Public key infrastructure (PKI) SHA-1 to SHA-2 migration service

Meeting the challenges of upgrading your PKI hashing algorithm

HIGHLIGHTS

- Expertise to help you efficiently select among migration options
- In-depth knowledge of complexities to help you avoid pitfalls and mitigate risks
- Thorough upfront planning to minimize downtime

Cryptographic hashes form the basis of certificate-based message authentication in virtually all Internet protocols. With the SHA-1 hashing algorithm now considered unsafe, organizations have been rapidly migrating to SHA-2. All major browser vendors will soon stop supporting SHA-1 signed certificates.

Moving to SHA-2 presents a complex problem due to the integral nature of hash algorithms within PKIs, as well as various industry and application incompatibilities with SHA-2. Entrust Professional Services (PS) can help you securely manage the complexities of this critical migration.

Industry shift from SHA-1 to SHA-2

SHA-2 is now the standard for self-managed and public CAs, although SHA-1 is still in use. There is widespread recognition that SHA-1 certificates are unsafe, and U.S. NIST advised that SHA-1 should not be trusted past January 2014.

Collision attacks and SHA-1

SHA-1 is no longer considered safe from collision attacks, where two different blocks of input data yield the same output hash. Such an attack is fatal for a hashing protocol as it allows hackers to offer malicious content carrying the same hash value as a genuine article, thus enabling fake certificates.

Navigating incompatibilities with SHA-2

Updating to SHA-2 can be complicated by compatibility issues with older Android and Windows OSs still widely used today, as well as new and legacy versions of Microsoft Office.

The more complex and aged your PKI, the more likely you are to encounter incompatibilities. For example, earlier supervisory control and data acquisition

Public key infrastructure SHA-1 to SHA-2 migration service

(SCADA) systems, payment systems based on hardened versions of Windows XP, older BYOD handsets, and even simple applications like macro signing can present challenges.

Entrust PS has the experience to help you work around incompatibilities between SHA-2 and the applications you may be using in your PKI.

Planning your migration to SHA-2

Your PS consultant will work with you to understand your PKI's dependencies on SHA-1 hashes as an essential first step, and will perform the following functions to plan for a successful migration:

- Analyze your PKI environment
- Map your end points to evaluate SHA-2 compatibilities
- Assess risks and recommend mitigation strategies and migration options

Understanding your options

Your PS consultant has the in-depth knowledge to help you make the best choice among various options, for instance, deploying a hybrid system; converting to a new SHA-2 root; or creating a parallel SHA-2 PKI and migrating over time.

Supporting your migration

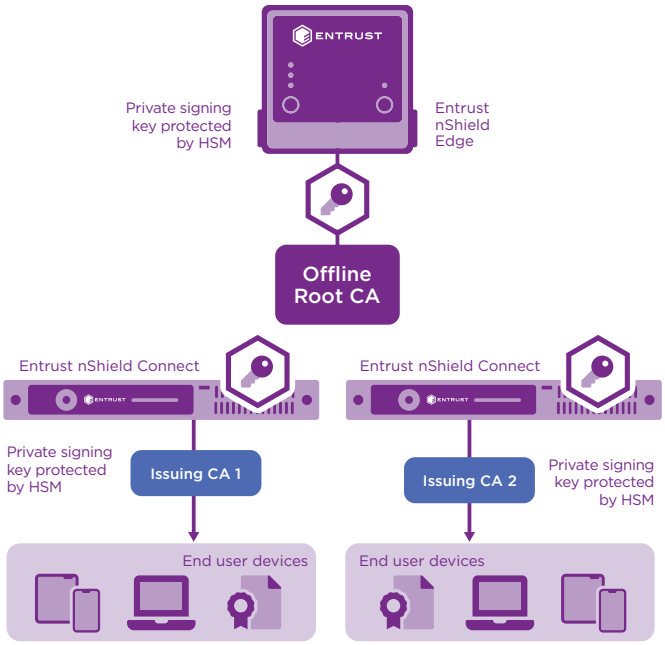
Your PS consultant will guide you through your migration as needed, from planning and documentation through testing and deployment.

About Entrust professional services

Entrust PS offers a full range of products and services designed to assist you in achieving your PKI goals in a safe, risk-managed fashion. We can help you identify end-point compatibility issues, develop a migration plan, deploy an auditable key management strategy, and provide technical support, from root key ceremony through production roll-out.

Learn more

To find out more about Entrust nShield® HSMs visit **entrust.com/HSM**. To learn more about Entrust's digital security solutions for identities, access, communications and data visit **entrust.com**



Learn more at
entrust.com/HSM

ENTRUST

Contact us:
HSMinfo@entrust.com