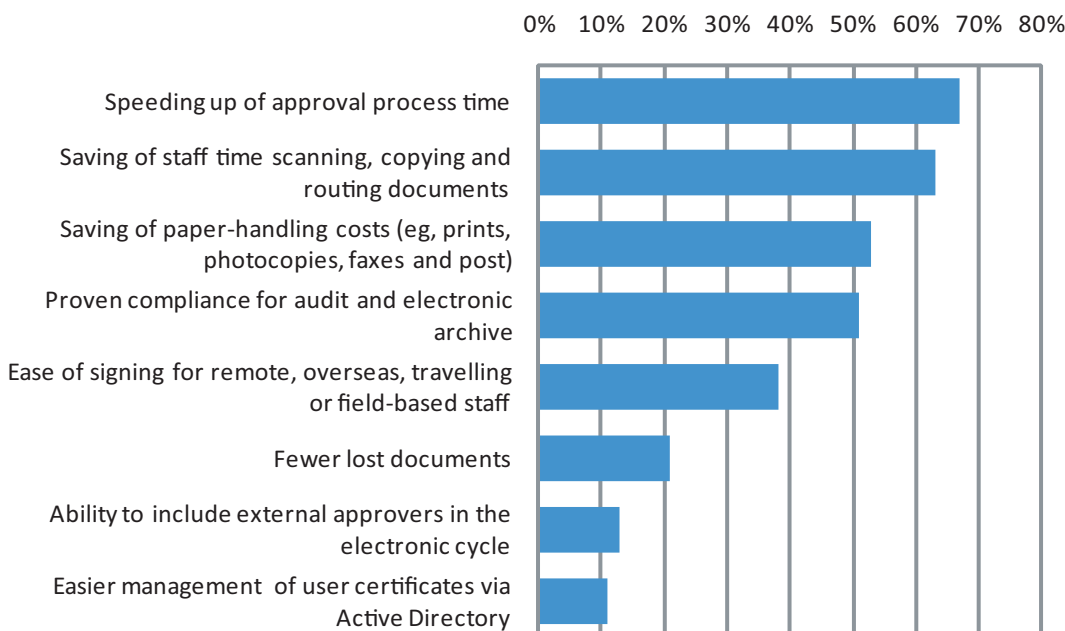
The expectations of those planning a system were very similar, except for a slightly higher expectation for the hard dollar benefits of cost saving on paper handling, with less on time savings.

When asked to put a financial figure on the benefits compared to the set up costs, nearly two-thirds of users achieved ROI in 12 months or less, and 78% in 18 months or less. This was well ahead of the expectations of those planning an installation, and represents an excellent return for any IT project.

Figure 10: Considering financial, operational and customer-service benefits, what would you consider to be the payback period from your investment in digital signature systems? (N=84 Users, 78 Planned users)
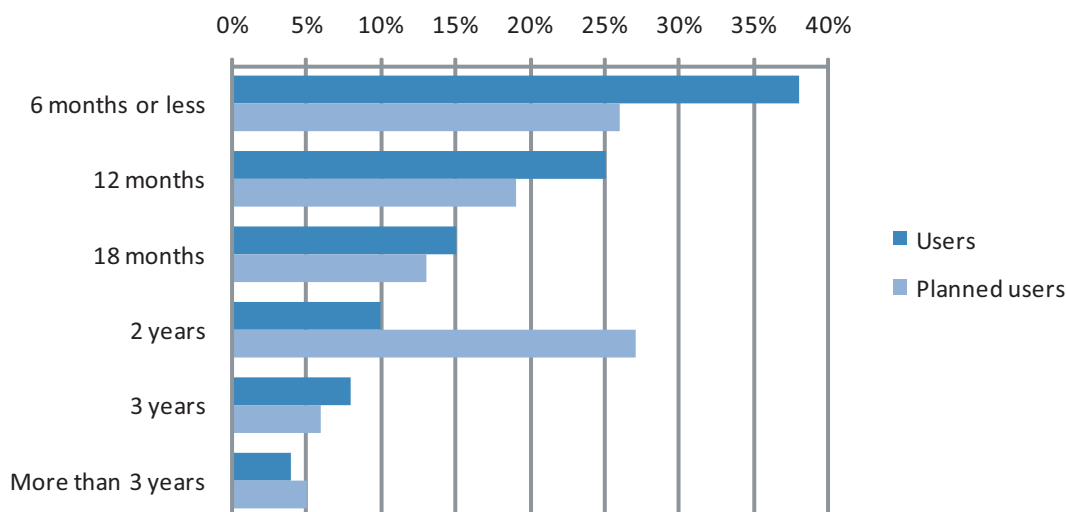
Features, Functions and Decision Makers

As regards to how people source their digital signature solutions, we found a fairly even balance amongst existing users between 3rd party solutions integrated with document management (DM) or ECM systems, 3rd party solutions not integrated, and in-house developed systems. Interestingly, however, those planning to purchase in the next 12 months showed a strong preference for integration with DM and ECM, perhaps reflecting a lack of simplicity in previously available offerings.

Figure 11: Who provides or is likely to provide your main digital signature solution?
(N=78 Users, 74 Planned users, excl 15% Don't Knows)
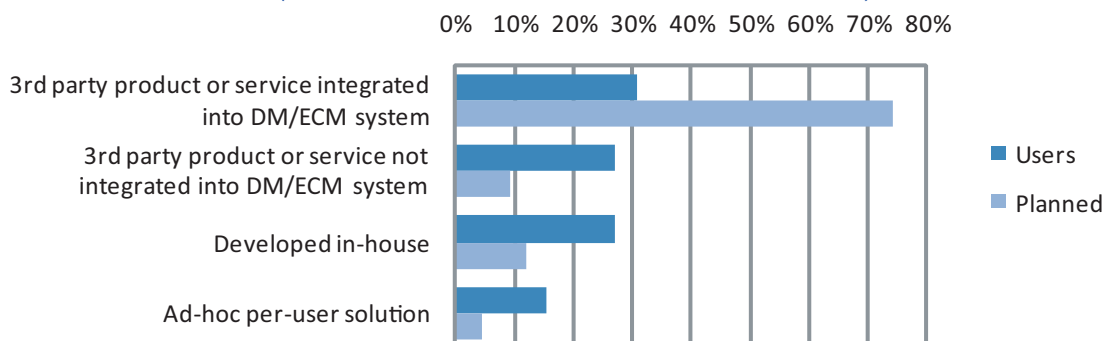
There are a number of ad hoc mechanisms for digital signatures, including those offered within Adobe Acrobat for PDF files and Microsoft Office for Word and Excel files. The simplest of these will likely involve self-certified signatures, not trusted 3rd party ones. One of the issues that arises is that if multiple signatures are required, a simple sign and encapsulate function from the first signee will prevent a subsequent signee being able to add their signature to the document. A further issue is corporate control of the certificates rather than individual ownership, and the management issues that go with that.

Figure 12: Which of the following features do you have/will be important to have in your current/proposed digital signatures solution? Max 4 (N=84 Users, 78 Planned users)
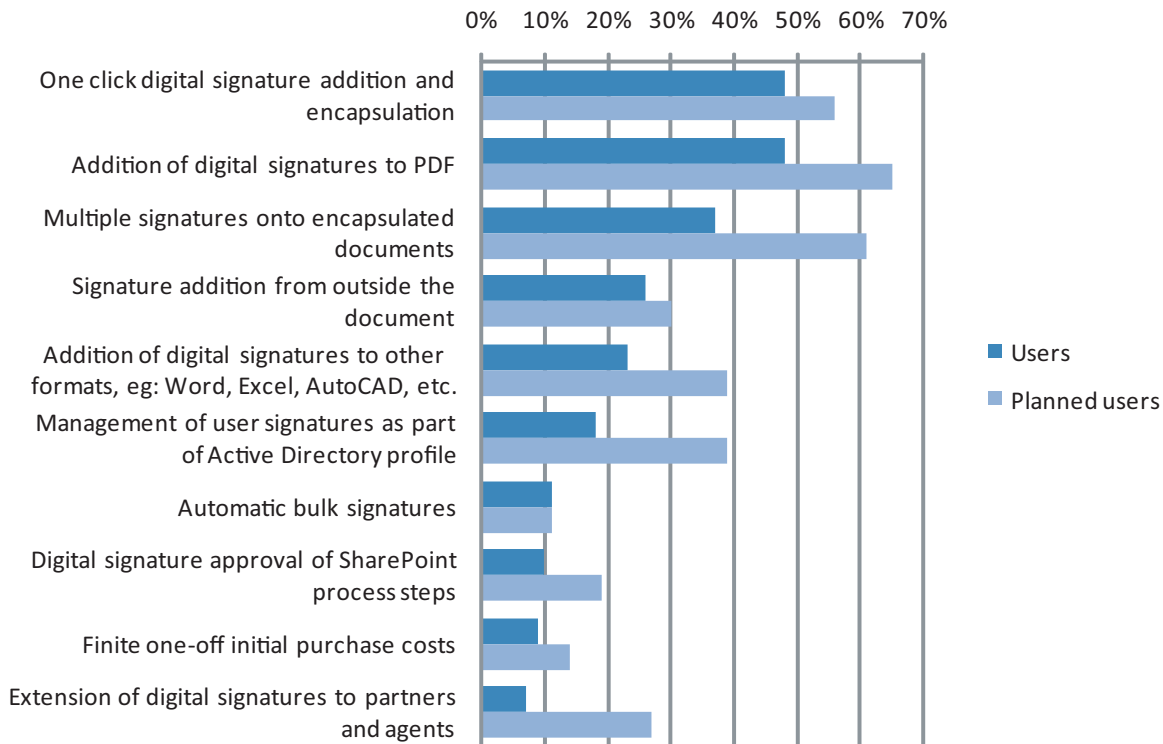

One-click operation and multiple signatures are important to all respondents, with prospective purchasers of more modern systems also looking for support for multiple file formats, integration with Active Directory, and extensibility to partners and agents.

One feature we did not research was the use of specific hardware signing tablets, PIN-number generators or biometrics to further validate the digital signature, although this did crop up in the free comments area of the survey.

Decision Maker

As indicated in Figure 13, outside of IT, it is difficult to identify a single likely decision maker. The fact that Line of Business managers are only involved as decision makers in a tenth of organizations perhaps explains why the process improvement benefits are not coming to the fore.

Figure 13: Who would you say is the decision-maker in your organizational unit as regards digital signature solutions? (N=368, all respondents)
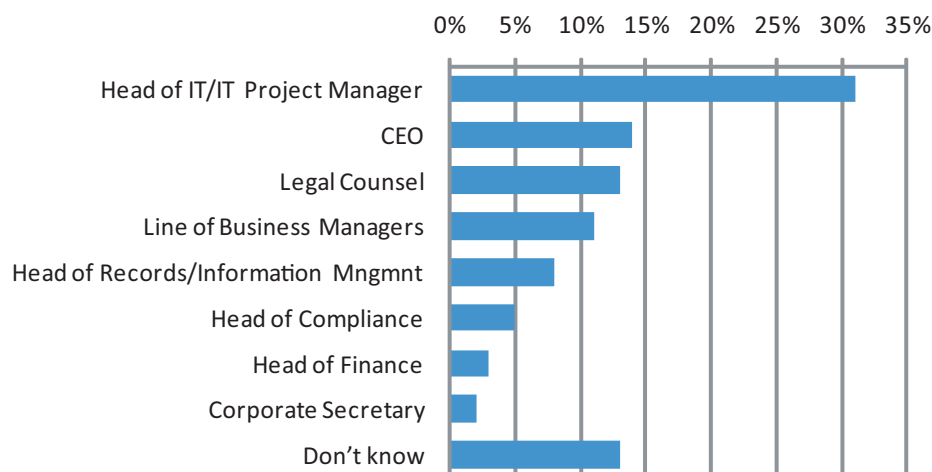
Conclusion and Recommendations

We have shown that digital signature solutions can provide a very rapid return on investment – generally within 12 months. In our survey, 24% of responding organizations are already using digital signatures, with a very high 21% stating an intention to implement in the next 12 months.

The primary benefit seen by existing users is in speeding up the approval process, but it also saves staff time and the cost of photocopies, post, etc. We have found that nearly 60% of all process documents would not need to be printed if a digital signature system was in place.

Despite the business benefits reported by existing users, digital signature projects are not given a high priority within IT departments. Elsewhere in the business, non-familiarity with the technology and a reluctance to change time-honored ways of working are given as barriers to adoption. Convenience and simplicity of both use and administration are obvious factors here. We have seen that those intending to purchase a digital signature system are also looking for it to be easily integrated into their ECM system.

With the rapid adoption of SharePoint as both a document management and a workflow approval system, we feel it is important that users adopt a rigorous digital signature system from the outset, using trusted certificates rather than self-certification. Ease of use and ease of maintenance are even more important in a SharePoint implementation due to the likely number of users spread across the enterprise.

References

1. Computer Desktop Encyclopedia www.computerlanguage.com

2. ISO 15489, Section 7.2

3. BSI BIP 0008, Code of Practice for legal admissibility and evidential weight of information stored electronically

4. Electronic Signatures in Global and National Commerce, Public Law106–229—June, 2000 ref.

5. Digital Signature Standard (DSS) http://csrc.nist.gov/publications/fips/fips186-3/fips_186-3.pdf

6. ISO 32000-1

Appendix 1

Survey Demographics

Survey Background

The survey was taken by 388 individual members of the AIIM community between January 5-15, 2010, using a Web-based tool. Invitations to take the survey were sent via email to a selection of the 65,000 AIIM community members

Organizational Size

Survey respondents represented organizations of all sizes. Larger organizations (over 5,000 employees) represented 29%, with mid-sized organizations (500 to 5,000 employees) at 36%. Small-to-mid sized (10 to 500 employees) - were 31%. Just 4% of organizations were less than 10 employees so these are included in the results.
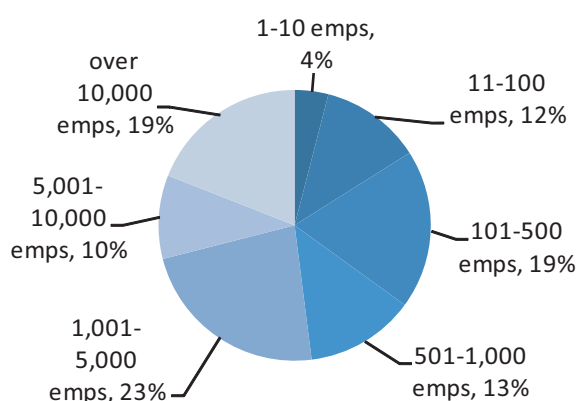
Industry Sector

Local government makes up 20% of the demographic, with the finance sector taking a further 17%. The remaining sectors are evenly split. The participation of 3% ECM suppliers was not considered sufficient to bias the report.

UNDERWRITTEN BY

www.arx.com
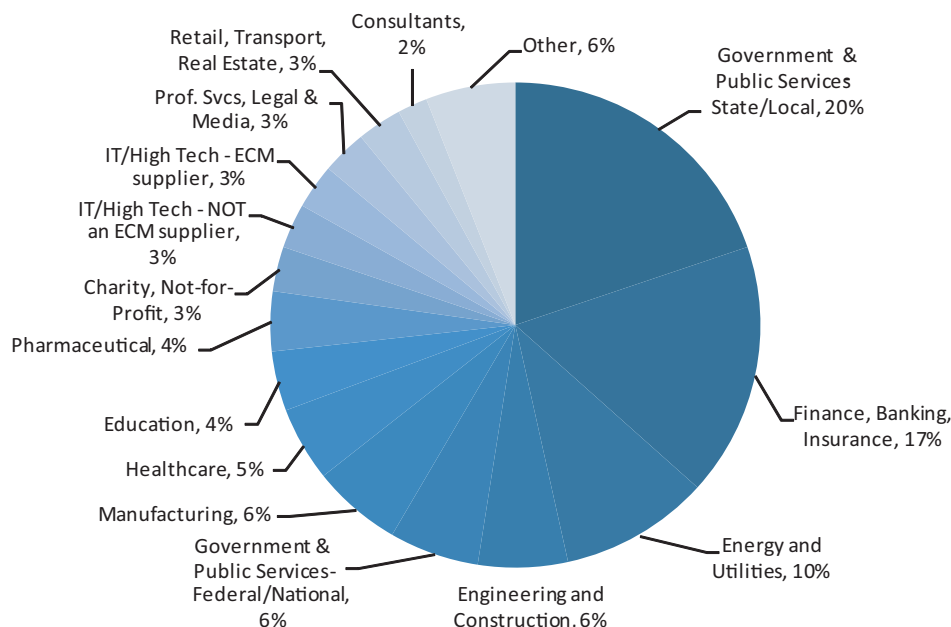
ARX (Algorithmic Research) is a global provider of cost-efficient digital signature solutions for industries such as life sciences, healthcare, government, and engineering. ARX engineers and scientists have more than 20 years of experience in security and standard digital signature application. ARX helps businesses secure, streamline, and scale their business processes and transactions with the proper controls required by legislation, regulation, and industry best practice.

ARX's CoSign® digital signature solution automates approvals affordably in a compliant manner, allowing organizations to go paperless, expedite business processes and save costs. CoSign signatures are globally accepted by external partners and customers without the need for proprietary-validation software. CoSign is also centrally managed through the organization's user/customer directory for reliable control of signature privileges, and ease of use and administration.

Learn more about ARX and CoSign at www.arx.com.

CoSign Central Digital Signature Add-on for SharePoint

The CoSign Central digital signature platform integrates with SharePoint out-of-the-box and enhances SharePoint's capabilities by enabling it to provide compliant signature-based approvals on PDF's and lists.

CoSign provides digital certificate and key management from a secure network-attached appliance, plus centralized control over authorized signers (through Microsoft Active Directory or other directory services). When implemented with SharePoint, CoSign features appear as a natural part of the familiar SharePoint and Microsoft Office interface. This enables signature-based approval processes to remain paperless while complying with regulations, expediting processes, and cutting costs. Because CoSign for SharePoint allows digital signing via the SharePoint interface, it permits users to leverage their pre-existing investment in SharePoint in order to digitally sign various Enterprise, B2B and B2C content. A flash demo of CoSign digital signatures for SharePoint is available here.
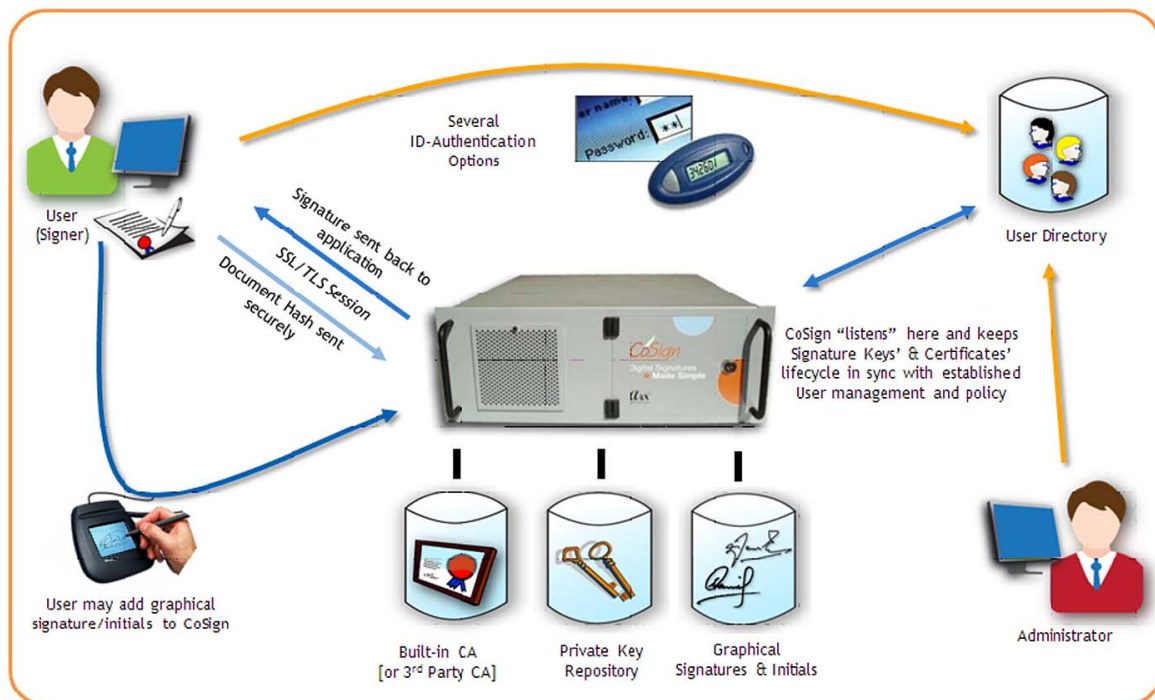
aiim®

Find, Control, and Optimize
Your Information

AIIM (www.aiim.org) is the community that provides education, research, and best practices to help organizations find, control, and optimize their information.

For over 60 years, AIIM has been the leading non-profit organization focused on helping users to understand the challenges associated with managing documents, content, records, and business processes. Today, AIIM is international in scope, independent, implementation-focused, and, as the representative of the entire ECM industry - including users, suppliers, and the channel—acts as the industry's intermediary.

© 2010
AIIM
1100 Wayne Avenue, Suite 1100
Silver Spring, MD 20910
301.587.8202
www.aiim.org

AIIM Europe
The IT Centre, Lowesmoor Wharf
Worcester, WR1 2RR, UK
+44 (0)1905 727600
www.aiim.eu