![GlobalSign GMO INTERNET GROUP]

SSL/TLS as a Service

Integrate SSL/TLS into your services to enable encryption by default and gain a business advantage

In this "encrypt everything" era, end users have come to expect encryption as a basic website property. SSL/TLS Certificates to secure web transactions and provide trust are no longer nice-to-haves and users are turning to their eCommerce platforms, website builders, Application as a Service (AaaS/XaaS) providers, Content Delivery Networks (CDNs), and other providers of cloud services for solutions. To meet this expectation, while providing accessible, user-friendly options, you need an automated, scalable certificate solution that integrates directly into your existing platforms and services.

SSL/TLS as a Differentiator

Competition in the cloud-based services market is fierce and gaining a competitive advantage, from both a marketing and security perspective, is key to success. Privacy and security continue to be major concerns – highlighted by many recent newsworthy breaches. Encryption is now more important than ever. Have you thought about how TLS can provide that competitive differentiator?

Why Build Security into Your Service?

- **Enable Encryption by Default**
  Taking the responsibility away from your customers to opt in or order a certificate from a separate vendor and instead including it as standard within your offering helps create a more secure, safer Internet for everyone.

- **Improve Customer Experience**
  Offer a superior user experience by keeping your customers in your platform rather than pushing them to another vendor for their security needs.

- **Free Customers from Technical Burdens**
  Removing the burden of technical knowledge and certificate management from your customers allows them to focus on growing their business.

- **Gain a Competitive Advantage**
  Stand out from the competition by not just bundling security services into your existing offerings, but by seamlessly integrating them.

- **Boost Customer Conversion Rates & Search Rankings**
  Google uses HTTPS as a ranking signal, plus, HTTPS and other security indicators have been shown to increase conversion rates by providing visitors with more confidence and trust.

Key Benefits

- Build trust and security into your services with a highly scalable SSL/TLS solution

- Leverage security as a competitive marketing advantage

- Improve user experience for your customers by keeping them in your platform instead of pushing to another vendor for SSL/TLS

- Your customers get the security and business benefits of SSL/TLS without having to understand and manage certificates themselves

- Differentiate your service and grow your business

Why Partner with GlobalSign?

Support

We pride ourselves on our support, with a globally-distributed, multi-lingual tier 1-3 customer support and verification team, a Sales Engineering organization for integration projects (available on site if needed), and SaaS service descriptions and Service Level Agreements on reliability and velocity, as needed.

Flexible Licensing Models

We work with you to customize a solution that best fits your needs, whether they are technical or financial. Our flexible licensing enables you to choose the most optimal way to implement our hosted Certificate Service.

Experience

As a Certificate Authority for over 20 years, we have extensive industry expertise and embedded trust, providing validated identities through Digital Certificates. We've supported multiple successful high-velocity (hundreds of thousands of certificates in short periods) TLS as a Service deployments.

Scalability and Velocity

Whether you are an established high volume brand or a young innovative solution, we offer scalable and cost effective models to suit service providers of all sizes. GlobalSign's highly scalable Managed PKI services can issue up to 3,000 certificates per second.

The Technology Behind SSL/TLS as a Service: CloudSSL

CloudSSL is a SSL/TLS distribution service designed specifically for providers of cloud-based services that need to secure services or communications for many customers.

How CloudSSL Works

CloudSSL Certificates are issued to the service provider at the Organization Validated (OV) level. Customer domains can then be added as Domain Validated (DV) SANs after domain control is verified.

CloudSSL uses a SAN licensing model and each certificate can accommodate up to 500 SANs. Providers can add or remove SANs on-demand and if a SAN is removed, the license can be re-used for another domain without incurring any additional costs.

Automate deployments; no strain on internal support

CloudSSL Certificate issuance and domain addition and removal is done via APIs so it can be completely automated. This allows service providers to deliver TLS to all of their customers without putting a strain on internal support teams.

Take burden of certificate management and installation away from customers

The only time customers need to be involved in CloudSSL administration is to prove domain ownership and in many cases, the service provider can handle this step for the customer as well, removing the customer from TLS administration entirely.