Frequently Asked Questions

Frequently Asked Questions: Prioritizing Trust: Certificate Authority Security Best Practices

Symantec™

Norton™ SECURED
powered by VeriSign

Prioritizing Trust: Certificate Authority Security Best Practices

CONTENTS

Q1: What is a Certificate Authority (CA), and why are CAs necessary?

A commercial Certificate Authority (CA) is an organization that issues digital certificates to be used by other parties. These certificates contain the certificate holder's public key, and also authenticate the certificate holder's identity. CAs are needed because they act as trusted third parties that certify the identity of certificate owners, and sign the digital certificates which enable encryption of data transmitted between certificate owners and relying parties.

Q2: What is the greatest challenge facing the CA industry today?

SSL/TLS technology still provides excellent protection against evolving cyber security threats. With the right tools and processes, CAs are fully capable of providing the greatest assurance possible that their certificates – and the websites that use the certificates – are genuine and safe for online business. The problem is not the technology but the way it is being implemented and the practices around it. Currently, there's no overarching system or authority to rate, rank, or approve CAs that issue SSL/TLS certificates, and there are no standards for how certificates are issued. As a result, some CAs have prioritized cost and performance over security, resulting in several high-profile security breaches.

Q3: What are the most critical responsibilities that CAs should be focused on?

In general, there are three basic areas of responsibility that CAs should focus on:

- **Security** – Securing the certificate infrastructure through physical and logical controls.
- **Performance** – Maintaining a highly available, highly responsive infrastructure, especially the infrastructure needed to serve certificate revocation status.
- **Authentication** – Following strict authentication practices and procedures is extremely important because authentication forms the basis of trust on the Internet.

Q4: What are the key elements to maintaining a secure certificate infrastructure?

Maintaining a secure infrastructure depends on a certificate authority's ability to define and enforce strong, effective security policies through an ongoing process that revolves around three key activities:

- **Policy governance** – Security policies should be planned, managed and supported at the highest level of the organization, and they should cover every aspect of the digital certificate life cycle and associated trust services. These policies should take the form of a Certification Practice Statement (CPS) and a Certificate Policies (CP) document and both of these documents should be made publicly available.
- **Design** – Once a CA has defined its policies, all IT infrastructure and business processes should be designed to meet these requirements – everything from applications, hardware, physical infrastructure, network security to hiring and personnel practices.
- **Implementation** – CAs must demonstrate proper implementation of these policies, and disciplined operation of the CA through monitoring, logging, and third-party audits.

Q5: What are the Certification Practice Statement (CPS) and Certificate Policies document and why are they so important?

These documents set forth the business, legal, and technical requirements for approving, issuing, managing, using, revoking, and renewing, digital certificates, and providing associated trust services for all participants. These requirements are critical because they protect the security and integrity, and comprise a single set of rules that apply consistently across all operations, thereby providing assurances of uniform trust.

Q6: What are some of the most important environmental controls to consider?

Here are a few of the most important IT infrastructure controls that CAs should implement:

- **Security planning and governance:** Information security should be planned, managed and supported at the highest level of the organization. There should be an information security policy document that includes physical, personnel, procedural and technical controls, is approved by management, published and communicated to all employees.
- **Asset classification and management:** CA assets and subscriber and relying party information should receive an appropriate level of protection.
- **Personnel security:** CAs should provide reasonable assurance that personnel and employment practices enhance and support the trustworthiness of the CA's operations, identifying Trusted Roles, assigning specific responsibilities to (and performing background checks on) people in these roles.
- **Physical security:** Physical access to CA facilities and equipment must be limited to authorized individuals, protected through restricted security perimeters. This includes the facility itself, as well as all equipment.
- **Operations:** CAs must ensure the correct and secure operation of CA information processing facilities, minimize the risk of systems failure or infection by malware/viruses, develop incident reporting and response procedures, and protect media from theft, loss, damage or unauthorized access.
- **System access:** CAs must limit access to authorized individuals; this includes user access controls, as well as access to operating systems, databases, and applications.
- **Systems development:** CAs must provide assurance that development and maintenance activities are documented, tested, authorized, and properly implemented to maintain CA system integrity.
- **Business continuity:** CAs must develop and test a business continuity plan that includes a disaster recovery process to minimize potential disruptions to Subscribers and Relying Parties as a result of the cessation or degradation of the CA's services.
- **Monitoring and compliance:** CAs should be able to demonstrate conformance with the relevant legal, regulatory and contractual requirements; compliance with the CA's security policies and procedures; maximization of the effectiveness of the system audit process with minimal interference; and detection of unauthorized CA system usage.

Q7: What steps does Symantec take to ensure adequate performance and availability?

Symantec uses 13 data centers around the globe to provide our Certificate Authority services to customers for optimal performance. Symantec can go live with a new global root key across our infrastructure in 8 minutes without causing any disruption to our customers, and our validation infrastructure has experienced 100% uptime since 2004. In addition, Symantec's infrastructure supports on average 4.5 billion Online Certificate Status Protocol (OCSP) certificates lookups every day. Symantec provides a less than 1 second response time for OCSP queries. In comparison, the standard response time proposed in the Certificate Authority/Browser Forum suggests a requirement of up to 10 seconds. Last but not least, Symantec posts revoked certificates to their OCSP and CRL systems within 5 minutes of revocation. In comparison, the time proposed in the Certificate Authority/Browser Forum standard suggests posting revocations within 24 hours.

Q8: What are some of the key challenges that CAs need to address in terms of authentication?

Apart from the CA/Browser rules governing Extended Validation (EV) certificates and the newly adopted CA/Browser Baseline Requirements, CAs are largely responsible for governing their own processes and procedures. Symantec has been operating its authentication service for more than a decade and has established authentication mechanisms and policies such as separation of duties, database tracking, and other methods to offer the highest possible level of assurance about the identity and integrity of the certificate holder.

Q9: What steps should CAs take to monitor and correct vulnerabilities?

Document and follow a vulnerability correction process that addresses the identification, review, response, and remediation of vulnerabilities. The process should use manual or automated tools to probe internal and external systems to check and report on the status of operating systems, services, and devices exposed to the network and the presence of vulnerabilities listed in the NVD, OWASP Top Ten, or SANS Top 25.

CAs should also undergo or perform a Vulnerability Scan on public and private IP addresses identified by the CA or Delegated Third Party as the CA's or Delegated Third Party's Certificate Systems. Scans should be performed at least once every three months, when determined necessary by the CA or the CA/Browser Forum, or after any significant system or network change. In addition, CAs should perform a penetration test performed on their Certificate Systems at least once a year, when determined necessary by the CA or the CA/Browser Forum, or after any significant infrastructure or application upgrade or modification.

Q10: Why is it more important than ever for CAs to adopt and follow rigorous security and authentication practices?

Being a Certificate Authority is not something to take lightly. It is a serious responsibility. We make it possible for people to trust and share information online, but recent attacks on CAs are threatening to undermine confidence in the system. Symantec strongly believes that now is the time for the industry to pull together and focus on improving our operations and practices. Furthermore, CAs can't just focus on their own infrastructure, but must also hold their partners to the same standard. Symantec requires all its partners to meet the same standards or risk having the relationship severed, and this should be a practice that all CAs follow.

More Information

Visit our website

http://go.symantec.com/trustontheinternet

To speak with a Product Specialist in the U.S.

Call 1 (866) 893-6565 or 1 (650) 426-5112

To speak with a Product Specialist outside the U.S.

For specific country offices and contact numbers, please visit our website.

About Symantec

Symantec is a global leader in providing security, storage, and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored.

Symantec World Headquarters

350 Ellis Street
Mountain View, CA 94043 USA
1 (800) 721 3934
www.symantec.com

Symantec™

Norton™ SECURED
powered by VeriSign

UID:127/7/12