Public key infrastructure (PKI) healthcheck service

Determine the health and status of your PKI deployment

HIGHLIGHTS

- Decades of experience with PKIs enables Entrust to deliver thorough and actionable recommendations to rectify issues and enhance the health of your PKI

- Comprehensive analysis extending beyond PKI technology to include policy and governance provide the convenience and efficiency of a one-stop shop

- Expert advice on security-enhancing Hardware Security Modules (HSMs) with the backing of thousands of Entrust HSMs deployed globally

Many organizations use a public key infrastructure (PKI) to provide digital certificates to help secure critical business assets. Knowing that your PKI is deployed in a secure state and that it is optimally configured for your business provides assurance that the PKI is providing real business benefit and value to your organization. The Entrust professional services (PS) team can provide a "PKI healthcheck" service to give you the further assurance that your PKI is performing in the most secure and optimal manner possible.

Key features

The Entrust PKI healthcheck covers the following areas of your PKI deployment:

- Policy framework

- Governance

- Certificate lifecycle management

- HSM installation, configuration, and deployment (if using HSMs)

- Operations

- Deployment

- Backup and recovery

- CA installation and configuration

- Subscriber/relying party certificate usage and integration

- Audit and logging

- Security controls

Public key infrastructure healthcheck service

The PKI healthcheck process

The PKI healthcheck is undertaken in two phases. Prior to phase 1, your Entrust PS consultant will ask you to complete a short questionnaire covering some basic aspects of your PKI. This will enable the consultant to tailor the engagement to focus on key areas.

Phase 1 - data gathering

The consultant will visit your site to evaluate all aspects of your PKI, with a particular focus on the areas highlighted in your initial questionnaire. The consultant may ask you to provide specific information from your PKI deployment and to run tools provided with your PKI software to gather information. The consultant will look at documentation related to your PKI and discuss with key personnel how the PKI operates and is managed. All information discovered during this phase will be included in the report that your consultant will provide you.
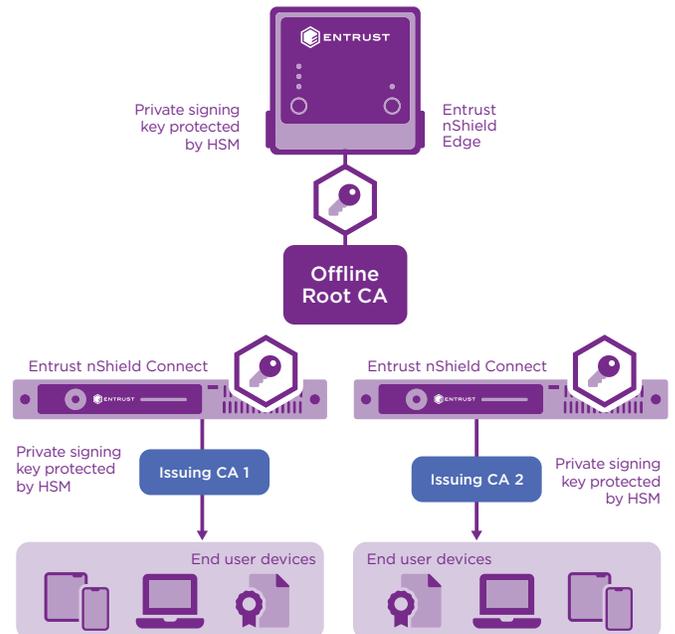
Phase 2 - analysis and reporting

The consultant will analyze the data collected during Phase 1 and produce a report detailing discoveries from the on-site analysis as well as recommendations and guidance on how to rectify any issues. The consultant will also present to you a slide deck on the findings.

The Entrust difference

In addition to addressing the technical properties of your PKI, the Entrust PKI healthcheck also covers policy and governance aspects of managing and operating a PKI. Clear policy, repeatable management processes and robust governance are key parts of any successful PKI deployment and are areas which are often overlooked. Entrust consultants have a wealth of experience in managing, operating and deploying PKIs "at scale" and are well equipped to analyse and provide guidance in this crucial area.

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**

Private signing key protected by HSM

Entrust nShield Edge

Offline Root CA

Entrust nShield Connect

Entrust nShield Connect

Private signing key protected by HSM

Issuing CA 1

Issuing CA 2

Private signing key protected by HSM

End user devices

End user devices

Learn more at
entrust.com/HSM

Contact us:
HSMinfo@entrust.com