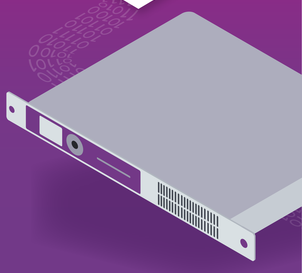
ENTRUST
SECURING A WORLD IN MOTION

Top 5 Reasons for Securing Your PKI With an HSM

PKI certificates can identify users and devices to protect information, but only when you can maintain secrecy of the private key. Entrust nShield® hardware security modules (HSMs) are tamper-proof physical devices that safeguard cryptographic keys, providing the highest form of key protection.



1 Help achieve compliance

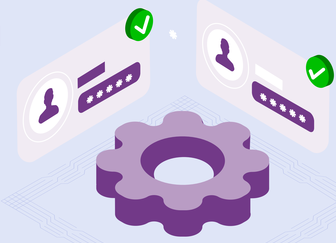
Industry regulations such as FIPS, Common Criteria, GDPR, HIPAA, and PCI DSS mandate the use of HSMs to ensure keys are protected to the highest standard. Highly regulated authorities (governments, banks, healthcare providers, globally trusted CAs, etc.) rely on HSMs to protect mission-critical private keys.

2 Software keys are easy to steal

When software generates a key for a certificate and stores it as a permissions-protected file on your computer, an attacker with administrative access or a server backup can easily extract the software key.

3 Apply access control through policies

HSMs have role-based access control features that allow you to apply policies for individual key containers, such as requiring a quorum of PKI administrators to provide a smart card and PIN to unlock the offline root CA private key stored in the HSM.

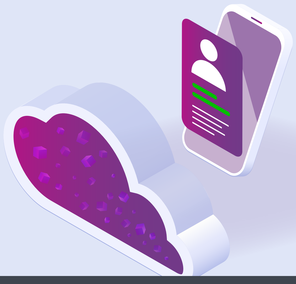


4 Demonstrable ROI

The costs associated with HSMs are negligible compared to the impact of a key compromise. The value of any key is equivalent to the value of all the data it is used to protect, making keys one of your most precious assets. Hacks come with reputation damage, huge fines, and loss of investor/customer confidence.

5 Support critical use cases

Both the traditional (user/device authentication, email security) and the newer (cloud, IoT) use cases depend on a robust and secure PKI.



HSM Root of Trust

Entrust nShield® HSMs are among the highest-performing, most secure, and easy-to-integrate HSM solutions, facilitating regulatory compliance and delivering the highest levels of data and application security for enterprise, financial, and government organizations. FIPS 140-2 and Common Criteria certified, with unique nShield® Security World key management architecture, they provide strong, granular controls over access and usage of keys.

Secure your PKI with an Entrust HSM today

Learn More

ENTRUST