Protecting Critical Infrastructure

Digital certificates provide strong identity, encryption, and signing while enforcing access control.

CHALLENGE

The Expanded Attack Surface

One of the greatest challenges organizations are facing today is an expanded attack surface. Applications and systems moving to the cloud, the ability to work from anywhere, and the sheer number of devices and machines connecting into networks means that organizations have more to secure than ever. And much of that exists outside the traditional confines of the IT environment. The security perimeter has disappeared. Strong identity is the new perimeter.

Not only that, but sensitive and confidential data is constantly moving over public and private networks – whether it's a user logging on to an online portal or sending an email, or machine-to-machine communication that occurs without any human intervention. With the increasing volume and sophistication of cyberattacks, it's critical that every single connection and endpoint is secured.

In order to mitigate these issues, more and more organizations are looking to security best practices – like Zero Trust – to help them form a strategy to ensure:

- Trusted identities are established
- Access and permissions are enforced
- Risk mitigation and response measures are in place

BENEFITS

- Public and private PKI with up-to-date certificate policy, operational procedures, and change controls
- Unified public and private certificate management console providing centralized visibility and control of digital certificates
- Built in crypto-agility
- CA resilience and best-practice incident response
- CA keys stored in certified data centers
- Support at all stages of the customer cloud journey
- Extendable to CLM, cryptographic asset discovery, key and secrets management, APIs, and more
- Broad portfolio of solutions that extends beyond identities to securing data, network, apps, and workloads and that integrates with a broad partner ecosystem

Learn more about our identity-centric Zero Trust solutions at entrust.com

Protecting Critical Infrastructure

From strong device identity to encryption to micro-segmenting, digital certificates are the most scalable, resilient, and secure way to achieve this.

SOLUTION

Digital Certificates

Our security solutions allow you to issue digital certificate-based identities to corporate assets, while also including best practices, governance, and security controls via your PKI, including:

- Strong issuance and revocation controls
- Up-to-date certificate policy
- Operational procedures
- Change controls

Entrust's **public TLS/SSL certificates** offer strong identity verification, least privilege administrations, rapid incident response, and automated controls.

Our **private TLS/SSL certificates** offer best practices, governance, and security controls, from how they were architected to strong issuance and revocation controls.

Both our public and private certificates deliver three key outcomes:

- Strong device identity – from IoT and mobile devices to servers and virtual machines
- Encryption for web servers, networks, and other systems
- Enforced access control to micro-segmented networks, applications, and systems

Certificate Lifecycle Management (CLM)

The more digital certificates an organization has, the greater the need for management and automation tools. CLM is an important component of your overall strategy by making sure you have strong issuance protection for your certificates.

Entrust's CLM solutions:

- Provide full visibility into your full certificate estate across environments
- Centralize control of those certificates
- Provide the automation layer required to mitigate the risks that come with a high volume of certificates across multiple distributed environments

CLM ensures you have strong issuance protection for your certificates and mitigates common risks such as a rogue certificate being issued that gives too much access or privilege. Entrust's CLM solutions deliver the visibility, control, and automation you need to have a strong security practice today but also to prepare for a post-quantum future.

Entrust's robust CLM solutions help customers:

- **Verify explicitly** – making sure the right certificate is provisioned to the correct endpoint or target
- **Manage least privilege** – providing the right assurance, access, and privilege by picking the correct certificate and lifecycle controls
- **Assume breach** – contain an attack and limit the loss and damage through revocation

Protecting Critical Infrastructure

THE ENTRUST DIFFERENCE

Delivering PQ-Ready Solutions

The threat that quantum computing poses to digital security is expected to be realized within the decade, so organizations need to begin preparing today. Entrust can help with the PQ-preparedness journey to help future-proof your organization, including:

- Gaining visibility of all cryptographic assets across environments
- Assessing crypto-agility maturity and developing a strategy/roadmap to implement post-quantum cryptography (PQC)
- Testing and implementing quantum-safe scenarios and infrastructure with our PKIaaS – the world's first commercially available PQ-ready PKI

PKI Experts

As globally recognized experts in PKI for more than 25 years, Entrust recognizes that there is no one PKI solution that fits all needs, so we have a portfolio of scalable PKI solutions and deployment models to fit any need. All Entrust PKIs and their operations are aligned with industry and regulatory best practices.

Learn more at
entrust.com

ENTRUST

Global Headquarters
1187 Park Place, Minneapolis, MN 55379
U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223