ARTICLE :

Industry Contribution: Digital signature as a method to strengthen enterprise risk management practices across the US government

By David Santiago and Israel Nery

US government agencies face a complex assortment of risks to their missions. Government agencies exist to serve the public interest, especially in areas where the private sector is either unable or unwilling to do so, and the way they execute their missions is subject to significant scrutiny and risk. When agencies cannot effectively manage risk, they can undermine trust in government.

In 2016, the US Chief Financial Officer's Council (CFOC) and the Performance Improvement Council (PIC) developed detailed guidance: *Playbook: Enterprise Risk Management for the U.S. Federal Government*[1] to help government leaders meet the requirements of the revised Office of Management and Budget Circular A-123,[2] while more broadly outlining important concepts and approaches for managing risk across government agencies. The CFOC and PIC define risk, at page 6, as the 'effect of uncertainty on objectives.' Risk Management 'is a coordinated activity to direct and control challenges or threats to achieving an organization's goals and objectives' and Enterprise Risk Management (ERM) 'is an effective agency-wide approach to addressing the full spectrum of the organization's significant risks by considering the combined array of risks as an interrelated portfolio, rather than addressing risks only within silos.'

Although the CFOC was founded to support the federal financial management community, and the PIC was founded to improve performance management in the federal government, the types of risks both councils are concerned with span a full spectrum of issues. The major risk types (outlined on pp 36-37) in the *Playbook: Enterprise Risk Management for the U.S. Federal Government* include: Compliance risk; Credit program risk; Cyber information security risk; Financial risk; Legal risk; Legislative risk; Operational risk; Political risk; Reporting risk; Reputational risk and Strategic risk. These risk types represent a daunting array of issues that are compounded by increasingly scarce resources and heightened expectations by the public that agencies will manage them efficiently and effectively.

Additionally, agencies must comply with various statutes and regulations that are all aimed at managing risk. Examples of federal statutes requiring agencies to demonstrate that they will manage risk while meeting strategic objectives include the Federal Managers' Financial Integrity Act (FMFIA) of 1982, the Improper Payments Information Act (IPIA) of 2002, and the Federal Information Security Management Act (FISMA) of 2002.[3] Other federal guidelines related to risk include NIST SP 800-63 Digital Identity Guidelines,[4] and the proposed USA Federal Privacy Legislation (ADPPA), following in the footsteps of the UK Data Protection Act 2018 and the EU GDPR,[5] which

[1] Developed and issued in collaboration with Federal Government organizations to provide guidance and support for ERM (July 29, 2016), available at https://www.cfo.gov/wp-content/uploads/2016/07/FINAL-ERM-Playbook.pdf .

[2] (2016), available at https://www.osec.doc.gov/opog/privacy/Memorandums/OMB_Circular_A-123.pdf ; for Appendix B revised (August 27, 2019), see https://www.whitehouse.gov/wp-content/uploads/2019/08/Issuance-of-Revised-Appendix-B-to-OMB-Circular-A-123.pdf .

[3] Karen Hardy, *Enterprise Risk Management: A Guide for Government Professionals* (Jossey-Bass, 2015).

[4] https://pages.nist.gov/800-63-3/ .

[5] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) OJ L 119, 4.5.2016, p. 1–88.

has bipartisan support and may become federal law.[6] At the state, local, tribal, and territorial levels of government, various statutes exist requiring governments to manage risk. For example, in the State of Tennessee, 'state statutes require the Department of Audit, Comptroller of the Treasury, to prescribe a uniform accounting system for entities that handle public funds.' These uniform accounting systems are needed in large part to ensure adequate internal controls.[7]

Cyber risk is of particular concern for government agencies more dependent than ever on digital technology to support their missions. Unauthorized access to government systems represents a major internal control deficiency and has been the subject to numerous government audits. For example, the US General Accountability Office (GAO) discovered in a 2019 report that the US Department of Treasury's Bureau of the Fiscal Service failed to establish adequate internal controls over financial reporting, allowing individuals to obtain access to, modify, or disclose sensitive data and programs without authorization.[8] Organizations should know who the legitimate users are of their critical information assets and systems, and a robust identity management system should establish and assure this as a precondition to allowing access to these assets and systems. Ransomware continues to succeed at exploiting weak, unreliable identity management systems. Protecting legitimate users – people – from identity hijacking and theft is the most cost-effective risk mitigation.[9]

While there are many ways to manage risk, one of the defining attributes of ERM is documentation. As a best practice, government agencies must be diligent with documenting how risks are identified, assessed, responded to, monitored, and communicated, all of which are essential to effective risk mitigation. Proper documentation enables more effective and repeatable risk-based decision-making throughout an organization. Since risks are typically evaluated in the context of a decision, government agencies document risks to support courses of action. The more important the decision, the more critical it is to document it. Unfortunately, this is where many government agencies fall short. Many of the most important decisions – for example, those related to governance, financial management, and personnel matters – are made through manual and paper-based processes that add risk to the way decisions are documented, stored, and reported on. According to a 2019 Forbes report, the government is featured as one of three sectors in significant need of digital transformation, reliant on paper-based processes such as handwritten forms (the other two industries featured in the article are finance and healthcare, both of which are highly regulated).[10]

The challenges with paper-based and manual processes are not new and have been highlighted in various studies around digitization and digital transformation. McKinsey,[11] Forrester,[12] the Harvard Business Review,[13] and others have published many articles on best practices related to digital transformation, but progress is inconsistent across the government. It is noteworthy that the role of digital signatures is a critical component to successful digitization and digital transformations that can be trusted. Too often this is overlooked. The importance of digital signatures often emerges as an afterthought rather than an essential design consideration of digital transformations that may

[6] https://www.congress.gov/bill/117th-congress/house-bill/8152/text .

[7] Jason E. Mumpower, Comptroller of the Treasury, Internal Control and Compliance Manual Division of Local Government Audit, for Governmental Units and other Organizations (December 2015), available at https://comptroller.tn.gov/content/dam/cot/la/documents/manuals/2015_ICCManual_Complete_redesign-Final.pdf .

[8] 'Management Report: Areas for Improvement in the Federal Reserve Banks' Information System Controls.' GAO, March 26, 2019, available at https://www.gao.gov/assets/gao-19-304r.pdf .

[9] For a brief explanation, see 'Avoiding Identity Theft', available at https://consumer.gov/scams-identity-theft/avoiding-identity-theft .

[10] Eric Johnson, 'Three Industries That Are In Dire Need Of Digitization', Forbes, July 19, 2019, available at https://www.forbes.com/sites/forbestechcouncil/2019/07/19/three-industries-that-are-in-dire-need-of-digitization/?sh=33977d995e8d .

[11] 'Unlocking success in digital transformations,' McKinsey & Company, October 29, 2018, available at https://www.mckinsey.com/capabilities/people-and-organizational-performance/our-insights/unlocking-success-in-digital-transformations .

[12] Ted Schadler, 'Successful Digital Transformations Focus On Three Core Elements,' Forrester, April 19, 2022, available at https://www.forrester.com/report/successful-digital-transformations-focus-on-three-core-elements/RES177355 .

[13] Tomas Chamorro-Premuzic, 'The Essential Components of Digital Transformation,' Harvard Business Review, November 23, 2021, available at https://hbr.org/2021/11/the-essential-components-of-digital-transformation .

also need to satisfy legal scrutiny. With respect to ERM, insufficiently digitized and automated processes can cause legal problems, audit findings, and other challenges. A lack of formally documented approvals is an especially problematic internal control deficiency and is highlighted in various legal cases and oversight settings.[14]

During a House of Representatives hearing in 2011, Congressional overseers questioned the Department of Justice and the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) about their decision-making process related to Operation Fast and Furious. From 2006-2011, ATF allowed firearms dealers to sell weapons illegally to Mexico with the hope of tracking the guns down to cartel leaders. The firearms were found at numerous crime scenes, including the death of a US Border Patrol Agent, and the policy did not lead to arrests. In the hearing transcript, the terms *authorized*, and *authorization* were brought up 16 times. The congressional overseers were particularly concerned about establishing documentary evidence around the decisions that led to the death of the Border Patrol Agent (page 166, emphasis added):

> 'Chairman ISSA. Who at Justice—if you know, I ask you to answer, who do you know was involved in the ***authorization*** of this, today? Do you know?'
>
> 'Mr. WEICH. We——'
>
> 'Chairman ISSA. Do you know?'
>
> 'Mr. WEICH. Well, Mr. Chairman, if you will permit me to answer the question. We sent a letter to Chairman Smith, who asked a question like that. We pointed out that this operation, as with other law enforcement operations, originated in the ATF's Phoenix office.'
>
> 'Chairman ISSA. That is not ***authorization***. Who ***authorized*** it at the highest level?'[15]

Maintaining proper documentation about government decisions is not just an exercise to mitigate oversight and compliance risk, but is a serious issue that is essential for good government. Had the ATF carefully documented its decisions in this case, including the use of digital signatures to provide proper attribution of signoffs and audit trails, they might have engendered greater trust with Congress and the public about their decision-making processes.

The value of digital signatures for enterprise risk management

Digital signature tools have been around for many years and have been able to support various use cases, such as processes related to human resources, procurement, and loan origination. Notwithstanding its success, the government has been slow to adopt the technology, especially in ERM. Many traditional digital signature use cases are centred on increasing productivity by reducing the amount of manual or paper-based steps, such as signing documents. Moreover, digital signatures can also serve as a powerful tool to reduce risk, an area that is often overlooked in digital signature implementations. Many customers of digital signature products focus on benefits related to analogue process replacement and automation, with risk mitigation being a secondary factor.

Since one aim of ERM is to support the making of informed decisions, and digital signatures are fundamentally about documenting and formally agreeing on decisions, there is significant potential to strengthen the way the government documents its most important decisions with this technology.

A signature has several purposes, one of which is to provide physical proof that the signer agrees on every part written in a document.[16] In some cases, a signer may sign to indicate a nonconcurrence on the contents of a

[14] Boyd Kumher, Tina Griffiths, Brian Bartos, 'Common Internal Audit Findings and How to Avoid Them', Case Western Reserve University, May 2, 2011, presentation available at https://case.edu/compliance/sites/case.edu.compliance/files/2018-03/Common-Internal-Audit-Findings-and-How-to-Avoid-Them-05-2-11.pdf .

[15] 'Operation Fast and Furious: Reckless Decisions, Tragic Outcomes', Committee on Oversight and Government Reform, United States House of Representatives, One Hundred Twelfth Congress, First Session (Serial No. 112–64, June 15, 2011), available at https://www.govinfo.gov/content/pkg/CHRG-112hhrg71077/pdf/CHRG-112hhrg71077.pdf .

[16] For a full list of the functions of a signature, see 7.11 – 7.19 in Stephen Mason and Daniel Seng, editors, *Electronic Evidence and Electronic Signatures* (5th edition, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2021), open access at https://ials.sas.ac.uk/publications/electronic-evidence-and-electronic-signatures .

document. If a nonconcurrence is done through an electronic signature, many software vendors allow recipients to decline signatures as part of a workflow where they will also be prompted to provide their rationale.[17] Regardless, of whether a recipient electronically signs or declines to sign the document, a decision is being made and recorded in the software application.

An electronic signature is another form of signature, and digital signatures can be a secure version of an electronic signature which uses digital certificates that are cryptographically bound to the document using public key infrastructure (PKI).[18] While both simple forms of electronic signature and digital signatures can be used to document and sign decisions, digital signatures are probably most appropriate for documenting critical government decisions, given their higher level of assurance.

Electronic and digital signatures also have the capability of addressing three main legal and security risks:

1. To verify identity for purposes of a signature, and to document authentication and provenance.

2. To provide for the authenticity of the document (such as the integrity of the document with respect to tampering or unauthorized alteration[19]).

3. To substantiate the organizational authority of the signer.[20]

In 2019, the Office of Management and Budget (OMB) updated guidance around US Identity, Credential, and Access Management (ICAM), through memorandum OMB M-19-17.[21] OMB furnished guidance, which affects digital signature technologies, recognizing that the way 'agencies conduct identity proofing, establish enterprise digital identities, and adopt sound processes for authentication and access control significantly affects the security and delivery of their services, as well as individuals' privacy.'[22] It is possible this policy will change in the future with the advent of Web3/Web3.0, specifically around potential changes involving a more decentralized, trust less, and permissionless internet.[23]

Arguably, the use of digital signatures in government is most valuable for issues that are serious. The definition will differ from agency to agency, but may include decisions affecting an entire enterprise, citizen-facing decisions subject to high levels of scrutiny, matters pertaining to finance and procurement, and so on. Nicholas Bohm and Stephen Mason, in an article in the *Computer Law and Security Review*, stress that this 'probably means that we only need to prove our identity for very serious things (whatever they might be), and the rest require a lower level of proof (for instance, of age when buying alcohol), with the relier accepting the risks.'[24] (Some digital signature solutions can support ID-based authentication in instances where a driver's licence or passport may be needed as part of the authentication process to verify age, for example. A similar process can be supported with identity proofing services, which are sometimes integrated into digital signature workflows to support authentication. Regardless of the method of implementation, for government services where this type of authentication is required, the agencies are using ID-based authentication to mitigate the risk of fraud, waste, and abuse.) The US Cybersecurity and Infrastructure Security Agency defines digital signatures as being significantly more secure than other forms of electronic signature, providing a virtual fingerprint unique to the individual that is valuable for the most important types of transactions.[25] These important transactions might include processes related to the disbursement of

[17] A workflow application is a software application which automates, to a lesser or greater degree, a process, or processes.

[18] For how PKI works, see *Electronic Evidence and Electronic Signatures*, 7.219 – 7.226; for the risks, see 7.254 – 7.271.

[19] A signature may still be valid with parts of the document omitted if the hashing has been designed to allow this. For example, if each page is hashed and then the whole document signed, the validity of a single page can be established providing it is presented with all the hashes.

[20] *Computer Law & Security Review*, Volume 26, Number 1, January 2010, 43 – 51, https://doi.org/10.1016/j.clsr.2009.11.003 .

[21] https://www.whitehouse.gov/wp-content/uploads/2019/05/M-19-17.pdf .

[22] Policies & Priorities Identity, Credentialing, and Access Management (ICAM), available at https://www.cio.gov/policies-and-priorities/ICAM/ .

[23] Nav Dhunay, 'Web3 Will Change Privacy As We Know It', Forbes Technology Council, November 9, 2022, available at https://www.forbes.com/sites/forbestechcouncil/2022/11/09/web3-will-change-privacy-as-we-know-it/?sh=830414b40252 .

[24] Nicholas Bohm and Stephen Mason, 'Identity and its verification', 47.

[25] Security Tip (ST04-018), 'Understanding Digital Signatures', Original release date: December 17, 2009; Last revised: August 24, 2020, CISA, available at https://www.cisa.gov/uscert/ncas/tips/ST04-018 .

government funds through grant management systems, the signing of government contracts, and signoffs related to collective bargaining agreements, to name a few. Less serious types of transactions, not requiring the same level of technical rigour to validate the authenticity and integrity of a document, and that might be more suitable for an electronic signature, include use cases related to certain types of permission slips, signoffs for office supply requests, and so on. For government interactions with entities or individuals outside the government system, a simple electronic signature may suffice for external parties where PKI credentials are not required, and a lower level of assurance is sufficient. Broadly speaking in the federal government, agencies require a Personal Identity Verification (PIV) or Common Access Card (CAC) system that includes PKI-based certificate credentials for most internal agency signing ceremonies, since internal digital signing processes are performed on the government's network which must adhere to Homeland Security Presidential Directive-12.[26]

It should be stressed that the use of workflow-driven digital signature technologies encompasses a broad range of issues as defined by the federal CFO Council. Nearly all auditable activities in government could benefit from either digital signatures or workflow-driven approval software packages, particularly in cases where the existing business processes are manual, and paper-based. Most leading digital signature providers offer low-code, custom workflow creation to help simplify and automate business processes involving signatures. Users of these products do not have to move from one system to another to complete their digital signature processes; they can complete the workflow entirely in the digital signature product or through integrated processes with other document management tools.[27]

Government leaders often associate risk with financial and administrative controls (as outlined in OMB Circular A-123), and this is an area where digital signatures can provide significant value. Internal controls and audit, on the other hand, are subsets of ERM associated with compliance risk as defined in the *Playbook: Enterprise Risk Management for the U.S. Federal Government*, and workflow-driven digital signatures should be viewed as a valuable tool to support the broader practice of ERM.

There are many software tools that facilitate approval workflows without a digital signature. These tools have value for a variety of business processes and are often incorporated into systems of records. Some vendors of workflow-driven signature technologies enable the use of low assurance, 'click-to-approve' simple forms of electronic signature or physical signatures rather than the higher assurance digital signatures (cryptographic). The vendors that take this approach focus on the function of the workflow and leave their customer organizations with the challenges around data protection compliance associated with peoples' identity data (PII) and digital signatures. As pointed out by Gartner, these approval workflow tools support internal approval processes where there are no legally binding documents involved and audit trails may not be necessary.[28] The Electronic Signature & Records Association,[29] assessing the 2010 case of *Adams v Superior Court of Orange County; Quicksilver, Inc.*,[30] stresses that creating and preserving audit trails is important to being successful in litigation. The plaintiff in *Adams v Superior Court of Orange County; Quicksilver, Inc.* challenged the validity of her electronic signature on an arbitration agreement, and the court agreed that the plaintiff's employer, Quicksilver, had failed to implement a system that fully captured the electronic signing process in an attributable and auditable manner.[31]

[26] Personal Identity Verification (PIV) of Federal Employees and Contractors. National Institute of Standards and Technology, (FIPS PUB 201-3, January 2022), available at https://www.cac.mil/Portals/53/Documents/NIST.FIPS.201-3.pdf .

[27] '2022 Gartner© Market Guide for Electronic Signature.' Gartner, July 6, 2022, the Report can be obtained by providing personal information, at https://www.infocert.digital/analyst-reports/2022-gartner-market-guide-for-electronic-signature/ .

[28] '2022 Gartner© Market Guide for Electronic Signature'.

[29] https://esignrecords.org/ .

[30] Court of Appeal, Fourth District, Division 3, California, February 22, 2010, 2010 WL 602515; for a high-level discussion, see Linda Owens, January 28, 2018, '7 landmark electronic signature legal cases', available at https://esignrecords.org/2018/01/28/7-landmark-electronic-signature-legal-cases/ ;' for a more detailed and nuanced discussion (the case law is not up-to-date), see Stephen Mason, *Electronic Signatures in Law* (4th edn, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2016), open access at https://www.sas.ac.uk/publications/electronic-signatures-law .

[31] There are several cases relating to systems such as Adobe and competitors across various States in the US. One problem that occurs, independent of the product employed by the user, is where the user fails to provide any evidence from or about the document signing business employed by the business, as in the case of *Fabian v Renovate America, Inc.*, 42 Cal.App.5th 1062 (2019), 255 Cal.Rptr.3d 695, 19 Cal. Daily Op. Serv. 11,641, 2019 Daily Journal D.A.R. 11,348, where the company offered no

Many of the most important and legally fraught decisions in the government require signoffs, and the processes tend to be manual, and paper based, such as decisions made in executive governance bodies, delegations of authority, and signoffs for policy and procedural documents.

Let us consider these scenarios for a moment. Governance is concerned with structure and processes for decision-making, accountability, control, and behaviour. Governance influences how an organization's objectives are set and achieved, how risk is monitored and addressed, and how performance is optimized.[32] Most agencies will have numerous governance bodies to oversee critical lines of business and important initiatives. These governance bodies are generally comprised of senior leaders – in many cases, the most senior officials in an agency – who make risk-based decisions. These decisions are often made in meetings through dialogue, debate, and voting. In many cases, the votes are recorded through meeting minutes or on a spreadsheet-based decision log. The challenge with this approach is that the decisions are not always readily attributable to the voter, there is no audit trail associated with the vote, and the decision-log is not stored in a central file repository that can be easily examined upon request. (This issue is not restricted to government agencies. Across all industries, a lack of effective recordkeeping, where decisions are not stored and accessible centrally, can lead to a variety of compliance and knowledge management challenges. Additionally, in organizations transitioning from paper signing processes to digital signing processes, the potential for critical, paper-based decisions to be lost, especially in instances where scanning and document storage workflows are not automated, is not trivial). Given that these decisions are often related to the most critical issues affecting an agency and are subject to review by oversight bodies such as Inspector Generals and Congress, this approach to documenting signoffs ironically adds risk to organizational processes, the very thing these governance bodies are attempting to mitigate.

Furthermore, some of the most senior government officials are political appointees with short government tenures (e.g., one to two years), particularly if they are supporting a presidential transition and are not confirmed by the Senate.[33] If their decision-making processes involve email or paper-based signoffs, it is much more difficult for the agency to later access, retrieve, and review the decisions that they made. Most leading digital signature providers have robust document routing, signing, tracking, auditing, and reporting capabilities that are purpose built for digital signing processes and are not native to most other software applications, including email.

A similar issue exists with delegations of authority. Many government agencies issue delegation of authority letters to formally transfer authority from one official to another. Delegations of authority may occur for a variety of reasons, including succession, emergency situations, and the delegation of certain financial transaction powers to a designated official. During internal control assessments, auditors will frequently review delegations of authority to determine if they are appropriate in relation to the assignment of responsibility.

For example, in 2014, the US Postal Service Office of Inspector General (OIG) found that the individuals given delegations of authority for the US Postal Service facilities contracts organization lacked contracting authority and should have been rescinded.[34] Similarly, and perhaps more problematically, in 2022, the US Department of State OIG

evidence about the process used to verify the homeowner's electronic signature via the business. See where an arbitration agreement between employer and employee, utilizing a document management system was upheld in the case of *Beckman v Zuffa LLC*, Slip Copy (2021), 2021 WL 5445464. In this case, the arbitration agreement was signed electronically by the employee via Adobe Sign and was subsequently accompanied by a unique transaction ID, indicating the electronic signature was certified by a third party, and that the certification of the ID was valid. The court held that although the defendants' showing would have been strengthened if the declarant had explained exactly how the electronic signature was transmitted, nevertheless it did not detract from the testimony about the Adobe Sign process.

[32] 'Governance: what is it and why is it important?', Governance Today (not dated), available at https://governancetoday.com/GT/GT/Material/Governance__what_is_it_and_why_is_it_important_.aspx ; Edmund Barrow, FRSA, 'Governance Governing Government', 31 .08. 2020, available at https://rightsandresources.org/blog/governance-governing-government/ .

[33] Eric Katz, 'The Biden Administration Will Allow Agencies to Appoint Some Employees Into 10-Year Temporary Jobs', Government Executive, December 2, 2022, available at https://www.govexec.com/workforce/2022/12/biden-administration-will-allow-agencies-appoint-some-employees-10-year-temporary-jobs/380374/ .

[34] Audit Report, Delegations of Contracting Authority Outside of Supply Management, Office of Inspector General United States Postal Service (Report number SM-AR-14-007, August 5, 2014), available at https://www.uspsoig.gov/sites/default/files/document-library-files/2015/sm-ar-14-007.pdf .

found that the US Department of State's Bureau of Diplomatic Security lacked delegations of authority for technical monitors.[35] The audit went on to discuss how the contracting officer did not properly oversee the technical monitors, which undermined the OIG's confidence that the Bureau of Diplomatic Security was following contracting processes according to federal and departmental standards. Central to this finding was the lack of proper documentation and record keeping, areas that could have been strengthened through workflow-driven digital signature processes.

Government agencies develop detailed policies and procedures as part of executing their mission. Policies and procedures are often needed to help navigate complex legislative, regulatory, ethical, and oversight requirements. When new policies and procedures are being drafted, the authors typically route the documents to major participants for feedback and concurrence. This process also tends to be manual and is sometimes paper based. Auditors have found deficiencies related to routing and signoffs. In 2018, for example, the National Records and Archives Administration (NARA) was found to have not properly routed the agency's IT Security Methodology to the appropriate participants, resulting in missing approvals.[36] In this situation, an overreliance on manual processes resulted in insufficient engagement by relevant participants and missing documentation. Had NARA used automated routing capabilities as part of a digital signature workflow, it is possible that they would have avoided receiving the audit finding.

In the examples noted above, arguably workflow-driven digital signatures would have helped strengthen the overall risk posture of the agencies. Digital signatures would have benefited these agencies by:

1. Documenting official decisions through trusted and attributable digital signatures.
2. Maintaining a readily searchable source that is authentic and trustworthy for digitally signed documents in document repositories.
3. Provisioning of reports to respond to audits, internal risk assessments, and requests for information.
4. Building trust with participants so that decisions are made in a transparent manner.
5. Streamlining concurrence processes through automated, workflow-driven digital signature processes.

As with any technology, vulnerabilities exist with digital signatures, which includes the threat of malware and other exploitive attacks. There have been instances of malicious people stealing private keys from infected servers to misrepresent digital signatures. This occurred during a Stuxnet malware attack in 2010 that later evolved into different variants of the virus, affecting many industries across the globe.[37] First, it must be noted that such attacks are very rare.[38] It is possible to mitigate the risk of malicious attacks by managing digitally signed documents through automated processes, using PKI or Pretty Good Privacy,[39] and confirming that digital signatures follow the Federal Information Processing Standards Digital Signature Standard, which specifies mathematical algorithms to generate digital signatures.[40]

Many vulnerabilities arise from insecure implementations of digital signature technology that fail to protect private keys from theft and hijacking, rather than the digital signature technology. Implementations and configurations, for example, can – should – ensure that an individual has exclusive, sole-control of their private key. The very integrity of

[35] Audit of the Bureau of Diplomatic Security's Oversight of Contractor Performance and Invoice Processing for the Domestic Guard Services Contract, Department of State OIG (AUD-SI-22-37, Wednesday, September 14, 2022), available at https://www.oversight.gov/report/DOS/Audit-Bureau-Diplomatic-Security%E2%80%99s-Oversight-Contractor-Performance-and-Invoice .

[36] Office of Inspector General of National Archives, 'Audit of NARA's Cybersecurity Risk Management Process' (OIG Audit Report No. 20-AUD-15, August 27, 2020), available at https://www.archives.gov/files/oig/reports/final-audit-report-audit-of-naras-cybersecurity-risk-management-process-20-aud-15.pdf .

[37] https://en.wikipedia.org/wiki/Stuxnet .

[38] *Electronic Evidence and Electronic Signatures*, 5.115; for examples of issuing a certificate to an impostor, see 7.254.

[39] https://en.wikipedia.org/wiki/Pretty_Good_Privacy .

[40] FIPS 186-5 Digital Signature Standard (DSS), February 3, 2023, available at https://csrc.nist.gov/publications/detail/fips/186/5/final .

workflow-driven digital signature processes is compromised when private keys are compromised. The irony of trust becoming the casualty.

When implemented correctly with appropriate controls, digital signatures can help simplify an organization's business processes and improve overall security, compared with manual and paper-based processes. The City of Seattle, which has introduced electronic and digital signature technology across government agencies, started its implementation with the finance, accounting, and procurement departments in part to reduce risk and strengthen internal controls. Additionally, the City of Seattle benefited from the conveniences of signing documents digitally as opposed to relying on legacy paper-based and manual processes which were time consuming and error prone.[41] By using digital signatures, government agencies can strengthen their overall risk postures, and generally improve trustworthiness and confidence both within the government and with the public about how decisions are made, documented, and retained.[42]

Conclusion

Government agencies are subject to significant oversight and often struggle with effectively managing risk and maintaining appropriate documentation. Although digital signature tools have been commercially available for many years now, the government is still in the early phases of adopting the technology. Workflow-driven digital signatures can function as an important tool in the toolbox for agencies interested in strengthening their ERM practices by helping to preserve vital decisions. The more transparent and accountable government agencies are with respect to their decision-making processes, the better they can serve their constituents while minimizing the potential for fraud, waste, and abuse.

The authors thank the peer reviewers of this article, including Stephen Mason, for their thoughtful feedback.

Mr. David Santiago is Adobe's Head of Industry for Public Sector for the Document Cloud. Mr. Santiago came to Adobe from the Federal Emergency Management Agency (FEMA) where he served as the Deputy Assistant Administrator for Grants Systems and Policy Integration and managed the Office of Enterprise Grant Services.

dsantiago@adobe.com

Mr. Israel Nery (Juris Doctor) serves as a Strategy & Consulting Manager in the private sector. Beforehand, Mr. Nery worked for the US Small Business Administration where he served as the acting Deputy District Director for the Los Angeles SBA District Office and led technology initiatives.

israel.nery.x@gmail.com

[41] Craig Peasley, 'City of Seattle relies on Adobe and Microsoft to help with operational continuity During COVID-19', Adobe, September 7, 2020, available at https://business.adobe.com/blog/the-latest/city-of-seattle-relies-on-adobe-and-microsoft-technology-to-help-with-operational-continuity-during-covid-19 .

[42] Note SP 800-63-4 (Draft) Digital Identity Guidelines, Date Published: December 16, 2022, available at https://csrc.nist.gov/publications/detail/sp/800-63/4/draft .