

OPEN-SOURCE

PKI mit OSS

Obschon sich Zertifikate mit einem Tool wie OpenSSL einfach generieren lassen, erfordert der firmenweite Einsatz von Client- und Server-Zertifikaten umfangreichere sicherheitstechnische und organisatorische Massnahmen. Erst eine robuste Public-Key-Infrastruktur (PKI) bietet sicheres Schlüsselmanagement, Schutz der Certificate Authority (CA) und Authentisierung von Antragstellern. Darüber hinaus definiert sie Richtlinien und Prozeduren für die Ausstellung, Registrierung, Verteilung und den Widerruf von Zertifikaten, für Benachrichtigungen beim Ablauf von Zertifikaten und für den Backup von CA-Schlüsseln. Die PKI soll ausserdem benutzerfreundlich, sicher und erweiterbar sein und sich nahtlos in die existierenden Betriebsprozesse und Administrationsrollen einfügen.

Die sicherheitstechnischen Bereiche werden von den meisten kommerziellen PKI-Produkten gut abgedeckt. Die Herausforderungen beim Auf-

bau einer PKI liegen denn auch weniger im technischen als im organisatorischen Bereich, wie etwa bei der Integration firmenspezifischer PKI-Richtlinien und -Prozesse in existierende IT-Umgebungen. Hier zeigt sich die besondere Stärke von Open-Source-Software (OSS): auf einer sauberen Projektbasis, mit erfahrenen Projektteams und Source-Code-Zugriff können sowohl technische wie organisatorische Anforderungen schnell und flexibel umgesetzt werden. Allerdings muss der Kunde bereit sein, die OSS-Lizenzbedingungen zu akzeptieren – insbesondere die Rückgabe von Weiterentwicklungen in die «Community».

Bei einem grösseren Kundenprojekt zur Realisierung einer PKI für Maschinen-Zertifikate blieben nach einer ersten Evaluation drei OSS-Projekte mit ausreichendem Reifegrad übrig: OpenCA (www.openca.org) basierend auf OpenSSL (www.openssl.org) und in Perl implementiert, Mozilla-PKI (www.mozilla.org) und die EJBCA (ejbca.sourceforge.net).

Als J2EE-Applikation in Java realisiert, bot die EJBCA die flexibelste Basis. Es fehlte aber eine Möglichkeit, die sicherheitskritische CA gut vom Netzwerk isolieren zu können: Nicht nur zum Schutz der privaten Schlüssel, deren Speicherung in einem Hardware-Security-Modul (HSM) zum Teil bereits implementiert war, sondern auch, damit keine unbefugten Signatur-Operationen ausgeführt werden können. Die Lösung lag in einer Verteilung der Software auf zwei Rechner mit je einem J2EE-Container mit Datenbank und angepasster EJBCA. Konfigurativ entstand so eine Online Registration Authority (RA) mit Web-Interfaces, LDAP-Publishing und E-Mail-Benachrichtigung und eine Offline CA mit Zertifikatsprofilen und auf HSM gelagerten CA-Schlüsseln. Ein eigener Polling-Prozess auf dem CA-Rechner erkundigt sich bei der RA periodisch nach neuen Zertifikatsanträgen. Auf dem CA-Rechner laufen somit keine Netzwerk-Services mit potenziellen Sicherheitslücken. Der EJBCA-Code selbst musste auch

erweitert werden. Die Registrierungsprozedur sollte beispielsweise mit einer zusätzlichen Bestätigung ausgestattet und Zertifikatsattribute direkt aus einem LDAP-Verzeichnis gelesen werden können. Durch den Zugriff auf den Source Code und dessen modulare Struktur war es ein Leichtes, diese Kundenanforderungen schnell umzusetzen.

Punkto Sicherheit stehen die erwähnten OSS-Projekte einer kommerziellen PKI in nichts nach – sofern die Umsetzung der Prozesse im gegebenen Umfeld sauber gelöst wird. Die OSS-PKI auf EJBCA-Basis bewährt sich zusammen mit einem zentralen Zertifikatsmanagementsystem beim Kunden im zweiten Jahr im produktiven Grosseinsatz. ■



Der Autor
Philipp Färber ist Senior Security Engineer bei der Adnovum Informatik AG. www.adnovum.ch

LEXIKON

DEEP WEB

Als Deep Web (auch Hidden Web, Invisible Web) wird der Teil des Internet bezeichnet, der bei einer Recherche über normale Suchmaschinen nicht auffindbar ist. Im Gegensatz zum Deep Web werden die über Suchmaschinen zugänglichen Webseiten Visible Web oder Surface Web genannt. Das Deep Web besteht im Wesentlichen aus themenspezifischen Datenbanken und Webseiten, die erst auf Anfrage dynamisch aus Datenbanken generiert werden. Grob kann das Deep Web unterschieden werden in Inhalte, die nicht frei zugänglich sind und sol-

che, die nicht indiziert werden. Schätzungen für die Grösse des Deep Web belaufen sich auf ein Vielfaches des direkt zugänglichen Webs. Da Suchmaschinen ständig weiterentwickelt werden, können Webseiten, die gestern noch zum Deep Web gehörten, heute schon Teil des Visible Web sein. *mk*

Info: Die 8. Auflage des Computerworld-Lexikons – 650 gesammelte Beiträge seit Bestehen der Rubrik – ist im Buchhandel oder auf www.computerworld.ch/lexikon erhältlich.

Preis für Abonnenten Fr. 22.– für Nicht-Abonnenten Fr. 28.– (inkl. MwSt. zzgl. Versandkosten)

ANZEIGE

Einfach Spitze – SyncMaster 204Ts

Mit seinem Edeldesign offenbart sich der SyncMaster 204Ts auf den ersten Blick als made by SAMSUNG. Und steht nur auf den ersten – hinter dem formstschönen Aussehen verbirgt sich 20 Zoll gepaart mit Spitzenwerten.

SIEDICO-IT AG – SAMSUNG Generalvertretung IT Produkte
Tel. 041 798 82 82, www.samsung.ch