x.509 - Hur hamnade vi här och vad kan vi göra åt saken

Jonatan Walck

jonatan@xwalck.se
xwalck AB

2012-10-18

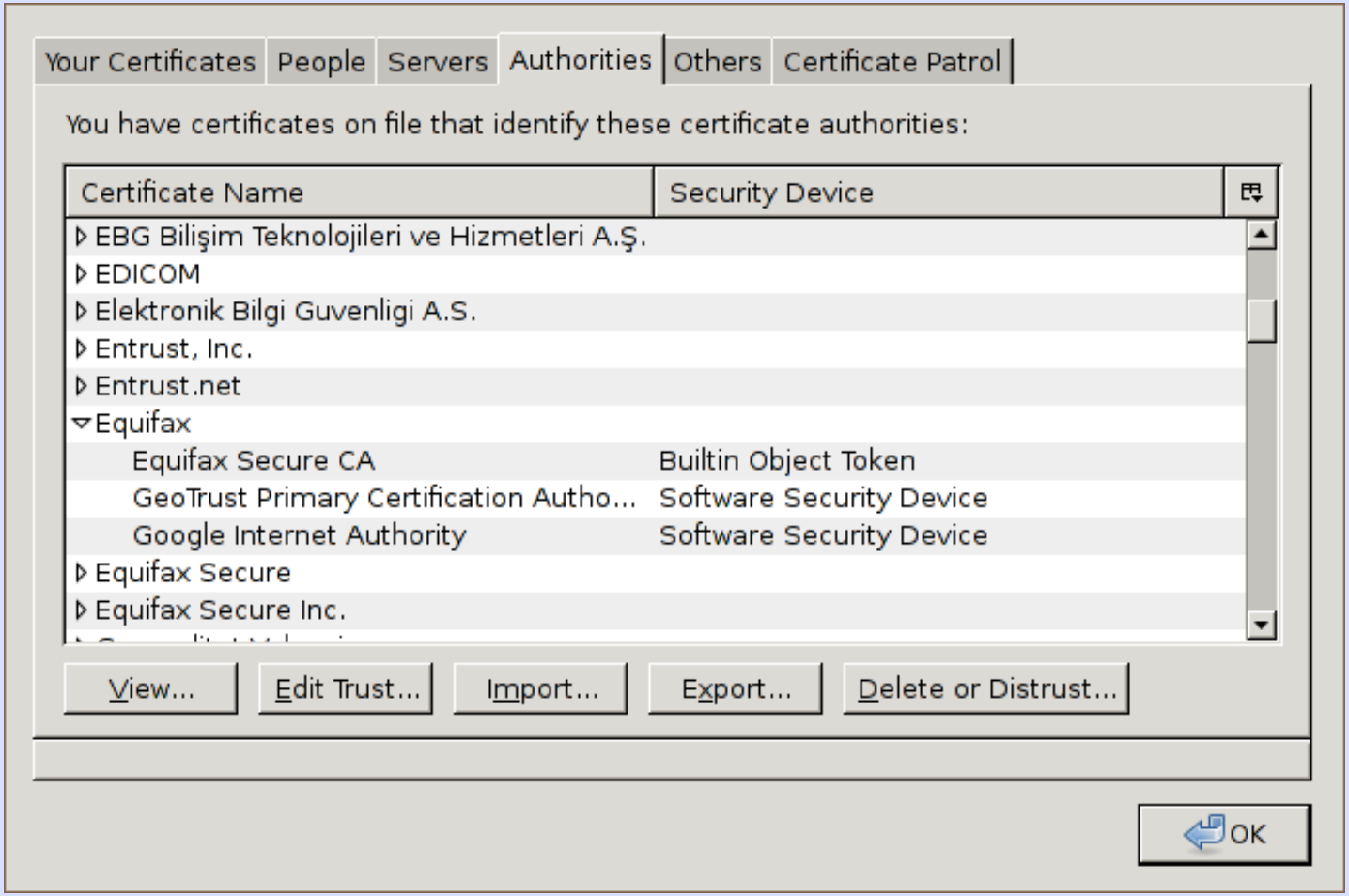
x.509 - Hur hamnade vi här och vad kan vi göra åt saken

- HTTPS - grunder
  - x.509 (PKIX)
- Andra säkerhetsproblem i WWW
  - Internet Explorer
  - BEAST och CRIME
- Tekniska utvägar
  - Begränsad CA-lista
  - Monkeysphere
  - Convergence
  - DNSSEC (DNS+DANE)
  - Darknets
- Sociala lösningar

CA hierarkin i korthet

- Strikt hirarkisk tillit
- Lista på auktoriteter i varje webbläsare
  - Subdeligeringar från dessa
- Fleratal “rouge” CA:s ute
  - Comodo 2011
  - Diginotar 2011-09
  - ???
  - (No) PROFIT!
- EV

Auktoriteter i Firefox



Exempel på ett certifikat

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 36876 (0x900c)
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=SE, O=xwalck AB, CN=xwalck Certificate Authority/emailAddress=info@xwalck.se
        Validity
            Not Before: Sep 24 21:54:29 2012 GMT
            Not After : Sep 24 21:54:29 2013 GMT
        Subject: C=SE, O=xwalck AB, CN=xwalck.se
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
                Modulus:
                    00:92:d3:c2:c9:c5:48:27:8a:96:9c:ff:2b:25:9e:
                    ... ... ...
                    b2:d3:9b
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                E8:D6:06:4A:A5:A3:F4:9C:C7:2E:FA:BE:26:D3:58:97:B8:58:D9:D5
            X509v3 Authority Key Identifier:
                keyid:ED:50:D9:07:5C:0F:3E:A6:33:C8:AA:33:5E:46:F5:94:15:68:C5:1C

            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Key Usage: critical
                Digital Signature, Non Repudiation, Key Encipherment
            Netscape Cert Type:
                SSL Server
            X509v3 Extended Key Usage:
                TLS Web Server Authentication
            X509v3 Subject Alternative Name:
                DNS:xwalck.se, DNS:www.xwalck.se
    Signature Algorithm: sha1WithRSAEncryption
         31:4d:6d:26:6c:d4:15:37:bd:d9:43:dc:97:78:00:49:00:2e:
         ... ... ...
         4d:37:49:da:3a:4a:b9:b9
```

Exempel på ett certifikat (2)

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 36876 (0x900c)
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=SE, O=xwalck AB ...
        Validity
            Not Before: Sep 24 21:54:29 2012 GMT
            Not After : Sep 24 21:54:29 2013 GMT
        Subject: C=SE, O=xwalck AB, CN=xwalck.se
        X509v3 extensions:
          ... ... ...
            X509v3 Subject Alternative Name:
                DNS:xwalck.se, DNS:www.xwalck.se
```

x.509 - Hur hamnade vi här och vad kan vi göra åt saken

- HTTPS - grunder
  - x.509 (PKIX)
- Andra säkerhetsproblem i WWW
  - Internet Explorer
  - BEAST och CRIME
- Tekniska utvägar
  - Begränsad CA-lista
  - Monkeysphere
  - Convergence
  - DNSSEC (DNS+DANE)
  - Darknets
- Sociala lösningar

Internet Explorer

Behöver det ens nämnas?

x.509 - Hur hamnade vi här och vad kan vi göra åt saken

- HTTPS - grunder
  - x.509 (PKIX)
- Andra säkerhetsproblem i WWW
  - Internet Explorer
  - BEAST och CRIME
- Tekniska utvägar
  - Begränsad CA-lista
  - Monkeysphere
  - Convergence
  - DNSSEC (DNS+DANE)
  - Darknets
- Sociala lösningar

BEAST - Browser Exploit Against SSL/TLS

- September 2011
- Påverkar TLS 1.0 och tidigare (TLS 1.1 släpptes 2006)

CRIME - Compression Ration Info-leak Made Easy

- September 2012
- Kan hämta ut en sessionskaka från en HTTPS-skyddad länk.

x.509 - Hur hamnade vi här och vad kan vi göra åt saken

- HTTPS - grunder
  - x.509 (PKIX)
- Andra säkerhetsproblem i WWW
  - Internet Explorer
  - BEAST och CRIME
- Tekniska utvägar
  - Begränsad CA-lista
  - Monkeysphere
  - Convergence
  - DNSSEC (DNS+DANE)
  - Darknets
- Sociala lösningar

Färre auktoriteter

- Inte en lösning utan primärt nya problem
- Kostnaden av att ta bort ett root CA...

x.509 - Hur hamnade vi här och vad kan vi göra åt saken

- HTTPS - grunder
  - x.509 (PKIX)
- Andra säkerhetsproblem i WWW
  - Internet Explorer
  - BEAST och CRIME
- Tekniska utvägar
  - Begränsad CA-lista
  - Monkeysphere
  - Convergence
  - DNSSEC (DNS+DANE)
  - Darknets
- Sociala lösningar

Monkeysphere - OpenPGP WOT certifikat

- Ingen ökad säkerhet utan kunskapsnivå
- Kräver ändringar hos klienten

x.509 - Hur hamnade vi här och vad kan vi göra åt saken

- HTTPS - grunder
  - x.509 (PKIX)
- Andra säkerhetsproblem i WWW
  - Internet Explorer
  - BEAST och CRIME
- Tekniska utvägar
  - Begränsad CA-lista
  - Monkeysphere
  - Convergence
  - DNSSEC (DNS+DANE)
  - Darknets
- Sociala lösningar

Convergence

- “Det senaste” för ett år sedan
- Mer “agile” (notaries kan förkastas, till skilland från root CAs)
- Kräver ändringar hos klienten

`http://convergence.io/`

x.509 - Hur hamnade vi här och vad kan vi göra åt saken

- HTTPS - grunder
  - x.509 (PKIX)
- Andra säkerhetsproblem i WWW
  - Internet Explorer
  - BEAST och CRIME
- Tekniska utvägar
  - Begränsad CA-lista
  - Monkeysphere
  - Convergence
  - DNSSEC (DNS+DANE)
  - Darknets
- Sociala lösningar

- DNSSEC behövs! (Av helt andra anledningar)
- Färre attackvektorer, mer centralisering
- “Fler ägg i samma korg”

Och på ämnet flera ägg i en korg... `<rant>`

När HTTP är det nya TCP

- When in doubt, HTTP API
- Istället för standarder (men det kan kalla för det)
- Inte bara overhead, HTTPS blivit så viktigt (och lidande).

`</rant>`

x.509 - Hur hamnade vi här och vad kan vi göra åt saken

- HTTPS - grunder
  - x.509 (PKIX)
- Andra säkerhetsproblem i WWW
  - Internet Explorer
  - BEAST och CRIME
- Tekniska utvägar
  - Begränsad CA-lista
  - Monkeysphere
  - Convergence
  - DNSSEC (DNS+DANE)
  - Darknets
- Sociala lösningar

I2P och TOR med vänner

- Helt annan lösningsväg
- För diskussion ikväll?

Utvecklare! Utvecklare! Utvecklare!

Det är kul att leka med, testa alternativen! (Det kan iaf inte bli värre.)

Utbildning! Utbildning! Utbildning!

Ett system blir aldrig säkrare än sin dummaste (läs minst utbildade) användare.:)

Tack!
Frågor? Lösningar?

jonatan@xwalck.se