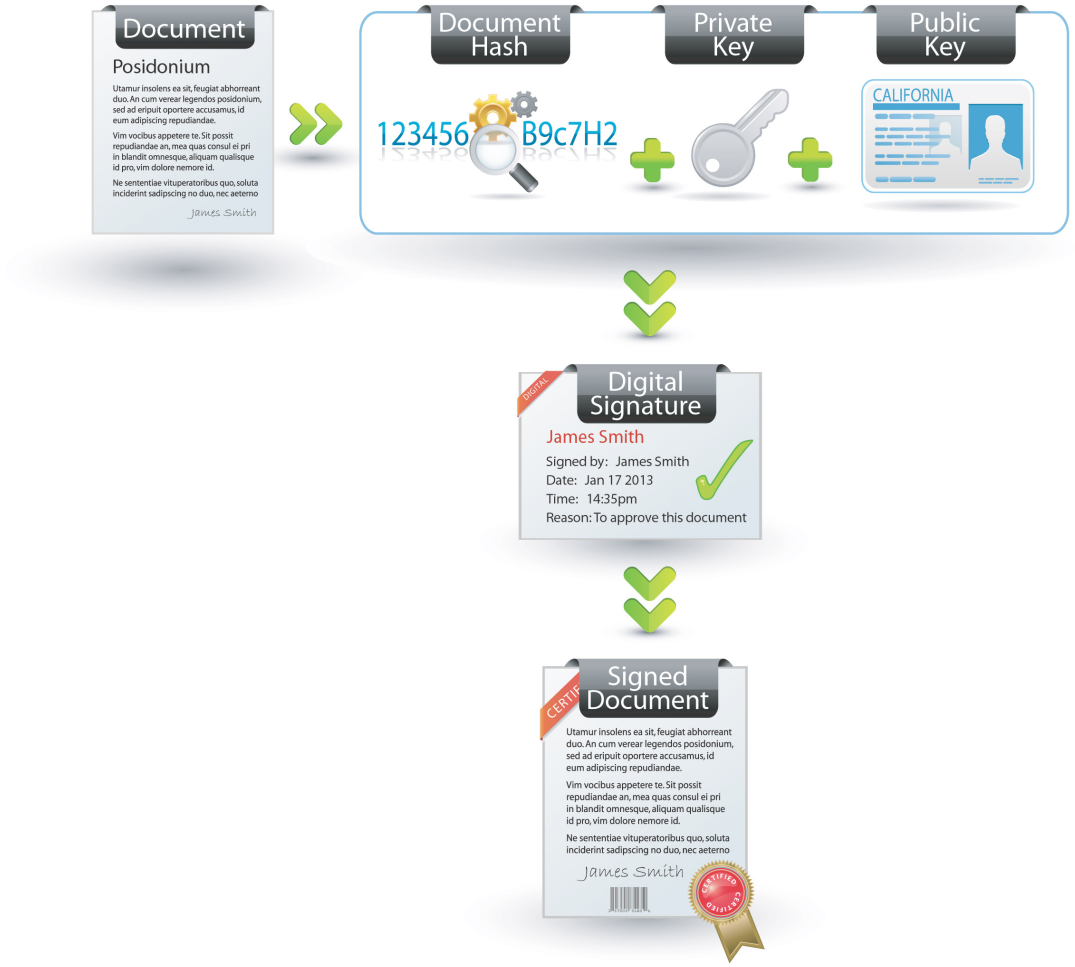

Document
Posidonium
Utamur insolens ea sit, feugiat abhorreant duo. An cum verear legendos posidonium, sed ad eripuit oportere accusamus, id eum adipiscing repudiandae.
Vim vocibus appetere te. Sit possit repudiandae an, mea quas consul ei pri in blandit omnesque, aliquam qualisque id pro, vim dolore nemore id.
Ne sententiae vituperatoribus quo, soluta inciderint sadipscing no duo, nec aeterno
James Smith
Document Hash
123456
B9c7H2
Private Key
Public Key
CALIFORNIA
DIGITAL
Digital Signature
James Smith
Signed by: James Smith
Date: Jan 17 2013
Time: 14:35pm
Reason: To approve this document
CERTIF
Signed Document
Utamur insolens ea sit, feugiat abhorreant duo. An cum verear legendos posidonium, sed ad eripuit oportere accusamus, id eum adipiscing repudiandae.
Vim vocibus appetere te. Sit possit repudiandae an, mea quas consul ei pri in blandit omnesque, aliquam qualisque id pro, vim dolore nemore id.
Ne sententiae vituperatoribus quo, soluta inciderint sadipscing no duo, nec aeterno
James Smith
CERTIFIED

Digital Signatures - making the business case

Sponsored

CoSign By Arx

aiim®
The Global Community of
Information Professionals

About the White Paper

As the non-profit association dedicated to nurturing, growing and supporting the user and supplier communities of ECM (Enterprise Content Management) and Social Business Systems, AIIM is proud to provide this research at no charge. In this way the entire community can take full advantage of the education thought-leadership and direction provided by our work. Our objective is to present the "wisdom of the crowds" based on our 70,000-strong community.

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: +1 415.839.8161
Website: www.arx.com

Process used and survey demographics

The survey results quoted in this report are taken from a survey carried out between 03 Oct 2012 and 05 Nov 2012, with 283 responses from individual members of the AIIM community surveyed using a Web-based tool. Invitations to take the survey were sent via email to a selection of AIIM's 70,000 registered individuals. Respondents cover a representative spread of industry and government sectors. Results from organizations of less than 10 employees have not been included, bringing the total respondents to 263.

About AIIM

AIIM has been an advocate and supporter of information professionals for nearly 70 years. The association mission is to ensure that information professionals understand the current and future challenges of managing information assets in an era of social, mobile, cloud and big data. AIIM builds on a strong heritage of research and member service. Today, AIIM is a global, non-profit organization that provides independent research, education and certification programs to information professionals. AIIM represents the entire information management community: practitioners, technology suppliers, integrators and consultants. AIIM runs a series of training programs, including the ECM Master course.
www.aiim.org/training/ECM-Enterprise-Content-Management-Course

About the author

Doug Miles is head 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. He was an early pioneer of document management systems for business and engineering applications, and has produced many AIIM survey reports on issues and drivers for Capture, ECM, Records Management, SharePoint, Big Data and Social Business. Doug has also worked closely with other enterprise-level IT systems such as ERP, BI and CRM. He has an MSc in Communications Engineering and is a member of the IET in the UK.

© 2012
AIIM
1100 Wayne Avenue, Suite 1100
Silver Spring, MD 20910
+1 301 587-8202
www.aiim.org

© 2012
ARX
855 Folsom Street, Suite 939
San Francisco, CA 94107
+1 415.839.8161
www.arx.com

Table of Contents

About the White Paper:

Introduction:

Drivers for Digital/Electronic Signing:

Adoption of Electronic/Digital Signatures:

Characteristics of Signature Solutions:

Benefits and Return on Investment:

Conclusion and Recommendations:

Appendix 1: Survey Demographics:

Appendix 2: Digital Signature Primer:

Appendix 3: Open ended comments

Underwritten in part by:

Introduction

As more and more organizations adopt paper-free processes and automate their document-based workflows, the “wet ink” signature stands out as something of an evolutionary laggard. Electronic signing mechanisms have been with us for a long time, but their adoption has been slow. Some of this is due to a lack of trust on the part of legal counsel – despite progressive legislation to the contrary – and some is due to confusion between the different mechanisms and technologies involved. All too often it is because the business case is not sufficiently prioritized to push it up the IT to-do list.

However, as we rely more and more on electronic workflows and less and less on document exchange via post, fax or courier, the discontinuities and delays caused by physical signing have become harder and harder to ignore. As we have found in this survey report, when existing users make a cost/benefit analysis for the adoption of electronic signing, the payback period is consistently one of the shortest we have seen for any IT investment. Whilst analyzing simple document exchanges provides one dimension of cost-savings, removing the disruptive and delaying effects of physical approval sign-offs within otherwise time-efficient electronic processes generally adds a much bigger benefit.

As we described in the “The Paper Free Office,[1]” replacing space-hungry, slow and unresponsive processes with electronic workflows has huge benefits, particularly as businesses look to become more diverse and more mobile. However, paper can easily creep back in if we let it. Printing documents to collect signatures is still very prevalent even in otherwise paper-free environments, slowing things down and clogging up desks.

In this report, we look at the drivers for electronic signing, the general understanding of the different technologies, the issues that might be preventing adoption, and the ROI that is being achieved by users. We also track changes from our previous survey in 2010.

For those needing a technical and legal appreciation of the differences between electronic signatures, and digital signatures based on Public Key Infrastructures (PKI), please refer to Appendix 2 and References 2-7.

Key Findings

ROI

The payback period is consistently one of the shortest we have seen for any IT investment:

- 81% of existing digital signature users have seen a payback within one 12-month budget cycle. 25% saw ROI in three months or less.
- The two biggest benefits are saving of staff time and speeding up the approval process. Saving of paper-handling costs comes next, particularly courier charges.

Drivers

Major process interruptions and delays due to employees still signing with pen and paper

- Authorization signatures are considered essential for 58% of responding organizations. Over half need to bring travelling, remote or home-based employees into the signing loop. 40% need signatures from people outside the organization.
- For 44% of organizations, half or more of their processes are interrupted by the need to collect physical signatures. The average across all respondents is that 42% of processes are interrupted.
- On average, 3.1 days is added to most processes in order to collect physical signatures. 22% of organizations add a week or more to their processes.
- 48% of process documents are printed for the sole purpose of adding signatures. For 26% of organizations, this rises to over 80% of printed process documents.

- 60% of respondents admit that they frequently print and sign documents and then scan them back in to their DM/ECM system. 64% frequently print, sign and file manually. 33% regularly print, sign and courier documents.
- On average, 2.1 additional copies are printed of each process document in order to collect signatures.
  32% create three or more copies of each process document.

Adoption

35% of organizations have already automated their signature-dependent processes

- 35% of organizations who have answered the survey are already using digital/electronic signatures, up from 24% in the 2010 survey. A further 11% have plans in the next 12 months.
- Self-managed in-house digital signature (PKI) solutions are the most popular with existing users, but planned users are evenly split between this and server or appliance-based PKI systems. 30% are using non-PKI solutions.
- Lack of familiarity with the technology is the most tangible reason for non-adoption, as it was in the previous survey. 35% still report general unfamiliarity with legal admissibility and industry specifics, 40% don't really understand digital signatures and PKI mechanics, and half are confused about encryption and the issues of self-certification.
- Lack of priority and the perceived level lack of financial return feature highly as reasons not to adopt. Difficulty of working outside the firewall with external partners and customers is ranked as number three.
- Process owners and signers are the most keen to adopt. Compliance/Records Managers and Finance are mostly in favour. Lawyers and auditors are not so keen. The IT staff have the biggest influence but are somewhat ambivalent.

System Characteristics

Highest ranked features: signing multiple file types and managing signatures through Active Directory profiles

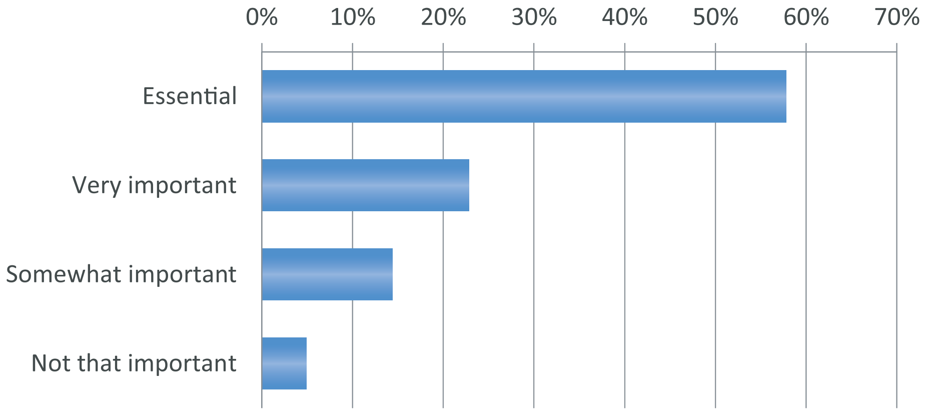
- 46% of user organizations have 50 signers or less. A quarter have more than 500. 45% are using an in-house-developed management interface or are managing individual certificates. Only 19% are managed through Active Directory.
- Two-factor authentication is used in 45% of organizations. Mostly numeric key fobs at login time, but also iPads or other tablets at signing time.
- Existing users look for the ability to sign multiple file types, and for one-click sign-and-encapsulate functions. It is also important that multiple signatures can be added to already signed and sealed documents.
- Managing signatures as part of Active Directory profiles is important, as is batch signing of documents in SharePoint. Approving workflow processes or forms with non-refutable signatures is particularly important for SharePoint users.

Drivers for Digital/Electronic Signing

Signatures in Business

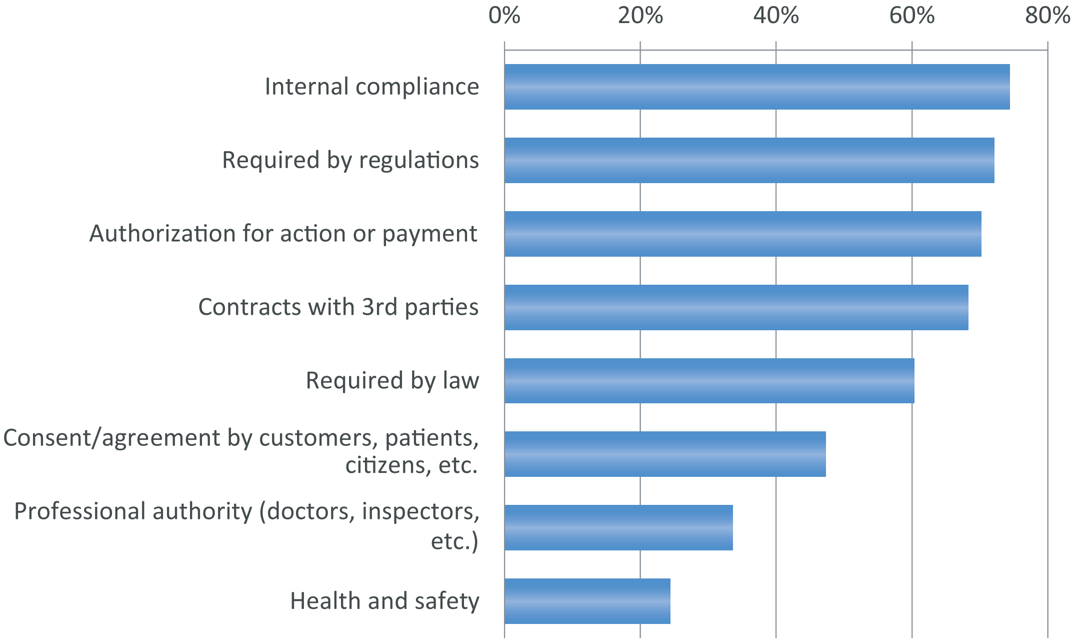
Unsurprisingly, the importance of signatures has not changed at all since our previous report in 2010, with 81% of respondents considering them to be very important or essential within their regulatory environment. Industry sectors of Government, Healthcare, Pharmaceutical and Banking and Finance place the highest store on signatures for their day-to-day activities. This also reflects a higher dependence in larger organizations (66% essential) compared to smaller ones (49% essential).

Figure 1: With regard to the regulatory environment or standard business practices in your industry, how important are authorization signatures within your organization? *(N=263)*



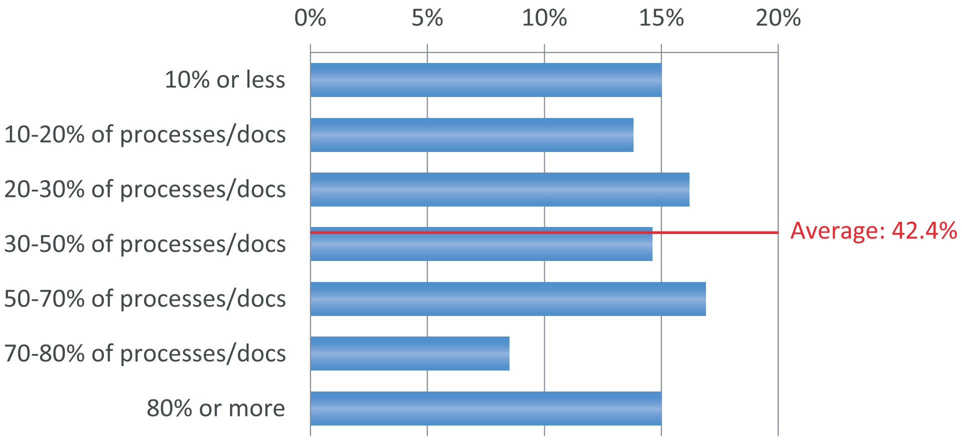
When it comes to why and where signatures are used, internal compliance, external regulation, and authorizations for contracts or payments are prevalent. 60% have a strong legal requirement for signatures.

Figure 2: For which of the following needs are authorization signatures considered essential in your organization? (Tick all that are significant) *(N=262)*



When analyzing the use of signatures, it is important to consider the process as a whole rather than just the document or form that is used as the carrier for the signature. On average, around half of the processes need signatures at some point, but in some organizations almost all processes require an authorization signature.

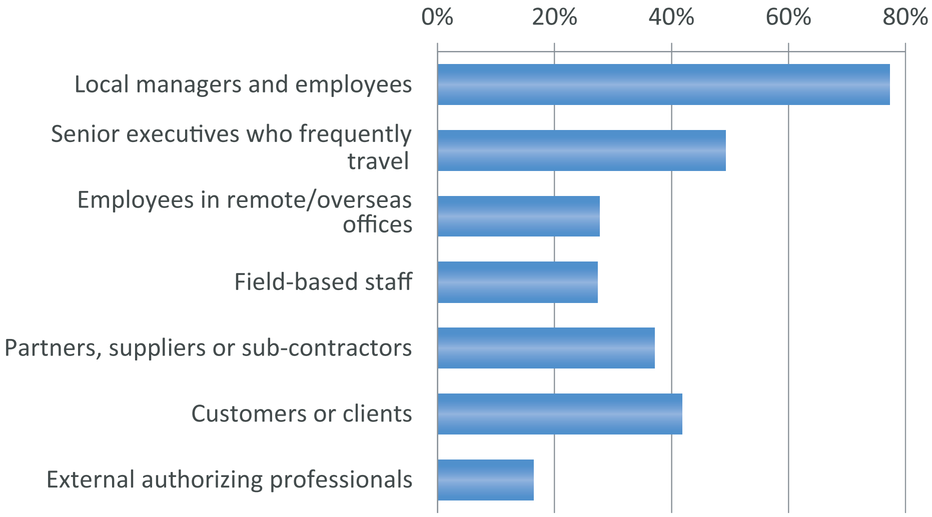
Figure 3: What percentage of the main business processes/documents in your organizational unit would you say require authorization signatures? *(N=260)*



Even quite small businesses will have a few authorized signers who formally sign documents two or more times a day. In larger organizations the number rapidly grows to many hundreds of people, signing thousands of documents a day.

It is increasingly the case that the managers who need to sign-off documents or processes are frequent travellers, or may be based in remote or overseas offices, and this creates problems for over half of our respondents. Distributing the documents electronically is not an issue these days, but collecting a physical signature is, and as we all get more connected, any delay in an authorization response becomes less and less acceptable. Forty-two per cent would also like to include customers and clients in the loop.

Figure 4: As part of your main business workflows, who of the following are required to sign and return documents or approve your process steps? *(N=256)*

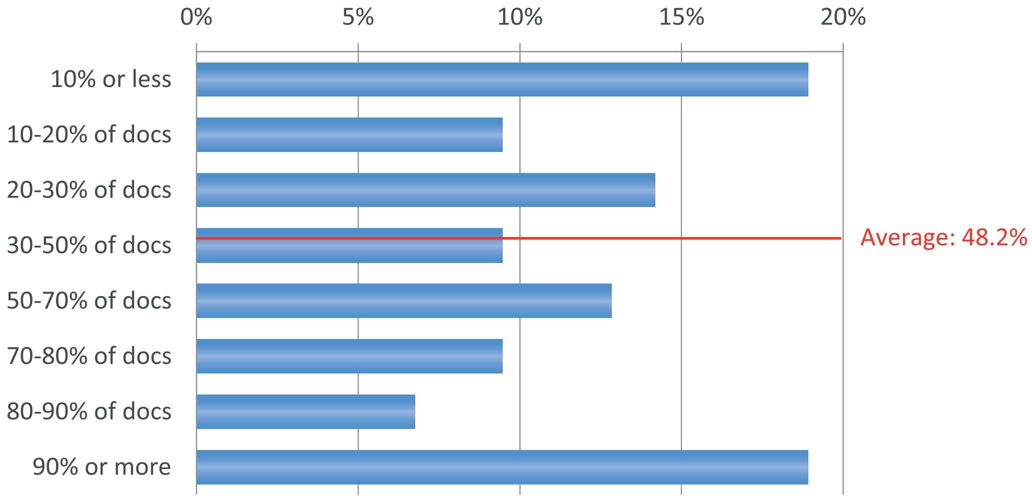


Needless Document Printing

Half or more of the printed process documents are printed just to add a signature in the 48% of organizations without digital signature solutions. Averaging the figure over all non-user organizations, 48.2% of all process documents would not need to be printed if a digital signature system was in place. See figure 5.

Wherever the signer is located, if documents have to be printed, posted, faxed, physically signed and rescanned, this adds costs, delays and staff inefficiencies.

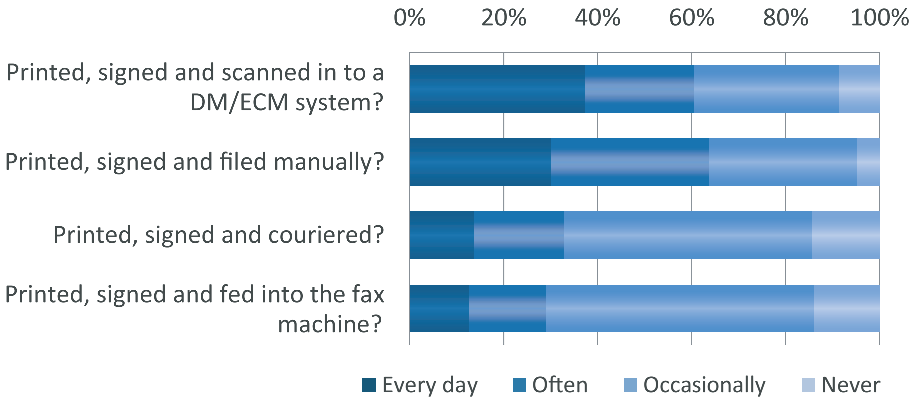
Figure 5: Considering the documents that are printed out as part of your formal approval processes, what proportion would you say are printed for the sole purpose of adding one or more signatures? *(N=153 non-users)*



We also found that on average, 2.1 additional print copies, photocopies or fax copies of each process document are likely to be needed in order to collect signatures. For a third of organizations it is three or more additional copies – all of which need to be handled distributed and filed.

Other wasteful practices include the 60% who frequently print born-digital documents for signature and then scan them into a document management or ECM system, including 30% who do this every day. To beat postal delays, 33% admit to regularly printing, signing and then couriering documents, with the associated costs and delivery difficulties. Just looking at Figure 6, and thinking of all the unnecessary handling costs involved, shows how this simple aspect of business creates so many inefficiencies.

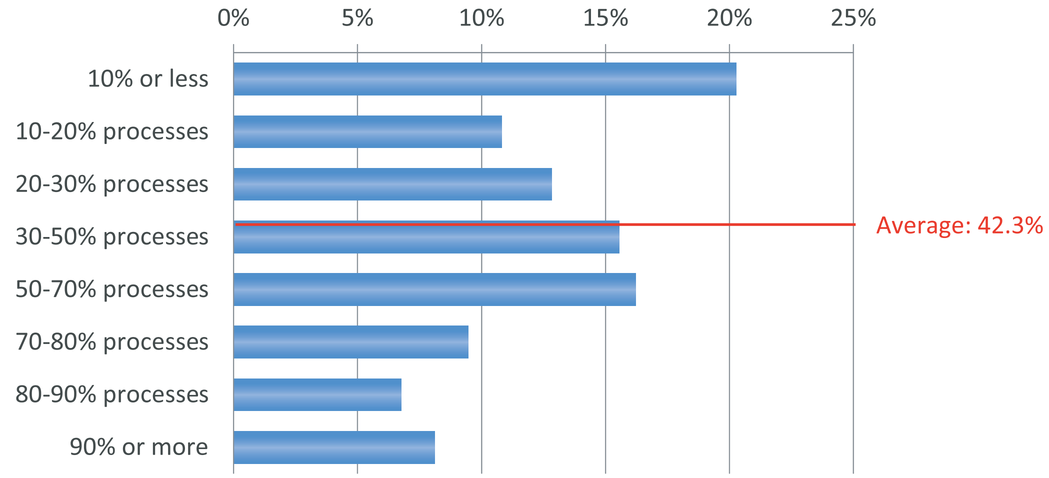
Figure 6: In your organizational unit, how frequently are documents: *(N=153, non-users)*



Interrupted Processes

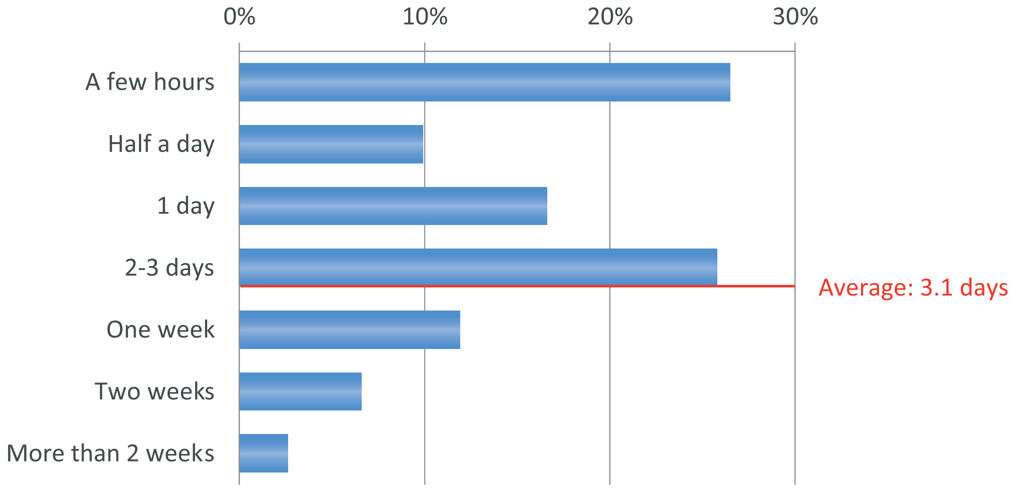
We also asked non-users what proportion of their electronic or scanned document workflows are interrupted or prematurely completed by the need to collect physical signatures. For 44%, half or more of their workflows are impacted. This is a rise of 4% since the last survey, indicating general progress towards more paper-free processes, despite that final hurdle of the signature placement. On average, 42.3% of processes are slowed down.

Figure 7: What proportion of your key processes would you say are interrupted, slowed down or prematurely completed by the need to collect physical signatures on paper? *(N=153 non-users)*



Looking at the extent of the slowdown, 65% think at least a day is added to their processes in order to collect physical signatures. For 22% it's a week or more. The average is 3.1 days. Just in terms of business agility, this is a serious issue, but if reflected into customer response, it indicates a major opportunity for improvement.

Figure 8: How much time would you say is generally added to a typical formal approval process as a result of this physical sign-off? *(N=151)*



Drivers for SharePoint

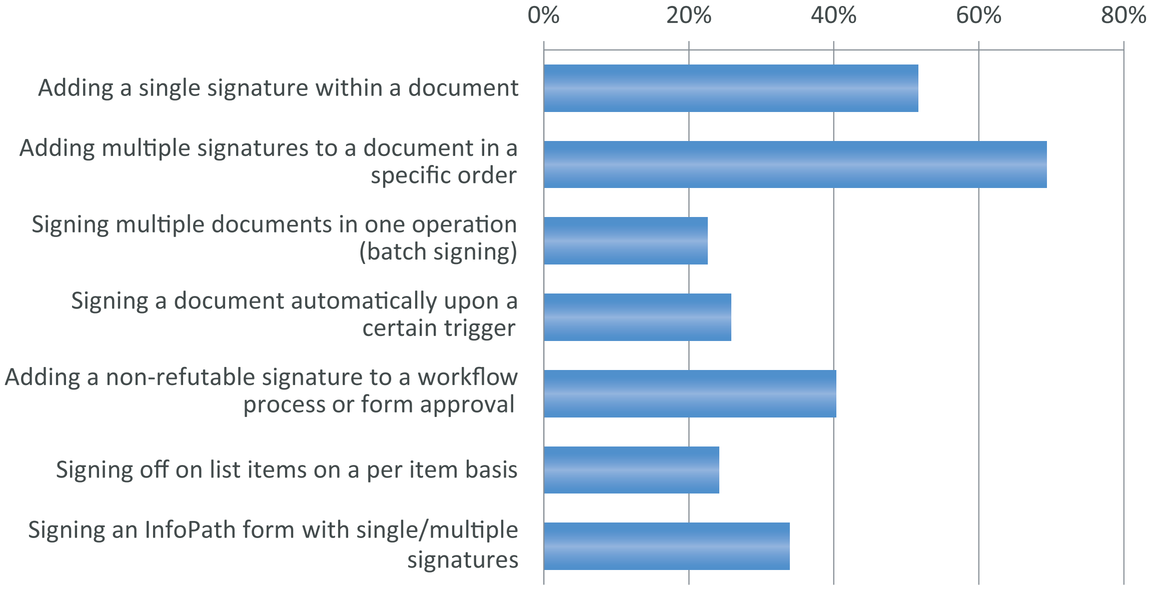
Only one in four SharePoint installations are used to manage documents or processes that need approval. Two thirds of the organizations in our survey use SharePoint in some way, but in more regulated industries, its use tends to be relegated to team collaboration and intranet portals.

SharePoint is relatively straightforward to use for many workflow processes including staff claims, purchase requisitions, project reports, etc. Generally, a tick box is used to indicate approval, relying on the login password for authentication.

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. Despite the ready availability of off-the-shelf digital signature solutions that readily integrate with SharePoint, IT departments may be tempted to create their own. They should be careful when creating or incorporating less standard electronic signature solutions to ensure that an auditable security regime is maintained. Manual PKI solutions should also be approached carefully due to ease-of-use and scaling issues.

69% of the organizations surveyed have a need to add multiple signatures to documents in SharePoint, generally in a specific order. 40% need to add a non-refutable signature to a workflow process or form approval, and 34% are using InfoPath forms that need to be signed. Users are also keen to sign off batches of documents in one operation, or to sign off list items on a per item basis.

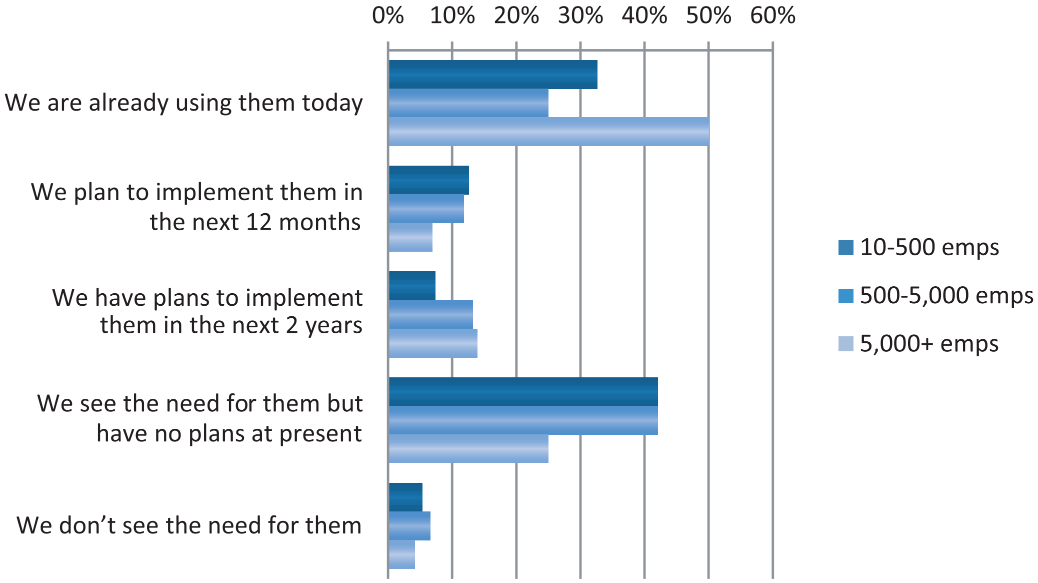
Figure 9: Do you have any of the following requirements within SharePoint?
(N=62, excl. 175 “None of these, N/A”)



Adoption of Electronic/Digital Signatures

Our survey response was self-elected, and so at 35%, it is likely to overestimate those already using digital signatures. In our previous survey we measured 24% of current users. Overall growth is very strong, with a further 22% planning to go ahead within the next 2 years. Half of the largest organizations are already users, compared to a quarter of the rest, but this is quite even across both small and mid-sized organizations.

Figure 10: How would you describe the use of digital/electronic signatures in your organizational unit? *(N=242)*

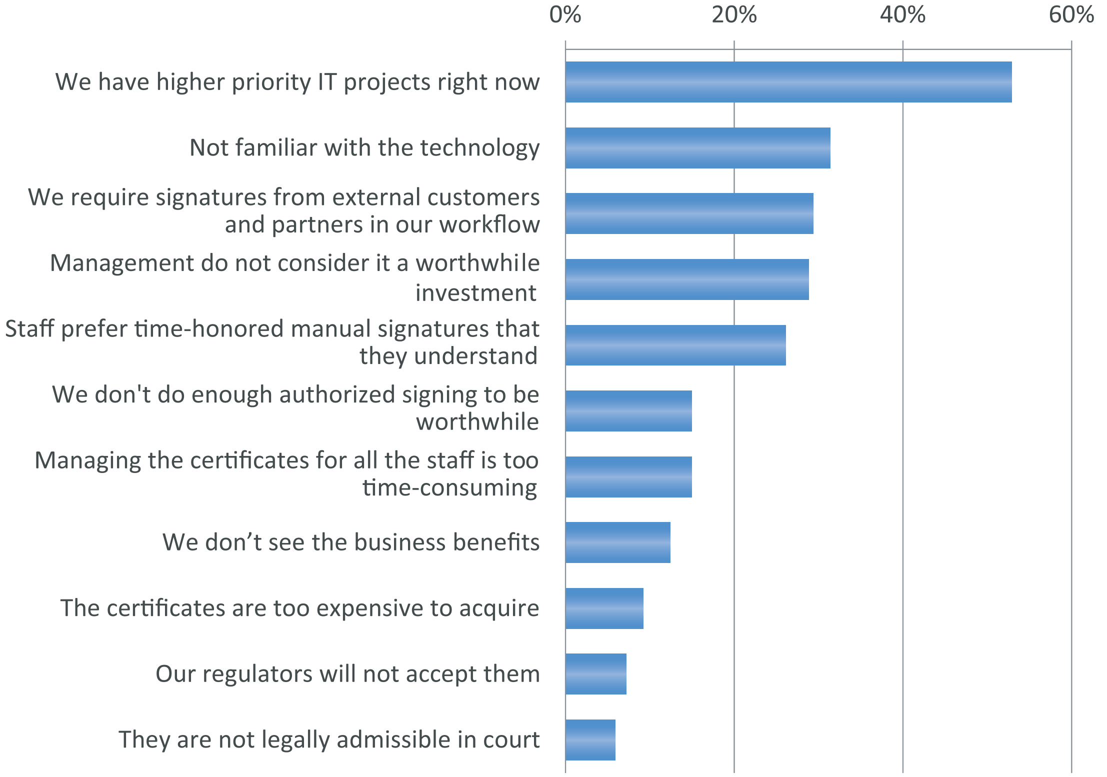


Non-Adopters

As indicated in the previous graph, everyone can see the need for digital signatures, but Figure 11 shows that it is not seen as a priority by the IT department. A number of other factors are also in play, the strongest of which is a lack of familiarity with the technology. This has not changed position since our previous survey—despite AIIM's efforts with regular webinars and conference presentations. Having said that, the preference for time-honoured methods has dropped slightly and the issue of dealing with external customers and partners beyond the firewall has come to the fore.

It is hoped that as secure cloud or SaaS solutions become more accepted, this issue can be overcome – and indeed 23% of respondents would have no problem with a cloud solution per se as long as it did what they need. The issue of legal admissibility in court has dropped three positions to last place compared to the previous survey, which is encouraging, although we will see later that there is still resistance from legal counsel and auditors to the idea of electronic signatures.

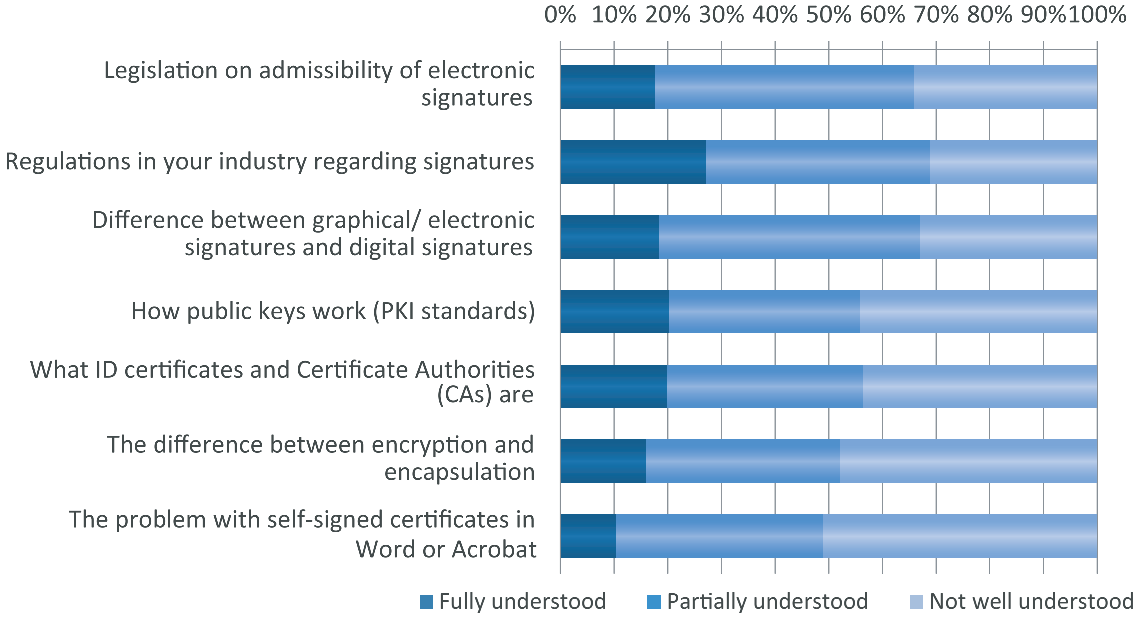
Figure 11: What would you say are the most prevalent reasons that digital/electronic signatures are not currently used in your organizational unit – maximum THREE? *(N=153, non-users)*



Technical Understanding

Looking in more detail at this unfamiliarity with how these systems work, we asked respondents how well understood various aspects of digital or electronic signing were in their organization – which is not to say that the respondents themselves are not sufficiently knowledgeable. All organizations are included here, users and non-users. For more details on topics, see Appendix 2.

Figure 12: How well understood would you say are the following aspects of digital/electronic signatures in your organization? *(N=223 All)*



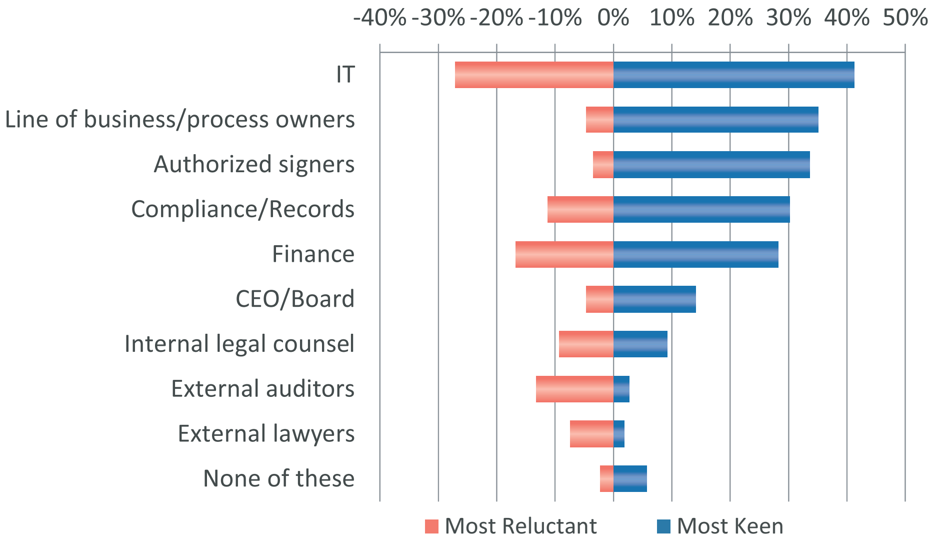
Champions and Objectors

One of the most revealing questions compares those who are the most keen to adopt electronic signing with those who are the most reluctant.

Process owners and in particular, authorized signers are the most in favour. Internal legal counsel and in particular external lawyers and auditors are the most resistant – although for the latter, this may be a perception rather than a reality. However, the length of the lines in Figure 12 indicates the degree of influence that these different departments have.

IT are the most likely to be involved in the decision, and the survey shows them to be the most ambivalent with equal numbers for and against

***Figure 13: Who in your organization would you say are/would be the most keen/most reluctant to move to electronic signing? (Max TWO)** (N=262)*



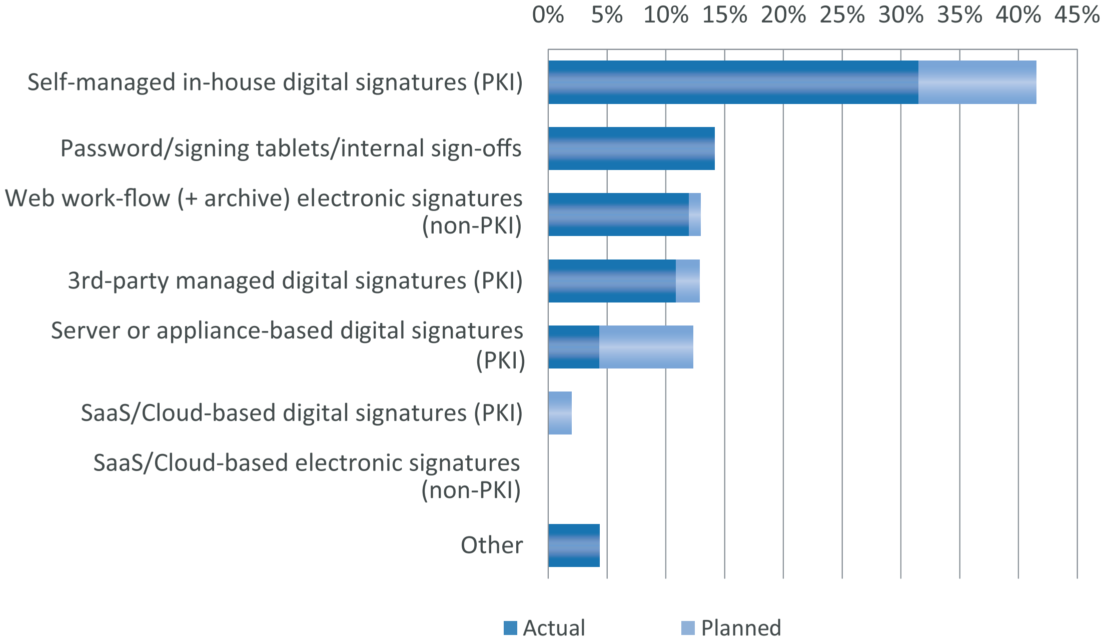
Characteristics of Signature Solutions

We discussed earlier that there was a general lack of understanding of electronic signature technology and to some extent this is because of the variety of solutions in the market which operate in quite different ways. There are also a number of national and international standards in this area which are only slowly converging. We are not going to discuss these differences here, but would once again suggest reading Appendix 2 particularly regarding the differences between “electronic signatures” and “digital signatures.”

From Figure 14 we can see that the “traditional” approach has been to use a self-managed or self-developed system using PKI certificates. This can be an expensive approach that is quite tricky to manage, and we can see that for those planning a system, server or appliance-based PKI solutions are becoming more popular, relatively speaking.

The largest organizations are nearly three times more likely to be using web work-flow and only half as likely to use self-managed PKI. Large companies have the experience that traditional PKI implementations are difficult and expensive to scale. Additionally, in the US, non-PKI “e-signature” web applications are used despite their lack of standards compliance and other limitations.

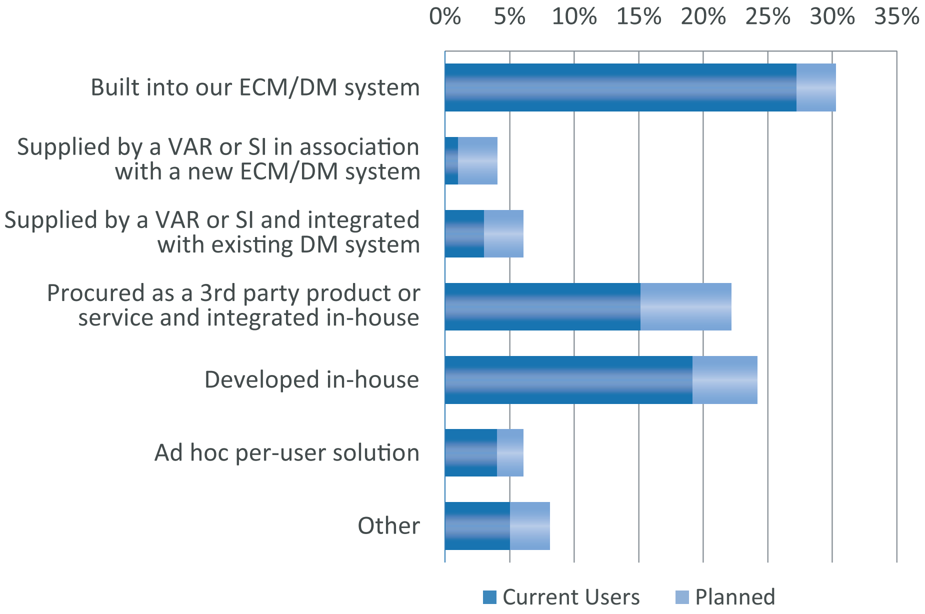
Figure 14: How would you describe your main digital/electronic signature solution?
(N=83 using now, 27 planned)



Sourcing

When it comes to the delivery method for a digital or electronic signature system, the traditional base of heavily regulated industries are likely to have acquired it as part of a DM or ECM system – particularly larger organizations (32%). Those planning a system now are more likely to procure a 3rd party product and to integrate it in-house. There are still some who are likely to develop a system themselves, particularly smaller businesses (36%), although the risk here is either that it will not be as secure as it should be, or that it becomes unwieldy to manage when scaled. All of the effort involved in implementing a digital signature solution will come to naught if its veracity cannot be upheld in court.

Figure 15: How was your digital/electronic signature solution delivered?
(N=83 using now, 27 planned)

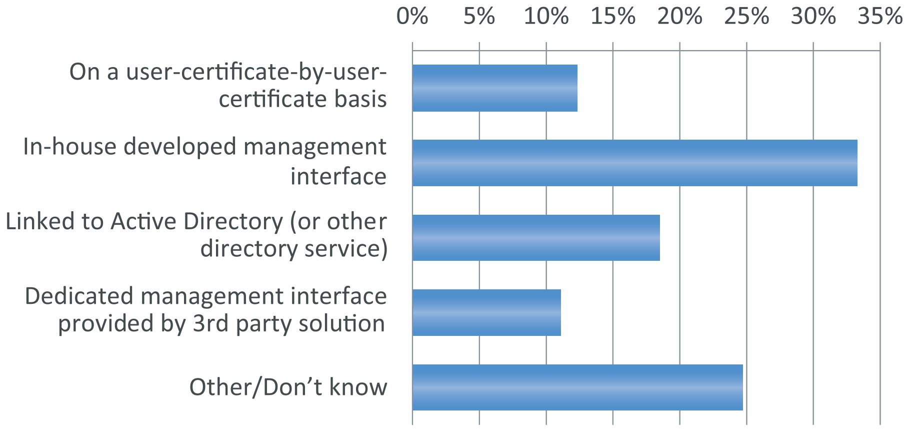


Management

When it comes to managing a system, especially those with many signers, it becomes particularly important to have automatic synchronization with the organization's Active Directory or similar system. This will minimize costs for enrolling, updating and "off-boarding" signers. It will ensure that when a staff member leaves, their signing certificate will automatically be immediately retired. Automating signatures should not add a new manual system for administering the community of authorized signers.

Signing systems in use cover a wide range of user numbers, with 24% having less than 10 signers, and 23% having more than 500. Scaleability of costs is therefore important, but smaller organizations should not assume that a digital signature solution will be too expensive.

Figure 16: How do you set up and maintain users of your digital/electronic signature system? *(N=81 users)*

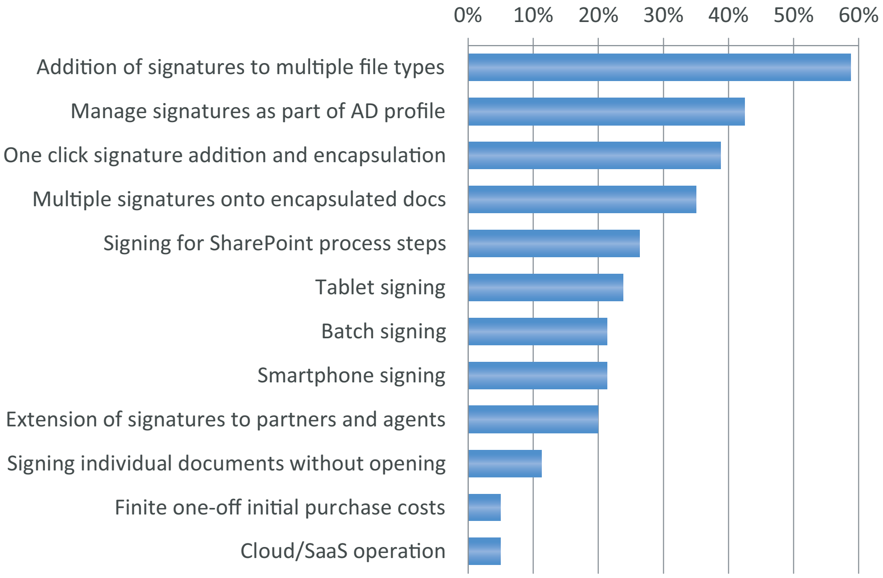


Functionality

Signing multiple file types is the most important feature for a digital signature solution. The next most important feature is integration with a directory service, showing the importance of minimizing administrative costs.

Feature sets are likely to vary considerably between different offerings, particularly modern systems compared with older ones, but to set a baseline, we asked existing users which functions they felt were the most important. One-click signing and encapsulation, and adding multiple signatures to otherwise encapsulated documents are also core requirements. For heavy SharePoint users, ready integration to SharePoint processes is also an important factor.

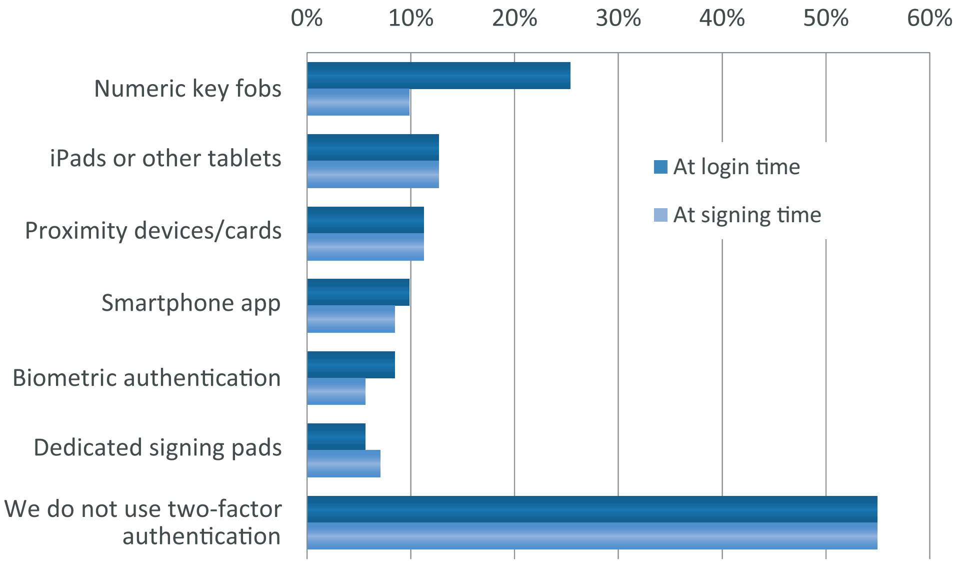
Figure 17: Based on your experience, which four of the following features, would you consider the most important in a digital/electronic signatures solution? (Max FOUR) *(N=80 users)*



Two-Factor Authentication

The addition of two-factor authentication can be important to the integrity of a signing system, and is almost essential if a PKI mechanism is not used. Numeric keyfobs will be familiar from banking systems, and are popular as both a login validation and a signature authentication, as are proximity devices or cards. Tablets and dedicated signing pads, and increasingly smartphone apps, are also in use, but not widely.

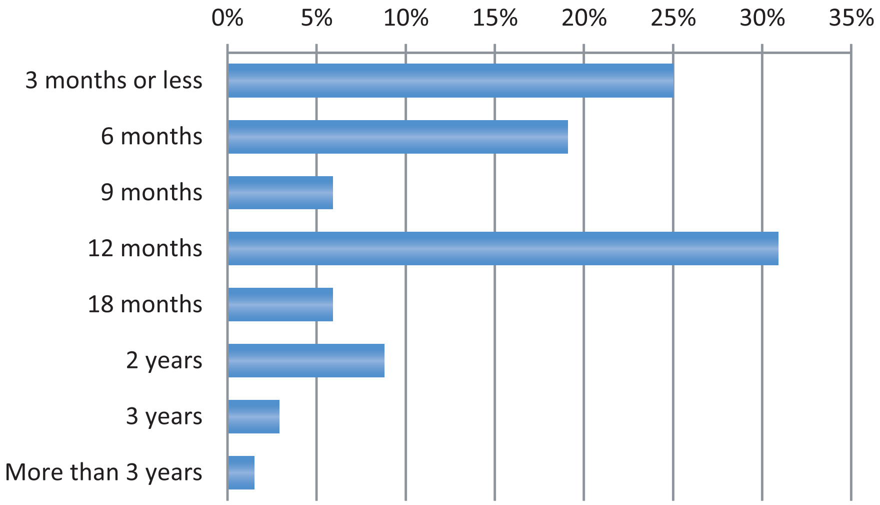
Figure 18: Do you use any of the following for two-factor authentication? *(N=71 users)*



Benefits and Return on Investment

Our survey shows that a digital signature project is usually an easy "win" for the IT department with 81% of users seeing a payback period of 12 months or less. 25% saw a spectacular ROI of 3 months or less. Our respondents are even more confident of the returns in this survey than they were two years ago when 63% saw an ROI of 12 months or less.

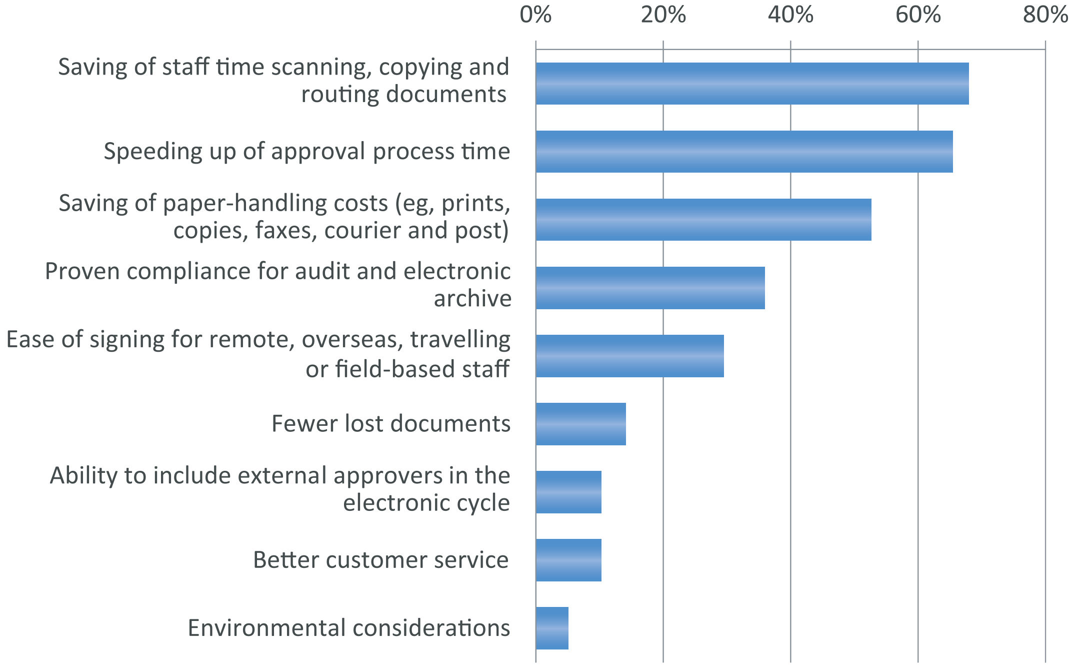
Figure 19: Considering financial, operational and customer-service benefits, what would you consider to be/will be the payback period from your investment in digital/electronic signature systems? *(N=68 users)*



We also asked those respondents planning a system for their payback expectation. Most (77%) were realistic in looking to a 12 month period, but only 35% predicted a 6 month or less payback, underestimating the 44% of actual users who achieved this. Few anticipate a 3 month payback.

As we have outlined throughout the report, savings on the time and costs of physically handling documents, and the speeding up of approval processes are the biggest benefits from digital/electronic signatures. Proven compliance for otherwise electronic processes is also a key factor, and ease of signing for remote or travelling staff. The ability to include external approvers in the electronic cycle is ranked fairly low here, although respondents were limited to three choices. The increasing availability of cloud-based PKI solutions could be an important factor in extending the signing system outside the firewall.

***Figure 20: Which THREE of the following would you describe as the biggest benefits of your digital/electronic signatures system? (Max THREE)** (N=78 users)*



Conclusion and Recommendations

We have seen that the adoption of electronic and digital signatures has moved on apace since our last survey, rising from 24% two years ago to 35% now. This is no doubt driven by the very high ROI that we reported then, and which existing users have rated even more highly in this report, with 25% seeing a return within 3 months and the vast majority (81%) in less than 12 months.

For those organizations who have not adopted digital or electronic signing solutions, the time-sapping requirement to halt processes and print off documents goes on, and the physical difficulties of putting those documents in front of signers who are remote, travelling or in other organizations continues to take up time and add costs for printing, postage, couriers, etc.

Despite the very positive benefits, digital or electronic signature projects seem to have a low priority within IT departments, and IT staff are somewhat ambivalent about the technology – most likely due to a lack of understanding about the different mechanisms. Business owners and authorized signers are keen to go ahead, and there is a clear majority of compliance and finance staff who are happy with the legal admissibility that digital (PKI) systems provide. Internal legal counsel are more evenly split, but there is a perceived impression that external auditors and lawyers are not enthusiastic, which may not in fact be the case, as they also incur huge costs from physical document handling.

It is important that signing systems are easy to use and to manage through directory services, and that they cater for a broad spectrum of document types. Handling multiple signatures and the ability to integrate with ECM systems and process platforms is also important, in particular SharePoint. Packaged server or appliance-based products have made considerable headway compared to older, custom-built systems, and the solid admissibility aspects of the PKI mechanism are overcoming legacy arguments about authenticity.

Recommendations

- Assess how many of your processes are interrupted by the need for a physical signature.
- Look at the delays introduced and the number of additional documents printed and handled.
- Consider the potential benefits if travelling and remote staff could quickly and easily sign off processes and approvals without the need to print and scan.
- For those processes where signatures are used, check regulatory and legal requirements to determine the validity of different signing options. Focus on authenticity, integrity, enforceability and non-refutability.
- Do not assume that your external auditors and lawyers distrust digital/electronic signatures – ask them.
- Check how many of your staff are using simple bit-map images of their signatures, self-certified digital signatures within Word or Acrobat, or ad hoc PKI certificates.
- When considering solutions, check which integrate with your existing DM/ECM systems and process platforms. Take particular care if you are using SharePoint for sensitive processes.
- Check features such as multiple file formats, sign-and-seal, multiple signatures applied in order, batch approval of documents, and sign-off of workflow processes.
- Make an assessment of how many signers would benefit from the digital solution, and consider how difficult it would be to manage these on a one-by-one basis. Consider which solutions integrate and automatically synchronize with your Active Directory system.
- Be particularly wary of developing an in-house system. The system and your procedures both need to be robust in the event that they are ever questioned in court. A reputable packaged system may prove to be more convincing, and more cost-effective.

References

1. AIIM Industry Watch, “The Paper Free Office – dream or reality” Feb 2012, www.aiim.org/research
2. Computer Desktop Encyclopedia www.computerlanguage.com
3. ISO 15489, Section 7.2
4. BSI BIP 0008, Code of Practice for legal admissibility and evidential weight of information stored electronically
5. Electronic Signatures in Global and National Commerce, Public Law106–229—June, 2000 ref.
6. Digital Signature Standard (DSS) http://csrc.nist.gov/publications/fips/fips186-3/fips_186-3.pdf
7. ISO 32000-1

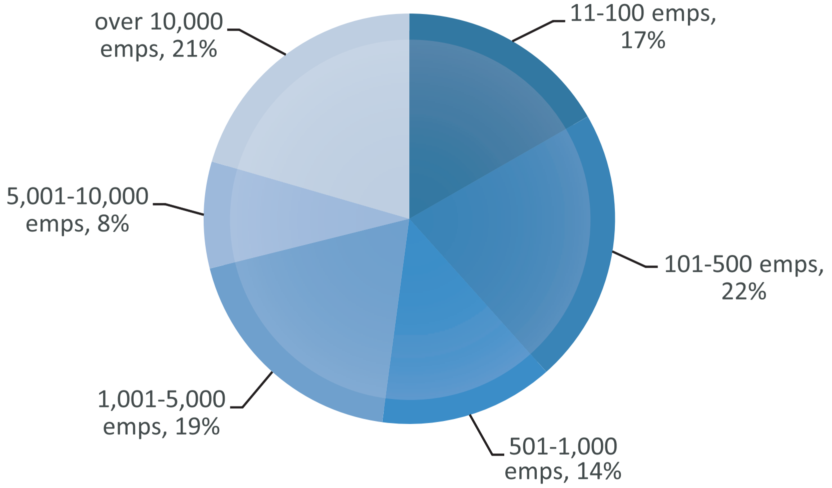
Appendix 1: Survey Demographics

Survey Background

The survey was taken by 283 individual members of the AIIM community between 03 Oct 2012 and 05 Nov 2012 using a web-based tool. Invitations to take the survey were sent via email to a selection of the 70,000 AIIM community members

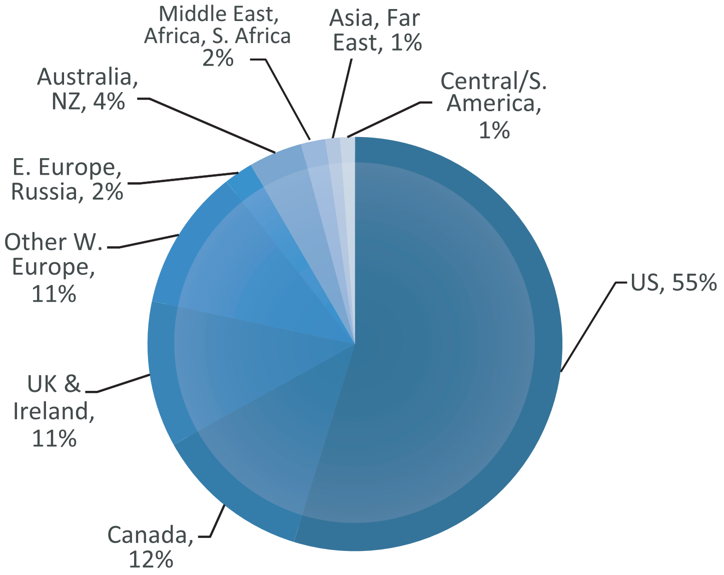
Organizational Size

Organizations with less than 10 employees are excluded from all of the results in this report, taking the total to 263. On this basis, larger organizations (over 5,000 employees) represent 29%, with mid-sized organizations (500 to 5,000 employees) at 33%. Small-to-mid sized organizations (10 to 500 employees) are 39%.



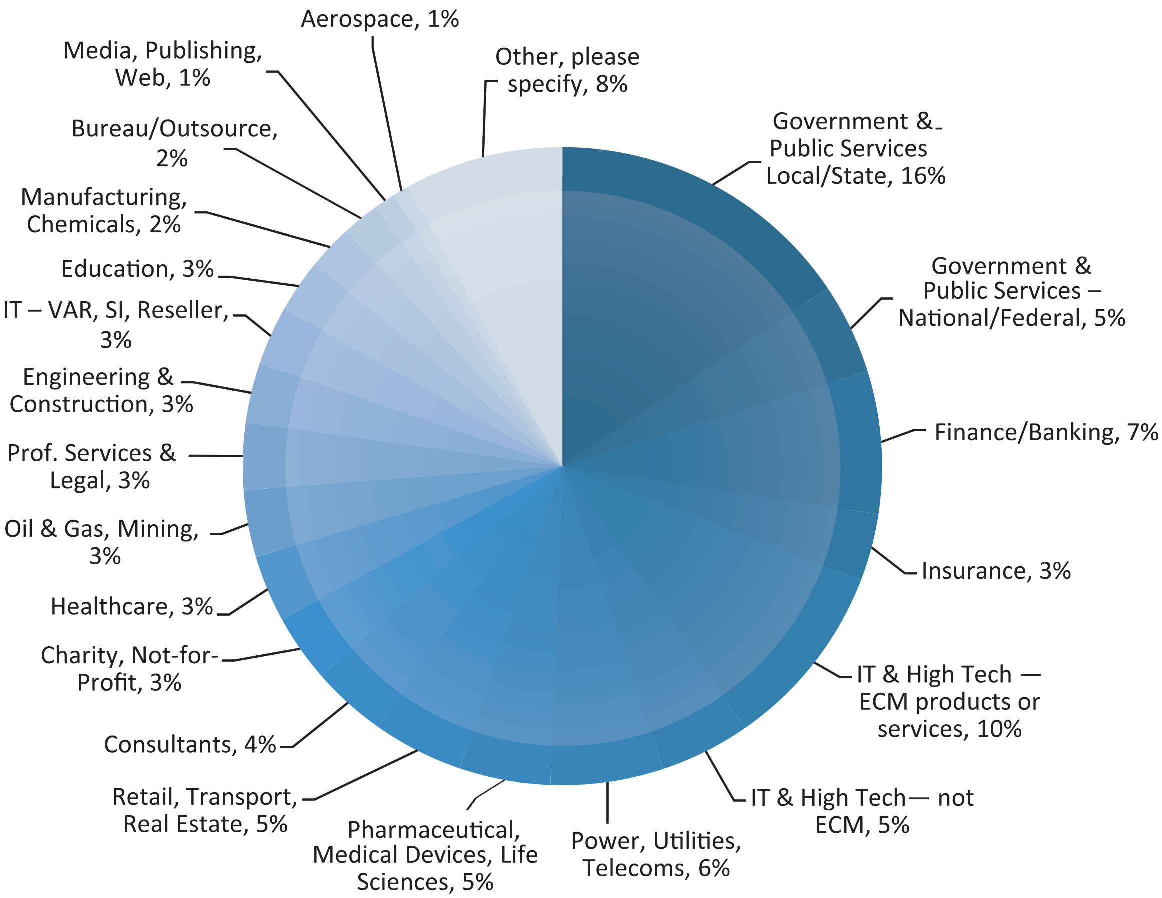
Geography

The survey was international, with US and Canada making up 67% of respondents, and 24% from Europe. We found only minor differences between US and European responses.



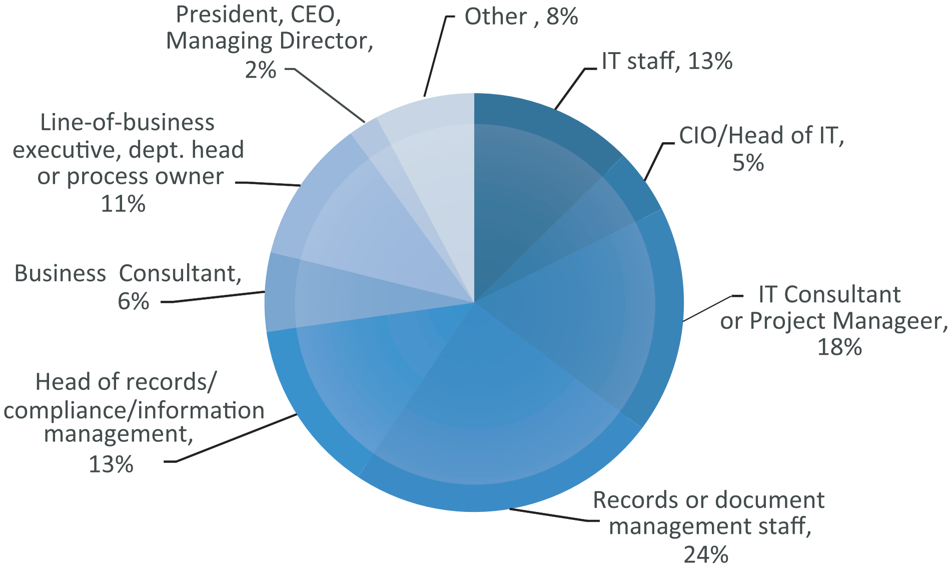
Industry Sector

Local government and public services represent 16% and national government 5%. Finance, banking and insurance represent 10%. The remaining sectors are evenly split.



Role

36% are from IT, 37% from RM/IM/Compliance, 27% have business roles.



Appendix 2: 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”[2]. 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[3,4,5]. 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 rigour 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 standard and 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 may be issued (purchased) from a trusted Certificate Authority (CA) or may belong to a corporation. Self-certified public keys at a corporate or organizational level may also be used, but they require an agreement with recipients because they do not automatically establish the verifiable identity of the signee. They work well within communities of signers. Digital signature standards are mature, and converging internationally[6,7].

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, each enterprise should have a root certificate that is trusted by all, and centrally issue certificates to all of its users. Unfortunately this ideal is not achievable today, with rare exceptions. The certificate authorities are rarely willing to enable organizations to issue certificates under the aegis of the CA. For business reasons, CAs are only willing to sell individual certificates to signers. The exorbitant cost of this approach combined with its high administrative costs make it unworkable in most cases.

An alternative approach that is commonly used is for each enterprise to establish its own root certificate and issue individual signer certificates from the root. This can be done fully automatically, synchronized with the Active Directory or similar system. The enterprise’s root certificate can be provided on the organization’s website for document recipients to download and install, thus establishing the trust relationship between the two organizations.

Appendix 3: Open ended comments (selective)

“Do you have any general comments to make about your signature projects?”

- Getting a hosted third party digital signature tool is a key initiative with huge benefits.
- This survey makes me realize deficiency in education of our staff to various issues
- Our legal counsel is the major roadblock, although they view it as necessary.
- Internal legal counsel is the single and most influential resistant office in this regard.
- Users want to see their graphical signature
- Using electronic signature where possible within specific apps that have workflow capabilities - purchasing requests, IT change requests, invoice processing, etc. Would like to extend into SharePoint without having to do custom development.
- Digital Signatures are a good idea, but the cost of implementation is the hurdle for us, a company that would use them only occasionally.
- You cannot see this separate of the documentation system it is based on. Electronic signature systems, even the most sophisticated, are non-compliant if not embedded in your Quality Management system.
- We have been using electronic signatures for more than a decade. This is not anything new.

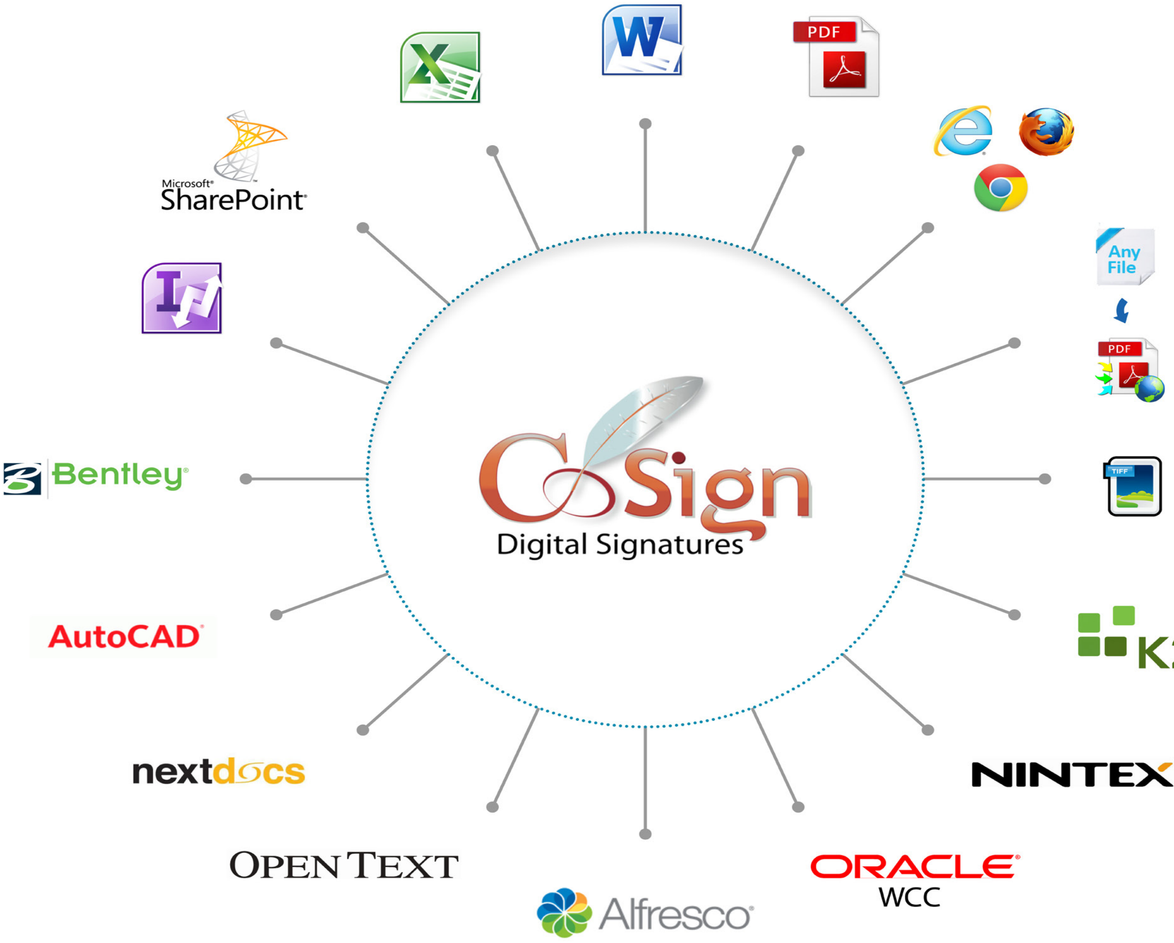
UNDERWRITTEN BY

CoSign® by ARX

ARX (Algorithmic Research) is the leading global provider of standard digital signature solutions with dominant market share in the life sciences, government and engineering (AEC) markets. Millions of signers at security-minded businesses and government organizations around the world have made CoSign by ARX the most widely-used proper digital signature solution.

By securely and affordably automating their signature-dependent business processes, our customers have been able to cut costs, shorten process times, increase efficiency and support compliance. CoSign is the only proven digital signature system that fully complies with strict industry and geographic regulations, technical standards and business requirements across multiple industries. The system's flexible design enables seamless integration of digital signatures into any content authoring software, and makes it easy to digitally sign documents in all major business applications and file types such as PDF, Word, Excel®, SharePoint, InfoPath®, AutoCAD® and TIFF.

To learn more about the CoSign digital signature solution, please visit www.arx.com.



About AIIM

AIIM (www.aiim.org) is the global community of information professionals. We provide the education, research and certification that information professionals need to manage and share information assets in an era of mobile, social, cloud and big data.

Founded in 1943, AIIM builds on a strong heritage of research and member service. Today, AIIM is a global, non-profit organization that provides independent research, education and certification programs to information professionals. AIIM represents the entire information management community, with programs and content for practitioners, technology suppliers, integrators and consultants.

aiim®
The Global Community of
Information Professionals

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