Certificate Pinning

Sparkassen-Finanzportal GmbH [DE] | https://www.sparkasse.de

Sparkasse

Wonach suchen Sie?

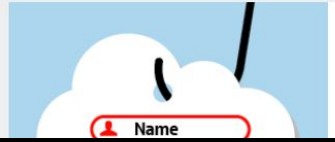
Online-Banking

Ihre Pläne | Unsere Lösungen | Geld einfach verstehen | #Gemeinsam | Service

Entscheiden ist einfach.

Mehr rausfinden

Online-Banking | Girokonto | Autokredit | Baufinanzierung | Geldanlage | Karriere



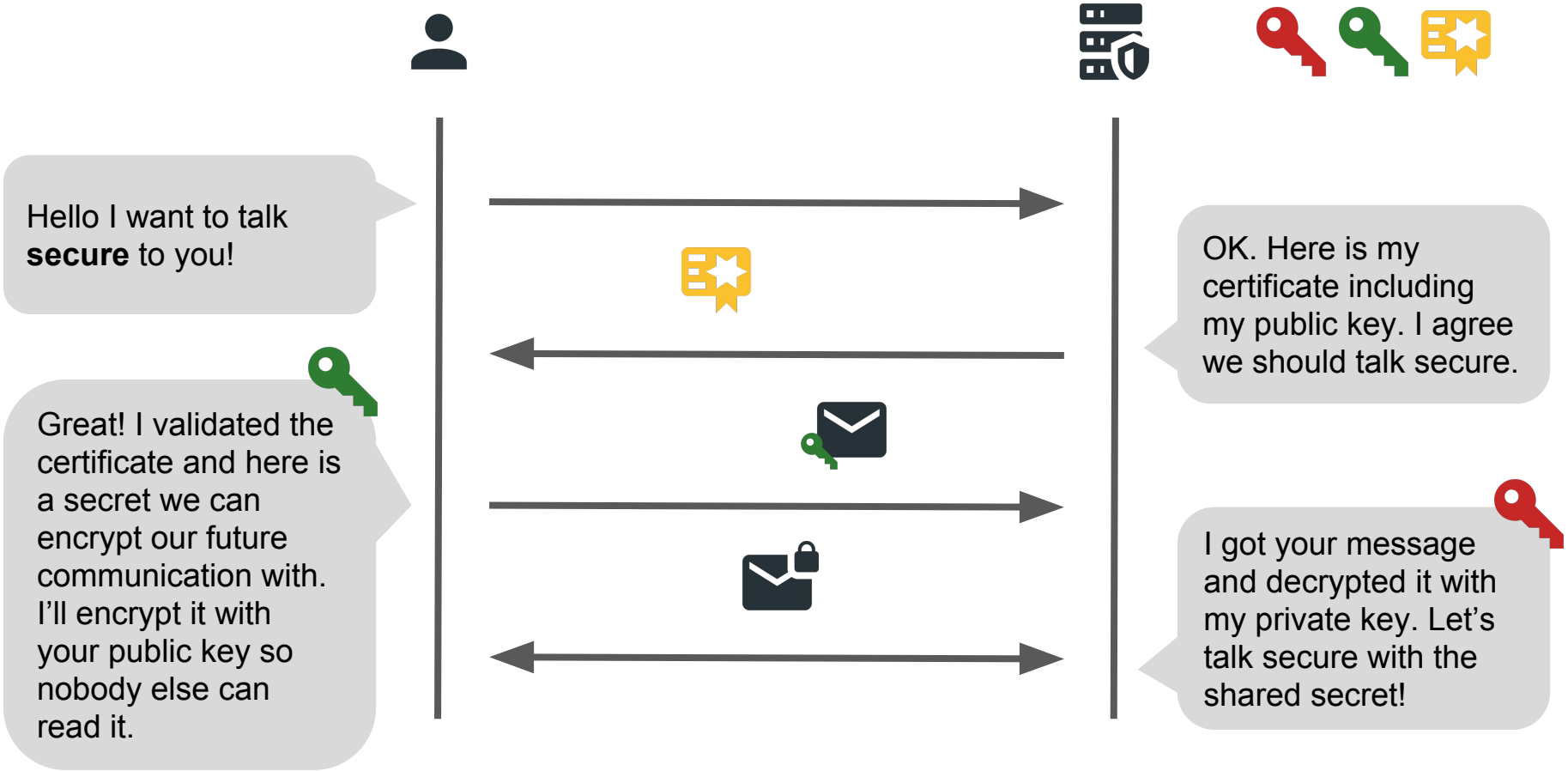
Vorsicht Phishing!

Passen Sie auf: Zurzeit sind wieder vermehrt Phishing-E-Mails im Umlauf. Beim Phishing versuchen Betrüger, an Ihre Daten und Passwörter zu kommen

Service

Filiale suchen

Filiale...


Hello I want to talk **secure** to you!
OK. Here is my certificate including my public key. I agree we should talk secure.
Great! I validated the certificate and here is a secret we can encrypt our future communication with. I'll encrypt it with your public key so nobody else can read it.
I got your message and decrypted it with my private key. Let's talk secure with the shared secret!

Certificate

Name: ...
Organization: …
Address: my domain
…
My Public Key:

Certificate Authority (CA) verifies the identity and encrypts with its own private key

Certificate

Name: ...
Organization: …
Address: my domain
…
My Public Key:

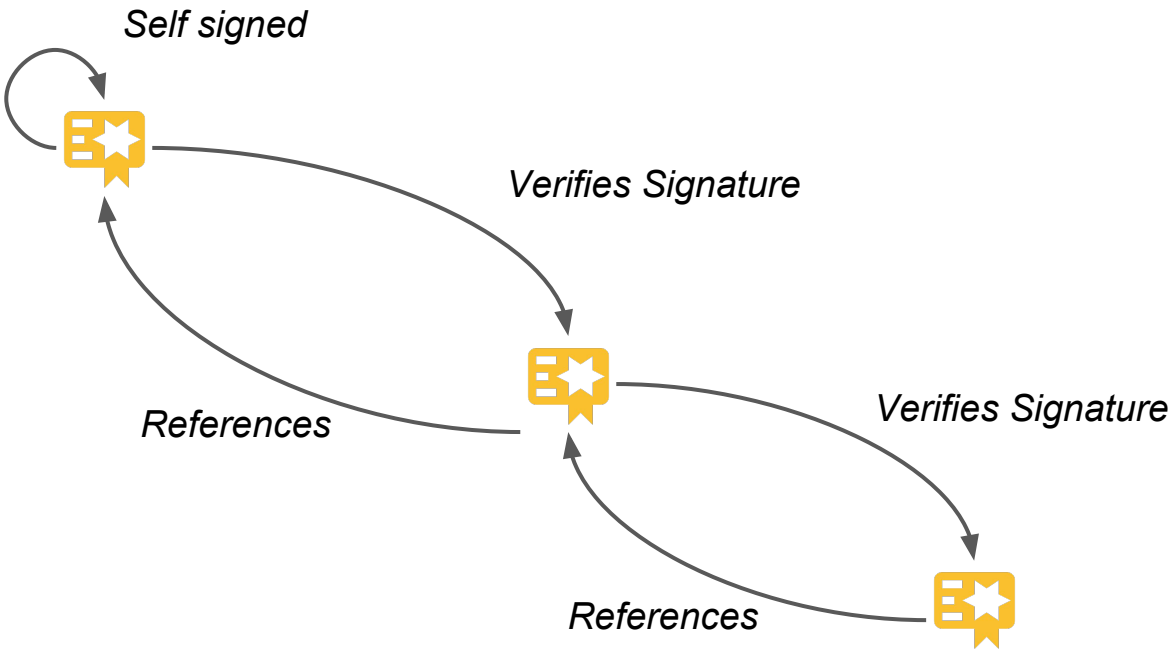
Digital signature of the certificate body by the CA

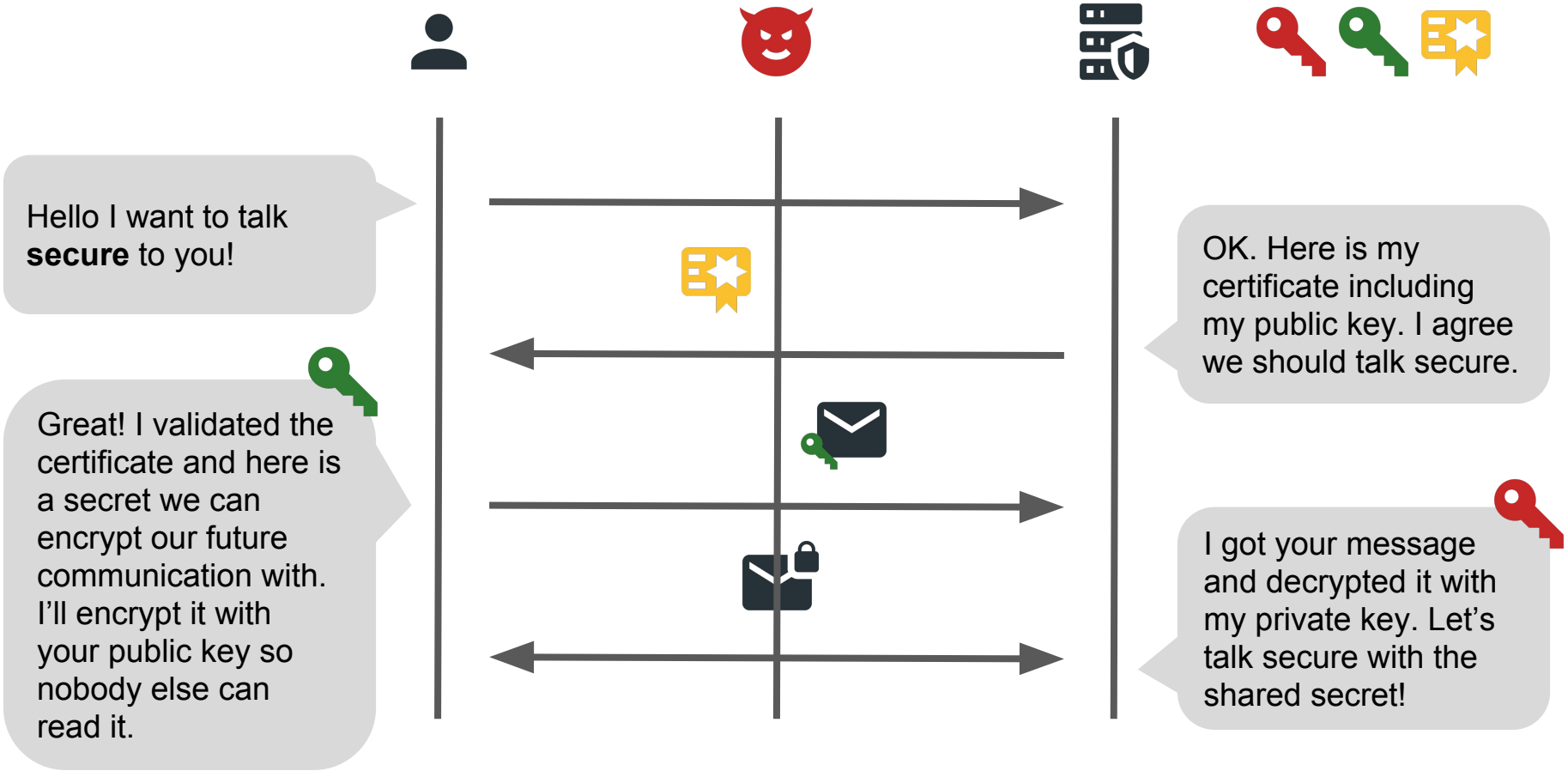
Chain of trust

Root Certificate

Intermediate Certificate

Leaf Certificate

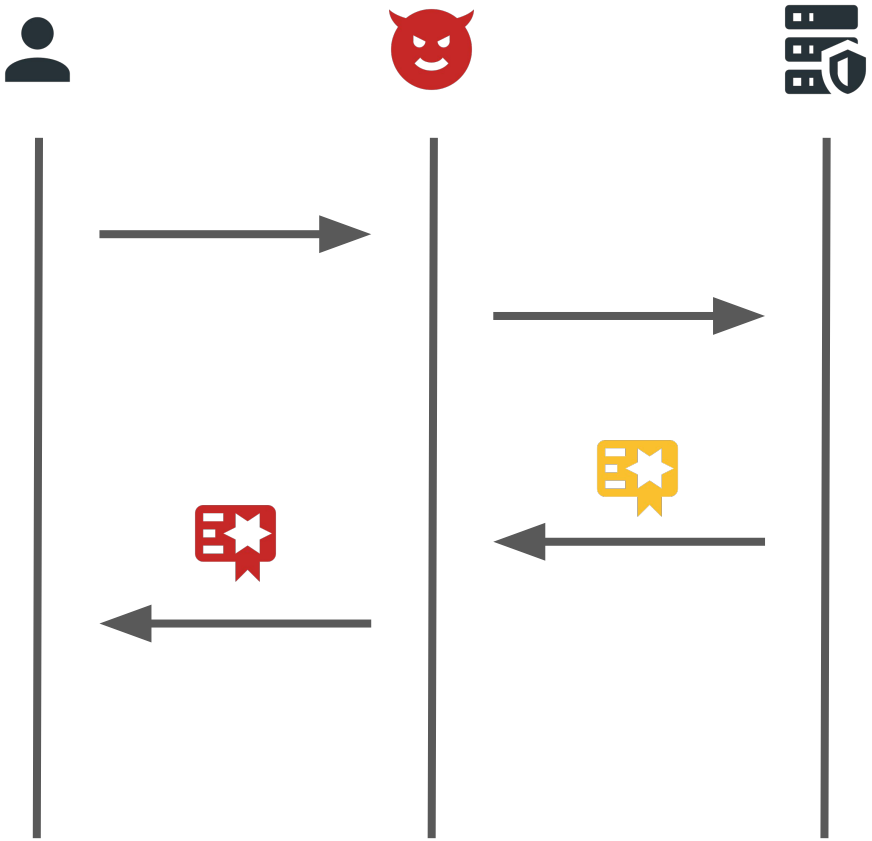


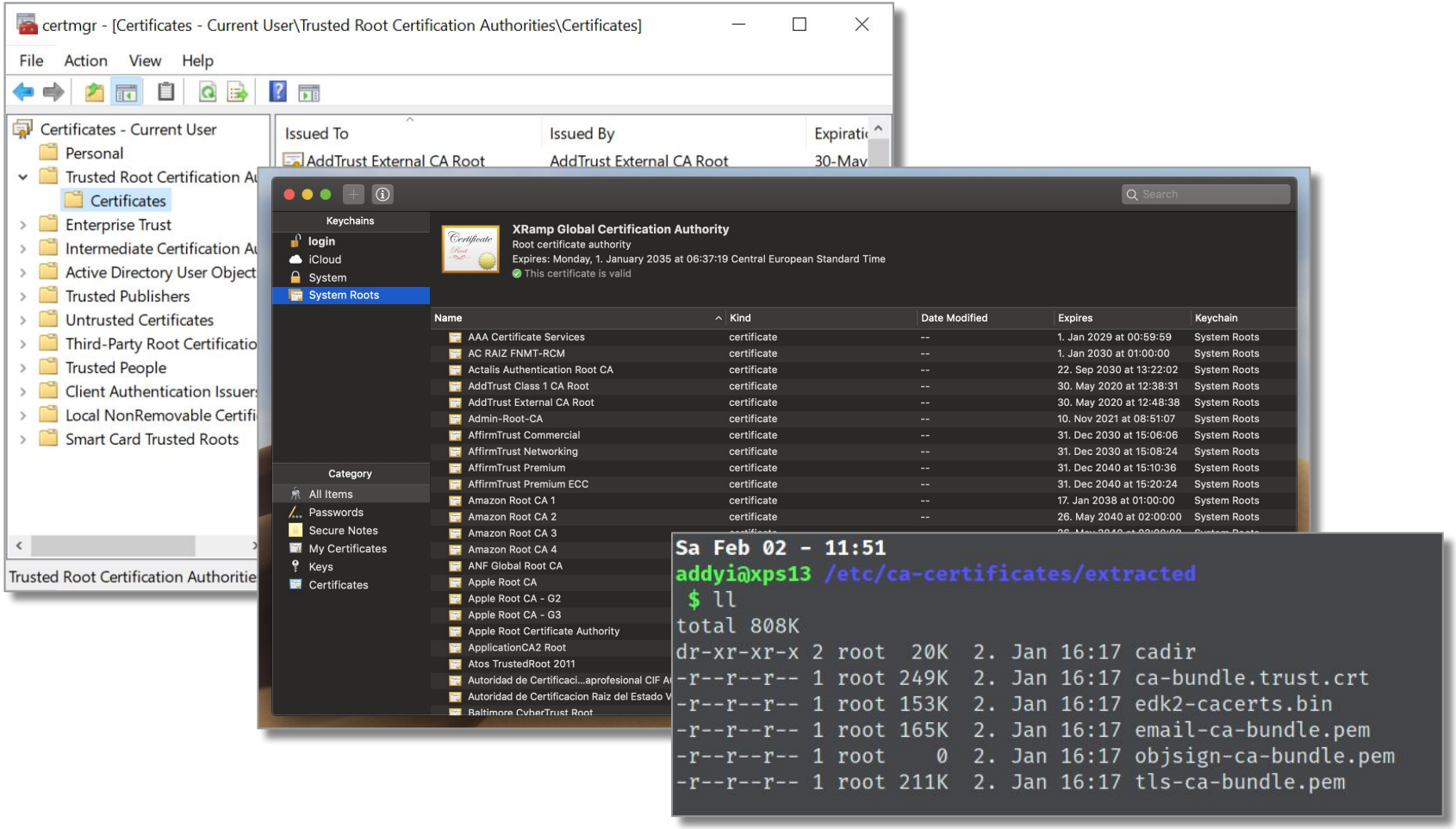

Hello I want to talk **secure** to you!
OK. Here is my certificate including my public key. I agree we should talk secure.
Great! I validated the certificate and here is a secret we can encrypt our future communication with. I'll encrypt it with your public key so nobody else can read it.
I got your message and decrypted it with my private key. Let's talk secure with the shared secret!

MITM-Attack

MITM-Attack

- Man In The Middle
- MITM returns wrong certificate
- MITM-techniques:
  - ARP cache poisoning
  - DNS spoofing
  - Public WIFI (restaurants, ...)
- Fraud prevention via Trust Store / Keychain
- Pre installed certificates




certmgr - [Certificates - Current User\Trusted Root Certification Authorities\Certificates]
File Action View Help
Certificates - Current User
Personal
Trusted Root Certification Au
Certificates
Enterprise Trust
Intermediate Certification Au
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certificatio
Trusted People
Client Authentication Issuers
Local NonRemovable Certifi
Smart Card Trusted Roots
Issued To
Issued By
AddTrust External CA Root
AddTrust External CA Root
Trusted Root Certification Authoritie
Keychains
login
iCloud
System
System Roots
Category
All Items
Passwords
Secure Notes
My Certificates
Keys
Certificates
XRamp Global Certification Authority
Root certificate authority
Expires: Monday, 1. January 2035 at 06:37:19 Central European Standard Time
This certificate is valid
Name
Kind
Date Modified
Expires
Keychain
AAA Certificate Services certificate -- 1. Jan 2029 at 00:59:59 System Roots
AC RAIZ FNMT-RCM certificate -- 1. Jan 2030 at 01:00:00 System Roots
Actalis Authentication Root CA certificate -- 22. Sep 2030 at 13:22:02 System Roots
AddTrust Class 1 CA Root certificate -- 30. May 2020 at 12:38:31 System Roots
AddTrust External CA Root certificate -- 30. May 2020 at 12:48:38 System Roots
Admin-Root-CA certificate -- 10. Nov 2021 at 08:51:07 System Roots
AffirmTrust Commercial certificate -- 31. Dec 2030 at 15:06:06 System Roots
AffirmTrust Networking certificate -- 31. Dec 2030 at 15:08:24 System Roots
AffirmTrust Premium certificate -- 31. Dec 2040 at 15:10:36 System Roots
AffirmTrust Premium ECC certificate -- 31. Dec 2040 at 15:20:24 System Roots
Amazon Root CA 1 certificate -- 17. Jan 2038 at 01:00:00 System Roots
Amazon Root CA 2 certificate -- 26. May 2040 at 02:00:00 System Roots
Amazon Root CA 3
Amazon Root CA 4
ANF Global Root CA
Apple Root CA
Apple Root CA - G2
Apple Root CA - G3
Apple Root Certificate Authority
ApplicationCA2 Root
Atos TrustedRoot 2011
Sa Feb 02 - 11:51
addyi@xps13 /etc/ca-certificates/extracted
$ ll
total 808K
dr-xr-xr-x 2 root 20K 2. Jan 16:17 cadir
-r--r--r-- 1 root 249K 2. Jan 16:17 ca-bundle.trust.crt
-r--r--r-- 1 root 153K 2. Jan 16:17 edk2-cacerts.bin
-r--r--r-- 1 root 165K 2. Jan 16:17 email-ca-bundle.pem
-r--r--r-- 1 root 0 2. Jan 16:17 objsign-ca-bundle.pem
-r--r--r-- 1 root 211K 2. Jan 16:17 tls-ca-bundle.pem

Trust Store

- Are we safe now?
- CA loses control
  - DigiNotar (Google Security Blog)
  - GlobalSign
  - Comodo
- Social Engineering
  - Elektronisches Anwaltspostfach (beA) by BRAK

Google Security Blog

The latest news and ins

An update on

August 29, 2011

Posted by Heather Adki

Today we received r

Google users, where

services. The peopl

fraudulent SSL certi

not issue certificate

Google Chrome use

detect the fraudulen

Root-Zertifikat führt zu Sicherheitsrisiko

Wie bereits unter [beA-Zertifikat zurückgezogen] und [Sondernewsletter der BRAK] berichtet, gab es am 22.12.2017 Komplikationen mit einem für das beA notwendigen Zertifikat. Dieses war nicht abgelaufen, wie teilweise berichtet worden, sondern es musste gemäß der Richtlinien (siehe hierzu: „About the Baseline Requirements") des CA/Browse Forum zurückgezogen werden.

Zertifikat musste zurückgezogen werden

Die Baseline Requirements regeln in der Ziffer *4.9. CERTIFICATE REVOCATION AND SUSPENSION / 4.9.1. Circumstances for Revocation / **4.9.1.1. Reasons for Revoking a Subscriber Certificate*** genau, unter welchen Umständen Zertifikate zurückzogen werden müssen. So müssen die Zertifizierungsstellen eine Zertifikat zurückziehen, dessen privater Schlüssel als nicht mehr sicher gilt oder weil der private Schlüssel bekannt gemacht wurde und damit als kompromittiert gilt.

Die aktuelle Version 1.5.4 der Baseline Requirements finden Sie hier.

So war aufgefallen, dass der im Rahmen des **beA** notwendig **beA**-Client bei der Installation auch den privaten Schlüssel des verwendeten Zertifikats auf den Client mit aufgespielt hatte.

Dies hatte heise online am 22.12.2017 berichtet – Schwere Panne beim elektronischen Anwaltspostfach.

- What can I do as a **web** user?
  - Check the grey/green padlock
  - Check the certificate
  - Check the chain of trust (CA)
- What can I do as an **app** user?
  - ¯_(ツ)_/¯
  - Trust the developer
  - I can't even verify that they are using SSL/TLS for their API
- What can I do as an **app** developer for my users?
  - Use a TLS secured API
  - ⇒ Certificate Pinning

Certificate Pinning

Certificate Pinning

- Detect and block many kinds of MITM attacks
- Extra step beyond the normal X.509 certificate validation
- (Application is shipped with pin)
- Pin demands specific certificate or which certificate must be in the chain of trust

Subject Public Key Info

```
04 6F F4 83 79 E4 50 FF ED 3A 75 D0 26 C5 FA 17
91 E2 56 66 9F 4C 67 82 0D 7E DB 42 93 3A 0D 02
8F 2A E5 05 08 BA 01 7A 80 01 BB DE D1 2C F3 AD
C4 C6 1A EB 6E 47 A7 DE A7 18 BE DA E7 37 6A 0A
7B
```

SHA-256
Base64

```
sha256/y2HhTRXXLdmAF1esYBb/muQUl3BIBdmEB8jUv
MrGc28=
```

Demo

- MITM-Attack with `mitmproxy` against Android Emulator
- A malicious certificate has been pre-installed on the Emulator
- GET Request to GitHub API
  - Unpinned
  - Pinned

- Code: https://github.com/addyi/CertPin

Challenges and Decision

- Protection
  - Protects the client, but not the server
  - Harder to snoop API
- Bypassing Certificate Pinning
  - Decompile & Recompile
  - Obfuscation
  - Harder not impossible
- WebView of an App
- `network_security_config.xml`
  - Min SDK 24
  - approx. 50% usage (Oct 2018)
- Emergency plan: Private Key leak?
- Pin against which certificate?
  - Root
  - Intermediate
  - Leaf
- Fail Hard or Fail Soft?
- Where to store the pin?
  - Hard coded in the app
  - Trust on first use
  - Pin server (pinned obviously)

Conclusion

Conclusion

- Process of secure connection
- MITM-Attack planned and executed
- Protected our users with Certificate Pinning
- Challenges and Decisions
- Objective: To ensure that our counterpart is the one he claims to be

Sources

- Matthew Dolan. *Android Security: SSL Pinning*. 13.01.2017. https://medium.com/@appmattus/1db8acb6621e (last seen 02.12.2018)
- Felipe Lima. *Bypassing Certificate Pinning on Android for fun and profit*. 05.03.2016. https://medium.com/@felipecsl/1b0d14beab2b (last seen 02.12.2018)
- Mark Allison. *Certificate Pinning ---- Part 1-3*. 26.10.2018. https://blog.stylingandroid.com/certificate-pinning-part-1/ (last seen 02.12.2018)

Image Sources

- Key Chain Icon: https://support.apple.com/en-us/HT204085 (last seen 12.02.2019)
- Icons are from: https://materialdesignicons.com/
- Some Screenshots

https://github.com/addyi/CertPin

Adrian Renner @addyi89

- What can I do as an **web** developer for my users?
  - There is “trust on first use” Certificate Pinning in the Browser but there is a lot of criticism
  - https://www.heise.de/security/artikel/Wachsende-Kritik-an-Public-Key-Pinning-fuer-HTTPS-3324703.html
  - https://en.wikipedia.org/wiki/Certificate_Transparency pushed by Google