WHITEPAPER

Transforming citizen experiences with trusted e-signature solutions

Why FedRAMP-authorized signature management matters.

Over the past few years, digital transformation has shifted into overdrive at all levels of government. The federal workplace is in flux, with telework and remote work remaining crucial for workforce plans.[1] This means that digital documents and online processes that have gained prominence over the last few years will remain important in the future, too. But without proper security, digital government services are more vulnerable to attacks and potential service failures. Digital documents increase efficiency and accuracy via automated workflows, but they also open up a different set of security risks.

Traditionally, the work of government has been all about paper-based processes. It's basically how we got the term "red tape" to describe government bureaucracy. Now, as agencies shift towards digital document workflows, the process of adding electronic signatures (also known as e-signatures) to those documents is also increasingly important. Digital document signing not only eliminates the need for a handwritten signature, but it also saves time. Parties can sign forms anywhere, at any time, on any device — which improves citizen experiences, builds trust in government, and extends services to people who might not have been able to make it into a government office before.

Cutting Through Red Tape

According to historians, the phrase "red tape" arises from the use of red ribbon to bind important government documents during the sixteenth century reign of Spanish King Charles V; an innovation later adopted by lawyers in Great Britain and its colonies. In David Copperfield, *published in 1849, Charles Dickens describes a character as "little more than a red tape Talking Machine."* [2,3]

In fact, federal agencies are moving towards offering a digital, mobile-friendly option for all paper-based processes, especially for citizen-facing processes. The recent Executive Order on "Transforming Federal Customer Experience and Service Delivery to Rebuild Trust in Government" addresses the use of e-signatures.[4] For example, it removes the requirements for physical signatures on Social Security-related documents.

E-signature solutions can strengthen security in a Zero Trust environment, but not all solutions are created equal. Some solutions just support basic e-signatures, where identities are verified through email or phone PINs. Others support digital signatures, which is an e-signature that is backed by a digital certificate issued by a trusted third party. Then, there are the solutions that support the whole signature spectrum.

This white paper explores how a scalable, standards-based signature solution can improve your agency's overall security posture. We'll look at the security concerns surrounding e-signatures, the value in FedRAMP-authorized signature solutions, and why the new Adobe Acrobat Sign for Government stands out as a trusted solution for user-friendly digital interactions.

The Security Gaps in Agency IT Modernization

Modernization is the name of the game for government agencies nationwide. In a world driven by mobile apps and online payment portals, many agencies have embraced digital government as a way to better serve constituents, empower employees, and widen access to services. But the disruption caused by the COVID-19 pandemic in many cases upended — and still impacts — the careful long-term planning that typically guides digital transformation efforts.

The challenge now is to ensure that the systems and processes that matter most for citizens are accessible and secure. Documents with e-signature capabilities can reduce paperwork processes and broaden the reach of government services. They help streamline everything from applying for a passport to supporting people through unemployment. But are your agency's digital document workflows secure?

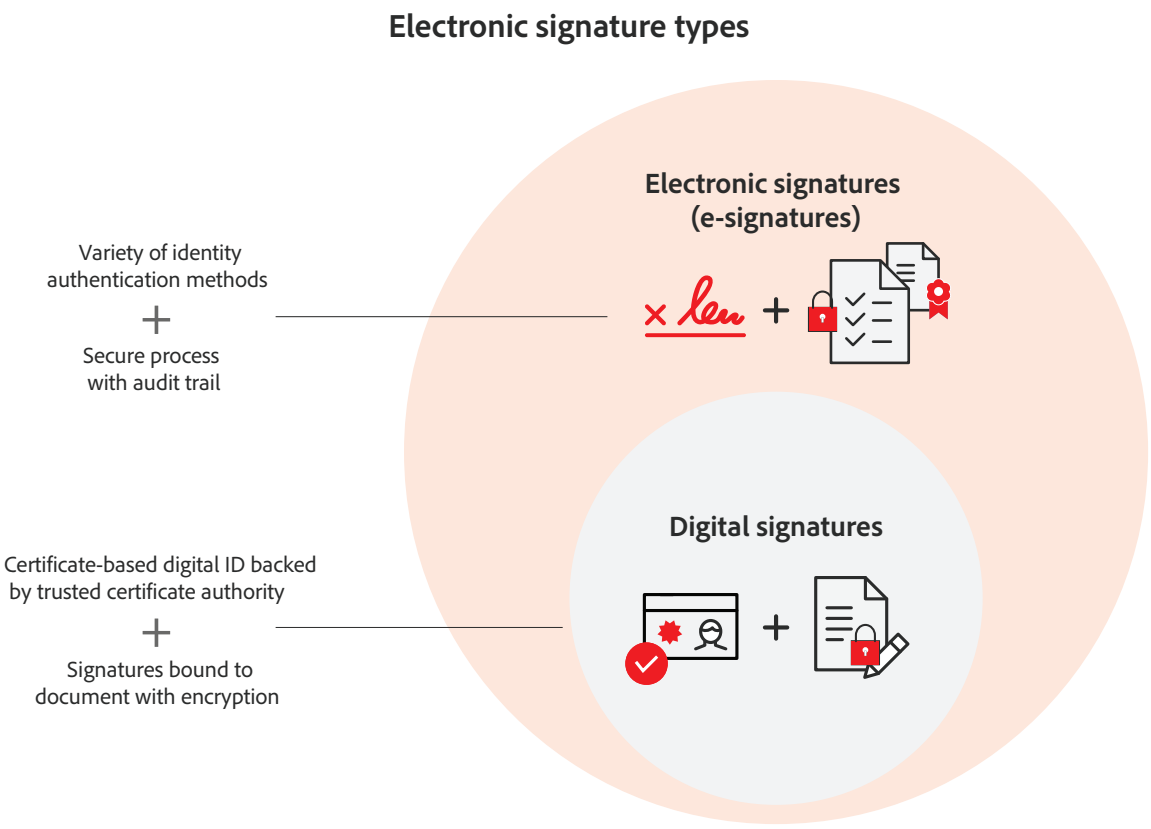
However, there are some cases where additional levels of assurance (LOA) for signer identification are needed, and that's where digital signatures come in. Digital signatures are a specific type of e-signature that is backed by a digital certificate as proof of a signer's identity that is cryptographically bound to the signature field using public key infrastructure (PKI). Digital signatures are used for things like government benefits applications, healthcare forms, and other documents that are part of higher-value, higher-risk, or strictly regulated processes. To achieve this strong security posture, digital signatures must:

- **Uniquely identify each signer** via the digital certificate issued by an accredited trust service provider (TSP) or certificate authority (CA).
- **Reconfirm identity of the signer prior to signing** — such as via a personal PIN, plus a secure "signature creation device" like a smart card, USB token, or cloud-based hardware security module (HSM).

E-signatures are legal, trusted, and enforceable throughout the United States, per the federal ESIGN Act of 2000[5], but security requirements can vary depending on the region, agency, data, and security classification levels. E-signatures:

- Meet the demand for anytime, anywhere signing via mobile devices and web browsers.
- Use common authentication methods like passwords and email verification to confirm the signer's identity.
- Demonstrate proof of signing via a secure process that often includes an audit trail, along with the final document.
- Help facilitate external customer and citizen-facing interactions, such as signing government forms without having to print and mail paper copies.

- **Demonstrate proof of signing** — that is, the signature is cryptographically bound to the document with a tamper-evident seal.
- **Provide long-term validation,** enabling authenticity to be re-confirmed for at least 10 years.



Document signing solutions need to be carefully considered as part of a full Defense-in-Depth approach — going beyond baseline compliance requirements to help protect against the latest threats, such as supply-chain attacks and fraud. As more agencies continue their move to the cloud and new attack vectors emerge, comprehensive cybersecurity practices are more important than ever.

The Benefits of FedRAMP solutions in a Zero Trust environment

To strengthen the security of government agencies, the Office of Management and Budget has outlined a Federal Zero Trust architecture that emphasizes strong enterprise identity and access controls, including multi-factor authentication.[6] The National Institute of Standards and Technology (NIST) provides a framework for incorporating Zero Trust principles and technologies into the agency environment.

In a nutshell, Zero Trust is about trusting no one — inside or outside the security perimeter. This approach decouples network, application, and data access to provide more control over each layer, regardless of where users reside. Instead of domain-level "allow/block" permissions focused on a hardened network security perimeter, with Zero Trust agency IT teams create and enforce more granular, context-based policies for every interaction to enhance protection.

Why Zero Trust?

A Zero Trust Architecture (ZTA) assumes that traditional perimeter security boundaries are inadequate, especially in a hybrid or cloud-based computing environment, and that both internal and external threats are always a risk to organizational resources. That means that there is no implicit trust between devices and networks, and that any resource, regardless of its physical or network location, requires verification, authentication, and thorough authorization before being allowed access to another resource. Zero Trust resources must be continually evaluated in a "least privileged" manner, meaning that only the minimum level of permissions are granted per request, and that each request is evaluated uniquely.

What does this mean for signature management? Agencies can use e-signatures for external-facing processes. But for agency employees and internal communications, digital signatures are a better complement for a Zero Trust architecture. This is because digital signatures utilize PKI to protect the transaction, to confirm the identity of the signer, and to guard against potential fraud. Audit trails also provide valuable information, such as the signer's IP address or geolocation, which can be used in third-party analytics tools as well as add non-repudiation of the signature.

While the Federal Risk and Authorization Management Program (FedRAMP) authorizes solutions at Low, Moderate, and High Impact levels, Moderate Impact solutions account for nearly 80% of the cloud applications that receive FedRAMP authorization.[7] The Moderate Impact level is designed to protect sensitive data, such as personally identifiable information (PII), and aligns with NIST controls for Zero Trust.[5, 8] Encryption management is also FIPS 140-2 verified, which ensures that cryptographic modules have met NIST security requirements.

With Adobe's FedRAMP Moderate authorized solution, you have the assurance that information stays in the U.S., managed by U.S. personnel, and only hosted on an authorized Microsoft Azure Government Community Cloud infrastructure. Agencies have the assurance that all information is maintained at the same FedRAMP security level.

The path to trusted, user-friendly digital interactions

Adobe Acrobat Sign for Government is a security-enhanced instance of Adobe's industry-leading SaaS application that enables agencies to rapidly replace manual, paper-based approval and signature processes with automated, all-digital workflows. This FedRAMP Moderate authorized solution is designated for the sole use of U.S. federal, tribal, state, and local government organizations, as well as U.S. government contractors and partners.

One of the key advantages of Adobe Acrobat Sign for Government is how it brings security into the existing Adobe processes agencies use today. The solution is designed to not only accelerate productivity — reducing the time required to capture signatures from days to minutes — but also to easily integrate with the full range of secure signature creation devices, including personal ID verification (PIV) cards, common access cards (CAC), and mobile credentials. Additionally, wrapping document creation, signature capture, tracking,

and archiving into a consolidated, secure workflow relieves agency employees of the burden of double- and triple-checking which documents need to be sent via secure email or with download credentials in order to comply with agency rules.

In fact, Adobe builds for compliance and security from the ground up, knowing that in the drive to develop new digital capabilities, protecting citizen and agency data is ever-critical. FedRAMP Moderate authorization means agencies have a compliant e-signature solution that ensures the security and protection of sensitive information with 325 security controls verified by a third-party auditor.

With more than 30 years of experience developing and refining PDF and signature technologies, Adobe is uniquely positioned to help agencies make the most of signature management in a Zero Trust world. In fact, Adobe Acrobat Sign for Government was validated by a high-transaction, high-volume, highly secure agency which worked alongside us in developing this solution, ensuring controls aren't just in place but are relevant for the needs of today's public sector. The right FedRAMP-authorized solution delivers exceptional signing experiences for employees and constituents — so public interactions can have the speed, ease, and security that modern government requires.

Five reasons Adobe is different

1. Pricing transparency for subscriptions and professional services
2. Expertise in transforming employee and constituent experiences
3. Microsoft's only preferred e-signature solution for seamless workflows
4. Integration with existing productivity tools, such as Microsoft 365, FedRAMP Moderate Word, PowerPoint, and Outlook, and Teams
5. Open standards leader for PDF and digital signatures in the cloud

Learn more

To learn more about protecting your digital document workflows and e-signatures, visit us online or contact us at: www.adobe.com/sign/contact.html

For more information about the security practices in Adobe solutions, visit: www.adobe.com/trust.html

[1] Nicole Ogrysko, "How 5 federal agencies are handling employee reentry in the new year — for now," Federal News Network, December 20, 2021. https://federalnewsnetwork.com/workforce/2021/12/how-5-federal-agencies-are-handling-employee-reentry-in-the-new-year-for-now/

[2] Dickson, Del (2015). The People's Government: An Introduction to Democracy. New York: Cambridge University Press. p. 176.

[3] Online Etymology Dictionary. https://www.etymonline.com/word/red tape. Retrieved April 4, 2022.

[4] "Executive Order on Transforming Federal Customer Experience and Service Delivery to Rebuild Trust in Government," The White House, December 13, 2021. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/12/13/executive-order-on-transforming-federal-customer-experience-and-service-delivery-to-rebuild-trust-in-government/

[5] "Electronic Signatures in Global and National Commerce Act," U.S. Congress, June 20, 2000 https://www.govinfo.gov/content/pkg/PLAW-106publ229/pdf/PLAW-106publ229.pdf

[6] Office of Management and Budget, "Memorandum for the Heads of Executive Departments and Agencies: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles," January 2022. https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

[7] FedRAMP, "Understanding Baselines and Impact Levels in FedRAMP," November 16, 2017. https://www.fedramp.gov/understanding-baselines-and-impact-levels/

[8] FedRAMP, "FedRAMP Prepares for 'Zero Trust' Stance," March 2, 2022. https://www.fedramp.gov/2022-03-02-prepares-for-zero-trust-stance/