Enhancing Trust and the Integrity of SSL

Certification Authority Best Practices

OTA
Online Trust Alliance

Developing and advocating best practices to mitigate emerging privacy, identity and security threats to online services, government agencies, organizations and consumers, thereby enhancing online trust and confidence.

Updated 3/7/2013

Table of Contents

Introduction

The Online Trust Alliance (OTA) is a non-profit organization with a mission to enhance online trust while promoting innovation and the vitality of the Internet. OTA's primary goal is to help educate businesses, policy makers, and stakeholders while developing and advancing best practices, as well as the tools to enhance the protection of users' security, privacy, and identity. The OTA supports collaborative public-private partnerships, benchmark reporting, meaningful self-regulation, and data stewardship.

The foundation of the utility and growth of the Internet is user and business trust in the sites they visit, the email they receive, transactions they complete, and the information they share. Since its formation, the OTA has advocated for meaningful and actionable best practices. With the goal of driving adoption and removing barriers to implementation, the OTA tracks adoption of trust-enhancing technologies and practices, highlighting "north stars" and early adopters. Annually the OTA publishes the Online Trust Honor Roll and Online Trust Index, (OTI), incorporating a composite analysis of sites' security measures, SSL implementation, privacy practices, and related online trust enhancing efforts.[1]

Encouraging SSL best practices has been at the foundation of many of OTA's initiatives spanning over six years. In 2007, the OTA began advocating the benefits of Extended Validation Certificates(EV SSL)[2], and in February 2012 began championing the business value of Always On SSL.[3] In October 2012, the OTA hosted a 2-day international meeting, including a working session entitled the Future of SSL Security & Site Optimization, soliciting input into best practices from the ecosystem.[4]

An essential part of the internet chain of trust is Secure Sockets Layer (SSL) (technically referred to now as "Transport Layer Security" or "TLS") technology. SSL is the standard security technology for establishing an encrypted link between a web server and the user's browser. Certification Authorities (CAs) serve as the intermediaries of that trust by issuing and selling digital SSL certificates which are used to encrypt and secure web sites. These technologies and protocols are well understood, widely adopted, and hugely scalable. This level of success has attracted the attention cyber criminals and hackers. The security ecosystem will continue to innovate to thwart future forms of attacks with new developments like TLS 1.2 and beyond.

[1] https://otalliance.org/news/releases/2012HonorRollRelease.html

[2] https://otalliance.org/resources/EV/index.html

[3] https://otalliance.org/resources/AOSSL/index.html

[4] https://otalliance.org/events/2012Forum/PPTS/TuesPDFs/FutureofSSL.pdf

Industry has recognized that with all best practices, the strength of a solution is only as strong as the weakest link. As experienced with other internet stakeholders and supply chain participants spanning from email providers toad networks to social networks, several CAs have experienced security incidents that have diminished trust in the SSL ecosystem. Fortunately, up to now these incidents have been detected and neutralized before measurable harm has occurred. At the same time we recognize that the severity and velocity of attacks targeting CAs will escalate, which underscores the urgency of raising the bar and the voluntary adoption of best practices by CAs. In response to these threats and by soliciting feedback from CAs, relying parties, the browser community, security experts, and government agencies, this paper outlines practices that organizations should demand from their CAs.

It is important to note that there are other efforts working in parallel that should not be discounted, and require collaboration by operating systems, browser vendors, and the relying party sites. Collectively we have a shared responsibility to protect the SSL infrastructure. While outside the scope of this paper, future OTA papers will address other promising best practices. Such efforts include but are not limited to Certificate Transparency, (CT), Certificate Pinning, Always on SSL[5], Hard-failing the SSL connection when revocation checking fails, DNSSEC with Certification Authority Authorization Resource Records, and OCSP Stapling, among others. These new approaches call for a holistic approach to protecting the PKI/CA/SSL ecosystem.

Executive Summary

We increasingly live, interact, and do business online, making online trust and information security more important than ever before. Online trust involves a system for securing the communications with websites that end-users visit. At the root of secure web sites are securely installed SSL certificates, which for nearly two decades have helped build trust on the public Internet. Given the important role of CAs in online trust, it is important for the public to know and distinguish those that follow the highest industry standards. In this whitepaper, the OTA surveys the current online trust landscape and presents a collection of CA best practices that enhance trust as part of an OTA initiative to highlight admirable practices in the CA industry that can possibly be used to demonstrate how policy makers, system administrators, and others can enhance their own security posture and data protection capabilities.

In 2011, a few highly publicized CA security breaches made it apparent that while CAs are generally "trusted equally" by inclusion as trust anchors in browsers, not all CAs follow the same strict security practices, and thus do not provide equal levels of assurance. This white paper attempts to address this undeserved equivalency of trust within the global SSL infrastructure.

[5] http://www.otalliance.org/resources/AOSSL/index.html

Internet security experts have been encouraging CAs to be more secure with standardized CA security practices for over two decades.[6] More recently, the Certification Authority/Browser (CA/B) Forum, a voluntary organization of CAs and web browser vendors, has published guidance that will continue to enable the secure issuance and management of certificates used to establish online business identity, and thereby help prevent online fraud. At the same time, as with most trade organizations they are encumbered by the need to reach consensus of a diverse group of global ecosystem stakeholders, forcing the bar to be lower than some core stakeholders would prefer.

As discussed below, the CA/B Forum took steps by adopting "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" ("Baseline Requirements"), the first international baseline standard for the operation of CAs issuing organization and domain validated SSL/TLS digital certificates natively trusted in browser software, and the "Network and Certificate System Security Requirements" ("Network Security Requirements"), effective January 1, 2013.[7]

While these are noteworthy steps, it is broadly acknowledged that more can be done by all CAs – including commercial and government-run - to implement better security standards. Starting with the Baseline Requirements and the Network Security Requirements, these implementations include evaluations of their own internal security with vulnerability scanning and penetration testing as discussed in this paper. Additionally, web browser developers, SSL certificate subscribers, and relying parties must hold CAs accountable for complying with these requirements. The OTA appreciates the work done by such auditing bodies as WebTrust and ETSI, and encourages a harmonized implementation of WebTrust and ETSI audit criteria and auditing procedures worldwide. This document outlines the security and authentication practices that CAs in the industry should be measured against to determine their qualifications and to justify their continued role in ensuring online trust.

OTA wishes to acknowledge input from the OTA Leadership and Advisory Council, with special thanks to Rick Andrews, Paul Meijer, and Jeannie Warner at Symantec, Ben Wilson at DigiCert, John Scarrow at Microsoft, Joe St. Sauver at University of Oregon, Adam Langley at Google, Ryan Hurst at GlobalSign, Brad Hill at PayPal, and Craig Spiezle of the OTA for their contributions and collaboration in this paper.

Updates of this report will be posted at https://otalliance.org/capractices.html. To submit comments, please email staff @ otalliance dot org.

[6] See ANNEX A to ITU Recommendation X.509, November 1988, and later versions of X.509 defining "certificate policy" as "a named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements."

[7] https://www.cabforum.org/documents.html

CA Response to Security Breaches

A few highly publicized CA security breaches in 2011 along with escalating level of organized cybercrime and state-sponsored cyber terrorism have sparked a debate about the future viability of whether SSL certificate technology and the entire CA industry that distributes it are adequate in today’s threat environment. Several CAs have demonstrated, though leadership and recognizing the long-term risk of maintaining the status quo, that there is a need to improve CA security practices. These CAs have come together to take critical steps toward an ever-improving security infrastructure that preserves global commerce and the free exchange of ideas without compromising user expectations of privacy and security. The aforementioned CA/B Forum Baseline Requirements and Network Security Requirements and efforts of the OTA SSL working group demonstrate an ongoing commitment to the SSL chain of trust.

While technical enhancements can and are being made, the most significant challenge facing the PKI ecosystem over the last couple of years is not a technological flaw or limitation, but rather the way it is being implemented and the practices around it. Not unlike the challenges in the interactive advertising and email industry, many of these issues can be rectified by operational discipline and adoption of best practices.

To address this problem, members of the CA/B Forum took steps towards a more robust, sustainable PKI ecosystem in December 2011 with the Baseline Requirements, which are applicable to CAs that issue organization-vetted and domain-validated SSL/TLS digital certificates natively trusted in browser software because their root certificate is embedded as a trust anchor in such software.

These Baseline Requirements and Network Security Requirements are just the beginning. The CA/Browser Forum and other groups will continue to improve the guidelines for better CA security practices for the entire industry, not just those issuing SSL/TLS certificates. As the important work of the CA/B Forum continues, leading global CAs are working in supportive fashion to help educate everyone with a stake in the internet on the importance and value of distinguishing security practices.

Publicly Trusted CAs Provide Valuable Trust Services for the Internet

A CA is an organization that issues digital certificates to individuals and organizations. CAs are responsible for ensuring that each certificate is strongly bound to the identity of the person or entity holding the public/private key pair that is used with the SSL/TLS protocol. Thus, it is very important that commercial CAs not only authenticate the identity of each certificate holder, but also prevent the impersonation of legitimate web sites by attackers who try to break online trust by intercepting secure communications with fraudulently obtained certificates. Thus, it is very important that CAs not only authenticate the identity of each web site that is issued a certificate, but also implement both pre- and post-issuance checks to prevent the impersonation of legitimate websites.

For nearly two decades, CAs have acted as trust brokers between entities on the Internet and end users, and it is estimated that more than 4.5 million sites are using website certificates issued by a CA.

The core or "kernel" of trust in the PKI system rests on the assumption that a publicly trusted CA is firmly committed to security that is beyond reproach. However, there has been a lack of binding requirements, or uniform standards, to govern the implementation of rigorous security and identity verification practices to be followed by CAs that issue SSL certificates and associated trust services.

CA Security Breaches Threaten to Undermine Online Trust

Though security is integral to the core business function of CAs, they nonetheless face the same (or even higher) security challenges when compared to those faced by other organizations. Particularly, recent events have shown CAs to be targets of hacktivists, cybercriminals and even geopolitical states.

Amid rising challenges, the number of publicly trusted CAs has grown from a handful several years ago to 65 or so holders of trusted root certificates today, along with hundreds of intermediate certificates in existence worldwide. About 99 percent of all SSL certificates issued originate from the world's seven largest providers, though smaller CAs also exist. CAs and browsers utilize third-party audits - such as WebTrust and ETSI - to gauge the CA's compliance with industry standards and these are generally effective in relation to the major providers. Groups like the CA Browser Forum are beginning to work on improved CA security requirements and audit criteria, but historically there has been no over-arching system or authority to govern how CAs operate, or that verifies that they can truly provide equal levels of assurance about their security and authentication practices. While newer efforts include periodic vulnerability scanning, penetration testing[8], and better browser oversight of Root CAs that are publicly trusted (see e.g. Mozilla's "Maintaining Confidence in Root Certificates"[9]), there continue to be a number of CA practices that have been identified as problematic, and some of these problems began coming to light in 2011 after several incidents involving CAs made the news:

- In March 2011, an attack originating in Iran compromised the access credentials of a Comodo reseller in Italy and used that partner's credentials / access privileges to generate fraudulent certificates for Live, Skype, Yahoo, Gmail, and other well-known sites.
- In May, it was reported that another Comodo partner –ComodoBR-- was hacked in Brazil.
- In July, DigiNotar, a Dutch CA, was fully compromised when the same Iranian attacker obtained fraudulent certificates for several dozen Internet domains, including those noted above, and the Dutch government and major Web browser vendors had to remove all trust from DigiNotar's CAs. DigiNotar immediately filed bankruptcy and the Dutch government had to take over operations.

[8] https://www.cabforum.org/Network_Security_Controls_V1.pdf

[9] https://wiki.mozilla.org/CA:MaintenanceAndEnforcement

- In December 2011, TurkTrust reported that in August 2011 it had mistakenly issued two intermediate certificates to organizations that should have received standard SSL certificates. The *.EGO.GOV.TR certificate was then used to issue an unauthorized digital certificate for *.google.com to a party other than Google.[10]

Fortunately, many CAs have stepped up to evolving cyber security threats and are improving the tools and processes used so that they remain fully capable of providing the greatest assurance possible that their certificates – and the websites that use such certificates – are genuine and safe for online business. To address this problem, members of the CA/Browser Forum took steps towards a more robust, sustainable PKI ecosystem in December 2011 with the Baseline Requirements, which are applicable to CAs that issue organization-vetted and domain-validated SSL/TLS digital certificates natively trusted in browser software because their root certificate is embedded as a trust anchor in such software. Implementation of these Baseline Requirements is just the beginning, however, and the CA/Browser Forum continues to improve its guidelines for better CA security practices for the entire industry, not just those issuing SSL/TLS certificates. Quality does not come with a low price tag attached – to maintain high standards, overhead costs are a consideration.

How Browsers and CAs Can Build a Stronger Chain of Trust

This white paper attempts to address this undeserved equivalency of trust, sometimes referred to as "the weakest link" in the SSL infrastructure, by suggesting best practices for CAs. Digital certificates are verified using a cryptographic chain of trust, and root CAs act as trust "anchors" for each certificate. Consequently, Web browser developers must be able to trust that CAs will do the following:

- Verify the identity of the requester and that the requester is lawfully entitled to be issued a certificate with the identifying information contained therein.
- Ensure that there is no way to issue a certificate without a permanent record regarding identifying information of the requester.
- Keep unalterable logs of all certificates they have signed.
- Audit, review, and/or examine those logs frequently for evidence of unauthorized issuance.
- Proactively communicate security events and certificate revocations.
- Protect their infrastructure to prevent intrusion or fraudulent certificate issuance.

When browser developers feel confident that a CA will adhere to these practices and procedures, they include that CA's root certificate[11] in the browser's Root CA store. All certificates in a browser's root store are trusted equally.

[10] It is alleged that a deep-packet inspection device on the client's site automatically generated this false certificate. This was the only certificate detected because Google hard-codes its own public keys into Chrome. This technique is called "pinning" or certificate pinning. See http://www.imperialviolet.org/2011/05/04/pinning.html.

[11] A root certificate is a self-signed CA Certificate issued by a top-level Certification Authority to itself

Raising the Bar to Ensure Equal Assurance and Trust

While businesses, banks and commerce sites have the choice of purchasing an SSL certificate from one of over 65 CAs, not all CAs should be granted equal trust without providing equal assurance. CAs and browsers utilize third-party audits, as those mentioned above, as one way of measuring good practices, but these kinds of audits - even with improvements recommended by the CA/Browser Forum,- are not adequate to determine how CAs should best operate.

This is one of the reasons why the OTA has created this set of CA Best Practices. The OTA hopes to raise awareness about this issue with a dialogue among industry stakeholders and to provide relying parties additional criteria to consider when selecting or renewing their certificates. Within 12 months OTA plans to begin tracking adoption and scoring of CAs to both recognize those CAs who have adopted best practices and to provide information to aid businesses in their CA selection.

Frameworks for assessing the adequacy and effectiveness of the controls employed by CAs have existed in various forms since at least the year 2000. However, historically there has been a lack of binding requirements or uniform standards to govern the implementation of rigorous security and identity verification practices followed by CAs that issue SSL certificates and associated trust services.

The events of 2011 and since are proof-positive that all CAs do not follow the same strict security practices and not all CAs provide equally high levels of assurance. At the same time, all CAs are afforded equal trust once they have been added to a browser’s trust-anchor list. The OTA believes we must begin to address this fundamental problem of equal trust without equal assurance seriously in order to ensure the future of online trust in the PKI ecosystem. OTA hopes to raise awareness about this issue with a dialogue among industry stakeholders by highlighting some best practices currently being followed by leading CAs.

There should also be a thorough path for a new CA to become trusted, via oversight and review by a third party auditor who reviews the CA’s practices and measures them against documented Best Practices before publishing their findings for Browsers other interested parties to review and assess. Additional to this, a new CA should undergo a security design review and penetration tests on all internet-facing devices and connections.

Not Everyone Can Be a Good CA

Because we do not expect these bad actors targeting CAs to slow down or go away, it is critical that CAs develop business strategies and top-down security policies that address the following key needs:

- Diligent investment in and upkeep of a secure application and network infrastructure
- Rigorous and consistent authentication and identity validation processes
- Comprehensive auditing and responsible breach notification practices

A focus on operational planning around these and other strategic objectives will help CAs to make security-conscious decisions and ensure the long-term sustainability of this trust model. Browser developers also have an important part to play by being more selective about trusting CA roots, implementing stricter online revocation controls, and insisting that CAs maintain compliance with the CA/Browser Forum Baseline Requirements and other standards that may come out in the future. Serious efforts are underway to enhance current standards, including improvements to communication methods for certificate validity and certificate revocation, as well as certificate issuance and audit logging, and browser support will be critical.

CA/Browser Forum's Baseline and Network Security Requirements – A Start

As part of an ongoing effort dating back many years to address and enhance CA security practices, the CA/Browser Forum adopted the Baseline Requirements, effective July 1, 2012. While adoption of the Baseline Requirements was proceeding, the CA/Browser Forum also drafted and adopted the Network Security Requirements with an effective date of January 1, 2013. These two initiatives for all certificates that are natively trusted in browser software will continue to improve and evolve, and the OTA has found them quite useful, among other resources, in developing criteria for gauging the trustworthiness of publicly trusted CAs. The following items constitute the areas of trust that a CA must properly engage: Maintaining a secure IT infrastructure, enforcing rigorous Identify Validation practices, and demonstrating compliance with policies and regulations.

But these requirements focus on the front end, of preventing incidents. As a logical follow up, all CAs must have incident response plans[12] that are tested and maintained to ensure that public trust is maintained in event of any security-related incidents. Business continuity management is a clear indication of resilience for a CA, but in the instance of online trust the need for transparency in the case of an incident is critical.

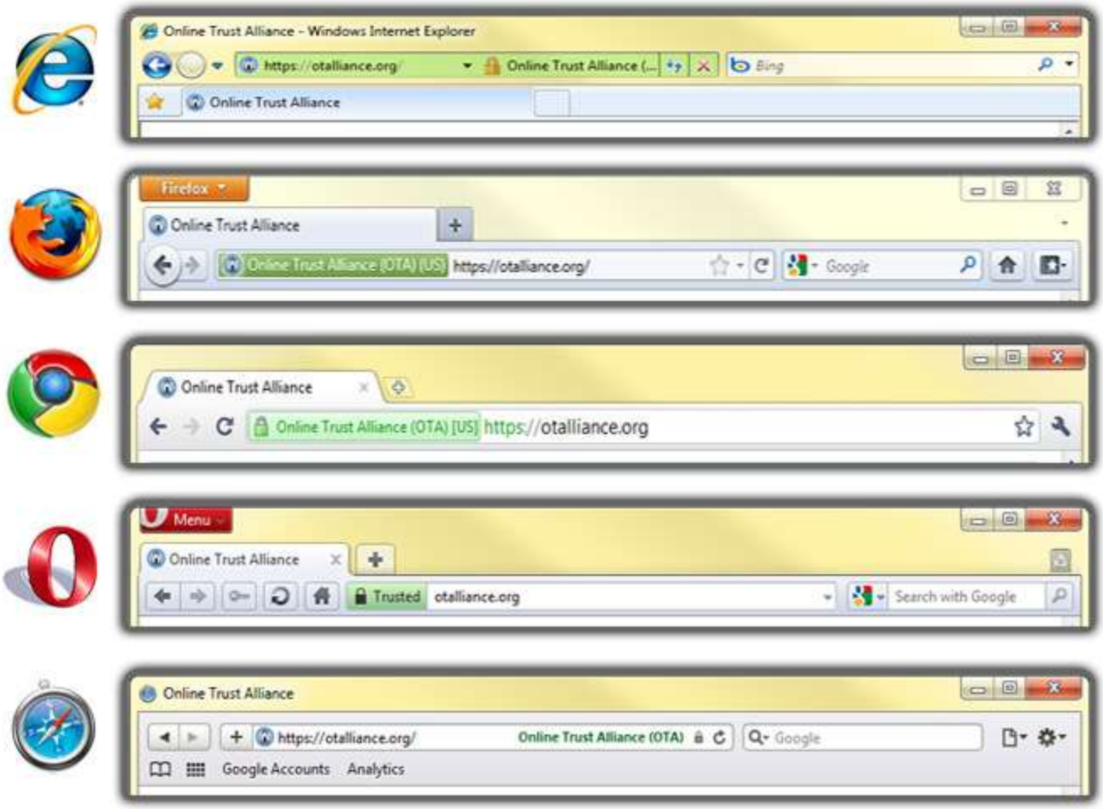
Business continuity plans are required as part of ISO 27001 and elaborated in the new proposed ISO 22301. ISO 22301:2012 "specifies requirements to plan, establish, implement, operate, monitor, review, maintain and continually improve a documented management system to protect against, reduce the likelihood of occurrence, prepare for, respond to, and recover from disruptive incidents when they arise."[13]

Another area that can be improved is clarity in public documentation. Many Certification Practice Statements (CPSs) are either vague or confusing. They also end up accumulating amendments and modifications over time. Some CAs issue amendments that apply to a base CPS, rather than the better practice of reissuing a CPS that incorporates all of the changes to-date. The OTA recommends that CAs work to improve the quality of their CPSs, and that amended CPSs be issued in full, with changes flagged for ease of reference.

[12] https://otalliance.org/resources/Incident.html

[13] http://www.iso.org/iso/catalogue_detail?csnumber=50038

Browsers can help here, too, by implementing the W3C's guidance on distinguishing Augmented Assurance Certificates[14] and by correctly processing other information and indications of trust to the end user. Currently, there are no visual manifestations or indications of difference between a Domain Validated (DV) certificate and an Organization Validated (OV) certificate. Only Extended Validation (EV) certificates have an indication by browsers – colloquially referred to as "the Green Bar" indicator – as illustrated below for the top web browsers. More details on the recommended uses and processing of this certificate-type metadata and certificate validity information will be found in future papers on Best Practices in Implementation.



[14] http://www.w3.org/TR/wsc-ui/

Maintaining a Secure IT Infrastructure

CAs must invest in security infrastructure, including up-to-date malware-protection systems, conducting regular third-party audits, running vulnerability assessments to ensure no holes exist that can be exploited, implementing multiple layers of security, and continuously monitoring the environment so that breaches can be detected as quickly as possible and stopped. The following are primary design objectives that CAs should incorporate:

Segregation of security zones – CA certificate infrastructures should be completely isolated from normal business operations and segmented into certificate systems into separate networks based on the functions that those systems perform. Root CA Systems should be maintained in a High Security Zone, either in an offline state or air-gapped from all other networks.

Network defense in depth – Security design should emphasize multiple, overlapping, and mutually supportive defensive systems to guard against single-point failures in any specific technology or protection method. This should include the deployment of properly configured and regularly updated firewalls, as well as gateway antivirus, intrusion detection, intrusion protection systems, and Web security gateway solutions throughout the network. (No system should be left in its default configuration unless that configuration is chosen after careful review.)

In order to support certificate validation over the internet, the CRL/OCSP infrastructure should be designed to be high performing, robust, and redundant wherever possible. When the CRL/OCSP services becomes unavailable, services relying on SSL can be dramatically impacted[15], either stalling or hanging until timeout value is reached.

Browser leaders understand and support this added attention and analysis of the CA networks: "Microsoft believes strongly that the security of the CA infrastructure is extremely important. To that end we support further work on audit controls, and developing new network and operational security measures to ensure users of the integrity of the CA system," Says John Scarrow, General Manager at Microsoft.

Verification practices – CAs should confirm that applicants either have the right to use, or had control of, the Fully-Qualified Domain Name(s) and IP address(es) listed in the Certificate, and that representatives were authorized by a person having such right or control (e.g. under a Principal-Agent or Licensor-Licensee relationship) to obtain a Certificate containing the Fully-Qualified Domain Name(s) and IP address(es).

CAs should take extra care in verifying the domain where the WHOIS has been cloaked by a proxy or privacy registration, with the WHOIS information verified from multiple perspectives wherever possible. They should require that the proxy/private registration be de-cloaked while processing the certificate request and collect relevant contact information before the certificate is issued. This includes situations where the whole top level domain, such as .RU, is most often cloaked or blinded.

[15] http://blog.cloudflare.com/post-mortem-what-todays-network-outage-looked

CA DNS and Domain Security – DNS record and domain management for the CA itself are critical. Each certificate contains pointers to the certificate's status information. If the CA loses control of its own domain or the routing to its servers, it loses control over its ability to respond appropriately to certificate status requests. The CA must ensure that its DNS and domain management systems are as resilient to attack as its other CA operations. The CA's registrar should also be alert for the CA's domain, and take an equal responsibility for the registration reminders as the CA itself.

Personnel security – Prior to the engagement of any person in the Certificate Management Process, whether an employee, agent, or an independent contractor of the CA, the CA should verify the identity and trustworthiness of such person via background checks. Sample items to review as part of a hiring policy include:

- Statutory debarment or dishonorable discharge
- Evidence of dishonesty in an application or examination process (e.g., falsification of application)
- Drug- or alcohol-related offenses or other felonies

Password policies – Weak passwords are a huge risk, and a good CA will utilize strong password policy across their entire data center / certificate production infrastructure. Passwords should be changed regularly, at least once every 90 days, and users should not be permitted to use their previous 4-5 passwords. Multi-factor authentication is strongly recommended. The SANS Institute has published a good guideline for password construction policy.[16] NIST also provides guidance on electronic authentication.[17]

Physical security – Physical security is often overlooked by typical tech company deployments, but this is not an option for a CA. It is critically important to protecting network, server and storage equipment, as well as the keys themselves. All Network and server equipment should reside in a data center that meets or exceeds the criteria for such data facilities.[18] Ideally, the most sensitive areas of the certificate infrastructure, such as the root private key storage, should be air-gapped as an additional layer of defense to complement logical boundaries. Access to processing facilities should be controlled and limited on an as-needed basis. All key-related activity should take place in an access-controlled area with multi-party controls (see below).

Secure application development – All systems and applications should be developed in a secure, change-controlled environment and follow a secure development process from system architecture design all the way through QA and security testing. The CA should be evaluated on whether it develops and implements applications in accordance with systems development and change management policies.

Breach Readiness Plan – Recognizing the likelihood of a data loss incident or breach, CAs must have a documented incident readiness plan. Such a plan must include 24/7 response to contain, mitigate and to notify affected parties within the SSL supply chain.[19]

[16] http://www.sans.org/security-resources/policies/Password_Policy.pdf

[17] http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf

[18] E.g., Tier 3 of ANSI/TIA-942 --- Telecommunications Infrastructure Standard for Data Centers.

[19] http://otalliance.org/resources/Incident.html

CA Practices	Good Required	Better	Best
CA hires qualified employees who receive background checks and regular training.	✓	✓	✓
CAs' statement of practices (CPS) is kept up to date with annual revisions.	✓	✓	✓
CA has an incident security response plan	✓	✓	✓
CA verifies the identity of certificate applicants by checking independently reliable (e.g. third party) records.		✓	✓
CA carefully follows a quality control program to prevent erroneous certificate issuance.		✓	✓
CA hires auditors who have computer security auditing experience and specialized training.		✓	✓
CA audit reports attest to the CA compliance with CAB Forum, EV Guidelines, and the Baseline Requirements.		✓	✓
Trust anchor root keys are kept off line and protected by multiple security layers and require at least two people to activate.		✓	✓
CA supports both CRL and OCSP, and responds to status queries within seconds.		✓	✓
CA regularly tests its business continuity and disaster recovery plans.	✓	✓	✓
CA regularly reviews computer activity logs, which are also recorded in a separate and reliable logging system.		✓	✓
CA conducts regular vulnerability scans and penetration tests.	✓	✓	✓
CA actively contributes to improvements in the technology and certification practices through its participation in industry organizations like the CA/Browser Forum, the IETF, and others.			✓

Enforcing Rigorous Identify Validation Practices

In addition to securing their critical information assets, CAs must consistently follow rigorous identity validation practices to ensure that the organizations and individuals to whom they issue certificates are genuine and safe to do business with. In accordance with the CA/Browser Forum requirements, CAs should confirm that all applicants currently have the right to use the registered domain name(s) and public IP address(es) listed in their Certificate. CAs should also take care to identify high risk certificate requests, including those purporting to be from the owners of famous trademarks, and conduct additional verification activity using fraud screening and detection techniques, and take any additional precautions that are reasonably necessary to ensure that such requests are properly verified under the CA/Browser Forum requirements. Operationally, domains with famous marks, those in government or military namespaces (e.g. .gov, .mil, etc.), and those found in the Alexa top 500[20] should require a higher level of scrutiny in process and procedure.

Process and Controls for the Protection of CA Keys

CA Keys should be stored on certified cryptographic hardware that ensures the protection of the private key. Use of the CA's Root Key to sign CA certificates should require the participation of at least three individuals and multiple authentication factors for access and use, with audio/video monitoring equipment to record all activities. When a certificate is issued by the Root CA, it should require an individual authorized by the CA (i.e. the CA system operator, system officer, or PKI administrator) to deliberately issue a direct command in order for the Root CA to perform the certificate signing operation.

Review Existing Revocation Technologies for Possible Improvement

Verifying the revocation status of existing certificates is also another critical activity. CAs should maintain a continuous 24x7 ability to accept and respond to revocation requests and related inquiries. This is not easy to accomplish without making a significant investment in a robust and reliable infrastructure and support personnel that can scale to handle millions of requests each day, with geographically distributed redundancy for backup, high availability, and rapid disaster recovery.

In accordance with the Baseline Requirements, CAs must operate and maintain their CRLs and OCSP capabilities with resources sufficient to provide a response time of 10 seconds or less. The CA should consider distributing its OCSP responses and/or advocate the practice of OSCP stapling to customers. In this latter case, the customer configures its servers to check the status of its certificate and "staple" the associated OCSP response for the certificate into its TLS handshake improving the speed and reliability of the TLS session.

[20] http://www.alexa.com/topsites

Demonstrating Compliance with Policies and Regulations

Without properly demonstrating compliance with internal policies and the CA/Browser Forum Requirements, there is no way to determine whether a CA has actually implemented the policies set forth in their Certification Practice Statement (CPS) documents. For this and many other reasons, it is critical that CAs undergo an audit in conformance with WebTrust guidelines, ETSI Technical Standards and Guidance, or another accepted audit scheme at least once each year. CAs are part of a critical infrastructure for many parts of the financial and e-commerce world, and it is the opinion of the OTA that guidelines created for such high-impact infrastructures be considered in the same manner for audit purposes. CAs should conduct internal threat or risk assessments long before their first audit.

The public, CAs, and browsers should expect to see the following as part of a third party’s audit:[21]

Planning Phase*:* The CA reviews certificate policy and audit criteria and engages the auditor/assessor to perform an audit that meets all of necessary audit requirements.

Policy Assessment Phase*:* The auditor/assessor reviews the written Certificate Policy, relative to RFC 3647 and browser requirements, and develops an understanding of the intended Certificate Policy requirements in the context of the business and operational environment.

Certification Practice Statement (CPS) Review Phase*:* The auditor/assessor reviews the suitability of the CA’s design and whether its certification practices satisfy Certificate Policy and browser requirements and generally accepted CA control standards (e.g. CA/Browser Forum requirements).

Operational Effectiveness Verification Phase*:* The auditor/assessor interviews staff, samples and reviews evidence (e.g. certificate requests, collected issuance approvals, and audit logs), and performs tests to determine the operational effectiveness of the certification practices as implemented.

Reporting Phase*:* The auditor/assessor provides a report to the CA’s operational management, and then, according to the procedures of the audit scheme, it is published. Browser root program administrators can then determine if the CA meets all of the necessary requirements.

Here are some of the many items that CAs must allow to be audited in order to ensure proper implementation of security policies and controls:

Key ceremony – It is essential that the key ceremony produces an unbroken evidentiary path demonstrating that every aspect of the certificate-generation process occurred in accordance with methods and procedures that comply with audit standards. You must ensure that sufficient evidentiary material is generated to demonstrate – in any legal proceeding – that proper practices were followed during the ceremony. For this reason, you conduct every key ceremony from a written script. To achieve a high degree of confidence, each ceremony step must be witnessed, documented, and certified.

[21] From Section 4.4 of Appendix 4, ABA PKI Assessment Guidelines (2003) ISBN 1-57073-943-9

Monitoring and alerts – It is vital that CAs monitor their network for intrusions, propagation attempts and other suspicious traffic patterns, and identify attempted connections to known malicious or suspicious hosts.

System and event logging – CAs should record details of the actions taken to process a certificate request and to issue a certificate, including all information generated and documentation received in connection with the certificate request; the time and date; and the personnel involved. The CA should make these records available to its auditor as proof of compliance with applicable requirements.

Vulnerability management – Most software vendors work diligently to patch exploited software vulnerabilities; however, such patches can only be effective if adopted in the field. Like everyone else, CAs need to be wary of deploying standard corporate images containing older versions of browsers, applications, and browser plug-ins that are outdated and insecure. Wherever possible, CAs should automate patch deployments to maintain protection against vulnerabilities across the organization, and work to keep systems up to date with the most recent patch that has been confirmed stable and secure.

Going Beyond the Baseline Requirements

The importance of establishing a common baseline standard for CA practices cannot be overstated. However, baseline requirements do not address all of the issues relevant to the issuance and management of publicly-trusted certificates, and are intended as a starting point of what is an ongoing effort to improve security practices.

The CA should constantly monitor its networks, both online and offline, in search of threats and vulnerabilities to protect its certificate authentication, issuance, management, and CA infrastructure.

The security of a CA's operations and customer support with installing certificates are important services that customers pay for when they buy an SSL certificate. A good CA will be diligent about monitoring its networks and continuously work to ensure that its infrastructure remains secure. The ability to maintain a strong security posture requires strong, effective security policies through an ongoing process that revolves around the following three activities:

Policy governance – Security policies should be planned, managed and supported at the highest level of the organization. They should cover every aspect of digital certificate life cycle and all associated trust services, not just for the CA but also for all partners, affiliates, and subscribers.

Policy design – The application and network infrastructure, along with all business processes, should be designed to meet the security audit requirements in support of the CAs policies. This includes incident management and business recovery policies.

Policy implementation – CAs must be able to demonstrate the implementation of rigorous policies and disciplined operation of the CA through monitoring, logging, and third-party audits.

It is also important that CAs hold their partners and affiliates accountable for adhering to the same standards and audit requirements, as demonstrated by the March 2011 attack that compromised the access credentials of the Comodo partner in Italy.

Governance

The CA/Browser Forum Baseline Requirements (links above) state that all CAs must "Develop, implement, enforce, and annually update a Certificate Policy and/or Certification Practice Statement that describes in detail how the CA implements the latest version of these Requirements," and that CAs must publish the document and commit to comply with it. The CA's decisions about security or authentication cannot be made by a single individual or merely for the expediency of business.

The CA's Certificate Policy and Certification Practices Statement (CPS), which delineates the practices underlying its CA services, should be sufficiently detailed and comprehensive to adequately disclose the CA's main security practices. Too often, as noted on page 9 above, a CA's CPS documents will be vague and lack detail. This makes them very open to interpretation, difficult for comparison, and ineffective for ensuring compliance with security policies.

Also, the CPS should not merely "parrot" Certificate Policy requirements. Granularity and detail are critically important in the context of policy creation. It is one thing to define a policy that states, "The CA must have a disaster recovery system in place" and another thing altogether to define specific operational goals for that system, such as time-to-recovery targets.

Separation of duties is another important principle to follow. Cross-functional operations, where processes are performed by individuals from separate departments who do not report up to the same chain of management, ensure proper PKI design, change control, and implementation.

Similarly, the CA must implement technical and procedural mechanisms that require the participation of multiple trusted individuals to perform sensitive CA cryptographic operations. This can be accomplished with technical constraints, such as split key shares, where more than one person is required to participate in activating the use of a CA private key (i.e. at least two trained and trusted individuals serving in "Trusted Roles" can operate the particular hardware cryptographic module to activate a CA private key stored on the module).

Physical and Logical Security Design

The physical construction of CA Operations Centers should provide a high level of security and availability for services and communications purposes. A tiered approach to the physical environment of the CA operations should be nested like an onion with increasing levels of security. Individuals are granted selective access to tiers on only a "need to know" basis, and the highest tiers should require two or more authorized people to enter or remain. Use of video monitoring and other techniques should be employed throughout the CA Operations Center. The security architecture of the logical CA systems should also isolate sensitive signing servers and certificate databases from business operations. This architecture provides defense in depth, as an intruder must pass through or compromise multiple firewalls and air gaps just to reach the back-end infrastructure.

Implementation and Processes

Implementing a secure design based on robust policies requires a high degree of skill, experience, and discipline. CAs must regularly have their systems tested and audited to ensure ongoing compliance with internal policies and external requirements.

The CA must be audited annually in accordance with the Baseline Requirements, subordinate CAs under the root should be assessed for equal compliance, and CA systems should be continually and actively monitored for any signs of intrusion in accordance with the Network Security Requirements. The Network Security Requirements require that the certificate issuance components of the CA infrastructure be monitored for security compromises or attempted security compromises. In the event of a detected compromise, monitoring systems should notify the appropriate personnel for action by e-mail alert, pager alert, or console monitoring. Logs are generated for routers, firewalls and network machines; database activities and events; transactions; operating systems; access control systems; and mail servers. These logs should be archived and retained in a secure location for a minimum of 12 months. Importantly, all key lifecycle management events, certificate lifecycle management events, and security-related events such as firewall activity and facility visitor entries must be logged and routinely reviewed.

Vulnerability scans and audits must be performed by trained professionals in accordance with the Network Security Requirements in order to ensure that adequate security measures are in place. These scans must be performed both internal and external to the network as required by the CA/Browser Forum. Any findings of sufficient security vulnerability must be remediated in accordance with the Network Security Requirements.

Third-party penetration tests must also be performed at least as often as specified by the Network Security Requirements. A penetration test is a series of exercises performed from outside the system to determine if there are any exploitable openings or vulnerabilities in the network. In particular, it uses the known techniques and attacks of hackers to verify that the network is safe from unauthorized penetration.

Conclusion – A Call to Action

The PKI/CA/SSL ecosystem is the foundation of trust on the Internet. These technologies and protocols are well understood, they are widely adopted, and they are hugely scalable. That success has attracted the attention cyber criminals, politically motivated black-hats, and hackers, and the ecosystem continues to innovate to thwart future forms of attacks. Some of these innovations are known as Certificate Transparency, Certificate Pinning, Hardfail, DANE, Trust of First Use, and Certificate Stapling. These new approaches call for an ecosystem approach to protecting the PKI/CA/SSL ecosystem, and will involve efforts from the CAs, the Browsers Providers, webserver providers, and others with security product development. Watch for future updates from the OTA on best practices in these areas.

Meanwhile it is imperative that we immediately raise the floor to ensure the entire security of each browser trust store, which provides the current trust model that the Internet relies on every single day. The OTA believes that while no security infrastructure is immune to breaches, CAs must be willing to invest in infrastructure and make a binding commitment to improving security as a first priority. With a set of CA standards in place, approved by the OTA and in the hands of third party auditors, it will be easier for browser developers to review the audit finding lists and establish trusted CAs for better adoption of root and intermediate certificates that promote safer transactions on the internet.

About The Online Trust Alliance (OTA) https://www.otalliance.org/

OTA is an independent non-profit with a mission to develop and advocate best practices and public policies which mitigate emerging privacy, identity and security threats to online services, organizations and consumers, thereby enhancing online trust and confidence. By facilitating an open dialog with industry, business and governmental agencies to work collaboratively, OTA is making progress to address various forms of online abuse, threats and practices that threaten to undermine online trust and increase the demand for regulations.

Material in this publication is for educational and informational purposes only. Neither the publisher, the Online Trust Alliance (OTA), its members nor the authors assume any liability for any errors or omissions nor how this publication or its contents are used or interpreted or for any consequences resulting directly or indirectly from the use of this publication. OTA makes no assertions or endorsements regarding the security or business practices of companies who may choose to adopt such recommendations outlined. For legal or other advice, please consult your attorney or other appropriate professional. The views expressed in this publication do not necessarily reflect the views of OTA member companies or affiliated organizations.

OTA MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT. No part of this publication may be reproduced or distributed in any form or by any means, or stored in a database, web site or retrieval without the written consent of OTA.