



Why you should care about audits

A PKI audit is essential. Without one, you could wind up with fraudulent certificates issued to untrusted people.

Audits are not just a tool for wary organizations to track down suspicious employee activity. No, an audit's true value lies in preventing *accidental* security breaches—the kind committed or overlooked by even the most loyal, security-conscious IT staff. Even with a high level of technical and security expertise, IT personnel can't know everything, and will make mistakes from time to time. An audit is important because it exposes all security oversights and ensures they are corrected.

Every year, Entrust undergoes a best-in-class audit conducted by a professional auditing firm with real-world PKI experience. Their annual recommendations allow Entrust to continually improve the security of its managed PKI offering.

Our auditors ask tough questions

- Is the CA's root key—which is the key responsible for signing user certificates and ultimately the single most important piece of data in your PKI—generated and maintained according to strict, thorough, and well-implemented guidelines?
- What is the process for issuing certificates, and are there any security vulnerabilities in this process?

- What screening is performed on the people who are allowed to access the CA?
- How is users' personal information protected when it is accessed, processed, stored, transmitted, viewed, or otherwise handled?
- What IT controls are used—firewalls, for example—and how are they implemented?
- Is dual control required to access the CA?
- How is the physical site security maintained? What is the state of the building? Is there a backup facility? Are badges or biometric devices used to control access?

We use independent, certified auditors

Entrust undergoes an annual audit by an independent, professional auditing firm. Our auditors are:

- Used by the US Federal Government to conduct its annual PKI audits
- Recognized and accepted by Fortune 1000 companies
- CISA accredited

Certified Information Systems Auditors (CISAs) are recognized worldwide, by all industries, as the preferred choice for Information System (IS) auditors. Their governing body, ISACA, was founded in 1967, and has 86,000 members spread across 175 chapters in 70 countries worldwide.

- PKI experts
Our auditors have an intimate knowledge of PKI, having assumed many critical roles within the industry including architect, system administrator, and policy writer to name a few. Their experience enables them to conduct audits with a thoroughness that would exceed the capabilities of other professional certifications.

We use industry leading audits

Using a combination of WebTrust for CA and ISO 21188 audit formats at its various locations, Entrust undergoes independent 3rd party audits to ensure the most current and effective security practices.

The ISO 21188 and WebTrust for CA audits are:

- Based on established standards
The WebTrust for CA and ISO 21188 audits are derived from one of the most widely known and adopted standards for CA operations, the *American National Standards Institute (ANSI) X9.79:2000 PKI Practices and Policy Framework*.
- Accepted by Microsoft
WebTrust for CA and ISO 21188 are among the few audits accepted by Microsoft for their Root

Certificate Program. Organizations must join this program to have their root CA certificate installed in every copy of Internet Explorer worldwide.

- Able to satisfy public trust requirements
You can purchase the public trust option and Entrust handles browser vendor audit requirements.
- Created specifically for PKI

Unlike SAS 70, which only assesses generic IT controls, the WebTrust for CA and ISO 21188 audits include CA control criteria covering topics like certificate lifecycle management, root key generation ceremonies, the handling of CA keys, and compliance with the *Certificate Policy* and *Certification Practice Statement*.

Information

Contact an Entrust representative at 888-690-2424 to request more information.

- For an easy-to-read overview of key policies and procedures related to Entrust Managed Services PKI, request the *Entrust Managed Services PKI Information Security Review FAQ*.
- For official policies and procedures, request the *Certificate Policy*.

About Entrust

Entrust provides identity-based security solutions that empower enterprises, consumers, citizens and Web sites in more than 4,000 organizations spanning 60 countries. Entrust's identity-based approach offers the right balance between affordability, expertise and service. For strong authentication, fraud detection, digital certificates, SSL and PKI, call 888-690-2424, e-mail entrust@entrust.com or visit www.entrust.com.

Entrust[®] Securing Digital Identities & Information

Entrust is a registered trademark of Entrust, Inc. in the United States and certain other countries. In Canada, Entrust is a registered trademark of Entrust Limited. All other Entrust product names and service names are trademarks or registered trademarks of Entrust, Inc. or Entrust Limited in certain countries. All other company names, product names and logos are trademarks or registered trademarks of their respective owners. © Copyright 2011 Entrust. All rights reserved.