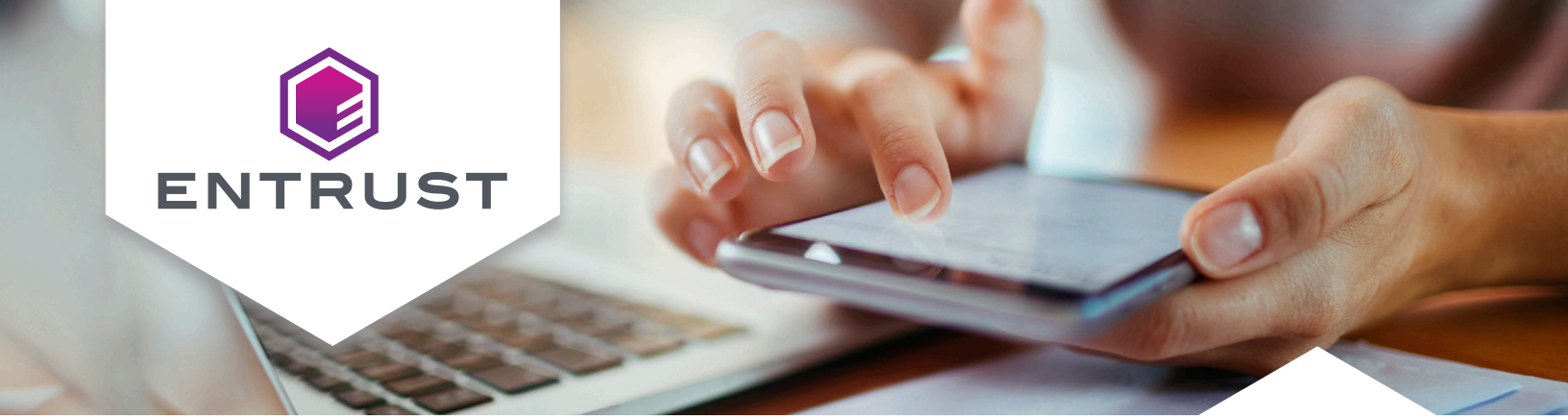


Application Security End-to-End (ASE2E) Encryption

Secure login credentials and data communicated via browser or mobile app

The Challenge

Banking and finance regulators in many jurisdictions require “end-to-end” encryption of login credentials, but the digital security issue is broader and applies to any business or organization that has end-users logging in via a browser or a mobile app.

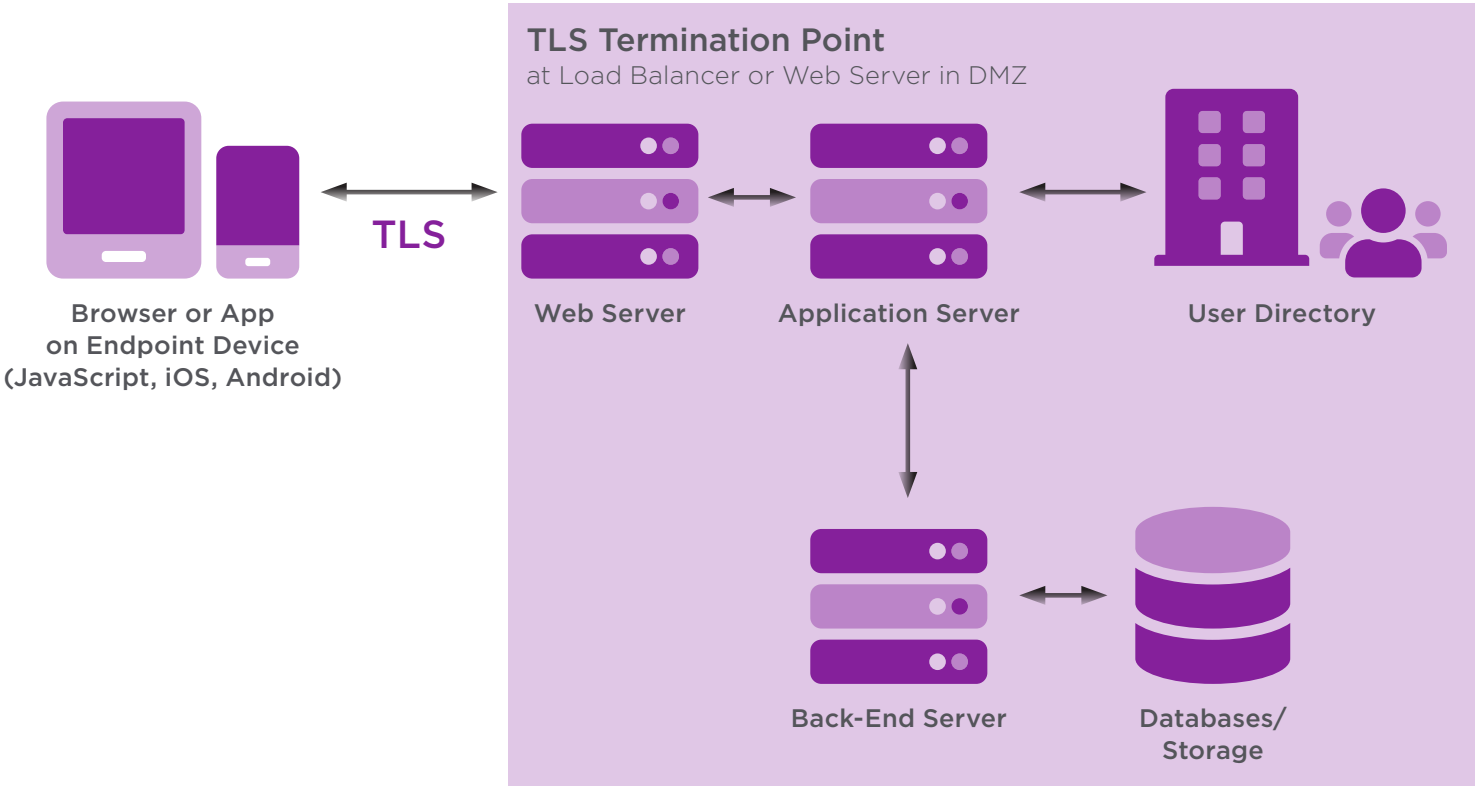
Login credentials and data communicated between browsers or apps and back-end servers are typically protected by TLS over the Internet. But TLS protection typically stops at a firewall, load-balancer, proxy server, or other server in the outer part of the organization’s infrastructure. Within the rest of the infrastructure, the data is typically in plaintext and therefore prone to attack inside the organization.

(See illustration on next page.)

BENEFITS

- Provides end-to-end encryption from the end-user all the way through to back-end systems
- No exposure of passwords outside the hardware security module (HSM)
- Customizable and extensible for legacy password hashing algorithms and other customer requirements
- User/device pre-registration not required – solution can be seamlessly added to existing password management
- High performance
  - Hundreds of transactions per second per HSM
  - HSMs can be pooled using Entrust nShield Security World architecture
  - Multiple calling servers with multiple calling threads per server

Application Security End-to-End (ASE2E) Encryption



Application Security End-to-End (ASE2E) Encryption

The Solution

Entrust Application Security End-to-End (ASE2E) encryption solution, delivered by the Entrust Professional Services team, protects logon credentials and data against insider attacks, hackers, and data breaches.

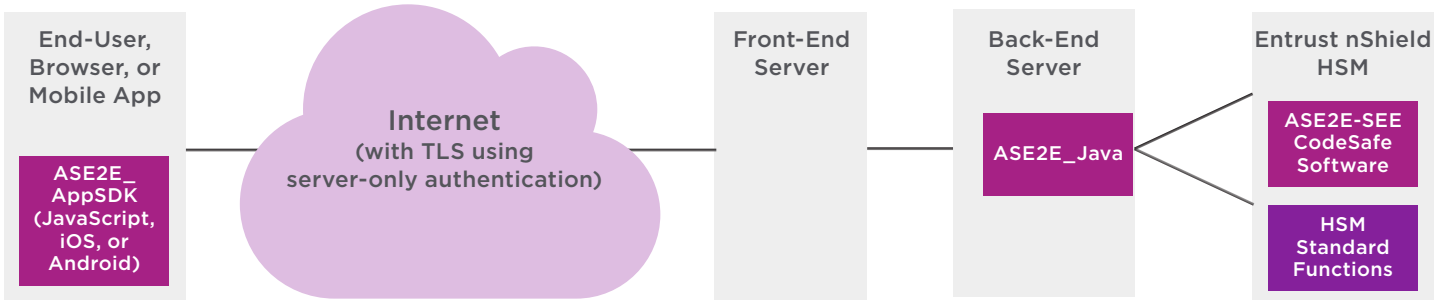
PINs, passwords, and one-time password (OTP) keys are never exposed in plaintext and remain protected by FIPS 140-2 and Common Criteria certified Entrust nShield® Hardware Security Modules (HSMs). This ensures best practices and helps facilitate compliance with security standards and regulations for end-to-end encryption.

The solution components are:

ASE2E_AppSDK (for JavaScript, Android, iOS)
These libraries are included in the customer's webpage code or mobile application software that runs on the end-user's device. They secure passwords and data with authenticated encryption. The encrypted passwords or data can then be sent to the back-end systems. Only HSMs at the back-end can decrypt and validate the data.

ASE2E_Java back-end system
Called by the customer's back-end systems using Java, this module in turn calls both standard Entrust nShield HSM functions and the ASE2E CodeSafe software. Multiple servers (and multiple threads per server) with a pool of Entrust nShield HSMs can be used for high throughput. Optionally, a REST API can be provided in front of ASE2E_Java.

ASE2E_SEE CodeSafe software running inside the HSMs
This is called by the ASE2E_Java back-end system. It verifies passwords and checks constraints within the secure environment of the HSM, so no passwords or partial results are exposed outside the HSM.



The customer's existing password hashing methods can be supported, allowing seamless transition, without the need to force users to update their passwords.

The solution implements mature key management and password security best practices, including strong separation of key types, man-in-the-middle attack protections, and optional forward-secrecy.

Application Security End-to-End (ASE2E) Encryption

About Entrust nShield HSMs

Entrust nShield HSMs are among the highest-performing, most secure, and easiest-to-integrate HSMs available. They help facilitate regulatory compliance and deliver the highest levels of data and application security for enterprise, financial, and government organizations. Our unique Security World key management architecture provides strong, granular controls over access and usage of keys. For more information visit entrust.com/HSM.

The Professional Services Difference

With decades of experience, the Entrust Data Protection Solutions Professional Services team offers unmatched expertise in designing and implementing crypto applications for the world's most security-conscious organizations. Our Professional Services consultants work closely with clients to design and deploy the right solution for their unique environments and to leave their teams with the knowledge to maintain it for years to come.

ABOUT ENTRUST CORPORATION

Entrust keeps the world moving safely by enabling trusted identities, payments, and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services, or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.

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
info@entrust.com **entrust.com/contact**