
Broken by Design:
Warum wir PKIs
nicht trauen können
(aber keine andere Wahl haben)
Nils Kaczenski
MVP Cloud & Datacenter Services
Head of Consulting, ATD | Systemhaus
ATD
SYSTEMHAUS
Experts Live Germany


PKI ist mies™

Nils Kaczenski
Head of Consulting | ATD GmbH
N.Kaczenski@atd.de

ATD GmbH | Linnéstraße 5 | 38106 Braunschweig
Telefon +49 531 23824 0

https://www.linkedin.com/in/nils-kaczenski/

Bild: Experts Live 2023

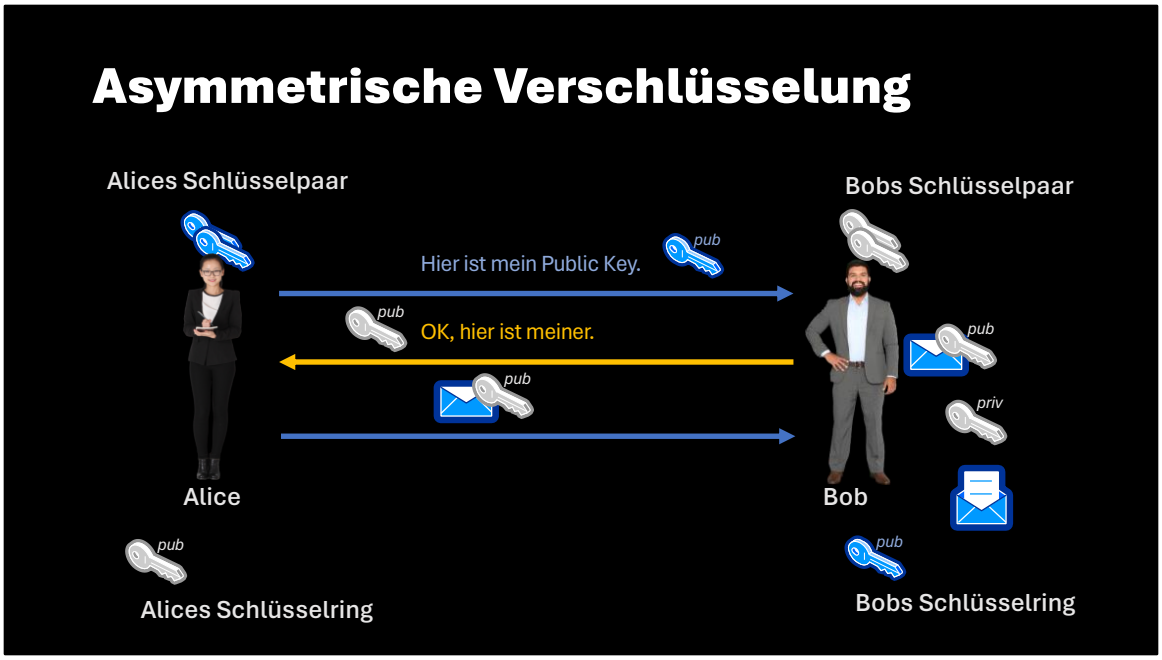
1. Ääh … Zertifikate?!
2. Vertrauen ist alles
3. Widerrufe und Trauerspiele
4. It’s the Sorgfalt, stupid!


1. Ääh ... Zertifikate?!
2. Vertrauen ist alles
3. Widerrufe und Trauerspiele
4. It's the Sorgfalt, stupid!

1

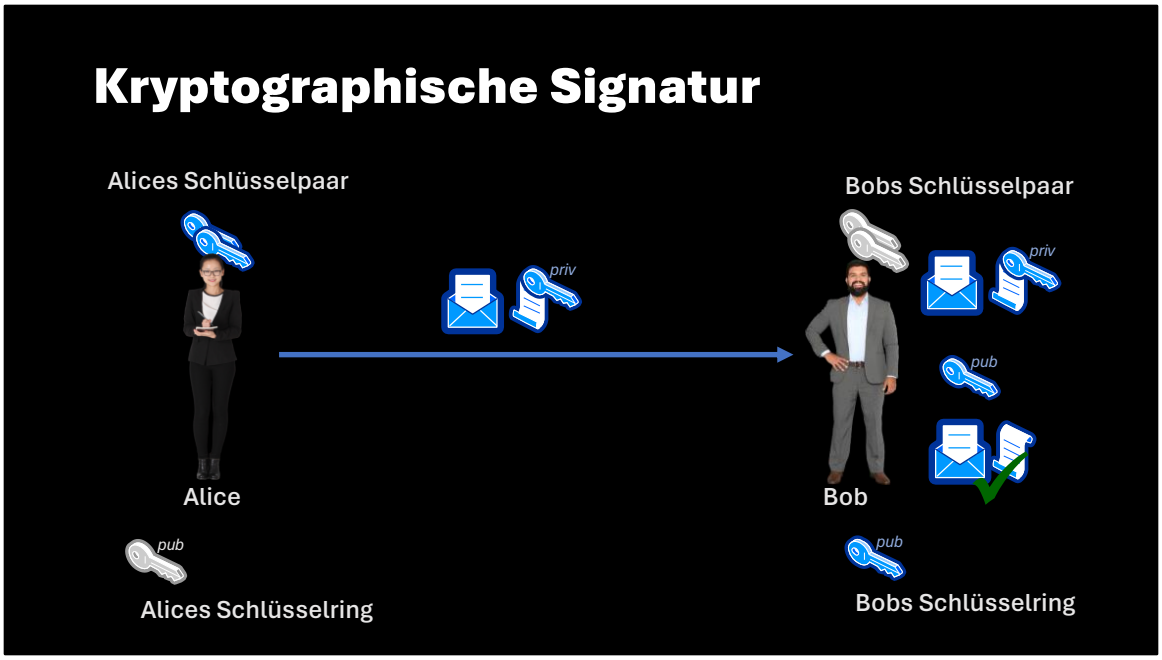
Ääh … Zertifikate?!

Kurze Auffrischung: Was Zertifikate sind und wie sie funktionieren



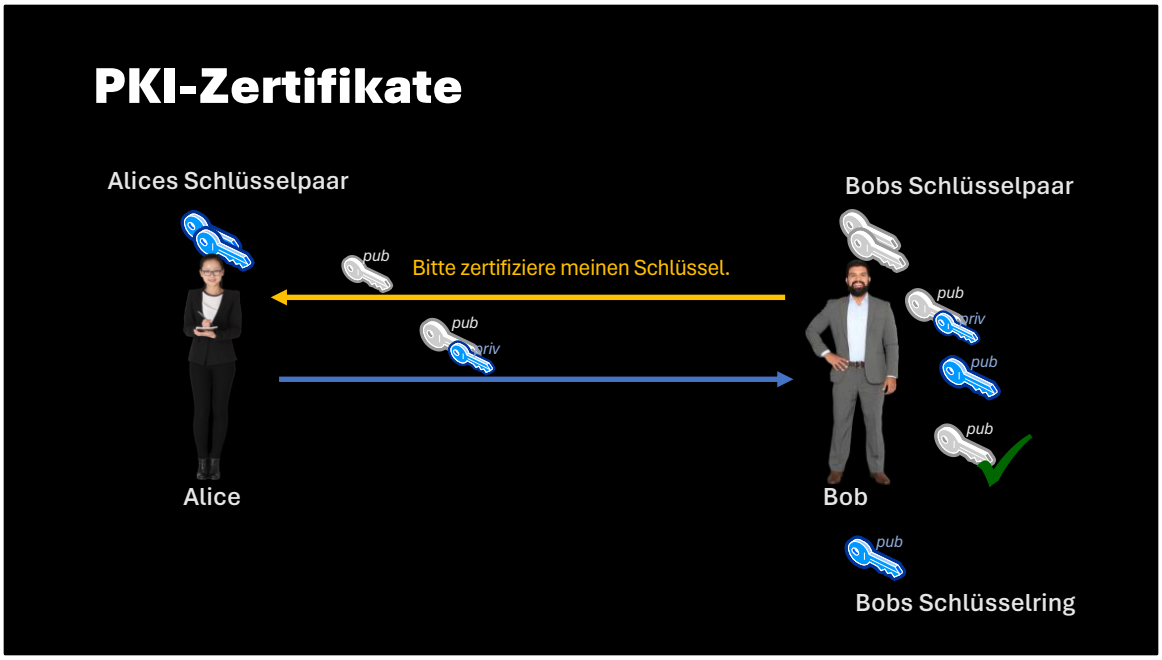
Asymmetrische Verschlüsselung:

- Zwei Parteien A und B wollen „sicher“ kommunizieren
- Jede Partei erzeugt ein kryptografisches Schlüsselpaar
  - Der Private Schlüssel ist geheim und wird nie weitergegeben
  - Der Öffentliche Schlüssel darf und soll an Kommunikationspartner weitergegeben und gern auch pauschal veröffentlicht werden
  - Beide gehören zusammen: Was mit dem einen Schlüssel verschlüsselt wurde, kann nur mit dem anderen wieder entschlüsselt werden
- Im ersten Schritt übergibt Partei A ihren Öffentlichen Schlüssel an Partei B
- Dann übergibt Partei B ihren Öffentlichen Schlüssel an Partei A
- Nun kann Partei A eine Nachricht mit dem Öffentlichen Schlüssel von Partei B verschlüsseln
- Nur Partei B kann die Nachricht mit ihrem Privaten Schlüssel lesbar machen



Kryptographisches Signieren:

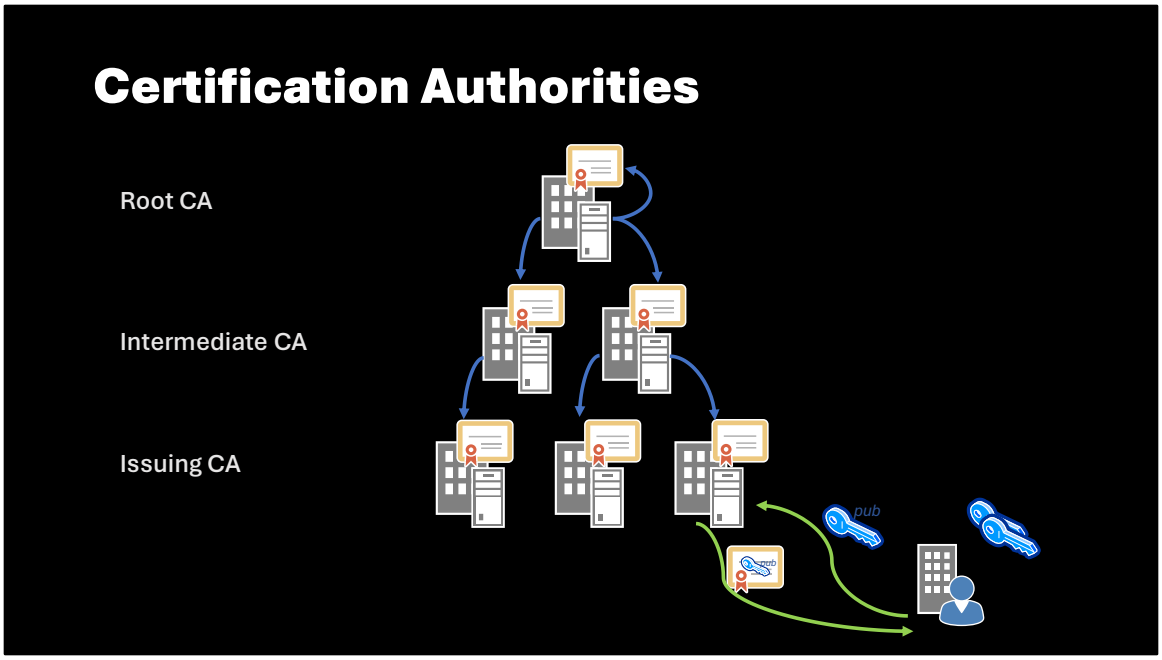
- Partei A will nachweisen, dass eine Nachricht wirklich von ihr stammt
- Dazu verschlüsselt sie eine Kopie (oder einen Hash) der Nachricht mit ihrem Privaten Schlüssel und hängt die Kopie (bzw. den Hash) an ihre Nachricht an
- Partei B empfängt diese Nachricht und nutzt den Öffentlichen Schlüssel von Partei A, um die Kopie (bzw. den Hash) der Nachricht zu entschlüsseln
    - Wenn die Kopie bzw. der Hash identisch mit der eigentlichen Nachricht sind, dann kann die Verschlüsselung nur von Partei A stammen
- Es ist nachgewiesen, dass die Nachricht von Partei A kommt



Die Idee hinter einem Zertifikat ist, dass eine Partei A bestätigt, dass ein bestimmter Öffentlicher Schlüssel zu Partei B gehört.
Dies tut Partei A, indem sie den Öffentlichen Schlüssel von Partei B kryptografisch mit ihrem eigenen Öffentlichen Schlüssel signiert. Dies ist – im Wesentlichen – das Zertifikat.
Der Nutzen: Wenn jemand Partei A kennt und ihr vertraut, kann sie prüfen, dass Partei A die Echtheit des Öffentlichen Schlüssels von Partei B bestätigt.

Ein Zertifikat ist ein öffentlicher Schlüssel einer Partei A, der von einer anderen Partei B signiert ist.
Wenn Sie Partei B vertrauen, können Sie überprüfen, ob sie den Schlüssel von Partei A signiert hat.
Sie wissen, dass Partei B selbst Partei A überprüft hat.
Sie können (!) Partei A vertrauen.

Das ist alles. In der Praxis gibt es noch einiges Beiwerk, aber das meiste ist nur da, damit kommerzielle CAs Geld verdienen können (z.B. verschiedene Zertifikatstypen) – die eigentliche Technik ist immer gleich.



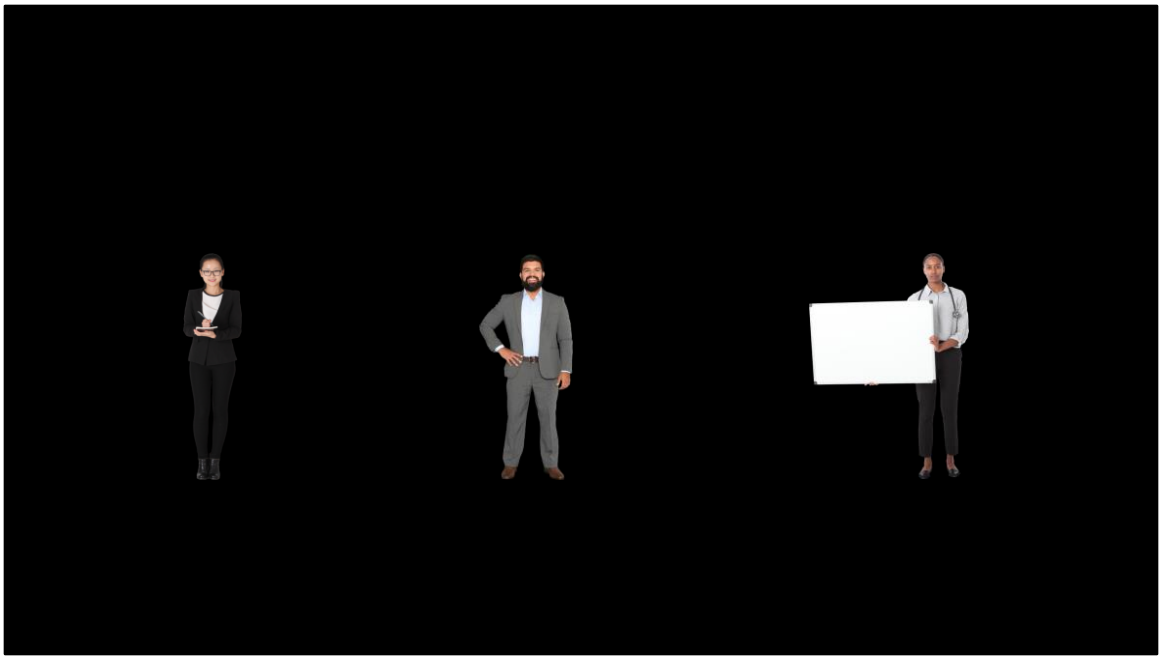
Schematischer Aufbau einer größeren PKI

- Die Root CA ist die „Wurzel des Vertrauens“. Sie stellt sich selbst ein Zertifikat aus. Ihr einziger Zweck ist, die CA-Zertifikate für die untergeordneten CAs auszustellen. Mit diesen Zertifikaten können die CAs nachweisen, dass sie zu der PKI gehören.
  Eine Root CA stellt keine Zertifikate für Benutzer oder Computer aus, auch wenn sie das technisch tun könnte.
- Intermediate CAs gibt es typischerweise nur in großen PKIs, wenn z.B. verschiedene Geschäftsbereiche mit eigenen Zweigen der PKI arbeiten sollen oder wenn technische Abstufungen nötig sind. Eine solche CA dient nur dazu, CA-Zertifikate an die untergeordneten Issuing CAs auszustellen.
  Auch eine Intermediate CA stellt keine Anwender- oder Computerzertifikate aus.
- Die Issuing CA ist die Instanz, um die es eigentlich geht: Sie stellt Zertifikate für Computer oder Benutzer aus. Damit andere diesen Zertifikaten vertrauen, muss die „Trust Chain“ von der Issuing CA bis hoch zur Root CA lückenlos sein und die Kommunikationspartner müssen mindestens der Root CA vertrauen.

2

Vertrauen ist alles

Das ganze Prinzip von PKI beruht auf Vertrauen.
Aber ist unser Vertrauen gerechtfertigt?



In den einfachen PKI-Modellen betrachten wir immer wenige Parteien, die einander kennen und vertrauen.
In Wirklichkeit haben wir es aber mit Computern, Software und Firmen zu tun. Worauf gründen wir also unser Vertrauen?

Im Web und im Business allgemein wird Vertrauen ersetzt durch Verträge, die Firmen miteinander schließen, die wir gar nicht kennen.

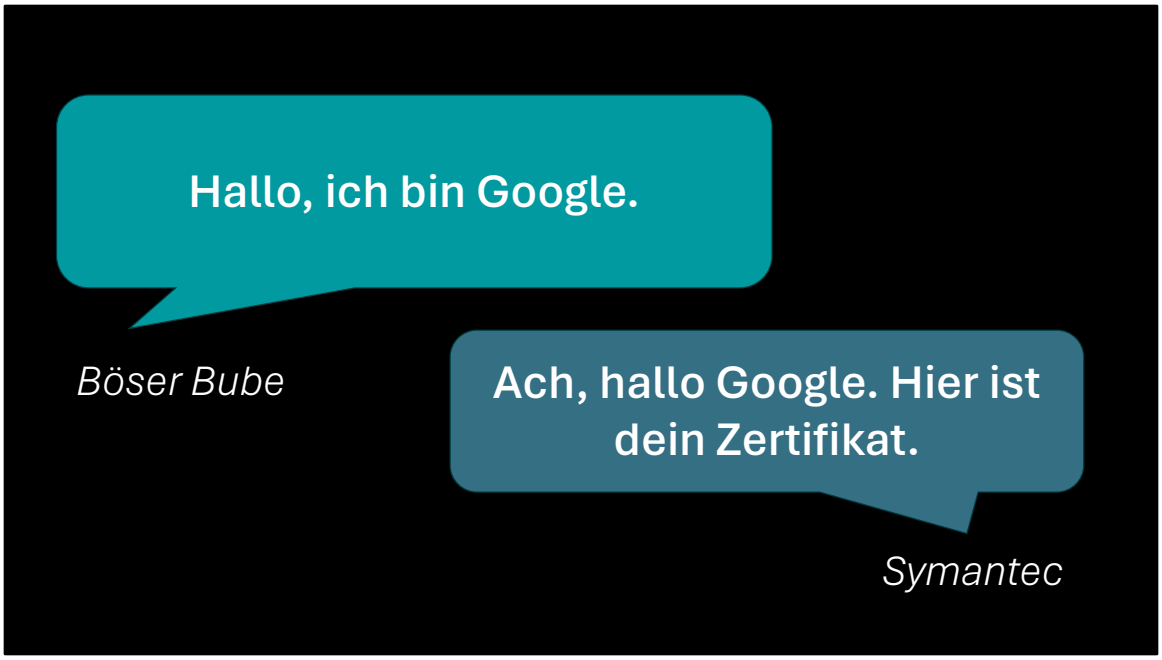
Demo: Firefox-Zertifikatsliste durchsehen (Einstellungen – Datenschutz & Sicherheit – Zertifikate – Zertifikate anzeigen)

Demo: DV-Zertifikat am Beispiel von faq-o-matic.ent

Demo: EV-Zertifikat am Beispiel des BSI
Hier ist gut erkennbar, wem man dort vertrauen soll

Demo: OV-Zertifikat am Beispiel der LBS Nord
leitet weiter auf lbs.de; Zertifikat ausgestellt für S-Communication Services GmbH, die im Impressum der Seite nicht auftauchen … vertrauenswürdig?!

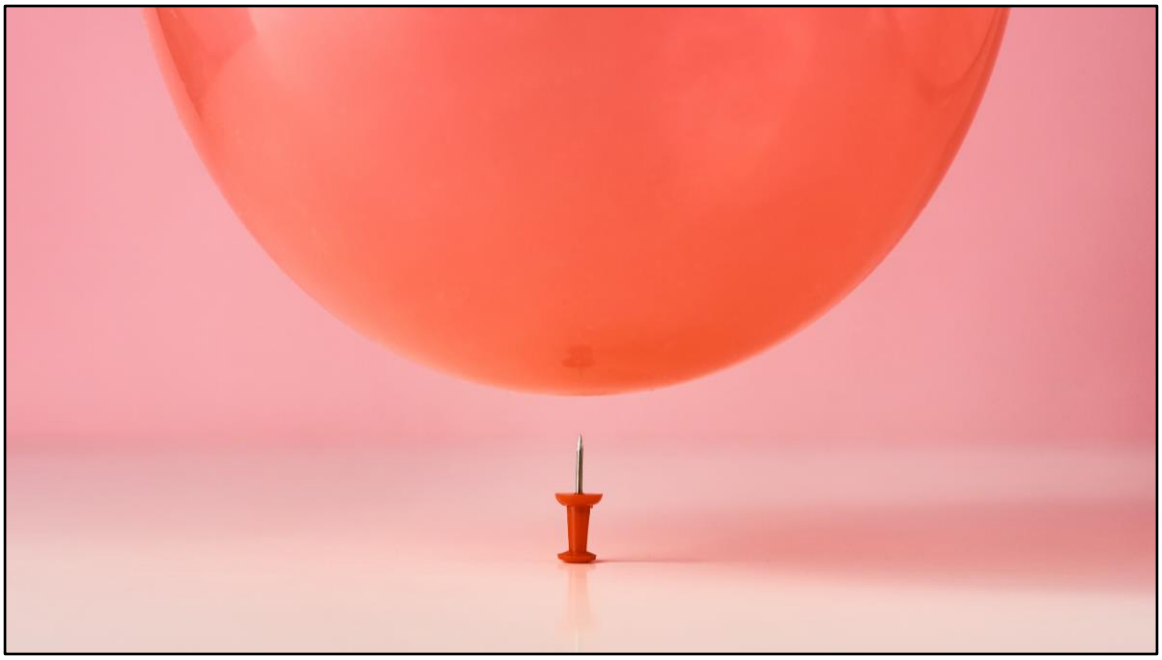
Kann man hier überhaupt von „Vertrauen“ sprechen?



... auf die Weise hat Symantec über 30.000 falsche Zertifikate ausgestellt.

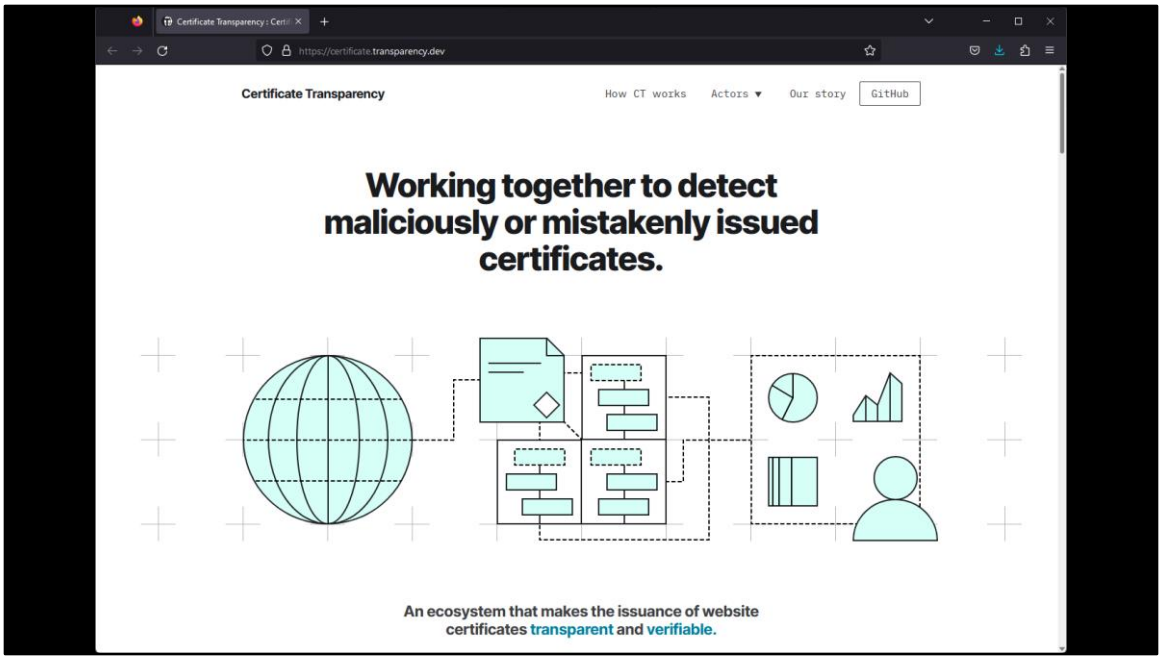
Abhilfe: Certificate Pinning (HTTP Public Key Pinning, HPKP)

Das Zertifikat gibt an, wer es ausstellen darf. Der Browser übernimmt dies beim ersten Besuch und akzeptiert für die Domain nur noch Zertifikate von der angegebenen CA.



... das führte aber dazu, dass massenhaft Domains nicht mehr erreichbar waren, weil die Web-Admins das nicht hinbekommen haben.

Kein Browser akzeptiert das Verfahren noch.



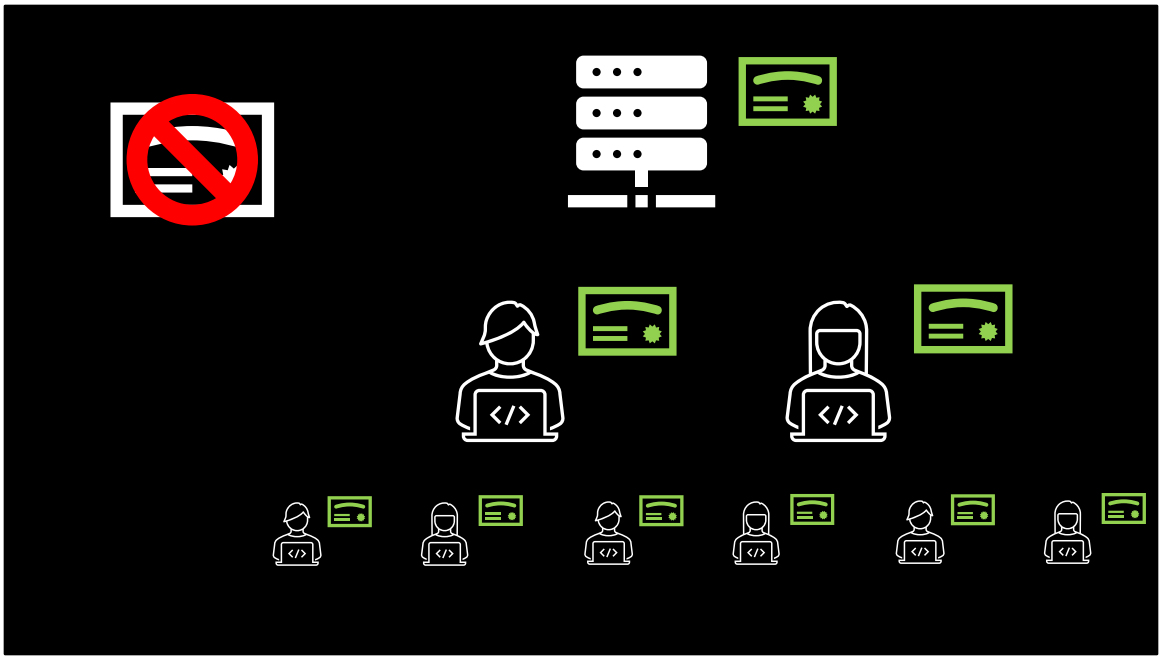
Aktueller Ansatz: Certificate Transparency

Jedes Domain-Zertifikat muss in einer CT-Datenbank stehen, sodass man prüfen kann, wer es ausgestellt hat. Chrome akzeptiert nur noch solche Zertifikate.

Demo: crt.sh (Webdienst), Beispiel für ct.de: https://crt.sh/?q=ct.de
... dabei hübsch zu sehen: offenbar gibt es Leute bei heise, die mit Webservern ihr eigenes Süppchen kochen

3

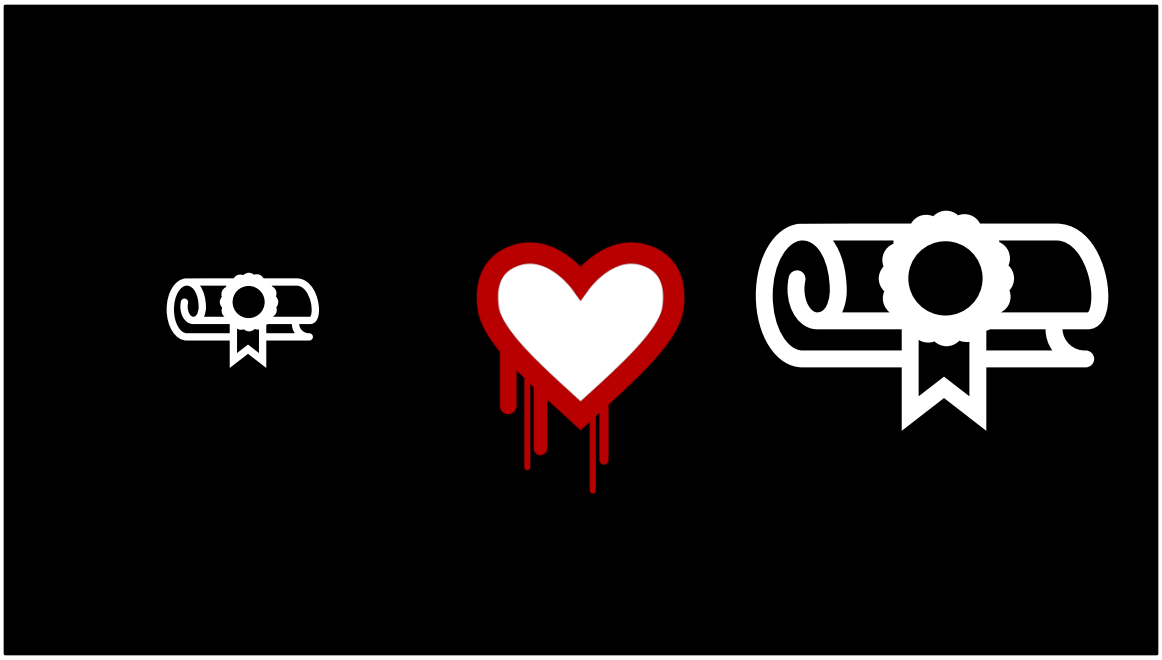
Widerrufe und Trauerspiele



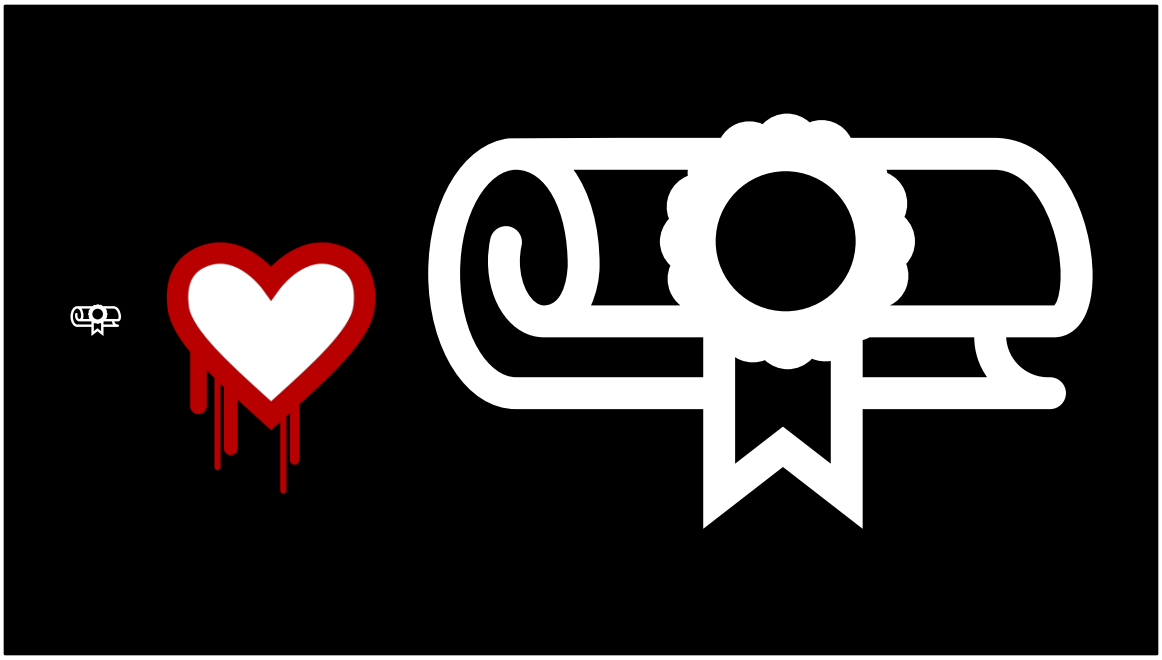
- Problem: Widerruf von Zertifikaten
  - Man müsste sofort alle informieren, die das Zertifikat nutzen, auch passiv - also alle Webseitenbesucher, Mail-Empfänger usw.
    - Nebenproblem: Wenn man dies täte, wie weist man in diesem Moment seine Identität nach?
    - Kann man nicht, also akzeptiert man das Risiko widerrufener Zertifikate …!

Demo: CRL analysieren

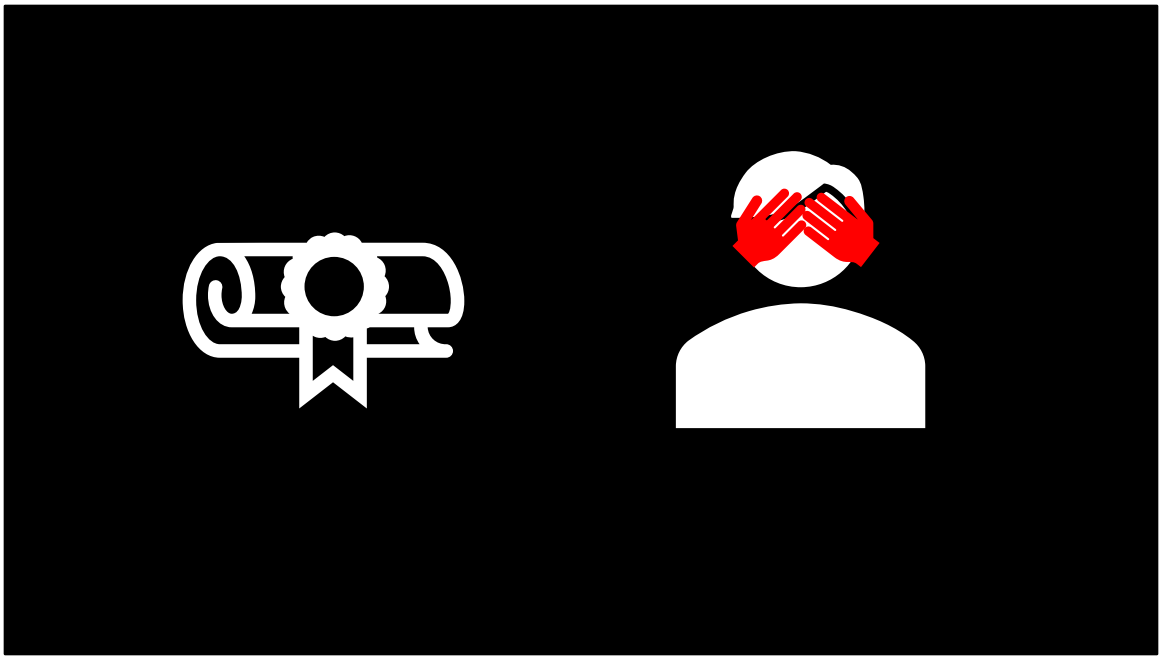
- CRL des BSI öffnen
  - http://crl.d-trust.net/crl/d-trust_ssl_class_3_ca_1_ev_2009.der.crl
- CMD: certutil -dump <Dateiname>
- Am Anfang steht die Zahl der Einträge, die ältesten Zertifikate stehen relativ weit vorne - ausrechnen, wie viele Zerts pro Jahr widerrufen werden
- Man sieht auch unterschiedliche Bearbeitungen, z.B. manchmal ein Grund angegeben, meist aber nicht; Wechsel des Seriennummern-Formats usw.



- Problem: Größe von CRLs (z.B. nach Heartbleed wuchs die CRL von Cloudflare schlagartig von 22 KB auf 4,7 MB)
    - Macht Handhabung schwierig
    - Führt dazu, dass CRLs erst gar nicht geprüft werden



- Problem: Größe von CRLs (z.B. nach Heartbleed wuchs die CRL von Cloudflare schlagartig von 22 KB auf 4,7 MB)
  - Macht Handhabung schwierig
  - Führt dazu, dass CRLs erst gar nicht geprüft werden

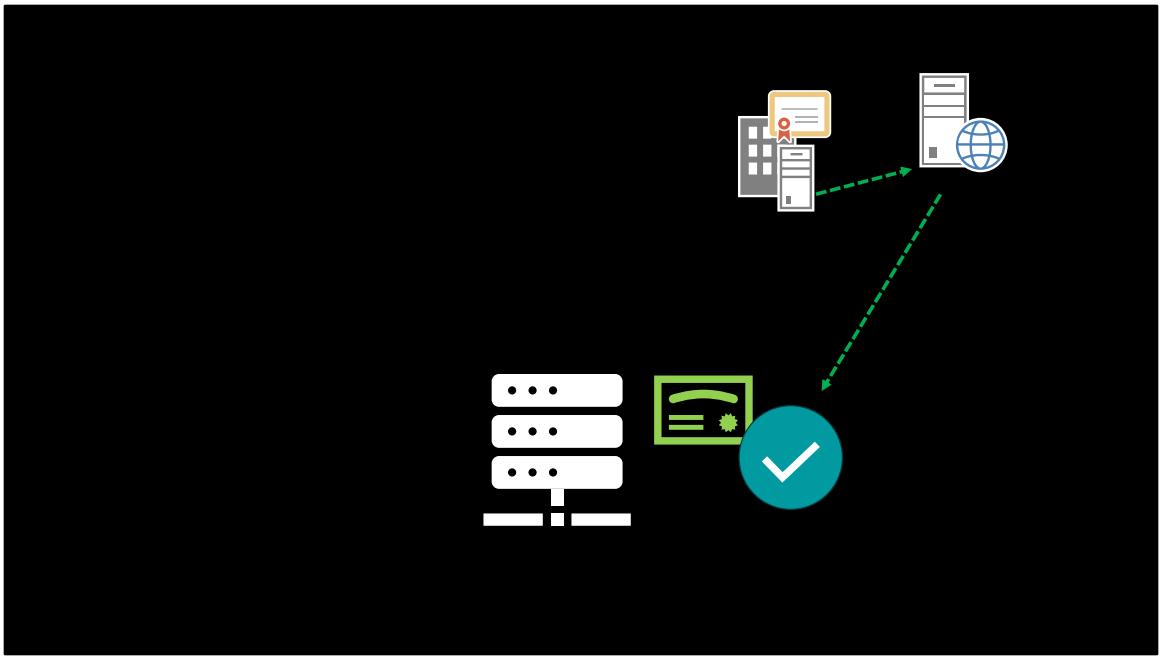


- Problem: Größe von CRLs (z.B. nach Heartbleed wuchs die CRL von Cloudflare schlagartig von 22 KB auf 4,7 MB)
    - Macht Handhabung schwierig
    - Führt dazu, dass CRLs erst gar nicht geprüft werden

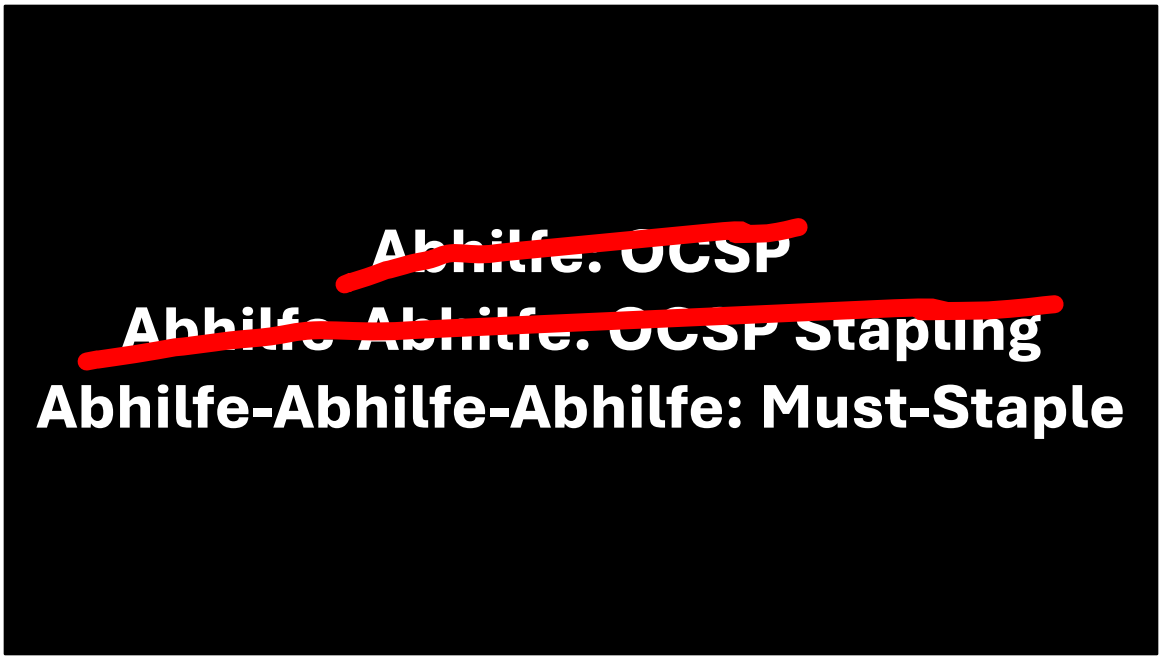
Abhilfe: OCSP

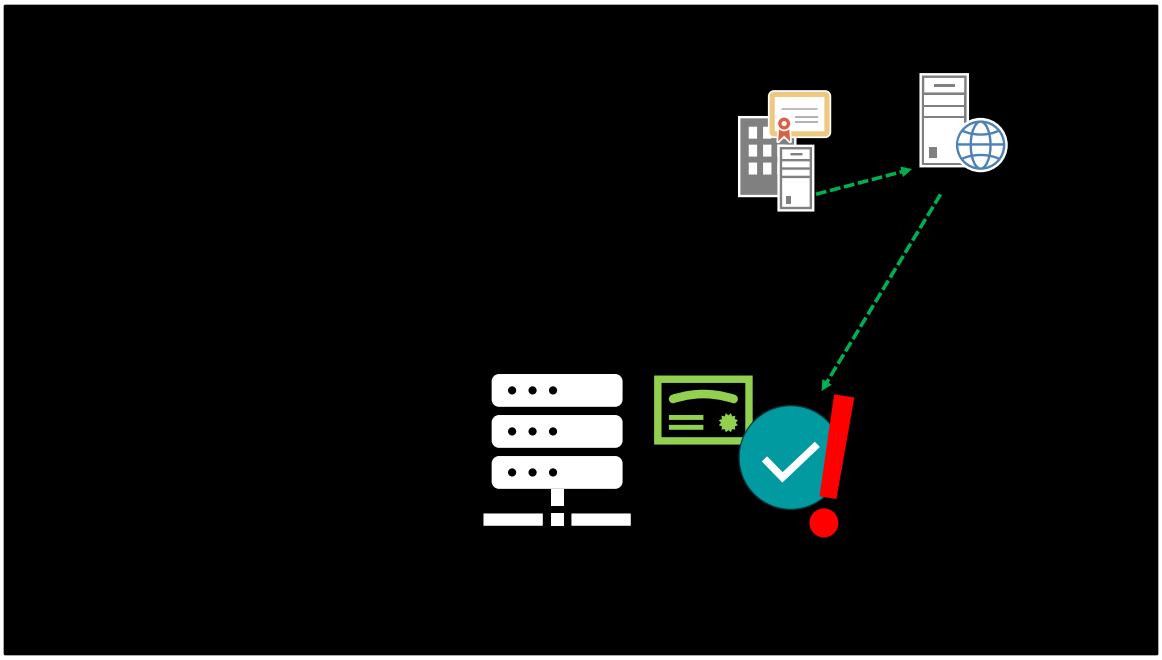
- Abhilfe: OCSP
  - Löst das Bandbreitenproblem …
  - … aber nicht das Aktualisierungsproblem
  - … und schafft ein neues Problem, weil die CA nun weiß, welche Webseite man aufrufen will
  - … ist noch dazu anfällig für Replay-Attacken, weil die Antwort mehrere Tage gültig ist und so von einem Angreifer vorgespiegelt werden könnte


Abhilfe-Abhilfe: OCSP Stapling

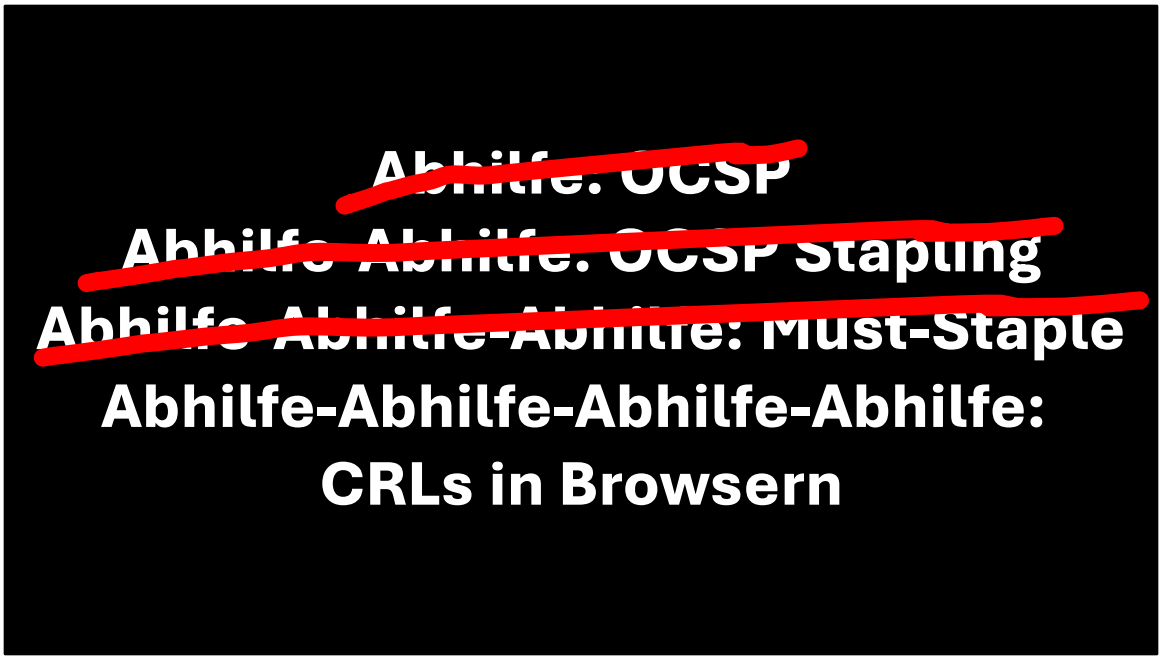


- Abhilfe-Abhilfe: OCSP Stapling
  - Webserver übermittelt die OCSP-Antwort gleich selbst mit
  - Ist aber leicht zu umgehen: Angreifer sendet einfach keine OCSP-Antwort mit …


Abhilfe: OCSP
Abhilfe-Abhilfe: OCSP Stapling
Abhilfe-Abhilfe-Abhilfe: Must-Staple



- Abhilfe-Abhilfe-Abhilfe: "Must-Staple"
  - Zertifikat kann erzwingen, dass eine OCSP-Antwort mitgeliefert wird
  - … hat aber nie ordentlich funktioniert, sich daher nicht durchgesetzt und wird auch nicht empfohlen
  - … und wäre ebenso leicht von einem Angreifer zu umgehen, der Must-Staple bei seinem Zertifikat ja auch weglassen kann
- Chrome nutzt OCSP gar nicht erst!



- Abhilfe-Abhilfe-Abhilfe-Abhilfe: CRLs in den Browsern
  - Chrome und Firefox liefern CRLs mit dem Browser aus
  - … die sind aber sehr unvollständig und nur ein Notbehelf

... in der anderen Richtung funktioniert es auch *nicht*

- User-Authentifizierung per Zertifikat gilt oft als moderner, sicherer Weg
- Tatsächlich haben wir hier aber ein verschärftes Problem, wenn ein Zertifikat widerrufen wird:
    - Der Admin der Zielumgebung erwartet, dass der User sofort nicht mehr zugreifen kann
    - Tatsächlich kommt die Zielumgebung aber nicht auf die Idee, weil sie von der Sperrung nichts weiß
    - Erst wenn die CRL planmäßig aktualisiert wurde, wirkt sich das gesperrte Zertifikat aus
- In der Praxis braucht es also noch einen separaten, zusätzlichen Mechanismus, um einen User wirksam zu sperren, sodass er nicht mehr zugreifen kann
    - … und das Problem, dass ein möglicherweise gestohlenes Zertifikat noch akzeptiert wird, lässt sich auch nur in der Zielumgebung beheben, indem dort das Zertifikat ausgetauscht wird

Und nun?

4

It’s the Sorgfalt, stupid!

- PKI = Sicherheitskomponente
- Entweder macht man es richtig, oder man lässt es

- Die natürlichen Feinde der PKI:
  - Der "Passt schon"
  - Und der "Mal eben" (mit seiner Unterart "Mal eben schnell")

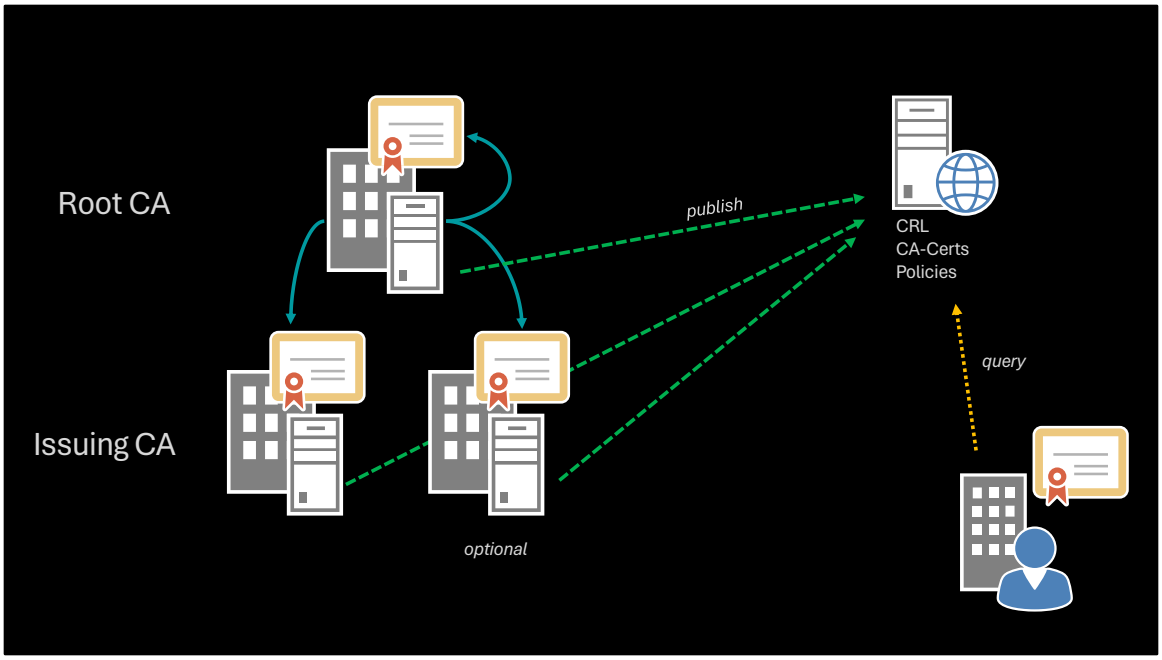
Meine eigene PKI

Nur dann eine PKI betreiben, wenn man sie wirklich braucht

Meine eigene PKI

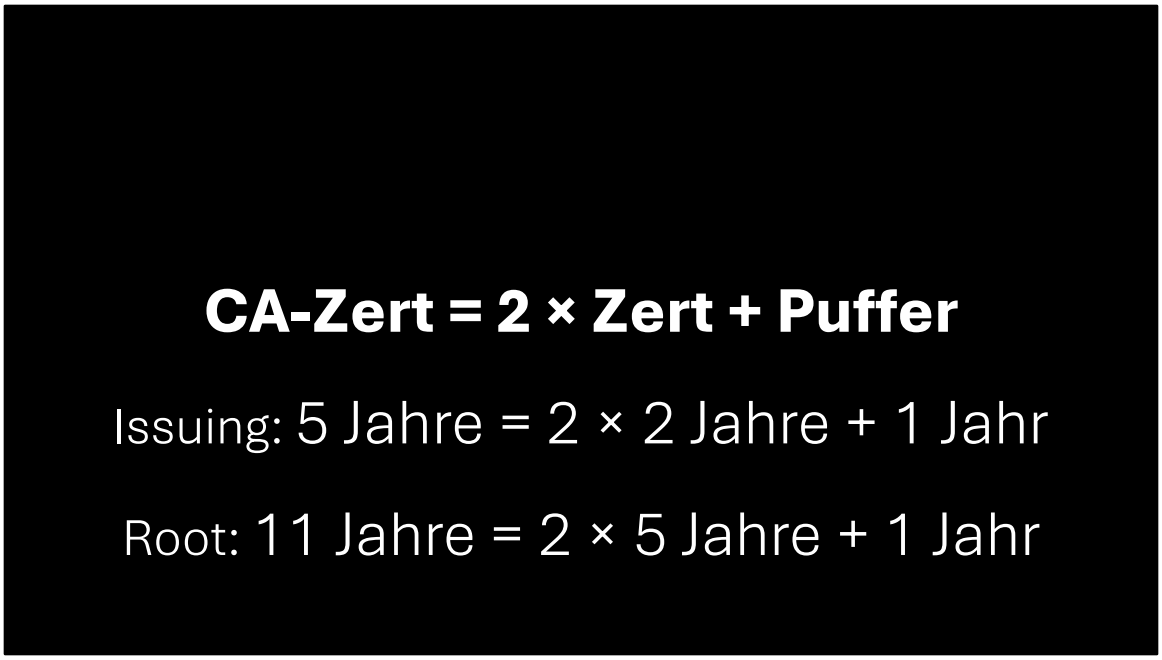
1. Lass es bleiben
2. Mach es richtig

Nur dann eine PKI betreiben, wenn man sie wirklich braucht



- 2-stufig
  - Eine Offline-Root
  - Typ. eine Issuing CA; mehrere nur bei Bedarf
- Kalkulierte CA-Zertifikats-Laufzeiten
  - 2 Jahren Maximum für Zerti´fikate mit 1 Jahr als Standard
  - CA-Zertifikate nach Formel berechnen (Issuing 5 Jahre, Root 11 Jahre)
- Genau ein Verteilpunkt und ein CRL-Punkt
  - Intern wie extern identisch erreichbar (ein externer Webserver)
  - tendenziell redundant
- Gesicherte Backups
  - Alles sichern
  - Nicht als Image/VM (oder nur zusätzlich)
  - Zugriff aufs Backup strikt beschränken
- Selektive Vorlagen, minimal automatisiert
  - Insbes. nur dann autom. Ausstellen, wenn nötig
- Kompetenter Betrieb
  - Renewals
  - Updates
  - Offline = offline

    - Monitoring
- Wo immer es geht, kommerzielle Zertifikate einsetzen



Formel, um die Laufzeit von CA-Zertifikaten zu berechnen

„Zert“: maximale Laufzeit ausgestellter Zertifikate

Buchtipp:

Peter Kloep: PKI und CA in Windows-Netzwerken. Das umfassende Handbuch, Rheinwerk 2024 (3. Auflage), ISBN ISBN 978-3-8362-9641-0

Take care of your Zertifikat

Mit Zertifikaten nicht schludern

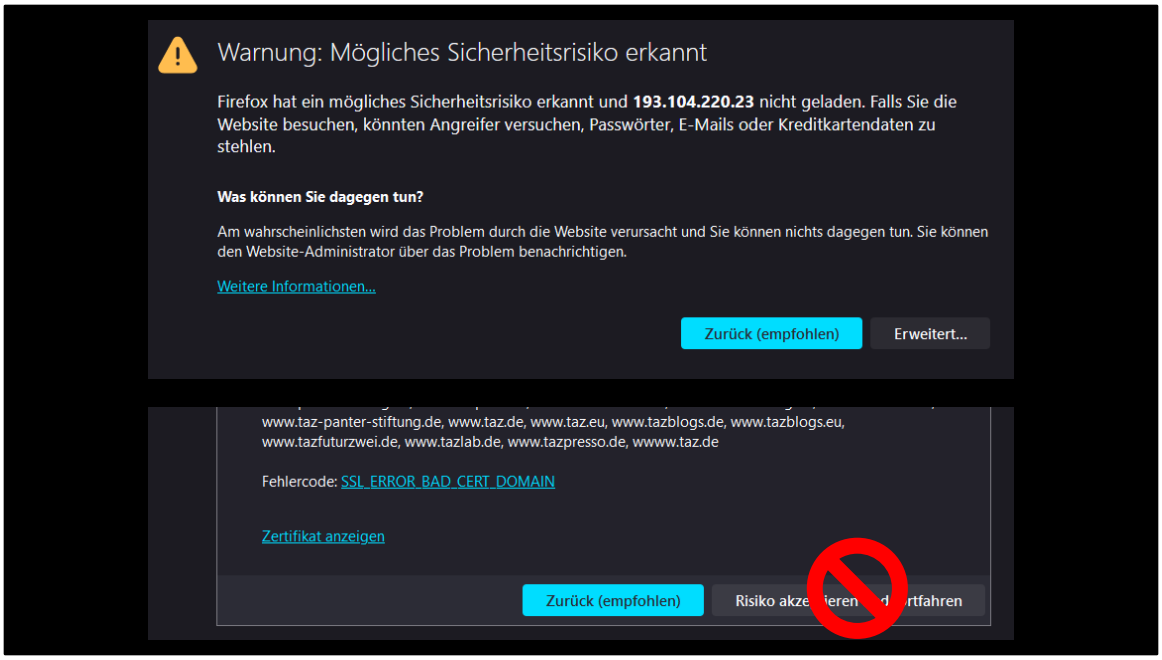
Foto: Beth Macdonald
https://unsplash.com/de/fotos/brauner-holztisch-und-stuhle-a1O67ZQmaYc

Private Schlüssel privat halten: Zertifikate nur mehrfach nutzen, wenn es gar nicht anders geht

Bild: Anna Zhakarova, https://unsplash.com/de/fotos/eine-gruppe-von-metallschlusseln-die-auf-einem-tisch-sitzen-CdJN7JFVLd8

CAs meiden, die den privaten Schlüssel selbst mit erzeugen

Foto: Dan Dennis, https://unsplash.com/de/fotos/gelbe-plastiktute-auf-braunem-teppich-Bo9v-I7lGKY



Zertifikatswarnungen und -fehler nicht ignorieren

Call to Action: Was könnt ihr mitnehmen?

1. Nehmt Zertifikate ernst, arbeitet euch ein, schaut hin
2. Sorgfalt statt Bequemlichkeit
3. Betreibt keine eigene PKI, aber wenn doch, dann ordentlich


Vielen Dank an unsere Sponsoren!
Platinum
primeLine SOLUTIONS
Mainzer Datenfabrik
Lenovo
VANQUISH
Ihr VAD für Managed Services & Cloud Access
FUJITSU
bluechip
CREATING COMPUTERS.
Gold
SVA
THOMAS KRENN
TD SYNNEX
Hewlett Packard Enterprise
control UP
SquaredUp
DELL Technologies
PATCH MY PC
VANQUISH
Ihr VAD für Managed Services & Cloud Access
Silber
NiCE
reinheimer_systemlösungen
MAT
Experts Live Germany


Bitte gebt uns euer Feedback!
Feedback geben und Geschenk mitnehmen
Vielen Dank!
ATD | SYSTEMHAUS
Experts Live Germany