SPS
Digitální důvěra

Rychlé opakování pojmů

- Symetrická kryptografie
  - Jeden klíč
  - Problém s jeho výměnou
- Asymetrická kryptografie
  - Dva klíče – veřejný a privátní
  - Bezproblémová výměna
  - Možnost použití pro autentizaci

Rychlé opakování pojmů

- Autentizace
  - Ověření proklamované identity subjektu

  Autorizace
  - Ověření oprávnění k přístupu
- Hash
  - Výstup hashovací funkce, reprezentace většího objemu dat menším
- ASN.1 / Abstraktní Syntaktická Notace verze 1
  - formální jazyk pro popis strukturovaných dat pro komunikační protokoly.

Důvěra v „normálním“ světě

- Normální svět = fyzický (=neelektronický) styk
- Ověření identity – tvář, ostatní
- Dlouhodobé budování důvěry mezi subjekty
- Smlouvy, právo, zákony

Public key infrastructure (PKI)

- Označení pro infrastrukturu správy a distribuce veřejných klíčů pro asymetrickou kryptografii
- Centralizovaný / hierarchický model s CA
- Decentralizovaný / síť důvěry / web (network) of trust

Decentralizovaný model

- Vzájemné podepisování veřejných klíčů na základě vztahů mezi jednotlivci
- Označení úrovně důvěry
- Prosím rozhodněte, nakolik důvěřujete tomuto uživateli, že správně verifikuje klíče jiných uživatelů (prohlédnutím cestovních pasů , kontrolou fingerprintů z různých zdrojů...)?

  1 = Nevím nebo neřeknu

  2 = Nedůvěřuji

  3 = Důvěřuji částečně

  4 = Důvěřuji úplně

  5 = Důvěřuji absolutně

  m = zpět do hlavního menu

Centralizovaný model

- Důvěřuje se hierarchicky
- Každý certifikát je podepsán nějakou autoritou
- Kořenový certifikát = podepsán sám sebou
- Certificate chain – řetěz certifikátů – cesta ke kořenovému certifikátu
- CA, která podepíše jiný CA certifikát je odpovědná za všechny certifikáty v tomto listu

Digitální certifikát

- Podepsaný veřejný klíč
- Je to ta věc, ke které si potřebujete vybudovat důvěru
- Vznik:
  - Vygenerování veřejného klíče (public key)
  - Vygenerování žádosti o certifikát (certificate signing request)
  - Podpis certifikátu privátním klíčem certifikační autority

Obsah certifikátu

- Sériové číslo / serial number
- Common name / Subject
- Algoritmus podpisu / Signature Algorithm
- Vydavatel / Issuer
- Platnost od-do / Valid From – To
- Veřejný klíč / Public key
- openssl x509 -text -in cert.crt

Postup tvorby certifikátu

- Vygeneruj pár klíčů veřejný/privátní
- Vygeneruj žádost o certifikát (Certificate Signing Request, CSR)
- Doruč CSR certifikační autoritě – důležité
- CA ověří identitu a podepíše klíč, dá vám certifikát (.crt)
- CA vám obvykle nahraje aktuální CRL, či svůj „certificate chain“

Obvyklá podoba PEM certifikátu


```
-----BEGIN CERTIFICATE-----
MIIGKjCCBRKgAwIBAgIBATANBgkqhkiG9w0BAQUFADBZMQswCQYDVQQGEwJDWjEs
MCoGA1UECgwjxIxlc2vDoSBwb8WhdGEsIHMucC4gW0nEjCA0NzExNDk4M10xHDAa
BgNVBAMTE1Bvc3RTaWdudW0gUm9vdCBRQ0EwHhcNMDUwNDA2MDk0NTExWhcNMzAw
NDA2MDk0MjI3WjBZMQswCQYDVQQGEwJDWjEsMCoGA1UECgwjxIxlc2vDoSBwb8Wh
dGEsIHMucC4gW0nEjCA0NzExNDk4M10xHDAaBgNVBAMTE1Bvc3RTaWdudW0gUm9v
dCBRQ0EwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC4OrLAx+0mAPpc
fvUNrOic7u6DJcokEJLoWSv0ZurD5pXVZG+zN9pKX5P3iH7DZtuZ2qwzg4tHReCe
u6SR+aAn962eG2ZEw1uv411QrZUgVkOe8Tvfr0Cv1HOzgZn0AFZNZ8TnHS67SMP/
z//VyFLqSBm44QtJDeiAvzwLXFAp5HYeIBMXVMfp1aY2t8RN7B0WSgO8aU1UgRvi
KR4qCJao0iCuQV/4f0Exf1o4AyjXlTZ4wbKD5ZAwuI8a+aZKjtIW1Ucioa/0kyLx
3DHLq0Lsll5OaVP2awfPkxXGyPOSYrEXxoNm32CfKeXjY1xTIwm0cIx5AEpNP8t7
Ku5hPwY7AgMBAAGjggL7MIIC9zCCAYsGA1UdHwSCAYIwggF+MDCgLqAshipodHRw
Oi8vd3d3LnBvc3RzaWdudW0uY3ovY3JsL3Bzcm9vdHFjYS5jcmwwMKAuoCyGKmh0
dHA6Ly9wb3N0c2lnbnVtLnR0Yy5jei9jcmwvcHNyb290cWNhLmNybDCBiqCBh6CB
hIaBgWxkYXA6Ly9xY2EucG9zdHNpZ251bS5jei9jbiUzZFBvc3RTaWdudW0lMjBS
b290JTIwUUNBLG8lM2RDZXNrYSUyMHBvc3RhJTIwcy5wLiUyMFtJQyUyMDQ3MTE0
OTgzXSxjJTNkQ1o/Y2VydGlmaWNhdGVSZXZvY2F0aW9uTGlzdDCBiqCBh6CBhIaB
gWxkYXA6Ly9wb3N0c2lnbnVtLnR0Yy5jei9jbiUzZFBvc3RTaWdudW0lMjBSb290
JTIwUUNBLG8lM2RDZXNrYSUyMHBvc3RhJTIwcy5wLiUyMFtJQyUyMDQ3MTE0OTgz
XSxjJTNkQ1o/Y2VydGlmaWNhdGVSZXZvY2F0aW9uTGlzdDCBoQYDVR0gBIGZMIGW
MIGTBgRVHSAAMIGKMIGHBggrBgEFBQcCAjB7GnlUZW50byBjZXJ0aWZpa2F0IGJ5
bCB2eWRhbiBqYWtvIGt2YWxpZmlrb3Zhbnkgc3lzdGVtb3Z5IGNlcnRpZmlrYXQg
dmUgc215c2x1IHpha29uYSAyMjcvMjAwMCBTYi4gYSBuYXZhenVqaWNpY2ggcHJl
ZHBpc3UuMA8GA1UdEwQIMAYBAf8CAQEwDgYDVR0PAQH/BAQDAgEGMB0GA1UdDgQW
BBQrHdGdefXVeB4CPIJK6N3uQ68pRDCBgQYDVR0jBHoweIAUKx3RnXn11XgeAjyC
Sujd7kOvKUShXaRbMFkxCzAJBgNVBAYTAkNaMSwwKgYDVQQKDCPEjGVza8OhIHBv
xaF0YSwgcy5wLiBbScSMIDQ3MTE0OTgzXTEcMBoGA1UEAxMTUG9zdFNpZ251bSBS
b290IFFDQYIBATANBgkqhkiG9w0BAQUFAAOCAQEAsWkApNYzof7ZKmroU3aDOnR/
2ObgD0SnE3N+/KYYSGCzLf4HQtGspMjUEDMULUqAWQF76ZbPRbv6FSVyk5YuAxkI
DvNknsfTxz6mCnGNsL/qgTYaK2TLk8A1b6VEXMD0MjOXODm5ooa+sSNxzT3JBbTC
AJbtJ6OrDmqVE9X+88M39L1z7YTHPaTt1i7HGrKfYf42TWp0oGD+o0lJQoqAwHOj
ASVmDEs4iUUi6y3jboBJtZSoUDkzK5mRlJELWtdvANTpcrf/DLj7CbG9wKYIUH0D
KQuvApdC79JbGojTzZiMOVBH9H+v/8suZgFdQqBwF82mwSZwxHmn149grQLkJg==
-----END CERTIFICATE-----
```

Uložení CSR


```
-----BEGIN CERTIFICATE REQUEST-----
MIIB2zCCAUQCAQAwgZoxCzAJBgNVBAYTAkNaMRowGAYDVQQIFBHEjGVza8OhIHJl
cHVibGlrYTEOMAwGA1UEBxMFUHJhaGExGDAWBgNVBAoTD1RydXN0aWNhIHMuci5v
LjEZMBcGA1UEAxQQTWljaGFsIE1lZHZlY2vDvTEqMCgGCSqGSIb3DQEJARYbbWlj
aGFsLm1lZHZlY2t5QHRydXN0aWNhLmN6MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCB
iQKBgQDFcbtcxRbz49sLMt30rhZpU1Iy6tnRI0qfqGutJw3MZKGu417WZVPCW7AN
a3MXeZRxQY7tszG88TQIhDf35biYGmYRBdZZQpz4LnxdlEfZQ7x3As7iFLD1uWO5
i/AykvoG/AOroSAKVZbeutqaDPRPrzLJqMoByeARTY6BdF67qwIDAQABoAAwDQYJ
KoZIhvcNAQEFBQADgYEAEAkNUOSeWJkuMhiKfpevXgecvtrHWJEG04L1PiWk7xd+
tzOs9iudfVAhgtnJVMBIMqUFy8BJULFDxrX1oi57I5ZWnT+0xP0NcY+M9TymY3Oq
ieOxvbRTmPZkjaZX+INqAQUHgoQi86Psz/QlFHGz/Du3RRkvqnGznGiQnQHej+s=
-----END CERTIFICATE REQUEST-----
```

$ openssl asn1parse -in medvecky.req

Forma uložení certifikátu

- DER (Distinguished Encoding Rules)
  - Binární forma ASN.1
  - Obvyklá přípona .cer, .crt, .der
- PEM (Privacy Enhanced Mail)
  - DER forma zakódovaná Base64
  - Obvyklá přípona .pem
- PKCS#12
  - Souborový formát RSA laboratories, pro uložení privátního klíče i certifikátu
  - Obvyklá přípona .p12

Certifikační autorita

- Technicky: Je sada kryptografických prvků, tvořících celek pro zajišťování služeb podepisování, revokace a distribuce certifikátů
- Je instituce, která vydává certifikáty na základě své certifikační politiky a buduje vztahy důvěry svých klientů a ostatního světa

Certifikační autorita

- Privátní klíč CA (veledůležitá věc)
- Certifikát CA
  - Veřejný klíč CA
  - Podpis CA
- Certifikační politika
- Registrační autorita
- CRL
- Systém distribuce dat

Ukončení platnosti certifikátu

- Revokace = ukončení platnosti certifikátu před dobou uvedenou v metadatech
- Důvod zneplatnění certifikátu
  - 10 různých typů (RFC5280)
  - Kompromitace privátního klíče
  - Ukončení fungování držitele
  - Změna údajů
- Vydání CRL na veřejném místě
  - CRL = seznam podepsaný autoritou

Postup ověření platnosti certifikátu

- Zjisti, kdo je vydavatelem certifikátu a zda mu důvěřuješ
- Anebo ověř, že jsi dostal certifikát, který cestou nikdo nemodifikoval
- Podívej se do metadat certifikátu na platnost
- Ověř, zda dnešní datum spadá do intervalu platnosti certifikátu
- Ověř, zda certifikát není přítomen v CRL

CA v ČR

- První certifikační autorita, a. s.,
- Česká pošta, s. p.,
- eIdentity a. s.,
- https://www.mvcr.cz/clanek/prehled-kvalifikovanych-poskytovatelu-certifikacnich-sluzeb-a-jejich-kvalifikovanych-sluzeb.aspx
- Dne 28. 12. 2009 nabylo účinnosti rozhodnutí EK 2009/767/ES

Software pro CA

- OpenSSL / OpenCA
- Microsoft CA (zahrnuto od Windows server
- 2003)
- Pure CA
- RSA Keon
- A další..