TeleTrusT
Pioneers in IT security.

TeleTrusT-interner Workshop

Nürnberg, 21./22.06.2012

Jens Bender
Bundesamt für Sicherheit in der Informationstechnik

PKI-Sicherheit: DigiNotar – und dann?

Das BSI

- Gründung 1991 per Gesetz als nationale Behörde für IT-Sicherheit
- Unabhängig und neutral
- ~ 550 Mitarbeiter
- IT-Sicherheitsdienstleister des Bundes
- Enges Zusammenwirken mit Wirtschaft, Bürgern und Forschung
- Beratung der Länder

Handlungsrahmen des BSI

Technik

IT-Sicherheit
(sichere Identitäten,
Kryptoinnovationen,
Cyber-Sicherheit etc.)

BSI-Gesetz
IT-Recht
Recht in IT-Projekten

IT-Steuerung Bund
IT-Investprogramm
Koalitionsvertrag
IT-Planungsrat
Cyber-Sicherheitsstrategie

Recht

Politik

Angriffstrend

weg von *direkten Angriffen*, hin zu Angriffen auf *Sicherheitsdienstleister / Sicherheitsprodukte*

indirekter Angriff, Schwächen der Schutzmaßnahmen

Infrastrukturangriffe erlauben weitere Ziele

BSI und PKI

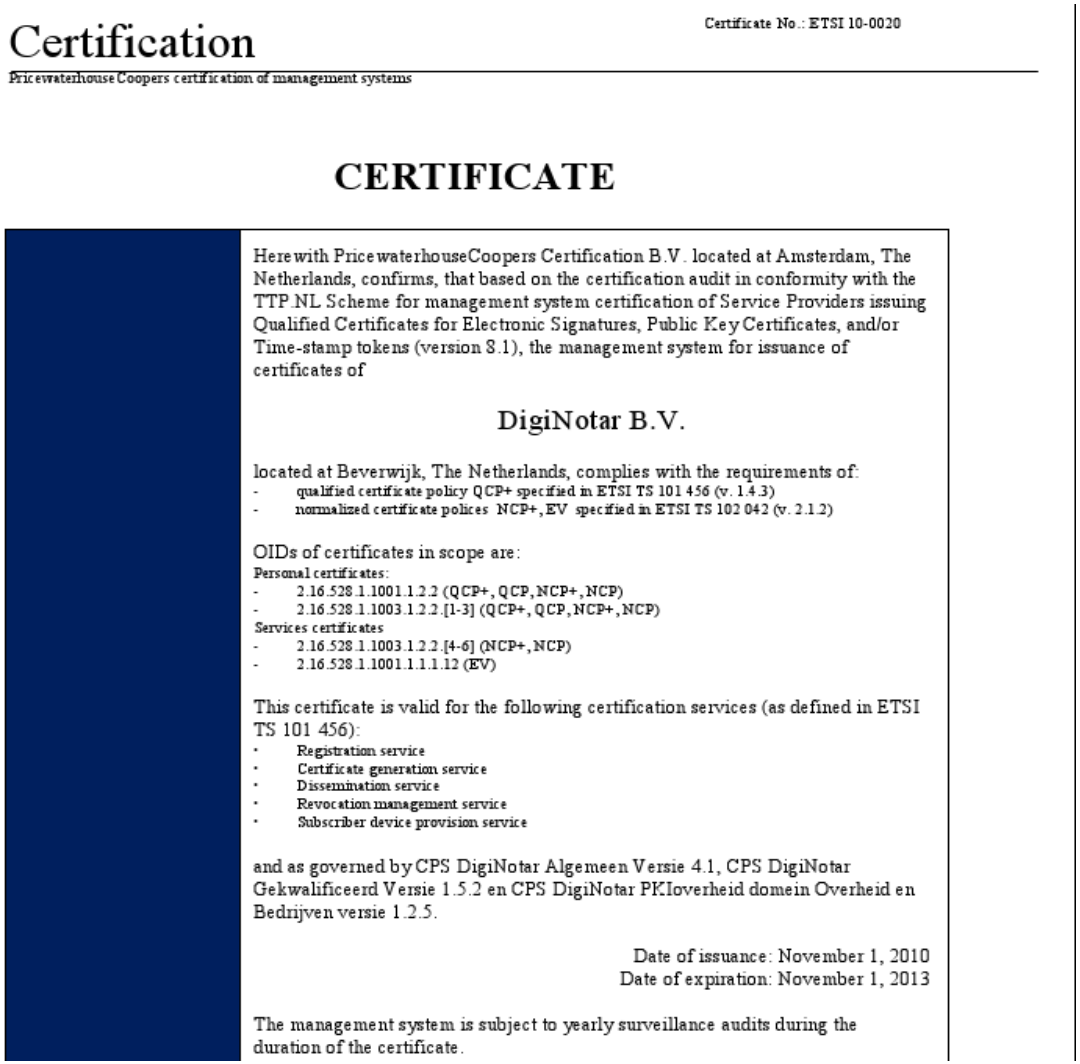
- BSI ist Architekt, Betreiber und Nutzer von PKIen
- BSI betreibt
  - Wurzelinstanzen Hoheitliche Dokumente (ePass, ePA, ...)
  - Wurzelinstanz Verwaltungs-PKI (V-PKI)
  - Wurzelinstanz BOS
  - Diverse PKIen im VS-Bereich
- Vorgaben für
  - SubCAs dieser PKIen
  - IVBB-PKI, DOI, Antragsdaten hD, …
- Nutzung für email, SSL, Mobile Geräte, Externe Zugänge, ...
- Incident Response: CERT-Bund/Bürger-CERT

DigiNotar B.V.

- Niederl. Zertifizierungsdienstleister
  - Spezialisiert auf Dienstleistungen für Notare und die niederl. Regierung
  - Gehört seit 2011 zu VASCO Data Security Int.
- DigiNotar SSL Root CA in der Liste vertrauenswürdiger CAs vieler Internet-Programme
- Sub-CA für niederl. staatliche PKI (PKIOverheid)
  - Viele staatliche Online-Dienste verwendeten DigiNotar-Zertifikate (DigiD, KFZ-Zulassung, ...)
- Stellt auch QES-Zertifikate aus

Sicherheit bei DigiNotar

- ETSI-Audit von PwC
- Ausgestellt am 01.Nov 2010
- Gültigkeit: 3 Jahre



Certificate No.: ETSI 10-0020

Certification

PricewaterhouseCoopers certification of management systems

CERTIFICATE

Herewith PricewaterhouseCoopers Certification B.V. located at Amsterdam, The Netherlands, confirms, that based on the certification audit in conformity with the TTP.NL Scheme for management system certification of Service Providers issuing Qualified Certificates for Electronic Signatures, Public Key Certificates, and/or Time-stamp tokens (version 8.1), the management system for issuance of certificates of

DigiNotar B.V.

located at Beverwijk, The Netherlands, complies with the requirements of:
- qualified certificate policy QCP+ specified in ETSI TS 101 456 (v. 1.4.3)
- normalized certificate polices NCP+, EV specified in ETSI TS 102 042 (v. 2.1.2)

OIDs of certificates in scope are:
Personal certificates:
- 2.16.528.1.1001.1.2.2 (QCP+, QCP, NCP+, NCP)
- 2.16.528.1.1003.1.2.2.[1-3] (QCP+, QCP, NCP+, NCP)

Services certificates
- 2.16.528.1.1003.1.2.2.[4-6] (NCP+, NCP)
- 2.16.528.1.1001.1.1.1.12 (EV)

This certificate is valid for the following certification services (as defined in ETSI TS 101 456):
- Registration service
- Certificate generation service
- Dissemination service
- Revocation management service
- Subscriber device provision service

and as governed by CPS DigiNotar Algemeen Versie 4.1, CPS DigiNotar Gekwalificeerd Versie 1.5.2 en CPS DigiNotar PKIoverheid domein Overheid en Bedrijven versie 1.2.5.

Date of issuance: November 1, 2010
Date of expiration: November 1, 2013

The management system is subject to yearly surveillance audits during the duration of the certificate.

Was ist PKI?

PKI = Zertifizierung von Identitäten/Attributen

- PKI erlaubt das Verifizieren von Identitäten/Attributen
- Nicht Zuweisung von Identitäten/Attributen

PKI ist Vertrauen

- Alle vertrauen der Root
- Die Root delegiert Vertrauen an SubCAs
- PKI funktioniert nur, wenn das Vertrauen gerechtfertigt ist

Daher: Vertrauensverlust ist katastrophal

Vorfallsverlauf
2011

- 06.Juni Erste Vorfälle bei DigiNotar
- 17.Juni Mehrere DigiNotar Server gehackt
- 19.Juni Erste Erkennung eines gehackten Systems
- 10.Juli Erste fälschliche Generierung eines SSL Zertifikats
- 19.Juli DigiNotar erstellt Zertifikat für *.google.com
- 22.Juli DigiNotar untersucht den Angriff vom 19.Juni
- 28.Aug Zertifikat für *.google.com wird erkannt
- 29.Aug Updates von MS, Mozilla, Google
- 31.Aug Fox-IT beginnt mit der Untersuchung
- 03.Sep Black-Tulip Report, Vertrauensentzug durch NL
- 20.Sep Start der Liquidation von DigiNotar

FOX-IT Report
Operation Black Tulip

- Keine Trennung der Netzbereiche (Büronetz / CA-Server)
- CA-Server waren Mitglied einer einzelnen Domäne
- Einfaches Admin-Passwort
- Fehlende Antivirensoftware
  - Schadsoftware wäre von gängigen Produkten erkannt worden
- Software der Webserver war stark veraltet
- Keine zentralisierte Logging-Funktionalität

Unzureichende „klassische“ IT-Sicherheit

Der Audit hat nicht funktioniert

Liste falscher SSL-Zertifikate

Common Name	Number of certs issued
CN=*.*.com	1
CN=*.*.org	1
CN=*.10million.org	2
CN=*.JanamFadayeRahbar.com	1
CN=*.RamzShekaneBozorg.com	1
CN=*.SahebeDonyayeDigital.com	1
CN=*.android.com	1
CN=*.aol.com	1
CN=*.azadegi.com	1
CN=*.balatarin.com	3
CN=*.comodo.com	3
CN=*.digicert.com	2
CN=*.globalsign.com	7
CN=*.google.com	26
CN=*.logmein.com	1
CN=*.microsoft.com	3
CN=*.mossad.gov.il	2
CN=*.mozilla.org	1
CN=*.skype.com	22
CN=*.startssl.com	1
CN=*.thawte.com	6
CN=*.torproject.org	14
CN=*.walla.co.il	2
CN=*.windowsupdate.com	3
CN=*.wordpress.com	14
CN=Comodo Root CA	20
CN=CyberTrust Root CA	20
CN=DigiCert Root CA	21
CN=Equifax Root CA	40
CN=GlobalSign Root CA	20
CN=Thawte Root CA	45
CN=VeriSign Root CA	21
CN=addons.mozilla.org	17
CN=azadegi.com	16
CN=friendsvault.com	18
CN=login.live.com	17
CN=login.yahoo.com	19
CN=my.screenname.aol.com	1
CN=secure.logmein.com	17
CN=twitter.com	19
CN=wordpress.com	12
CN=www.10million.org	8
CN=www.Equifax.com	1
CN=www.balatarin.com	16
CN=www.cia.gov	25
CN=www.cybertrust.com	1
CN=www.facebook.com	14
CN=www.globalsign.com	1
CN=www.google.com	12
CN=www.hamdami.com	1
CN=www.mossad.gov.il	5
CN=www.sis.gov.uk	10
CN=www.update.microsoft.com	4

>500 Zertifikate

Globaler Missbrauch

OCSP-Anfragen für das *.google.com-Zertifikat (04/09-29/09)

Nebenbemerkung: Beachte das Spannungsverhältnis von OCSP
zwischen IT-Sicherheit und Datenschutz (Tracking)

Comodo & Globalsign & StartCom & KPN & ...

- Comodo
  - Kompromittierung eines Accounts eines ext. Registrars
- GlobalSign
  - Stoppt CA-Betrieb für 1 Woche.
  - Vorfallsuntersuchung durch Fox-IT
    - Angriffe auf isolierten Webserver.
- StartSSL
  - Angriff auf mehrere, von CA-Prozessen abgekoppelte Webserver.
- KPN Getronics
  - CA-Betrieb wird für 2 Wochen eingestellt, nachdem Kompromittierungen entdeckt wurden

Projektgruppe PKI-Sicherheit

Als Reaktion auf 2011 wurde im BSI die Projektgruppe „PKI-Sicherheit“ eingerichtet

- Aufarbeitung der Angriffe
- Kurzfristige Maßnahmen um Auswirkungen zu verringern
- Mittelfristige Erhöhung der Vertrauenswürdigkeit
  - Bessere Transparenz bei Vorfällen
- Langfristige Erhöhung der Sicherheit
  - Anforderungen, Prüfkriterien und Zertifizierung
  - Weiterentwicklung von Konzepten

„Lösung“

- Convergence: Bei Aufbau einer SSL-Verbindung werden „Notare“ gefragt, ob das Server-Zertifikat echt ist
  - Sind die Notare vertrauenswürdig?
  - Woher weiß der Nutzer, daß die Antwort des Notars authentisch ist?
- Pinning: Browser prüft, ob das gesendete Server-Zertifikat das gleiche ist wie bei früheren Verbindungen
  - Initiales Vertrauen?
  - Regulärer Zertifikatswechsel/mehrere Zertifikate für gleichen Host-Namen
- DANE: SSL-Zertifikate werden im DNS eingetragen und per DNSSEC gesichert
  - Wie wird DNSSEC gesichert?
  - Wie kommen die Zertifikate (authentisch!) ins DNS?

Hilft alles nichts → SSL-CAs wird nicht vertraut, stattdessen muss anderen Stellen vertraut werden

Lösung

Einzige Lösungsmöglichkeit:
Vertrauen in alle CAs erhöhen/wiederherstellen

- Transparent Anforderungen an CAs
  - Gesamtblick auf CAs, keine „Detailanforderungen“
  - Klassische IT-Sicherheit
- Klarer Auditprozess
  - Derzeitiger Audit-Prozess ist intransparent
    - Keine klaren Qualifikationsanforderungen an Auditoren
      - **Ist ein Wirtschaftsprüfer ein geeigneter IT-Sicherheits-Auditor?**
    - Keine klaren Vorgaben, was auditiert wird
      - **Z.T. wird nur die Buchhaltung auditiert**
    - Keine Vergleichbarkeit von Audits verschiedener Auditoren
  - Qualitätsaudit als Qualitätsmerkmal

Anforderungen und Audit

- Vorhandene Anforderungs-/Audit-Regimes
  - Webtrust → SSL, Ausrichtung auf „Checks and Balances“
  - CAB-Forum → nur für SSL
  - ETSI → Schwerpunkt QES/SSL, wenig zum Audit
  - Weitere für spezielle CAs (SigG, ...)

- Der Plan:
  - Erstellung einer Technischen Richtlinie mit (weitgehend) anwendungsunabhängigen Anforderungen an CAs
  - Klare Anforderungen an Auditoren
  - Klare und eindeutige Auditanforderungen
  - BSI-Zertifizierung

ISO 2700x und Common Criteria

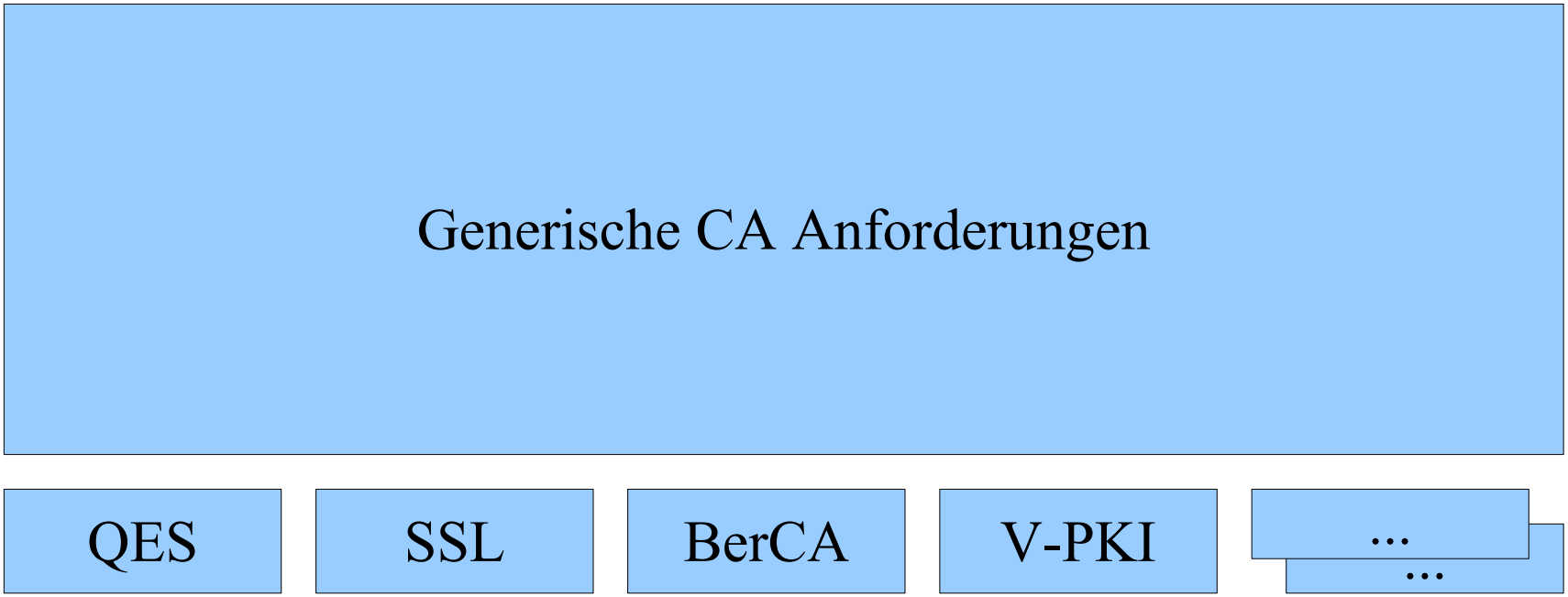
- ISO 2700x
  - Sicherheitskonzepte für Systeme
  - Keine konkreten Sicherheitsanforderungen, sondern Methodik
- Grundschutz
  - Konkrete Maßnahmen für normales Sicherheitsniveau
- Common Criteria
  - Stark formalisiertes Verfahren für Komponenten

Gebraucht wird: Systemsicherheit auf hohem Sicherheitsniveau mit formalen Verfahren zur Erhöhung der Verbindlichkeit/Vergleichbarkeit

Struktur

- Orientierung an Formalismus der Common Criteria
  - Strukturierung nach
    - Zu schützende Werte – Assets
    - Bedrohungsanalyse – Threads
    - Sicherheitsanforderungen – Requirements
  - Mapping von Anforderungen auf Ziele („Rationale“)
- Systemansatz nach ISO 2700x
- Kriterien für Anforderungen
  - Sicherheitsziel wird erreicht
  - Notwendigkeit zur Erreichung eins Ziels
  - Aufwand und Nutzen stehen in sinnvollem Verhältnis
- Kompatibilität (ETSI, CAB-Forum, SigG, ...)
- Öffnungsklauseln um „atypische“ Systeme zu ermöglichen

Generisch und Spezifisch



90% anwendungsunabhängig + 10% anwendungsspezifisch
→ Vereinfachung für CAs durch „Grundaudit“

Prozesse

- Prozessorientiert
  - Bei einem CP nach RFC 3647 ist nicht klar, ob alle Prozesse lückenlos abgedeckt sind
- Abzudeckende Prozesse
  - Identifikation und Registrierung
  - Schlüsselerzeugung
  - Zertifikatserstellung und -verteilung
  - Sperrung, Statusdienste
  - Migration, Key-Rollover
  - Outsourcing
  - Notfallmanagement
  - ....

Beispiel

- Requirement:
  - The secret key(s) of the CA MUST be generated and stored in a secure hardware device certified according to [selection: CC PP-SSCD, CC PP-HSM, FIPS 140-2, other].
    - If „other“ is selected, a rationale is required
- Auditing:
  - The auditor MUST check
    - The secret key is generated and stored in a device according to …
    - All requirements from the Guidance Document of the device are fullfilled
    - ...
  - If the device is capable of key backup, the auditor MUST check
    - The key backup is part of the security certification of the device
    - Only authorized personell has the technical means to backup/restore a key
  - ...

Zielgruppe

- Verpflichtung für vom BSI verantwortete PKIs
  - Berechtigungs-CAs für die eID-Funktion des ePA
  - SubCAs der V-PKI
- Basis für andere Verfahren
  - ...
- Angebot an alle anderen CAs
  - Zertifikat/Gütesiegel als Marketingvorteil
  - Audit als Maßnahme zu Qualitätssicherung der eigenen Prozesse
- Internationale Ausrichtung

Empfehlungen für kurzfristige Maßnahmen

- Präventiv
  - Grundschutz/ISO2700x Sicherheitskonzept und Audit
    - Das Sicherheitskonzept muss auch eingehalten werden!
    - → Basissicherung
- Reaktiv
  - Rückruf (CRL/OCSP) muss funktionieren!
  - Incident Response → Meldung von Vorfällen an das CERT
- Business Continuity im Rückruffall
  - Zertifikate sind kritisch für viele Geschäftsprozesse
  - Rückruf verzögert, da wichtige Kunden keine Notfallpläne hatten → unnötige Gefährdung Dritter

Beobachtungen „Internet-PKI“ RFC 5280

- Sinnvolle PKI-Struktur
  - Sparsame Verwendung des Root-Schlüssels
  - Trennung von Anwendungen durch verschiedene SubCAs
    - SSL-Serverzertifikat, Code-Signing, ...
- Intelligente Nutzung der Möglichkeiten von X.509/RFC 5280
  - Nutzung von (Extended)KeyUsage, pathLenConstraint, …
    - PrivateKeyUsage ist leider deprecated
  - Keine Wildcard-Zertifikate
- Sichere Kryptoverfahren
  - Wurzel-Zertifikatslaufzeiten maximal 7 Jahre
  - MD5 schon lange tot, SHA-1 sollte abgelöst werden
  - Empfehlung: TR-02102 „Algorithmen und Schlüssellängen“
  - Migration von vornherein einplanen!!!!

Zusammenfassung

- BSI: Anforderungen an CAs und Prüfvorgaben an Audit
  - Systematisch → Vollständige Abdeckung
  - Generische Grundanforderungen → Vereinfachung für CAs
  - Klare Auditkriterien → Vergleichbarkeit der Audits, Assurance
  - Zertifizierung → Marketing
- „Klassische“ IT-Sicherheit ist wichtig, dabei aber Kryptographie nicht aus dem Auge verlieren
- Angriffsziel bisher hauptsächlich SSL
  - Aktuell: Code Signing / Flame
    - Zertifikat erlaubt „aus Versehen“ Code Signing
    - MD5-Kollision
    - Update notwendig, um Zertifikate ungültig zu machen

Federal Office
for Information Security

Kontakt

Bundesamt für Sicherheit in der
Informationstechnik (BSI)

Jens Bender
Godesberger Allee 185-189
53175 Bonn

Tel: +49 (0)228-9582-5051
Fax: +49 (0)228-99-10-9582-5051

jens.bender@bsi.bund.de
www.bsi.bund.de
www.bsi-fuer-buerger.de