Digital signatures have emerged as one of the technology priorities for local and state governments for the purpose of gaining both operational efficiencies and legal assurances.

To benchmark the current usage levels and overall perception of digital signatures at government organizations, CoSign by ARX commissioned American City & County to conduct a study of its audience during July 2014.

The results focused on several areas, ranging from the problems caused by traditional (pen & paper) signature processes, and all the way to the potential benefits of implementing a digital signature solution.

The majority of those who responded (63%) were top government administration officials – mayors, city or county council members, city or county managers and CFOs. The remaining 37% are involved in various areas of public works or public safety disciplines. The majority of those who responded (63% of the more than 400 respondents to the survey) were top government administration officials – mayors, city or county council members, city or county managers and CFOs. The remaining 37% are involved in various areas of public works or public safety disciplines.

Of the respondents, nearly 40% sign documents more than 8 times per week and more than 20% sign 4-7 times a week. Not surprisingly, those who sign the most documents are also much more likely to already be using signature automation solutions or at least planning to implement them.

Following a short introduction to digital signatures, this document lays out a detailed analysis of the survey results.
What are Digital Signatures?

The short answer is that digital signatures are the most advanced form of electronic signatures – the most secure, most flexible and most compliant with laws and regulations. For the longer answer you will first need to understand the differences between “digital signatures” and “electronic signatures,” which are sometimes (and incorrectly) used interchangeably.

Electronic signature is an umbrella term for any technology used to associate a person with the electronic content they are trying to sign. It is defined by ESIGN (the Electronic Signatures in Global and National Commerce Act of 2000) and UETA (the Uniform Electronic Transactions Act) as “an electronic sound, symbol, or process.” Examples include a scanned image of a signature, the “I Accept” checkmark on a website, and a signature captured using an electronic pad at a grocery store. By themselves, most electronic signatures cannot ensure signer identity or content integrity, nor do they eliminate the risk of signers denying that they signed the document.

Digital signatures, on the other hand, are the most secure form of electronic signatures. They are based on Public Key Infrastructure (PKI) technology, the only signature standard published, maintained and accepted by governments around the world, including the US, Canada, the European Union and Latin America, as well as by independent bodies such as ISO, OASIS, IETF and W3C. When governmental organizations explore their options regarding electronic signatures, they typically decide that digital signatures are the best option because of their non-proprietary nature, global acceptance, compliance with local regulations, security assurance, and ability to work with the most commonly used authoring applications.

Through the use of cryptographic operations digital signatures create a “fingerprint” unique to both the signer and the content, thus ensuring both signer identity and content integrity, while preventing the risk of deniability (non-repudiation). Because they are based on international PKI standards, digital signatures can be easily validated by anyone anywhere using widely available applications such as Microsoft Word and Adobe Reader, without the need for proprietary software.

When it comes to laws and regulations, only digital signatures are compliant with the most stringent requirements set by government agencies, including major regulations such as ESIGN, UETA, EU regulations and VAT law, FDA 21 CFR Part 11, HIPAA and SOX. For government agencies requiring a higher level of security, some digital signature solutions also offer FIPS 140-2 Level 3 systems that have been certified by the National Institute of Standards and Technology (NIST).
Governments require signatures for a wide variety of reasons:

- Approvals and authorizations: 88%
- Compliance with legal and regulatory requirements: 76%
- Agreements and contracts: 73%
- Compliance with internal procedures: 71%
- HR, finance, and other internal documents/forms: 68%

Key Findings

Drivers:
- Local Government officials who responded to the survey clearly understand the need for signatures to authorize everything from financial transactions and employee reviews to meeting legal and regulatory requirements. They also know the areas where those signatures are required and were unambiguous in regards to which ones were the most valuable.

The Breakout

<table>
<thead>
<tr>
<th>Category</th>
<th>Already use</th>
<th>Plan to implement</th>
<th>See the need</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approvals and authorizations</td>
<td>81.4%</td>
<td>87.9%</td>
<td>91.6%</td>
</tr>
<tr>
<td>Legal and regulatory compliance</td>
<td>84.7%</td>
<td>72.4%</td>
<td>75.8%</td>
</tr>
<tr>
<td>Agreements and contracts</td>
<td>74.6%</td>
<td>74.1%</td>
<td>73.6%</td>
</tr>
<tr>
<td>Internal procedures compliance</td>
<td>72.9%</td>
<td>75.9%</td>
<td>74.2%</td>
</tr>
<tr>
<td>Internal documents/forms</td>
<td>66.1%</td>
<td>74.1%</td>
<td>70.2%</td>
</tr>
</tbody>
</table>

Adoptions:
- The breakout shows that across the board — those currently using digital signatures, the agencies that plan to implement them and the respondents who see the need but are still searching for more information before setting an implementation timeline — all agree on the key areas where signatures are required: Approvals, agreements, complying with legal and regulatory requirements and internal procedures.
- In most cases, even those who have yet to start using digital signatures strongly agree on the areas where they are most needed. It stands out that those who already sign digitally are much more likely to need the signatures for legal and regulatory compliance purposes.
Time added to a typical process requiring physical signatures:

<table>
<thead>
<tr>
<th>Time Added</th>
<th>Already Use</th>
<th>Plan to Implement</th>
<th>See the Need</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up to half a day</td>
<td>44.1%</td>
<td>29.3%</td>
<td>31.8%</td>
</tr>
<tr>
<td>1 day</td>
<td>18.6%</td>
<td>19.0%</td>
<td>22.5%</td>
</tr>
<tr>
<td>2-3 days</td>
<td>23.7%</td>
<td>37.9%</td>
<td>29.5%</td>
</tr>
<tr>
<td>4-7 days</td>
<td>6.8%</td>
<td>5.2%</td>
<td>11.0%</td>
</tr>
<tr>
<td>More than a week</td>
<td>6.8%</td>
<td>8.6%</td>
<td>5.2%</td>
</tr>
</tbody>
</table>

Key Findings

Drivers

- Requiring printed signatures on documents and forms is a costly time sink.
- The related costs, including printing, copying and paper, compound the problem.
- Most local governments are sensitive to environmental considerations in their purchases and processes.

Adoptions:

- No matter the category, all respondents report that they are spending a significant amount of time on collecting physical signatures.
- 37% of respondents currently using digital signatures say requiring physical signatures used to add between 2 and 7 days to the process.
- 51% of those who plan to implement a digital signature solution say requiring physical signatures currently adds between 2 and 7 days to the process.
Digital signatures are being recognized as a necessity for government operations:

See a need but don’t know enough about them to decide on a timeline: 49%

Already use digital signatures: 16%

Plan to implement within the next two years: 16%

Key Findings

Drivers:

• A government that is efficient in its administration of paperwork is also less costly to operate, which is why government officials are using and considering using more sophisticated technology to reduce the time required for collecting signatures. Nearly 30% of respondents said that more than half of the documents they print out are printed just for adding signatures. Another 29% print 25-50% of their documents just to get them signed.

Adoptions:

The Breakout

• While 16% of all respondents say they are using digital signatures, nearly 50% more say they understand they need to use them in their agency or department. However, that group has not set a timeline to purchase such a system because they still need more information before they make a decision on the technology and vendor.

• An additional 16% of the respondents have committed to purchasing a signature automation system in the next 12 to 24 months. That group would double the current number of agencies or departments using such a solution.
Top benefits of digital signatures for government agencies:

- Increased efficiency: 85%
- Shorten turnaround time on signature approvals: 80%
- Lower costs: 53%
- Legal, retention and audit requirements: 53%
- Establish a paperless office: 52%

Key Findings

Drivers

- Virtually all local governments have been forced to become more efficient and their processes more cost effective since the Great Recession. One of the ways governments are reaching those goals is by implementing signature automation solutions.
- As expected, the top two responses to this question address efficiency goals and two of the next three responses concern saving money. 44% of survey respondents also noted “environmental considerations,” including reducing paper waste and transportation-related impacts.

Adoptions:

- The breakout clearly shows that those already using digital signatures have experienced the efficiency benefits.
- The expectations of those who plan to implement or see the need to convert to an automated solution to save money or to create a paperless office are slightly higher than the reality seen by those who already use them.

The Breakout

<table>
<thead>
<tr>
<th>Benefit</th>
<th>Already use</th>
<th>Plan to implement</th>
<th>See the need</th>
</tr>
</thead>
<tbody>
<tr>
<td>Increase efficiency</td>
<td>94.8%</td>
<td>86.2%</td>
<td>85.9%</td>
</tr>
<tr>
<td>Shorten time for signature approvals</td>
<td>84.5%</td>
<td>82.8%</td>
<td>81.9%</td>
</tr>
<tr>
<td>Lower costs</td>
<td>50.0%</td>
<td>65.5%</td>
<td>54.2%</td>
</tr>
<tr>
<td>Legal, retention, audit compliance</td>
<td>51.7%</td>
<td>56.9%</td>
<td>55.4%</td>
</tr>
<tr>
<td>Create paperless office/ full digital automation</td>
<td>48.3%</td>
<td>60.3%</td>
<td>55.4%</td>
</tr>
</tbody>
</table>
Biggest reservations about digital signatures:

Concerns with security, control, integrity and location of sensitive data: 77%
Concerns with acceptance and/or legality: 74%
Concerns with compliance with regulations and/or audit requirements: 63%

Key Findings

Drivers:

• The top three concerns have been consistent for electronic solutions for several years. The fact that more than 60% of the respondents to the survey are often not technology-driven positions — mayors, city or county commissioners, city or county managers, CFOs — may account for such concerns.

• A survey conducted two years ago by AC&C showed that the top three concerns for electronic signatures were Security, Legal and Technical issues.

The Breakout

<table>
<thead>
<tr>
<th></th>
<th>Already use</th>
<th>Plan to implement</th>
<th>See the need</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sensitive data location, security, control, integrity</td>
<td>73.7%</td>
<td>77.6%</td>
<td>78.0%</td>
</tr>
<tr>
<td>Acceptance and/or legality</td>
<td>75.4%</td>
<td>77.6%</td>
<td>75.1%</td>
</tr>
<tr>
<td>Regulations and/or audit requirements compliance</td>
<td>56.1%</td>
<td>56.9%</td>
<td>63.8%</td>
</tr>
</tbody>
</table>

Adoptions:

• Those who already use digital signatures were slightly less concerned than those who plan to implement them or see the need to do so.

• However, concerns declined significantly with the remaining seven survey choices - “Higher IT Priorities” at 30% to “We don’t see the business benefits” at 4%.
Those most interested in adopting a digital solution:

Key Findings

Drivers:

- Those who frequently sign documents understand the lack of efficiency in using a non-technology-driven solution. Senior managers, who were the majority of respondents to the survey, know that they must become more efficient and their processes more cost effective.
- IT Managers and Process Owners were the third and fourth most interested in using digital signature solutions.

Adoptions:

- The breakout shows very little difference in the responses between those who plan to implement and governments who see the need to use digital signatures.
- Those most reluctant to use digital signatures included internal auditors, the compliance and legal departments, and finance officers.
- Clearly, more education needs to be done to convince the most reluctant government employees that digital signatures are in full compliance with laws and regulations.

The Breakout

<table>
<thead>
<tr>
<th></th>
<th>Plan to implement</th>
<th>See the need</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approvers/signers</td>
<td>67.3%</td>
<td>64.3%</td>
</tr>
<tr>
<td>Senior managers</td>
<td>69.1%</td>
<td>58.6%</td>
</tr>
<tr>
<td>IT</td>
<td>58.2%</td>
<td>55.4%</td>
</tr>
</tbody>
</table>
The most important factors in selecting digital solutions:

<table>
<thead>
<tr>
<th>Factor</th>
<th>Already use</th>
<th>Plan to implement</th>
<th>See the need</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security and integrity of sensitive data</td>
<td>80.3%</td>
<td>85.7%</td>
<td>91.4%</td>
</tr>
<tr>
<td>Ease of use</td>
<td>86.5%</td>
<td>85.1%</td>
<td>88.5%</td>
</tr>
<tr>
<td>Control over user management/governance policies</td>
<td>76.0%</td>
<td>80.4%</td>
<td>83.5%</td>
</tr>
<tr>
<td>Ease of implementation</td>
<td>82.0%</td>
<td>81.9%</td>
<td>82.8%</td>
</tr>
<tr>
<td>Acceptance by courts</td>
<td>66.0%</td>
<td>70.4%</td>
<td>83.1%</td>
</tr>
<tr>
<td>Integration with existing document management systems</td>
<td>80.0%</td>
<td>72.8%</td>
<td>77.4%</td>
</tr>
</tbody>
</table>

Key Findings

Drivers:
- Respondents know the potential pain points, as shown by the tightly knit factors that are important to them when selecting a signature automation solution.
- Local government officials often face the same issues when adopting any new technology (security, control, legal and integration, for example).

The Breakout

Adoptions:
- Very little difference between the three groups in the breakout, which speaks to the universality of expectations regarding digital solutions.
- However, those who are already signing digitally are less concerned with security and integrity compared to those who have yet to implement a digital signature solution.
Electronic Content Management systems (ECM) or Document Management Systems (DMS) used at government agencies:

- SharePoint: 21%
- Laserfiche: 15%
- Oracle: 9%
- OpenText: 2%
- Alfresco: 1%
- Other: 17%

Key Findings

Drivers:
- ECM and DMS software allow companies to manage content so users can easily communicate and collaborate and share and track information because it is stored in a central location.
- Digital signature should be an integral part of any content management project as they complete the “last mile” of automating document-related processes and workflows.

Adoptions:
- SharePoint has a commanding lead over its competitors in the local government marketplace, with Laserfiche and Oracle coming in second and third, far ahead of any other solution.
- More than 36 providers were listed by the respondents who selected “other.”

The Breakout

<table>
<thead>
<tr>
<th>Software</th>
<th>Already use</th>
<th>Plan to implement</th>
<th>See the need</th>
</tr>
</thead>
<tbody>
<tr>
<td>SharePoint</td>
<td>22.4%</td>
<td>44.6%</td>
<td>19.1%</td>
</tr>
<tr>
<td>Laserfiche</td>
<td>13.8%</td>
<td>14.3%</td>
<td>19.1%</td>
</tr>
<tr>
<td>Oracle</td>
<td>12.1%</td>
<td>12.5%</td>
<td>8.7%</td>
</tr>
<tr>
<td>OpenText</td>
<td>1.7%</td>
<td>1.8%</td>
<td>1.2%</td>
</tr>
<tr>
<td>Alfresco</td>
<td>-</td>
<td>-</td>
<td>1.2%</td>
</tr>
<tr>
<td>Other</td>
<td>36.2%</td>
<td>16.1%</td>
<td>14.5%</td>
</tr>
</tbody>
</table>
Resources: Want to Know More?

CoSign by ARX, the sponsor of American City & County’s Benchmark Digital & Electronic Signatures Survey, offers a number of helpful resources on digital signatures on their website, http://www.arx.com.

Webinars:
- Digital Signature Mightier than the Pen (Laserfiche & CoSign)
- Digital Signatures in Local Government
- Achieve More Security, Efficiency and Cost Savings with Digital Signatures

Case Studies:
- CoSign Keeps SCDOT Up to Speed
- Embracing the Latest Technologies, SFHA Chooses CoSign Digital Signatures
- Johnson County Follows the Yellow Brick Road to Digital Signatures
- The European Court of Human Rights Adds Digital Signatures to its SharePoint Platform
- Digital Signatures Enhance Document Management System Deployment at the County of Hawaii

White Papers, Articles and more:
- Digital Signatures: Best Practices for State and Local Government
- Seamless Integration of Digital Signatures with Laserfiche
- Digital Signatures for Local Government

Learn more:
- First-of-its-kind research by AIIM: Digital Signatures for Document Workflow and SharePoint
- Download the CoSign ROI white paper and ROI calculator spreadsheet

CoSign by ARX, the most widely used digital signature solution at local and national governments around the world, was recognized as “the strongest digital signature solution” in the Forrester Wave: E-Signatures Q2 2013 report. Millions of people around the world use CoSign daily on their computers and mobile devices to easily add secure digital signatures to documents in Word, Excel, PDF, SharePoint, OpenText, Oracle, Alfresco, Laserfiche, and many other applications and file formats.

By seamlessly integrating digital signatures into existing document-related workflows, applications and services across their organizations, CoSign customers easily transform slow and expensive signature-dependent processes into quick and efficient paper-free ones. They rapidly reach ROI through significant reductions in process times and paper-related costs, while ensuring trust, integrity, control and compliance across their entire business and IT environments.