Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Decommissioning Certification Authorities

Certification Authorities (CA) based on Public Key Infrastructure (PKI) are in regular use throughout the world. While there are increasing numbers of CA's initiated each month, the time may have come to decommission a "pioneer" CA installed in the early years of commercial PKI, roughly 1995 - 1999. Business, financial, legal or simply technology shelf life may lead to terminating a CA. Terminating a CA is as important an event as its initiation - both require planning physical, logical and human aspects. Security of i...

Copyright SANS Institute
Author Retains Full Rights

AD

Decommissioning Certification Authorities

Claudia N. Lukas

March 10, 2002

Overview

Certification Authorities (CA) based on Public Key Infrastructure (PKI) are in regular use throughout the world. While there are increasing numbers of CA's initiated each month, the time may have come to decommission a "pioneer" CA installed in the early years of commercial PKI, roughly 1995 – 1999. Business, financial, legal or simply technology shelf life may lead to terminating a CA.

Terminating a CA is as important an event as its initiation – both require planning physical, logical and human aspects. Security of information and reputation is at risk. The current and future needs of subscribers and other relying parties require consideration.

In contrast to the many sources available to learn about setting up a CA, there is a shortage of published reports and best practices on decommissioning a Certification Authority. Standards organizations provide a few guidelines for defining CA termination in the CA's Certificate Policy (CP) and Certification Practice Statement (CPS). This paper reviews these guidelines and discusses terminating a Certification Authority.

Public Key Infrastructure and Certification Authorities

Building on advances in cryptography to secure sensitive data, Public Key Infrastructure (PKI) relies on public-key cryptography (asymmetric cryptography) to encrypt and decrypt messages. RSA and Diffie-Hellman are examples of mathematical algorithms developed in the 1970's for encrypting and exchanging public-private key pairs.

The triple goals of message confidentiality, authentication and integrity are accomplished using public-key cryptography. The public keys of the sender and recipient are exchanged. The sender encrypting the message with the recipient's public key allows for *confidentiality* (since only the recipient can decrypt the message with their private key). The sender encrypting the message with their private key ("digitally signing") allows for both *integrity* of the message (using a message digest) and *authentication*. Public key cryptography is based on the assumption that private keys are not revealed to anyone; only public keys are exchanged.

A trusted third party, the Certification Authority, enables the digital signature to be further authenticated by producing a digital certificate containing the identity of the person and their public key. The CA certifies the digital signature according to its published policies and certification practice statements. A record of the signature certification enables *nonrepudiation* of the transaction.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Certificate Revocation
Proper issuing and revocation of certificates determine the reputation of a CA. Depending on the type of certificate being issued, an individual subscriber may be required to confirm their signature using a driver's license or passport. A letter from a company's Board of Directors, signed by their President, may be mandatory and might be verified by a telephone call to that President.

Revocation of certificates is more complex. A CA's Certificate Policy or Certification Practice Statement will usually outline the circumstances for revocation, the entity that can initiate and how revocation is accomplished. The Certificate Revocation List (CRL) has been the basis for handling revocation by the pioneer Certification Authorities. Essentially, a list of revoked certificates is kept and passed down the trust chain to all subordinate CA's. A certificate is authenticated only after determining that it is not on the CRL list.

The value of the CRL list is dependent on several aspects: accuracy and completeness of the list, sharing the list of revoked certificates down the trust chain on a timely and regular basis and the subordinate CA's updating their CRL on a regular basis. The Online Certificate Status Protocol (OCSP) has been developed to address the timeliness of CRL distribution. CA's might be sending lists regularly but even 24 hours lapsed time might invalidate a large dollar financial transaction.

OCSP, an Internet protocol, provides the ability for an application to determine the status (revoked, good or unknown) of a certificate without having to use CRLs. Acceptance of the certificate is suspended until the OCSP responder provides the certificate status to the OCSP client. OCSP can also provide a trust verification record listing when and how the authenticity was verified.

Most policies and practices indicate complete revocation of all certificates upon termination of a CA. This is absolutely necessary when a Root CA is terminated but may not be required for terminating an individual subordinate CA. The risks of allowing certificate expiration may be immaterial compared to the cost of updating CRLs or OCSP. As relationships between CA's become more complex, certificate revocation practices are being reviewed.

Creation and Termination of a Certification Authority
Creating a CA requires significant planning, funding, resources and time. Time lines of 6 months to several years for planning, installing, loading keys and initiating certificate issuance are common.

For example, the U.S. Patent Office developed its own PKI system for communications between patent applicants and the Patent Office [AUS]. Their private CA has unique requirements that no other CA can provide. After several years of planning and an implementation budget of approximately $4.5M over 3 years, the U.S. Patent Office was

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

able to reduce the cost of patent handling $60M in addition to managing patent and trademark applications with greater security.

A Certification Authority is valuable to their subscribers and relying parties, providing a service perhaps unavailable from another Certificate Authority. CA's provide certificates for email, web browsing, financial and other business transactions, checking out documentation from a repository, signing software code, server authentication and many other instances where confidentiality, integrity, authentication and nonrepudiation are critical.

The trust model is central to the creation and termination of the CA. "Pioneer" CA's are traditionally isolated and hierarchical (superior-subordinate) in nature. The subordinate CA or subscriber receives its certificate from the superior CA establishing a chain of trust. Generally, hierarchical trust models are privately implemented within an enterprise or trading group. Open (public) communities have fostered new models such as peer-to-peer CA relationships ("mesh PKI") and more recently, Bridge CA allowing connection of different PKI architectures [POL].

Termination considerations and procedures for a CA are dependent on the trust model. As a CA becomes part of a larger organization of CA's, its technical nature increases. This "web of trust" increases the complexity of terminating any portion of the trust model. Although this paper focuses on termination of pioneer CA's using a hierarchical trust chain, many of these issues apply to the termination of inter-related CA's.

Policies and Practices for Termination of a Certification Authority

CA termination is briefly touched upon in most documentation relative to operating a CA. Although the likelihood of CA termination increases over time, discussions and documentation of specific issues and related decisions are not available. Pre-planning for CA termination has not changed very much since 1996.

The American Bar Association Information Security Committee, Electronic Commerce Division, Section of Science & Technology Law, published the seminal "Digital Signature Guidelines" in August 1, 1996, and [ABA] defined the Certification Practice Statement: "a CPS is a statement of the practices which a certification authority employs in issuing certificates."

Chokhani & Ford published the Internet Engineering Task Force (IETF) paper on "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practice Statement Framework" in March 1999 [CPF]. Its guidelines define, "*Certificate policy* - 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." Additionally, "A more detailed description of the practices followed by a CA in issuing and otherwise managing certificates may be contained in a *certification practice statement (CPS)* published by or referenced by the CA."

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Both of these publications provide guidelines for termination of a CA that would be included in the CA's CP and CPS. [CPF] suggests the inclusion of required procedures for termination of a CA, termination notification and identification of a custodian for the archival records.

[ABA] recommends notifying the subscribers of valid certificates, ensuring minimal disruption to the subscribers and relying parties, and making arrangements for preserving records. Explanatory comments on the guideline indicate revoking all outstanding certificates "when a certification authority stops or curtails operations without adequate provision for an orderly transfer of its business to a reliable successor." Although the subscriber's certificate ceases being operational, archived records will validate that its digital signature was previously used. [ABA] also proposes a "rule of repose" to provide CRLs for a period after the termination.

In 1998, the National Institute of Standards and Technology (NIST) published their CPS for the Root CA of the Key Recovery Demonstration Project [KRD]. It specifies the mandatory revocation of all subordinate CA certificates. The CPS provides detailed CA termination requirements such as the identity of the authority (Project Manager of the Key Recovery Demonstration Project) and mechanism (official letter to the Root CA Registrar) to terminate the Root CA or subordinate CA's. Certified mail with return receipt for termination notification to the subordinate CA's and retention of the Root CA database for a minimum of 1 year is obligatory.

The American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CIVA) established their WebTrust (SM/TM) Program for Certification Authorities in 2000 [WEB]. The objective of the document is to provide "a framework for licensed WebTrust practitioners to assess the adequacy and effectiveness of the controls employed by Certification Authorities (CAs), the importance of which will continue to increase as the need for third-party authentication increases to provide assurance with respect to e-commerce business activities."

In [WEB], the section "Principle 1, the CA Business Practices Disclosure," uses [CPF] guidelines for the assessment 'criteria' and adds 'illustrative disclosures.' The illustrations include termination by the Board of Directors of the CA, compulsory revocation of all certificates, cessation of issuing certificates, one month notice to business units utilizing the services of the CA, archiving the CA records and transferring the records to a specified custodian. [WEB] also "provides uniform standards derived from the draft ANSI X9.79 [PKI Practices and Policy Framework] standard."

The American Bar Association Information Security Committee, Electronic Commerce Division, Section of Science & Technology Law published the "PKI Assessment Guidelines," in June 2001 [PAG]. These guidelines are "to help assess and facilitate interoperable trustworthy public key infrastructures." The concept of transition to another (successor) CA via certificate expiration is identified in this document as an alternative to complete termination of the CA and complete revocation of certificates. [PAG] continues to point out the importance of notifying subscribers and relying entities,

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

minimizing disruption during the CA termination and continuing revocation services. Consistency with applicable laws or contracts and notifying the recipients of CRLs are new concepts added to assessing the termination policies of a PKI.

VeriSign, Inc. further extends termination policies and practices of a CA in their August 2001 CPS [VRS]. Beyond notification, revocation of certificates and developing a termination plan to minimize disruption, [VRS] offers several new practices where applicable. These include continuing subscriber and customer support services, archiving records for a period of 10, 20 or 30 years, depending on the class of certificate, and providing compensation (if necessary) to subscribers with certificates that are unexpired and unrevoked (or alternatively issue replacement certificates by a successor CA). [VRS] provides disposal of the CA's private key (and related hardware tokens) and continues revocation services using CRLs or OCSP.

In February 2002, the Federal Bridge Certification Authority (FBCA) published their approved Certificate Policy for interoperability among Federal Agency PKI domains [BCA]. It follows [CPF] for its CA termination policies and includes advance notification, revocation of the FBCA certificates, archiving data and if possible, providing alternative sources of interoperation. To cut the bridge relationship between the different PKI's, [BCA] states "the Federal PKI Policy Authority shall advise agencies that have entered into MOAs [Memorandums of Agreement] with the Federal PKI Policy Authority that FBCA operation has terminated so they may revoke certificates they have issued to the FBCA." Termination of multi-domain PKI Certification Authorities requires a complex program of interdependent termination plans.

Conclusion

The above survey of policies and practices for termination of a Certification Authority, as published in a CA's Certificate Policy and Certification Practice Statement, covers the period of 1996 – 2002. Although more CA's were established every year during this period, guidelines for their successful termination are relatively similar. The following are recommendations for additional CA termination policies and practices:

- Form an Advisory Board, at initiation of the Certification Authority, with the responsibility of overseeing termination of the CA or termination of relationship with any other CA. The Board would include representation from subscribers, relying parties and related CA's.
- Address the termination of any back-up site used for business resumption.
- Conduct an audit of the CA's auditing records and the CA deconstruction event. Make this audit report available to subscribers, relying parties and related CA's.
- Escrow the CA's public key and its certificate.
- Provide the capability to re-validate any subscriber's digital signature after the CA is terminated.

As CA implementation technology becomes more complex, termination guidelines will need expansion, depth and subtlety. For example, a rogue certificate in a peer-to-peer

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

or bridged CA environment may not show up in CRLs and OCSP no matter how long a time period they are monitored. Risks that the current guidelines do not eliminate or mitigate will become evident as the pioneer CA's are decommissioned.

References

[AUS] Tom Austin, "Case Study: PKI Protects Patents," Information Security Magazine, March 2001.
URL: http://www.infosecuritymag.com/articles/march01/features6_cs.shtml

[POL] William T. Polk and Nelson E. Hastings, National Institute of Standards and Technology (NIST), "Bridge Certification Authorities: Connecting B2B Public Key Infrastructures," undated; web page "Last Modified: Tuesday, February 20, 2002"
URL: http://csrc.nist.gov/pki/rootca/
Embedded document: "Bridge Certification Authorities: Connecting B2B Public Key Infrastructures"

[ABA] American Bar Association Information Security Committee, Electronic Commerce Division, Section of Science & Technology Law, "Digital Signature Guidelines," August 1, 1996.
URL Document access:
ds-mas9w.wpd (557 kb) - WordPerfect
ds-mas9w.zip (119 kb) - "zipped" WordPerfect
ds-ms.doc (716 kb) - Microsoft Word 7
ds-ms.zip (164 kb) - "zipped" Microsoft Word 7

[CPF] S. Chokhani and W. Ford, Internet Engineering Task force (IETF), Request for Comment (RFC) 2527, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practice Statement Framework, March 1999.
URL: http://www.ietf.org/rfc/rfc2527.txt (Note: new PKIX Working Group Internet Draft released January 3, 2002.)

[KRD] National Institute of Standards and Technology (NIST), Key Recovery Demonstration Project, NIST Pilot Root Certification Practice Statement for the Key Recovery Demonstration Project, version1.1, February 23, 1998.
URL: http://csrc.nist.gov/krdp/CPS-2.doc

[WEB] AICPA/CICA WebTrust(SM/TM) Program for Certification Authorities, August 25, 2000.
URL: http://ftp.webtrust.org/webtrust_public/certauth_fin.doc

[PAG] American Bar Association Information Security Committee, Electronic Commerce Division, Section of Science & Technology Law, "PKI Assessment Guidelines (PAG) v0.30," June 18, 2001.
Homepage URL: http://www.abanet.org/scitech/ec/isc/

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

URL Document access: ***PKI Assessment Guidelines* ("PAG") - Public Draft for Comment v0.30**
http://www.abanet.org/scitech/ec/isc/pag/pag.html

[VRS] VeriSign Certification Practice Statement Version 2.0, effective date August 31, 2001.
URL: VeriSign's Certification Practice Statement (CPS)
http://www.verisign.com/repository/CPS/
Current CPS Version URL: Version 2.0 - Adobe Acrobat (PDF) Version - August 31, 2001; Version 2.0 - Microsoft Word Version - August 31, 2001

[BCA] Federal Bridge Certification Authority (FBCA), The Federal PKI Policy Authority approved the X.509 Certificate Policy for the FBCA dated February 11, 2002.
Homepage URL: http://www.cio.gov/fbca/lib/index.htm
Certificate Policy document URL: Adobe® document; Microsoft® Word document

© SANS Institute 2002, Author retains full rights.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 25th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced