ADOBE ACROBAT SIGN

Why digital certificates are important.

Learn how digital certificates improve cybersecurity and ensure the authenticity of cloud-based digital signatures.

Explore Acrobat Sign

JUMP TO SECTION

What is a digital certificate?

A digital certificate is an electronic credential that confirms the identity of a person or organization online. Issued by a trust service provider (TSP) or certification authority, a digital certificate ensures that when a person sends information like a digital signature to someone else, the receiver of that information knows they can trust it.

Why digital certificates are important.

Put simply, digital certificates prevent security risks.

Less simply, a person without a digital certificate can protect a message with public key cryptography (also known as a public key certificate), which is an encryption algorithm that allows the message sender to encrypt the message

with a private key (a long number). The receiver can then decipher the message with a public key placed in a central site. Public keys are managed by the public key infrastructure (PKI) to allow for secure traffic.

The flaw in this system is that a malicious third party can intercept the message, alter it, and disguise themselves as the sender with a fake key pair. If that third party poses as the original sender, the receiver of the information has no way of detecting the true digital identity of the sender or the nature of the original message.

Digital certificates solve this authentication problem with the help of certificate authorities (CAs) and other trust service providers (TSPs).

What TSPs and CAs do.

Both TSPs and CAs create digital certificates by verifying the details of a person's or organization's identity and requiring a personal PIN and other verification steps. They ensure that the certificate holder can attach their digital certificate to their public key and send it directly to the receiver instead of to a central site, eliminating the danger of what's known as a "man in the middle" attack.

Adobe Acrobat Sign works with several different TSPs, so you can choose the provider that gives you the type of certificate that best suits your compliance needs. They can issue you a certificate-based digital ID so that your digital signature always comes with a credential.

Information included in a digital certificate.

The certificate authenticates the owner's name, the public key and its expiration date, the issuer's name, and the issuer's digital signature. It can be easily verified, and recipients can confirm whether a document was modified after the signer signed the document. Timestamps are required for digital certificates to be compliant with U.S. and E.U. laws.

When you need a digital certificate.

Whenever you need to share personal or confidential information with someone on the internet, you can encrypt the message and use a digital certificate to make sure it's not tampered with en route. If you do business in Europe, you need to use certificate-based signatures to comply with eIDAS signature regulation. Also, pharmaceutical companies must use these types of signatures to comply with the SAFE BioPharma industry standard.

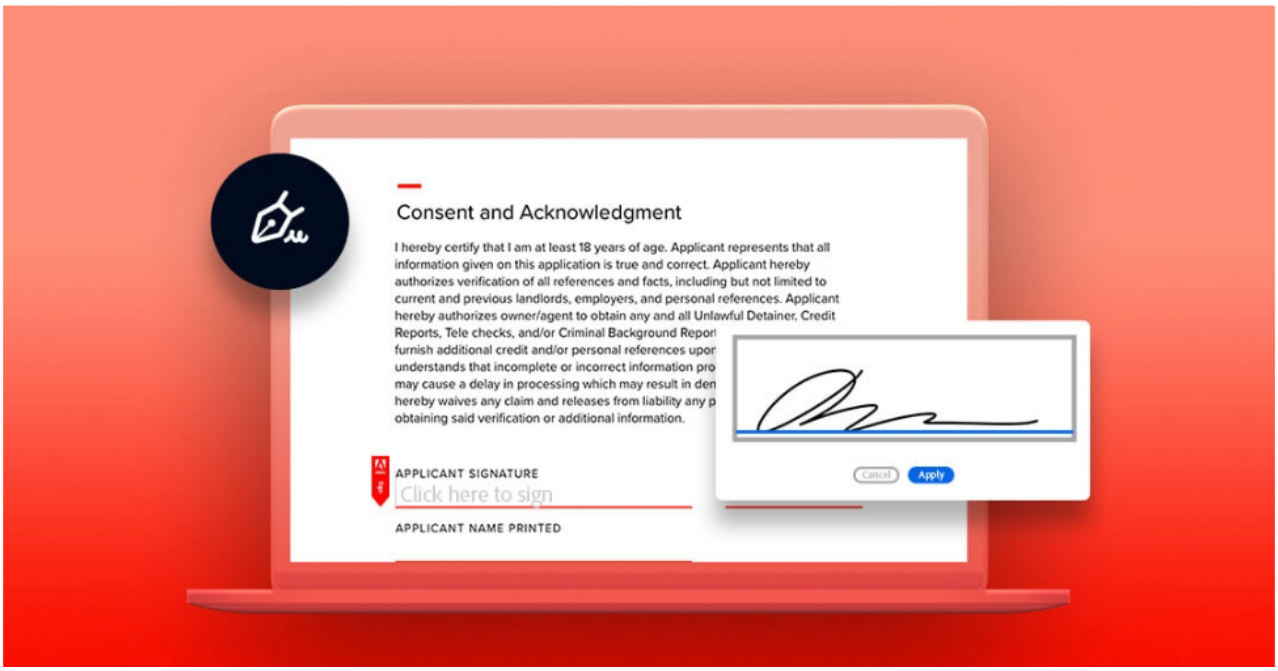
Digital certificates can help you as a consumer as well. Before you share your credit card information with a website, you can check their certificate to ensure that their identity has been verified by a trusted CA. To do this, just click the lock to the left of the URL at the top of your web browser. Click Certificate in the menu to see the details.

The most common digital certificates.

One of the most frequently used formats is the X.509 certificate. This includes the public key, signature, and other identifying information about both the sender and the CA who issued the certificate.

One type of X.509 is the SSL/TLS certificate, which secures websites using the HTTPS protocol. SSL stands for "secure socket layer," and it's the precursor to TLS, which stands for "transport layer security." Both of these work by creating an authentication process known as a "handshake" between two devices to establish that they're both legitimate.

These certificates include a public key, the registered domain name, the name of the business, and identifying information about the CA. As long as the certificate is signed by a trusted CA (there are about 50 of them around the world), you can feel secure in your level of protection.



How Acrobat Sign uses digital certificates.

With Acrobat Sign, a signer uses a digital identity certificate provided by a trust service provider. The signer's certificate is encrypted and bound to the document with the signer's unique private key.

During the validation process, the reciprocal public key is extracted from the signature and used to authenticate the signer's identity through the TSP and to ensure that no changes were made to the document since it was signed.

The audit trail of a document signed with a certificate-based digital signature provides further information, such as the signer's IP address or geolocation at the time the document was signed.

Acrobat Sign at work.

When you use Acrobat Sign for your business's e-signatures, you know you're in compliance with all local and industry regulations, no matter your industry or where you do business.

You can manage risk for any type of signing transaction — from simple e-signatures to highly regulated, qualified digital signatures in the cloud. Now you can always get the security and authentication you need, from one solution that offers maximum flexibility and compliance.

Banking with Acrobat Sign.

NatWest Group, one of the largest UK banking groups, used Acrobat Sign to cut operating costs, improve customer experience, and meet sustainability goals, while still making sure that signatures are secure and compliant.

"With fully digital document workflows, we can seal the PDF output to certify that files have not been changed," says Gaurav Arora, product owner at NatWest's Electronic Signatures Center of Excellence. "Between the audit trails and tamper-proof documents, the entire process provides a consistently secure environment, which adds to the confidence about our electronic signatures having even less risk than wet ink signatures."

Saving animals with Acrobat Sign.

You don't have to be a large organization to benefit from secure and compliant cloud signatures. The nonprofit Cats Protection relied on Acrobat Sign to take cat adoption online.

"We chose Acrobat Sign to enable e-signatures and make it possible to

do all the paperwork online instead of sending it back and forth through the post — so cats can get into their forever homes faster," says Helen Waterman, IT project and documentation officer.

With digital signatures protected and guaranteed by digital certificates, you can use Acrobat Sign anywhere, and trust that your transactions are secure and compliant.

Get started