Audit der DFN-PKI

Im vergangenen Jahr hat die DFN-PKI einen weiteren großen Schritt nach vorne gemacht: Die Zertifizierungsdienste der DFN-PKI im Sicherheitsniveau „Global“ wurden nach einem umfangreichen Auditprozess erfolgreich gemäß dem ETSI-Standard TS 102 042 zertifiziert. Hierdurch kann das hohe Sicherheitsniveau der DFN-PKI auch Dritten gegenüber nachvollziehbar dargestellt und so die Browserverankerung der ausgestellten Zertifikate für die Zukunft sichergestellt werden.

Text: **Jürgen Brauckmann** (DFN-CERT GmbH), **Dr. Ralf Gröper** (DFN-Verein)

Foto: © RioPatuca Images - Fotolia.com

Hintergrund

Digitale Zertifikate aus der DFN-PKI sind an vielen Einrichtungen im DFN nicht mehr wegzudenken. Von der Absicherung von Webservern per HTTPS über die Signatur und Verschlüsselung von E-Mails per S/MIME bis zu chipkartenbasierten Authentifizierungsmechanismen für Mitarbeiter und Studierende spielen Zertifikate eine entscheidende Rolle. Hierfür wurde der Dienst über viele Jahre entwickelt und immer wieder veränderten Gegebenheiten angepasst.

Entwicklung

Die DFN-PKI begann mit dem 1996 gestarteten Projekt „PCA im DFN – Aufbau einer Policy Certification Authority für das Deutsche Forschungsnetz“ an der Universität Hamburg. Im Projekt wurde zunächst davon ausgegangen, dass praktisch alle Einrichtungen im DFN ihre Zertifizierungsstellen selbst betreiben würden. Daher lag der Schwerpunkt der Arbeit auf der Ausstellung von CA-Zertifikaten und der Bereitstellung von Unterlagen zum Aufbau einer eigenen CA, wie z.B. dem DFN-PCA Handbuch „Aufbau und Betrieb einer Zertifizierungsinstanz“. Die ersten Policy-Dokumente wurden 1997 fertiggestellt, und regeln hauptsächlich das Ausstellen von CA-Zertifikaten und die Anforderungen an von einer Einrichtung selbst betriebene CA. Die Ausstellung von Zertifikaten für Anwender, die noch keine eigene CA betreiben, war aber ebenfalls schon vorgesehen.

Nachdem sich im Laufe der Zeit herausstellte, wie groß der technische und organisatorische Aufwand zum Betrieb einer eigenen Zertifizierungsstelle in der Praxis wirklich ist, stellte der DFN-Verein dann ab 2005 eine Erweiterung des Konzepts vor: Mit der neuen Zertifizierungsrichtlinie vom Februar 2005 konnten in der DFN-PKI die Aufgaben der Registrierungs- und der Zertifizierungsstelle von unterschiedlichen Parteien wahrgenommen werden. Dadurch konnten die Einrichtungen im DFN die technisch komplexen und personalintensiven Aufgaben eines CA-Betriebs an die DFN-PCA abgeben und nur die Aufgaben selbst wahrnehmen, die sinnvollerweise bei ihnen verbleiben sollten, wie z.B. die Identifizierung von Zertifikatinhabern. Mit diesem neuen Konzept konnte der Aufwand zur Nutzung der DFN-PKI deutlich gesenkt werden, so dass die Zahl der Teilnehmer und der ausgestellten Zertifikate deutlich stieg.

Root-Integration

Ein weiterer Grund für den Erfolg der DFN-PKI ist die Browserverankerung der ausgestellten Zertifikate durch die Root-Integration. Nur so können Betriebssysteme und Webbrowser automatisch die Vertrauenswürdigkeit der Zertifikate überprüfen. Andernfalls würden Warnmeldungen die Nutzer verunsichern und das einfache „Wegklicken“ dieser Warnungen das Vertrauensniveau unterlaufen.

Die Root-Integration des Sicherheitsniveaus „Global“ der DFN-PKI wurde 2007 durch eine Verkettung mit der „Deutsche Telekom Root CA 2“ umgesetzt. Hierdurch benötigt der DFN keine eigene „Root im Browser“, sondern erbt diese Eigenschaft durch die bereits browserverankerte Telekom CA.

Struktur der DFN-PKI im Sicherheitsniveau Global

Die Browserverankerung der DFN-PKI erfolgt über ein Wurzelzertifikat der T-Systems (Deutsche Telekom Root CA 2), von dem ein Sub-CA-Zertifikat für unsere PCA (DFN-Verein PCA Global – G01) ausgestellt wurde. Die Struktur ist in Abbildung 1 dargestellt. Von der PCA sind dann die einzelnen CAs für die teilnehmenden Einrichtungen ausgestellt – derzeit sind dies knapp 350. Die eigentlichen End-Entity-Zertifikate, also z.B. Server- und Nutzerzertifikate, werden dann schließlich von diesen CAs ausgestellt.

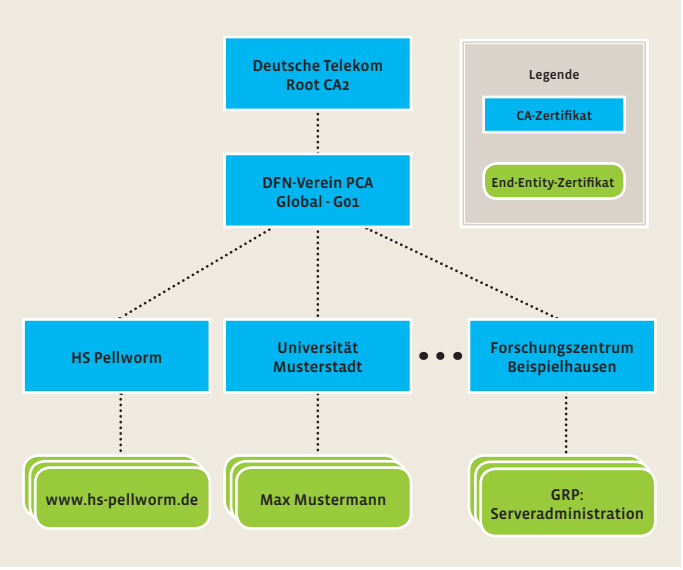

Abb. 1: Struktur der DFN-PKI „Global“

Neue Anforderungen an browserverankerte CAs

Angriffe auf Zertifizierungsstellen

War sichere Kommunikation Anfang der neunziger Jahre noch ein Hobby von begeisterten Informatikern, so ist die verschlüsselte und authentische Übermittlung von Daten inzwischen Grundvoraussetzung für praktisch alle ernstzunehmenden Anwendungen. Daher stehen SSL, X.509-Zertifikate und CAs als System zur Kommunikationssicherung seit einigen Jahren verstärkt im Blickpunkt, z.B. durch Vorträge auf der Blackhat-Konferenz wie „New Tricks for Defeating SSL in Practice“ von Moxie Marlinspike. Es lassen sich drei Themenbereiche unterscheiden, die besonderes öffentliches Interesse finden:

- Fehler in den zugrundeliegenden (kryptographischen) Protokollen

- Lücken in Anwendungssoftware
- Sicherheitslücken bei CAs

In allen drei Bereichen gab es spektakuläre Veröffentlichungen, z.B. die sogenannte BEAST Attacke im Herbst 2011, die mit einem Angriff auf die kryptographischen Grundfunktionen von TLS 1.0 die Entschlüsselung von Teilen von verschlüsseltem Netzwerk-Traffic ermöglicht. Diese kryptographischen Angriffe betreffen aber nicht die zugrundeliegende RSA-Verschlüsselung und so gab es jeweils schnelle Abhilfe durch entsprechende Updates für die beteiligte Software.

Besonders viel Aufsehen haben aber einige verheerende Angriffe auf browserverankerte CAs in den Jahren 2011 und 2012 erregt, bei denen nicht autorisierte Zertifikate ausgestellt wurden, die dann auch zum Abhören vermeintlich sicher verschlüsselter Verbindungen eingesetzt wurden. Im Nachgang dieser Angriffe stellte sich heraus, dass teilweise haarsträubende organisatorische und technische Mängel bei den betroffenen CAs diese Angriffe ermöglichten.

So wurde am 17. März 2011 eine externe Registrierungsstelle von Comodo kompromittiert und unautorisierte Zertifikate für u.a. login.live.com und mail.google.com ausgestellt. Durch eine schnelle Reaktion von Comodo wurden die Zertifikate in Zusammenarbeit mit den Browserherstellern innerhalb weniger Stunden gesperrt.

Im Juni 2011 musste mit StartSSL eine weitere CA für mehrere Tage ihren Betrieb einstellen, ohne dass die betreffende Firma die Ursache der Betriebseinstellung kommunizierte.

Im August 2011 wurde dann bekannt, dass die niederländische CA DigiNotar für mehrere Wochen kompromittiert war, und mehrere hundert unautorisierte Zertifikate, u.a. wieder für google.com, ausgestellt wurden. DigiNotar stellte nicht nur normale SSL-Zertifikate aus, sondern war auch eine Zertifizierungsstelle für qualifizierte Zertifikate für eGovernment-Services in den Niederlanden. Der Einbruch scheint durch ein veraltetes Content Management System ermöglicht worden zu sein. Die erbeuteten Zertifikate von DigiNotar wurden nachweislich für Man-in-the-middle-Angriffe auf Internet-Nutzer im Iran verwendet, um deren E-Mail-Kommunikation über Google Mail abzuhören. DigiNotar wurde als vertrauenswürdige CA aus allen Webbrowsern per Software-Update entfernt und ging wenig später in die Insolvenz. Für all diese Angriffe gibt es sogar eine Art Bekennerschreiben

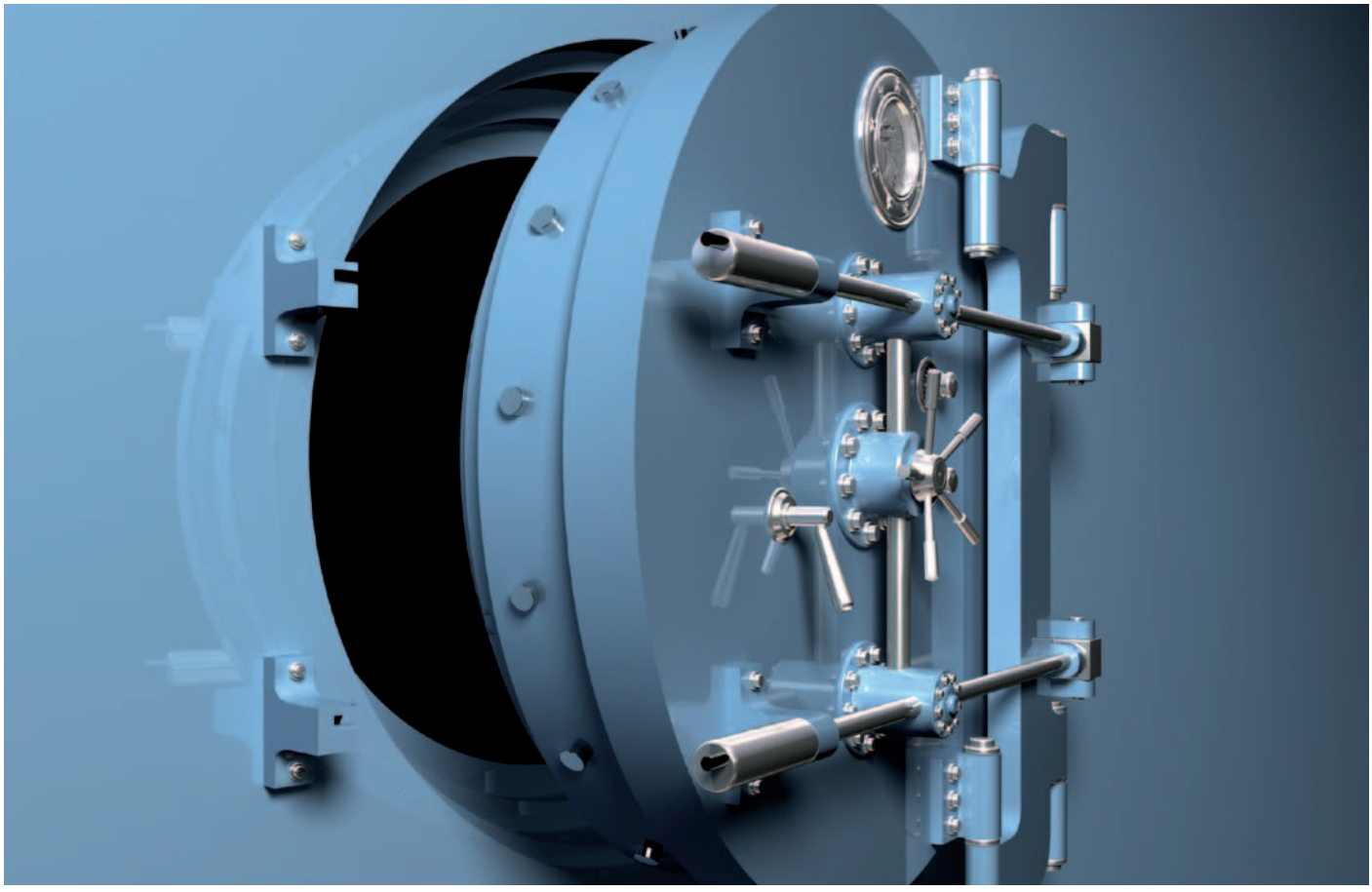

Foto: © PaulFleet - iStockphoto.de

auf pastebin.com. Dort wurde auch behauptet, dass eine weitere CA namens GlobalSign komplett gehackt wurde. Hier stellte sich aber heraus, dass „lediglich“ der Webauftritt, nicht aber die eigentliche CA-Infrastruktur kompromittiert wurde.

Organisatorische Unzulänglichkeiten
Nach den gezielten Angriffen wurden weitere Vorfälle bekannt, die ihre direkte Ursache in organisatorischen Unzulänglichkeiten hatten: Anfang November 2011 musste eine malaysische CA zugeben, dass sie mehrere Zertifikate mit zu schwachen Schlüsseln (512 Bit RSA!) und mit fehlerhaften Zertifikatnutzungen ausstellte. Auch diese CA wurde aus Webbrowsern entfernt.

Ende Januar 2012 wurde bekannt, dass eine im Browser verankerte CA namens TrustWave mindestens ein Zertifikat verkauft hat, mit dem in Produkten zur Data Loss Prevention ein Man-in-the-middle-Angriff auf Nutzer ermöglicht wurde.

Im Dezember 2012 entdeckte das Security Team von Google ein Zertifikat, das von der CA Turktrust ausgestellt wurde, und mit dem ein Man-in-the-middle-Angriff möglich gewesen wäre. Es stellte sich heraus, dass aufgrund eines Konfigurationsfehlers in der CA ein eigentlich für Webserver gedachtes Zertifikat auch als Sub-CA-Zertifikat nutzbar war und anscheinend versehentlich in einer SSL Inspection Appliance eingesetzt wurde.

Turktrust und TrustWave konnten darlegen, dass es sich um einmalige Vorfälle handelte, und es wurde vermutlich auch niemand geschädigt. Daher behielten beide CAs ihre Browser-Verankerung.

Reaktion der Betriebssystem- und Browserhersteller
Die beschriebenen Vorfälle fanden ein großes öffentliches Echo. Auch abseits der Fachpresse erschienen Berichte über das Thema und brachten es so in den Blickpunkt einer breiten Öffentlichkeit. Als Reaktion auf die Angriffe und Unzulänglichkeiten verschärften die Betriebssystem- und Browserhersteller die Anforderungen ihrer jeweiligen Root-CA-Programme. Die meisten Hersteller haben dabei zum einen ihre eigenen Regeln verändert und der neuen Bedrohungslage angepasst, und zum anderen die „Baseline Requirements“ des CA/Browser-Forums (siehe Kasten) als verbindlich vorgeschrieben.

Die T-Systems als Betreiber der Root-CA der DFN-PKI muss diese Anforderungen an ihre Sub-CAs und damit auch an den DFN-Verein weiterreichen.

Zwei Änderungen betreffen die DFN-PKI im Besonderen: Erstens mussten früher Sub-CAs unterhalb von im Browser verankerten Root-CA nicht nach einem vorgegebenen Standard auditiert werden. Das hat sich jetzt geändert, auch Sub-CAs benötigen nun ein externes Audit durch einen akkreditierten Auditor nach einem vorgegebenen Standard.

Und zweitens müssen die „Baseline Requirements“ eingehalten werden, was kleinere Anpassungen an den Prozessen und der Technik der DFN-PKI zur Folge hatte.

ETSI und Webtrust
In den letzten 15 Jahren haben sich mehrere Verfahren herausgebildet, nach denen der Betrieb eine CA auditiert werden kann. Betriebssystem- und Browserhersteller verlangen immer ein Audit der bei ihnen verankerten CAs nach einem von mehreren gebräuchlichen Standards. Mozilla akzeptiert beispielsweise folgende Standards:

- ETSI TS 101 456 „Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates“
- ETSI TS 102 042 „Policy requirements for certification authorities issuing public key certificate“
- ISO 21188:2006 „Public key infrastructure for financial services – Practices and policy framework“
- WebTrust „Principles and Criteria for Certification Authorities 2.0“
- WebTrust „SSL Baseline Requirements Audit Criteria V1.1“
- WebTrust „Principles and Criteria for Certification Authorities – Extended Validation Audit Criteria 1.4“

Diesen Standards ist gemein, dass es sich um umfangreiche Regelwerke handelt, in denen Leitlinien zum Zertifizierungsbetrieb in abstrakter Form aufgelistet sind. Im Rahmen eines Audits muss dann eine Abbildung zwischen diesen Leitlinien und den tatsächlich existierenden Verfahren der untersuchten CA gefunden werden. Dabei muss nicht nur die Policy betrachtet werden, sondern die gesamte Dokumentationsstruktur: Interne Betriebshandbücher, Administrationsdokumente, Dokumente für Zertifikatinhaber, Risikoanalysen, Zertifikatantragsformulare und vieles mehr.

Es ist nicht zu erwarten, dass jede Leitlinie sofort eine offensichtliche Entsprechung in der Dokumentation hat, und so muss zu jedem Punkt aus den Audit-Standards einzeln argumentiert werden, wieso dieser abgedeckt ist.

Ablauf des Audits der DFN-PKI

Klärung „Audit nach welchem Standard?“
Am Anfang eines Auditprozesses steht die Frage nach dem Standard, nach dem das Audit durchgeführt werden soll. Im Fall der DFN-PKI ergeben sich die Optionen aus den Anforderungen der Root-CA Programme der Browserhersteller (siehe oben). In Fra-

ge kommen aus diesen Optionen nur ETSI TS 102 042 sowie WebTrust „Principles and Criteria for Certification Authorities 2.0“, da die anderen Standards nur für CAs mit speziellen Aufgaben bzw. für CAs zur Ausstellung von Extended Validation Zertifikaten geeignet sind.

Im Jahr 2011 wurde mit der TÜV Informationstechnik GmbH (TÜViT) ein Audit nach ETSI TS 102 042 gestartet. Dieser Standard ist zur Auditierung der DFN-PKI sehr gut geeignet, da der Fokus des Audits auf den technischen und organisatorischen Sicherheitsmaßnahmen im CA-Betrieb und der Konformität der Policy liegt.

Erstes Voraudit

Der Auditierungsprozess der DFN-PKI begann Mitte 2011 mit einem ersten Voraudit. Hierbei wird die bestehende Situation vom Auditor mit dem Ziel geprüft, Abweichungen vom Standard zu erkennen und eine entsprechende Liste zu erstellen. Im Audit werden die Aspekte „Policy“, „Bauliche Sicherheit“ und „IT-Sicherheit“ getrennt betrachtet.

Um eines vorwegzunehmen: Das Ergebnis des ersten Voraudits war sehr positiv und die DFN-PKI hat vom TÜViT einen sehr guten Ausgangszustand bescheinigt bekommen. Der Großteil der festgestellten Abweichungen vom Standard folgte nicht aus einem mangelhaften Sicherheitsniveau der DFN-PKI, sondern daraus, dass viele Dinge zwar anders gemacht wurden, als es im ETSI-Standard vorgesehen ist, nicht aber schlechter. Das Ergebnis des ersten Voraudits soll hier anhand von einigen Beispielen erläutert werden.

Die Policy einer PKI wird vom Auditor mit dem zugrundeliegenden Prüfstandard verglichen. Hierbei muss der Prüfer für jede Anforderung aus dem Standard eine Entsprechung beim Prüfling finden. Im Bereich Policy mussten nach der ersten Sichtung der Dokumente fast 100 Punkte einzeln mit TÜViT abgeklärt werden, z.B.:

- „Im CP, CPS fehlt gemäß ETSI 7.1 a) der Verweis auf ETSI TS 102 042 und die zugehörige certificate policy.“
- „Im CP/CPS fehlt gemäß ETSI 7.2.5 a) die Angabe, dass CA-Schlüssel nicht für andere Zwecke verwendet werden.“
- „Wie wird der Zertifikatnehmer nach ETSI 7.3.6 f) darüber informiert, dass eine Sperrung seines Zertifikates erfolgt ist?“

Die allermeisten Punkte konnten entweder direkt geklärt werden oder benötigten lediglich eine kurze Ergänzung der Beschreibung. Nur bei zehn Punkten mussten tatsächlich Prozesse oder Technik leicht modifiziert werden.

Im Bereich „Bauliche Sicherheit“ untersuchte TÜViT in erster Linie die Brand- und Einbruchschutzmaßnahmen der Räumlichkeiten, in denen die CA-Infrastruktur betrieben wird. Die zu beantwortenden Fragen betrafen hauptsächlich Nachweise für bereits getroffene Maßnahmen, die noch beschafft werden mussten. Natürlich mussten auch kleinere Ergänzungen der Infrastruktur vorgenommen werden wie z.B. zusätzliche Brandmelder oder ein weiteres Schloss für einen Schaltkasten. Darüber hinaus wurden Sensoren zur Brandfrühesterkennung eingebaut, die bereits auslösen, wenn am anderen Ende des Raumes mit einem Lötkolben gearbeitet wird.

Der Bereich „IT-Sicherheit“ umfasst alle Sicherheitsmaßnahmen auf Netzwerk- und Server-Ebene. Es werden sowohl die organisatorischen als auch die technischen Aspekte betrachtet, beispielsweise das Patch-Management, die Netzwerk- und Firewallkonfiguration, die organisatorischen und technischen Maßnahmen zur Begrenzung des administrativen Zugriffs auf Server. In diesem Bereich waren am wenigsten Fragen der Auditoren zu klären.

Neue Policy 2.3 der DFN-PKI im Sicherheitsniveau Global

Nach dem ersten Voraudit musste die DFN-PKI aufgrund der Anforderungen der Browser- und Betriebssystemhersteller erst einmal die Baseline Requirements des CA/Browserforums umsetzen. Hierzu musste neben einigen technischen Änderungen bis zum 1. Juli 2012 eine neue Policy in Kraft gesetzt werden, die die entsprechenden Umsetzungen der Anforderungen enthält. Hierbei wurde gleichzeitig ein Großteil der aufgrund der Erkenntnisse aus dem ersten ETSI-Voraudit notwendigen Änderungen mit berücksichtigt. Die Policy in der Version 2.3 wurde am 26. Juni 2012 in Kraft gesetzt.

Die auffälligsten Änderungen betreffen die Verwendung von Begriffen in der Policy. Dies wurde notwendig, da in ETSI TS 102 042, aber auch in den Baseline Requirements, die Verwendung bestimmter Begriffe genau definiert ist, und die DFN-PKI hier teilweise andere Bezeichnungen verwendete oder in einer etwas anderen Bedeutung eingesetzt hat:

- Die Registrierungsstellen (RA) bei den Teilnehmern der DFN-PKI heißen nun Teilnehmerservice, die dort arbeitenden Personen Teilnehmerservice-Mitarbeiter (bisher: RA-Operator).
- Die einzige Registrierungsstelle (engl. Registration Authority) der DFN-PKI wird von der DFN-PCA selber in Hamburg betrieben.
- Aus dem Zertifikatnehmer wird der Zertifikatinhaber (engl. Subject)
- Der Anwender heißt nun „Teilnehmer“ (engl. Subscriber).
- Darüber hinaus wurden die RA-Operatorzertifikate, welche zur Authentifizierung der Mitarbeiter mit Prüfaufgaben (wie die persönliche Identifizierung von Antragstellern) dienen, auf persönliche Zertifikate anstelle der vorher verwendeten Gruppenzertifikate umgestellt.

Weitere wichtige Änderungen, die auch jede Einrichtung betreffen, sind:

- Zertifikate mit lokalen Hostnamen oder internen IP-Adressen dürfen nur noch mit einem Ablaufdatum bis Oktober 2015 ausgestellt werden. Nach diesem Termin gibt es keine Zertifikate mit lokalen Hostnamen oder internen IP-Adressen mehr in der DFN-PKI (und auch nicht von anderen Zertifizierungsstellen, die im Browser verankert sind).
- Viele Prüfungen sind nach 39 Monaten zu wiederholen, z.B. persönliche Identifizierungen oder der Nachweis über den Besitz an einer Domain, die in Zertifikaten erscheint.
- Bisher gab es für jede teilnehmende Einrichtung ein eigenes Certification Practice Statement (CPS). Dieses wird jetzt nicht mehr benötigt und durch ein gemeinsames CPS sowie die neuen Dokumente „Informationen für Zertifikatinhaber“ und „Pflichten der Teilnehmer“ ersetzt.

Darüber hinaus gab es viele kleinere Änderungen, die beispielsweise die Aufbewahrungsfristen von Papierdokumenten betreffen.

Zweites Voraudit

Im zweiten Voraudit im Jahr 2012 wurde die DFN-PKI erneut vom TÜViT geprüft. Da die DFN-PKI nun bereits an die Anforderungen aus ETSI angepasst war, war ein Prüfergebnis mit deutlich weniger Fundstellen zu erwarten. Trotzdem hatte die Liste der offenen Punkte im Bereich „Policy“ immer noch fast siebzig Einträge, also nur ungefähr ein Drittel weniger als im ersten Voraudit. Dies war zunächst überraschend. Im Workshop mit dem TÜViT stellte sich aber heraus, dass es sich fast ausschließlich um Nachfragen zur Policy handelte, die sich schnell klären ließen. An einigen Stellen wurde die Policy darauf hin noch ein wenig klarer formuliert, faktische Änderungen waren aber nicht mehr notwendig.

Bei der Prüfung der IT-Sicherheit ergaben sich keine größeren Auffälligkeiten. Einziger „Höhepunkt“: Bei Netzwerkscans wurden zwei Webserver mit gesperrtem bzw. abgelaufenem Serverzertifikat gefunden. Wir konnten TÜViT erklären, dass es sich dabei um unsere beiden Testserver https://revoked-demo.pca.dfn.de/ und https://expired-demo.pca.dfn.de/ handelt, die zum Testen des Verhaltens von Clientsoftware bei gesperrten oder abgelaufenen Zertifikaten dienen – also mit voller Absicht ungültige Zertifikate ausliefern.

Das Fazit des zweiten Voraudits war, dass die DFN-PKI für das eigentliche Audit bereit ist und keine weiteren Voraudits notwendig waren.

Neue Policy 3.0 der DFN-PKI im Sicherheitsniveau Global

Für das Audit der DFN-PKI mussten nun noch einige Änderungen in der Policy der DFN-PKI umgesetzt werden, die aus formalen Gründen leider noch nicht in die Version 2.3 aufgenommen werden konnten. Hierfür wurde am 15. November 2012 eine weitere überarbeitete Policy in Kraft gesetzt. Neben einigen verfeinerten Formulierungen ist die einzige inhaltliche Änderung der zusätzliche und formal notwendige Satz „Die DFN-PCA und alle ihre nachgeordneten CAs (Sub-CAs) erfüllen die Anforderungen von ETSI TS 102 042 nach der LCP Policy.“

Audit

Das eigentliche Audit lief ähnlich ab wie die Voraudits: Die Prüfer vom TÜViT prüften zuerst die Papierlage, also in erster Linie die Policy, aber auch die anderen relevanten Dokumente wie „Pflichten der Teilnehmer“ oder „Informationen für Zertifikatinhaber“. In einem anschließenden Workshop wurden wieder offene Fragen geklärt. Diesmal konnten alle Fragen des TÜViT abschließend beantwortet werden.

In einer beispielhaft durchgeführten Zertifikatbeantragung wurde überprüft, ob die tatsächlichen Prozesse auch den in der Policy definierten entsprechen. Hierzu wurde im Beisein des Prüfers ein Zertifikat beantragt und der gesamte Prüfprozess bis zur Aus-


Zertifikat

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH
bescheinigt hiermit dem Unternehmen

DFN-Verein e. V.
Alexanderplatz 1
10178 Berlin

für den Zertifizierungsdienst

DFN-PKI Sicherheitsniveau Global

die Erfüllung aller Anforderungen der Spezifikation

ETSI TS 102 042 V2.2.1 (2011-12), policy LCP.

Die Anlage zum Zertifikat ist Bestandteil des Zertifikats und besteht aus 19 Seiten.

Dieses Zertifikat gilt nur in Verbindung mit dem zugehörigen Prüfbericht bis zum 31.12.2013.

TÜViT 2012 Trusted Site
Voluntary Validation
© TÜViT - Member of TÜV NORD Group

Zertifikat-Registrier-Nr.: TUVIT-CA6727.12

Essen, 07.12.2012
Dr. Christoph Sutter
Leiter Zertifizierungsstelle

TÜV Informationstechnik GmbH
Unternehmensgruppe TÜV NORD
Langemarckstraße 20
45141 Essen
www.certuvit.de

DGA-ZE-014/99

Abb. 2: Das Zertifikat über die Erfüllung der Anforderungen nach ETSI TS 102 042

stellung des Zertifikats durchgeführt. Dies wurde einmal bei der DFN-PCA in Hamburg selber und am Ende des Audits noch einmal bei einem Teilnehmer der DFN-PKI vor Ort durchgeführt. Die IT-Sicherheit wird durch die theoretische Bewertung der Sicherheitsmaßnahmen, aber auch durch konkrete Netzwerkscans und Penetration Tests überprüft.

Am Ende des dreitägigen Vor-Ort Audits wurde vom Prüfer bereits vorab das Bestehen in Aussicht gestellt. Das formale positive Ergebnis war erst einige Zeit später verfügbar: Der TÜViT muss nach einem Audit erst noch interne Qualitätssicherungsmaßnahmen durchführen, bei denen ein am bisherigen Audit nicht beteiligter Mitarbeiter das gesamte Prüfergebnis noch einmal auf Plausibilität prüft. Diese interne Prüfung wird dann in einem formalen Akt mit der auch hier sogenannten Zertifizierung abgeschlossen, und es wird sogar ein Zertifikat ausgestellt: Eine Urkunde mit einer Unterschrift des Leiters der Zertifizierungsstelle (nicht zu verwechseln mit einer CA, die digitale Zertifikate ausstellt). Dieser letzte Schritt konnte dann Anfang Dezember 2012 abgeschlossen werden.

Gültigkeit des Audits

Jedes Zertifikat zu einem Audit hat nur eine beschränkte Gültigkeit von einem Jahr. Vor Ablauf des Jahres muss in einem erneuten Audit-Prozess nachgewiesen werden, dass die Prozesse der CA nicht inzwischen vom Prüfstandard abweichen. Deshalb wird auch im Herbst 2013 wieder ein Audit bei der DFN-PCA stattfinden. Im Prinzip sollte dieses Re-Audit keinerlei Überraschungen bieten und mit einem relativ geringen Aufwand und vor allem ohne weiteren Aufwand bei den Teilnehmern der DFN-PKI zu absolvieren sein.

Vorteile für DFN-Anwender

Wo bringt das Audit jetzt Vorteile? Schließlich war der Auditprozess mit nicht unerheblichen Mehraufwänden beim DFN, aber auch bei den an der DFN-PKI teilnehmenden Anwendern verbunden. Notwendige Änderungen wurden zwar so weit wie möglich in der DFN-PCA intern umgesetzt, um die Aufwände bei den Anwendern zu minimieren. Trotzdem ließen sich einige Aspekte nur durch die Änderung von Prozessen bei den Anwendern umsetzen. Umstellungen durch zwei neue Policy-Versionen, durch personengebundene Teilnehmerservice-Mitarbeiter-Zertifikate und durch geänderte Archivierungsfristen haben sicherlich auch bei den Anwendern für einige Arbeit gesorgt.

Den Mehraufwänden stehen aber viele Vorteile gegenüber: Gerade in diesem sicherheitskritischen Bereich ist es sehr wertvoll, eine Bestätigung von unabhängiger Seite über die Güte der Dienstleistung zu haben. Nur eine Überprüfung der Prozesse und der eingesetzten Technik durch Dritte gewährleistet einen langfristig sicheren Betrieb.

Darüber hinaus entwickeln sich die Anforderungen der Softwarehersteller weiter, so dass ein bestandenes Audit Voraussetzung für den Selbst-Betrieb einer Zertifizierungsstelle mit Browser-Verankerung ist. Damit haben wir durch den Audit-Prozess sichergestellt, dass auch in den kommenden Jahren browserverankerte Zertifikate in der DFN-PKI in der gewohnten Flexibilität und in dem hohen Volumen ausgestellt werden können.

Fazit

Trotz der auf den ersten Blick recht langen Dauer von eineinhalb Jahren und dem beträchtlichen Aufwand lief das Audit ohne größere Schwierigkeiten ab, was auch an dem bereits vorher realisierten hohen Sicherheitsniveau liegt. Dank der engagierten Mitarbeit der DFN-PKI-Teilnehmer konnten auch aufwändige Schritte wie der Austausch von Teilnehmerservice-Mitarbeiter-Zertifikaten in kurzer Zeit durchgeführt werden.

Mit dem Audit und der Zertifizierung nach ETSI TS 102 042 hat sich die kontinuierliche Weiterentwicklung der DFN-PKI der letzten Jahre fortgesetzt, so dass wir für die Zukunft gut gerüstet sind. ◆

„CA/Browser Forum“

Das CA/Browser Forum ist ein Konsortium von Browserherstellern und CA-Betreibern. Das CA/Browser Forum legt Richtlinien fest, nach denen browserverankerte CAs vorgehen sollen, um ein ausreichendes Sicherheits- und Vertrauensniveau für SSL-Zertifikate sicherzustellen. Ursprünglich wurde im CA/Browser Forum das Vorgehen zur Ausstellung von sogenannten „Extended Validation“-Zertifikaten definiert. Diese Regelungen hatten somit erst einmal keine Auswirkungen auf die DFN-PKI. Durch die Sicherheitsvorfälle der Jahre 2011 und 2012 bei browserverankerten CAs wurden aber auch die Aktivitäten beschleunigt, Anforderungen für nicht-EV-Zertifikate zu definieren. Am 1. Juli 2012 traten diese „Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates“ in Kraft. Die Mitglieder des CA/Browserforums verpflichteten sich selber zur sofortigen Einhaltung, andere CAs wurden anschließend durch die Anpassung der Root-Programme der Browserhersteller hierzu verpflichtet.