SSL.com

Trust is What We Do™

ACPM

Audit Consulting Project Management

BUDAPEST • DUBAI • KIGALI • KUALA LUMPUR
NAIROBI • PRETORIA • SHANGHAI • WIEN

https://www.ssl.com/

About

Founded in 2002, SSL.com is a Digital Identity and Trust Services Provider.

SSL.com provides publicly trusted digital certificates, cloud signing services, and enterprise PKI solutions.

Businesses and governments in over 180 countries utilize SSL.com solutions to protect their internal networks, customer communications, eCommerce platforms, and web services.

Certification Authorities WebTrust

Certification Authorities WebTrust BR - TLS

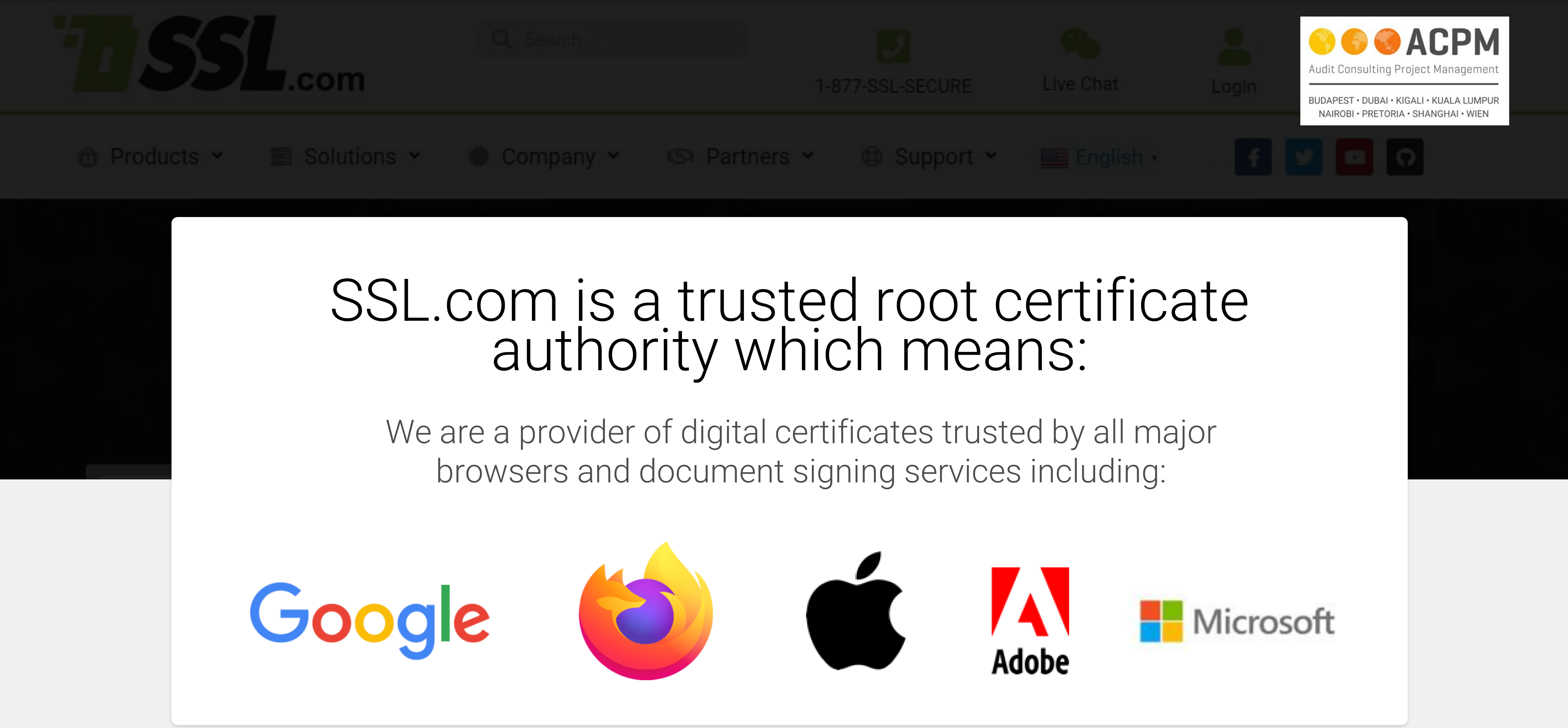
Certification Authorities WebTrust Network Security

Certification Authorities WebTrust BR - Code Signing

Certification Authorities WebTrust Extended Validation

We are voting members of the CA/Browser Forum, the Cloud Signature Consortium, the North American Energy Standards Board (NAESB) and are WebTrust certified through rigorous, regular security audits.

ACPM
Audit Consulting Project Management
BUDAPEST • DUBAI • KIGALI • KUALA LUMPUR
NAIROBI • PRETORIA • SHANGHAI • WIEN



SSL.com is a trusted root certificate authority which means:

We are a provider of digital certificates trusted by all major browsers and document signing services including:

SSL.com

SSL.com is a globally trusted certificate authority expanding the boundaries of encryption and authentication relied upon by users worldwide.

Founded in 2002, we have grown to be used in over 180 countries by leading organizations and governments of all sizes.

Who we work with:

VISA
Microsoft
PandaDoc
ORACLE
EPIC GAMES
Ford
NASA
JET BRAINS
CISCO
hp
intel
MARINES
THE OFFICIAL WEBSITE OF THE UNITED STATES MARINE CORPS
logitech

One Convenient Source for Every Digital Certificate, Cloud Signing and PKI Solution.

SSL/TLS

Trusted website encryption at scale

Use Case: Federal portals, .gov, and high-traffic SaaS needing secure multi-domain coverage

CLOUDFLARE

Device Access & Email Security

Secure email + control access to systems

Use Case: Agencies protecting sensitive comms & critical infrastructure

NIESB

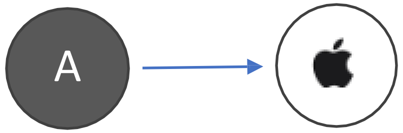
entergy

Club Car

Verified Mark Certificates

Display your logo in inboxes for trust & anti-phishing

Use Case: Government or enterprise brands increasing citizen trust in outreach



Document and Code Cloud Signing

Legally binding, Microsoft and Adobe-trusted e-signatures

Use Case: Contract workflows. Digital-first procurement, securing apps compliance workflows

PandaDoc

Proof

C2PA

Protect integrity of video, images, audio & OEM content

Use Case: Media, defense, or agencies fighting misinformation

C2PA

SSL.com

SSL Certificates

Get Strong Browser Trusted SSL, Wildcard, UCC, SAN, and EV Certificates

Basic and Premium SSL Certificates

Affordable single or multi-site protection under domain validation providing 2048+ bit RSA encryption and a $10,000 warranty.

SAN/UCC SSL

SSL / TLS certificates for multiple domains under organization validation. Wildcard SSL capable.

Organizational / High-Assurance Validation SSL/TLS Certificate

SSL / TLS certificates for multiple domains under organization validation. Wildcard SSL capable.

Enterprise Extended Validation SSL/TLS Certificate

Provides the highest level of validation available and the most thorough vetting process. Provides a $2,000,000 warranty.

SSL Certificates

Provisioning Models

Single Certificate

Purchase single-domain, wildcard, or multi- domain certificates as individual units with fixed duration. Certificates will not be revoked if engagement changes or ends.

Flexible Domain / SAN Bank

A bank of fixed-duration domains that can be used interchangeably as single domain, multi-domain, added SANs or wildcard certificates.

Subscription

A set limit of domains/SANs or distinct certificates that can be active at any given time during a subscription period regardless of re-issuance.

SSL.com’s eSigner cloud document signing service provides simplified remote access to Adobe-trusted digital signatures via a convenient web application and API.

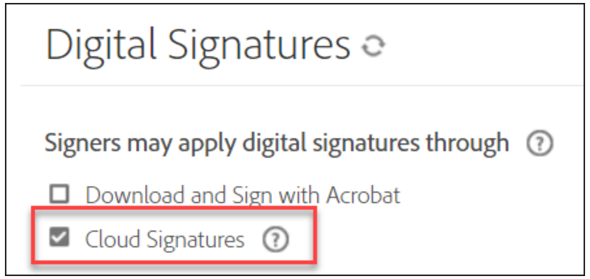
- Easily integrate high-volume automated eSealing of sensitive documents.
- Only CAs (like SSL.com) that are part of the Adobe Approved Trust List (AATL) can apply AATL signatures
- PKI is handled by SSL.com: no extra hardware and staffing expenses.
- Keys are stored securely and compliantly in SSL.com’s HSMs
- Cloud Signature Consortium (CSC) API for integration with front-end apps like Adobe Acrobat Sign.

eSigner

SSL.com

Adobe Registered Reseller

Enterprise Document Solutions combining SSL.com trust with Adobe Sign, Adobe Acrobat and Acrobat Studio.



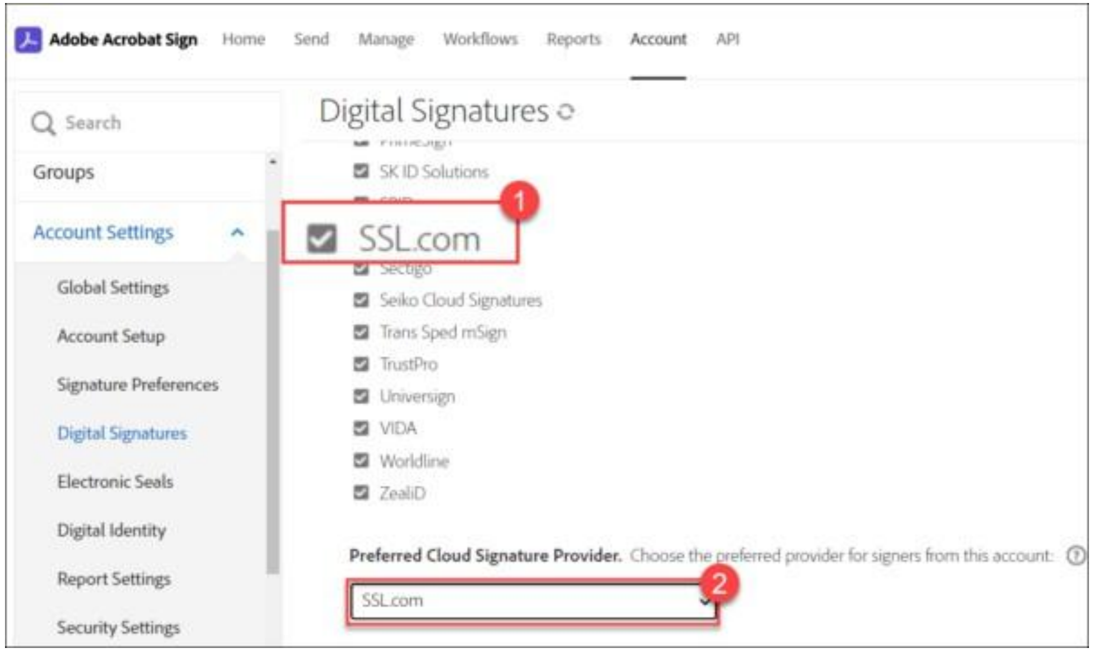
Digital Signatures

Signers may apply digital signatures through

☐ Download and Sign with Acrobat

☑ Cloud Signatures

Adobe



Digital Signatures

☑ SK ID Solutions

☑ SSL.com

☑ Sectigo

☑ Seiko Cloud Signatures

☑ Trans Sped mSign

☑ TrustPro

☑ Universign

☑ VIDA

☑ Worldline

☑ ZealiD

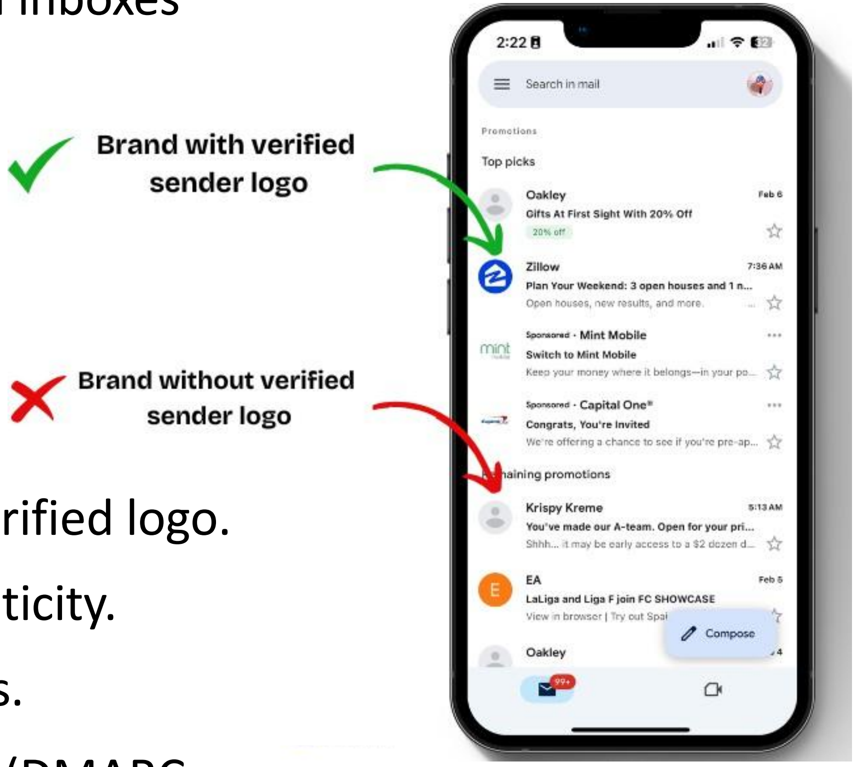
Preferred Cloud Signature Provider. Choose the preferred provider for signers from this account:

SSL.com

Verified Mark Certificates (VMCs) - Trust in Brand Communication

What is a Verified Mark Certificate (VMC)?

- A digital certificate that allows organizations to display their logo in email inboxes (Gmail, Yahoo, and others).
- Authenticates the sender's brand identity using DMARC enforcement.
- Issued by a publicly trusted Certificate Authority (CA) like SSL.com.



✓ Brand with verified sender logo

✗ Brand without verified sender logo

Oakley — Feb 6
Gifts At First Sight With 20% Off
20% off

Zillow — 7:36 AM
Plan Your Weekend: 3 open houses and 1 n...
Open houses, new results, and more.

Sponsored · Mint Mobile
Switch to Mint Mobile
Keep your money where it belongs—in your po...

Sponsored · Capital One®
Congrats, You're Invited
We're offering a chance to see if you're pre-ap...

Krispy Kreme — 5:13 AM
You've made our A-team. Open for your pri...
Shhh... it may be early access to a $2 dozen d...

EA — Feb 5
LaLiga and Liga F join FC SHOWCASE
View in browser | Try out Spai

Oakley

Advantages:

- Brand Visibility & Recognition – Stand out in recipients' inboxes with a verified logo.
- Enhanced Security – Reduces phishing risks by confirming sender authenticity.
- Higher Engagement – Increases open rates and trust with branded emails.
- Regulatory Compliance – Aligns with email authentication best practices (DMARC, BIMI).

Secure Your Email Communication

S/MIME certificates prevent impersonation, data leaks, phishing, fraud and tampering while increasing customer trust in your communication.

What is S/MIME?

S/MIME or Secure/Multipurpose Internet Mail Extensions is the leading standard for email signing and encryption.
It enables users to encrypt and decrypt messages to each other preventing unauthorized access while also signing messages with a validated identity to prevent impersonation.

Use Cases

- Protecting privileged and sensitive communications with email encryption
- Preventing intellectual property and trade secrets from compromise
- Validating a company or individual’s identity to an email recipient to prevent impersonation
- Securing customer financial data and preventing fraudulent payment requests

With SSL.com S/MIME solutions, you get:

- End-to-end email encryption between recipients
- Validation of senders’ identities
- Seamless email integration
- Easy deployment and management

Easy Bulk Ordering

Secure email communication for your entire staff with SSL.com’s S/MIME certificate bulk order tool. Pre-validate your organization for automated issuing and upload user info with a single CSV to automate issuance.

SSL.com

C2PA | Coalition for Content Provenance and Authenticity

C2PA

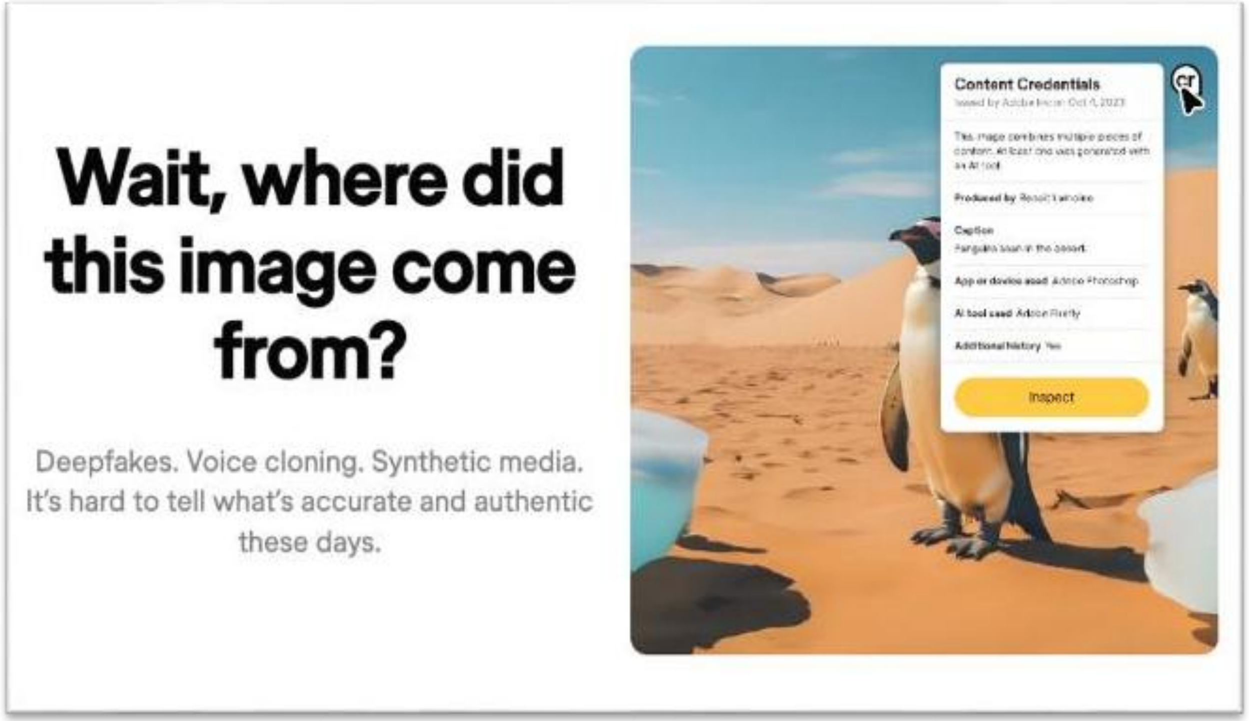
Digital Content Provenance

The Coalition for Content Provenance and Authenticity, or C2PA, provides an open technical standard for publishers, creators and consumers to establish the origin and edits of digital content.

It's called Content Credentials, and it ensures content complies with standards as the digital ecosystem evolves.

Use cases:

- Device manufacturers (camera's, audio recording)
- SaaS content production (Design software, security imaging, healthcare imaging)



Wait, where did this image come from?

Deepfakes. Voice cloning. Synthetic media. It's hard to tell what's accurate and authentic these days.

Content Credentials
Issued by Adobe Inc. on Oct 1, 2023

This image combines multiple pieces of content. At least one was generated with an AI tool.

Produced by Benoit Lemoine

Caption
Penguins seen in the desert.

App or device used Adobe Photoshop

AI tool used Adobe Firefly

Additional history Yes

Adobe · amazon · BBC · Google · intel · Meta

Microsoft · OpenAI · PUBLICIS GROUPE · SONY · truepic

Extended Validation Code Signing Certificates

Digitally sign your software development work with code signing certificates. Prevent tampering or compromising of applications by unauthorized parties.

- Highest organizational authentication assurance
- Signature and time stamping does not expire once certificate expires
- Immediate Extended Validation reputation with Microsoft SmartScreen®
- Company name, address and organization type displayed in the certificate
- Certificate store on FIPS hardware token prevents key duplication
- 2-factor authentication through hardware token and PIN combination
- Required for Windows 10 kernel-mode and user-mode drivers
- Required for Windows 10 Hardware Development Center Dashboard Portal access
- Strongest industry encryption with SHA-256 keys

SSL.com

Matter Protocol

- What it is:
  - Open-source, royalty-free standard for smart home and IoT.
  - Backed by the Connectivity Standards Alliance (CSA).
- Key Goals:
  - Interoperability – cross-brand compatibility.
  - Reliability – local communication (Wi-Fi, Thread, Ethernet).
  - Security – strong encryption, secure onboarding.
  - Simplicity – easy setup with QR/NFC.
- Supported Devices (initially):
  - Lighting, plugs, thermostats, locks, sensors, TVs, hubs.

Ecosystem Impact:

Reduces fragmentation in smart home market.
One protocol → broader compatibility.
Supported by Apple Home, Google Home, Alexa, SmartThings.

Enterprise Customer Solutions

SSL.com offers world-class capabilities to our Enterprise customers, including:

01

On-line Management Tools and Volume Discounts

Centrally manage and distribute high volumes of any type of digital certificate (SSL/TLS, code signing, S/MIME, ClientAuth, etc.).

02

Hosted or Internal Enterprise PKI

Manage the life cycle of any digital certificate directly through your CA interface, API or optionally through our Enterprise RA system.

03

Custom Branded Issuing CA

Leverage our technology and expertise to issue publicly-trusted X.509 certificates in your own name.

04

Internet of Things (IoT) Solutions

Secure your smart devices with SSL.com. Optimize the generation, installation and lifecycles of certificates with many infrastructure options.

Managing large volumes of certificates for your organization can be an expensive hassle, but SSL.com provides all the tools you need

1 SSL.COM MANAGEMENT TOOLS

Easily issue and manage large volumes of certificates using our public key infrastructure tools and services including our certificate management app and online RA portal.

2 AUTOMATED CERTIFICATE MANAGEMENT

Manage certificate lifecycles with a custom ACME-enabled issuing CA. ACME is an established, standard protocol for certificate management with many open-source client implementations..

3 SSL WEB SERVICES API

Order, download, rekey, and revoke certificates directly from your servers and/or smart devices.

Automation Options:

SSL Web Services API:

Automate every aspect of certificate issuance and lifecycle with SSL.com's RESTful API.

ACME Protocol:

An established, standard protocol for domain validation and certificate management with many open-source client implementations.

Cloud Signing API:

Integrate automated code signing into CI/CD pipelines and add automated eSealing to protect sensitive high-volume document distribution

Hosted or Internal Enterprise PKI

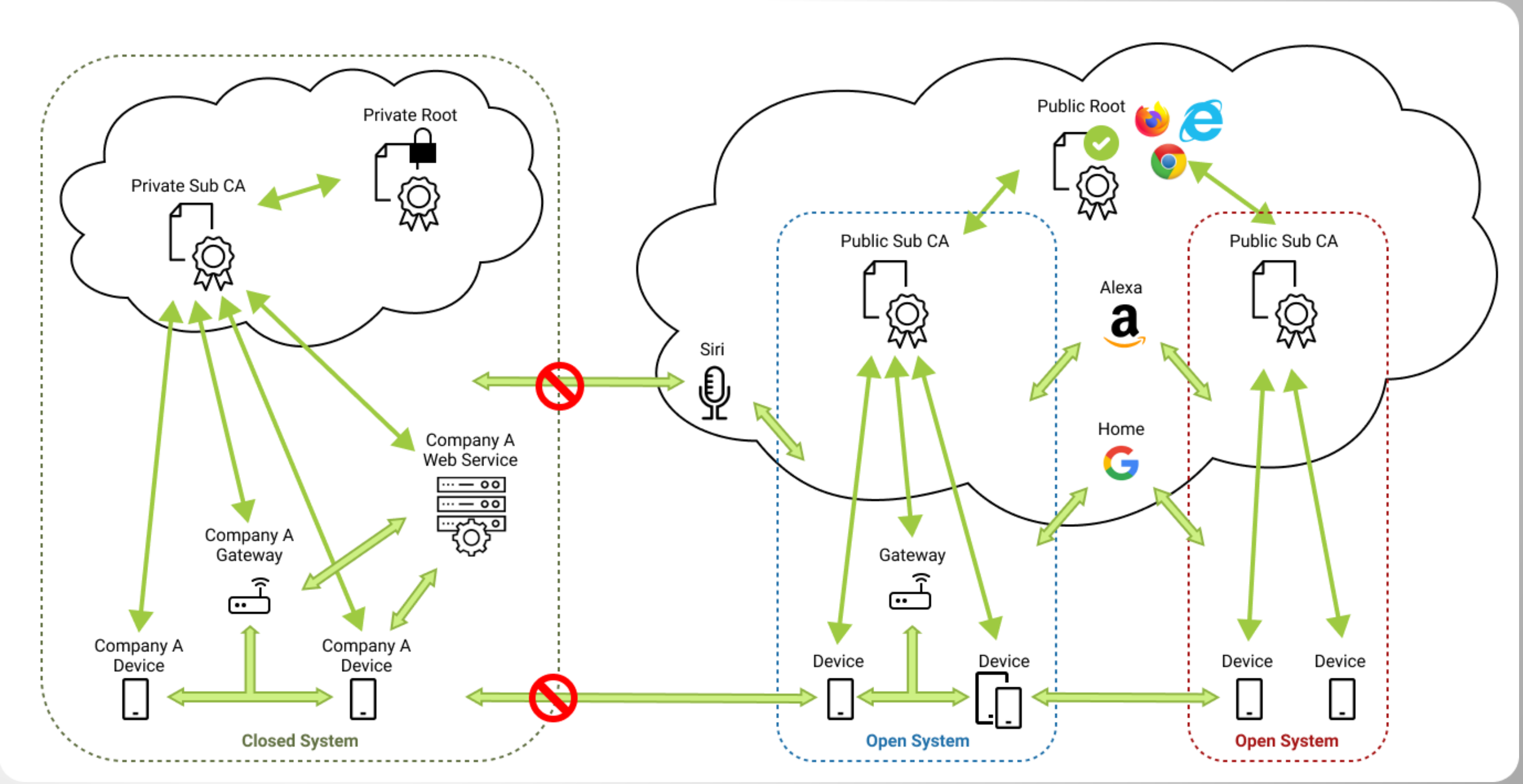
Power your certificate authority with SSL.com's World-Class PKI

Manage the life cycle of any digital certificate directly through your CA web interface, API or optionally through our Enterprise RA system.

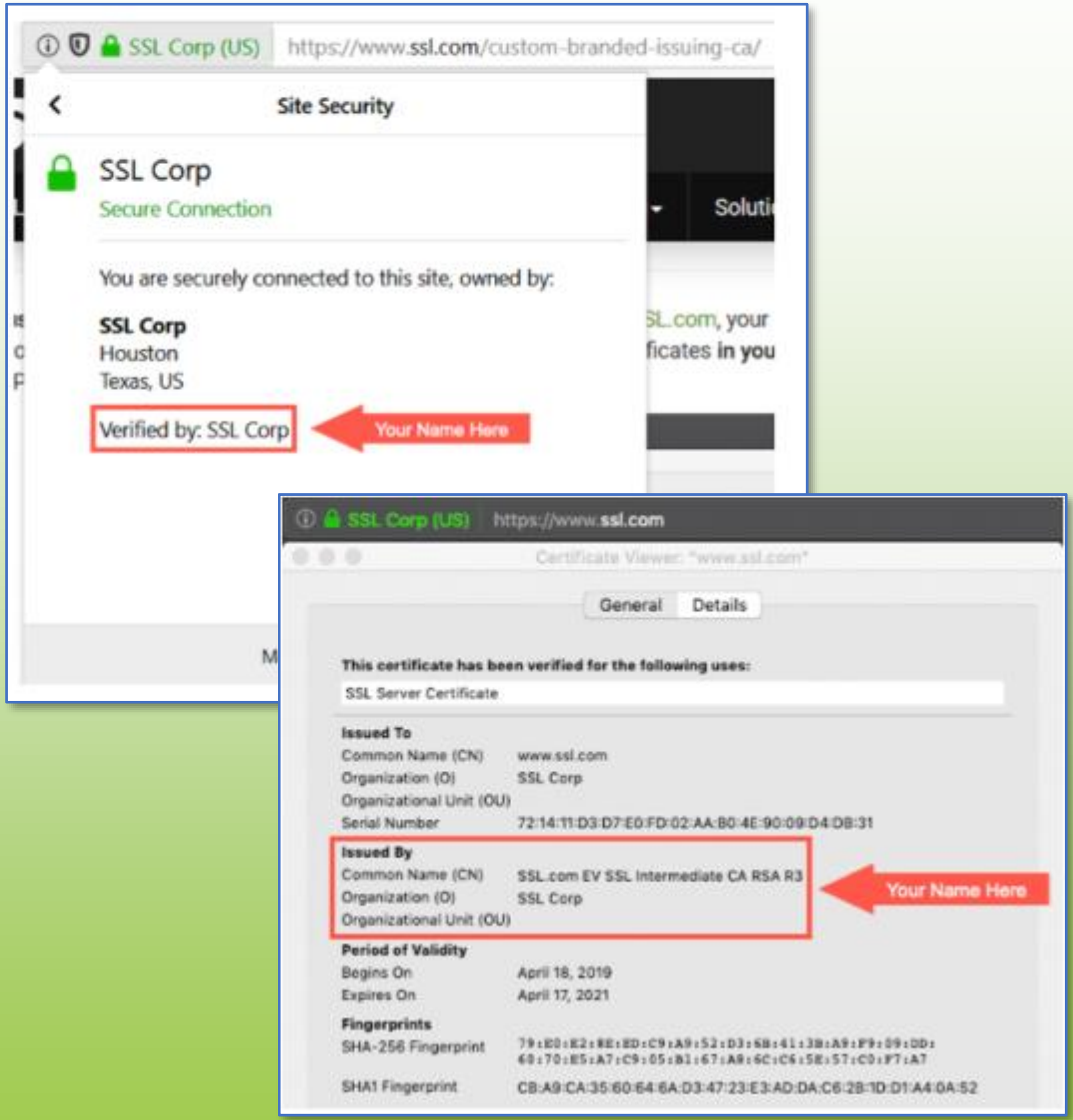
No need to purchase your own equipment or hire full time experts – resulting in significant cost savings.

We provide assistance with CA related services, such as authoring your own Certificate Policy and Certification Practices Statement or conducting an official Root Key Generation Ceremony.

Private vs Public PKI



https://www.ssl.com/blogs/whitepaper-hosted-enterprise-pki/



SSL Corp (US) https://www.ssl.com/custom-branded-issuing-ca/

Site Security

SSL Corp
Secure Connection

You are securely connected to this site, owned by:

SSL Corp
Houston
Texas, US

Verified by: SSL Corp

SSL Corp (US) https://www.ssl.com

Certificate Viewer: "www.ssl.com"

This certificate has been verified for the following uses:

SSL Server Certificate

Issued To
Common Name (CN) www.ssl.com
Organization (O) SSL Corp
Organizational Unit (OU)
Serial Number 72:14:11:D3:D7:E0:FD:02:AA:B0:4E:90:09:D4:DB:31

Issued By
Common Name (CN) SSL.com EV SSL Intermediate CA RSA R3
Organization (O) SSL Corp
Organizational Unit (OU)

Period of Validity
Begins On April 18, 2019
Expires On April 17, 2021

Fingerprints
SHA-256 Fingerprint 79:E0:E2:8E:ED:C9:A9:52:D3:6B:41:3B:A9:F9:09:DD:
60:70:E5:A7:C9:05:B1:67:A8:6C:C6:5E:57:C0:F7:A7
SHA1 Fingerprint CB:A9:CA:35:60:64:6A:D3:47:23:E3:AD:DA:C6:2B:1D:D1:A4:0A:52

Custom-Branded Issuing CA

Issue publicly-trusted certificates in your company's name

Also known as a subCA, your company or organization can leverage our technology and expertise to issue publicly-trusted X.509 certificates in your own name without having to invest in PKI infrastructure and staff.

Our facilities and processes go through regular reviews, testing and rigorous annual external audits to maintain our WebTrust certifications and provide you peace of mind.