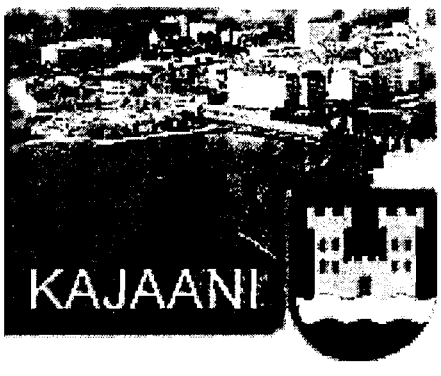
SUOMEN KUNTALIITTO
Sosiaali- ja terveysyksikkö

TERVEYDENHUOLLON 27. ATK-PÄIVÄT
4. - 5.6.2001

Käyttäjän todentaminen ja sähköinen allekirjoitus, tuotepäällikkö Teemu Kupiainen, Secgo Solution Oy



Käyttäjän todentaminen ja sähköinen allekirjoitus

Teemu Kupiainen
Product Manager
teemu.kupiainen@secgo.com

SecGo Solutions Oy

Terveydenhuollon27. ATK-päivät
Kajaani, 4.6. 2001

Agenda

- Julkisen avaimen infrastuktuuri (PKI)
- Käyttäjän todentaminen
- Sähköinen allekirjoitus
- Yhteenveto

Agenda

- **Julkisen avaimen infrastuktuuri (PKI)**
- Käyttäjän todentaminen
- Sähköinen allekirjoitus
- Yhteenveto

E-world requires E-Identity

- Methods for user authentication -

User name: TeemuK
Password: dsn2000

Private key and certificate in a file

secpo info@secpo.com
www.secpo.com

Public Key Infrastructure (PKI)

- Infrastructure behind E-Identity -

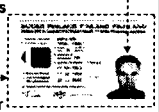
- PKI provides Electronic IDs - certificates (and private keys)
- Electronic IDs can be applied in
  - strong authentication
  - encryption
  - digital signatures
- Benefits
  - one infrastructure, security for several applications
  - efficient method for the key management, no need to maintain encryption key or password lists

secpo info@secpo.com
www.secpo.com

Public Key Infrastructure (PKI)

- Basics -

- Private key
  - secret key, which should be accessible only to the owner of the key
- Public key
  - should be accessible to everybody
  - usually stored and distributed in certificates
  - private key cannot be derived from the public key, or vice versa
- Certificate
  - binds user's public key, name etc. together
  - signed by the CA, i.e., if you trust the CA, you can trust the certificate



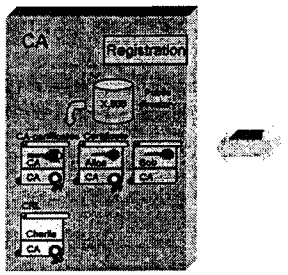
secpo info@secpo.com
www.secpo.com

Example: X.509v3 Certificate

```
use:Certificate:
    Version: 3 (0x2)
    Serial Number: 421 (0x1a5)
    Signature Algorithm: md5WithRSAEncryption
    Issuer: C=FI, O=Vaestorekisterikeskus, CN=FINEID Filer CA P3 1998
    Validity
        Not Before: Sep  4 05:34:00 1998 GMT
        Not After : Jul 31 00:00:00 1999 GMT
    Subject: C=FI, S=MANNISTO, G=TATU JUSSI/UID=9000000356,
    Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
        RSA Public Key: (1024 bit)
            Modulus (1024 bit): a6:e2:b1:61:cd: ... :c6:c6:0a:f5:5b
            Exponent: 01:00:01
    X509v3 extensions:
        X509v3 Authority Key Identifier: CA199801
        X509v3 Subject Key Identifier:   0
        X509v3 Key Usage:                digitalSignature, nonRepudiation
        X509v3 Certificate Policies:     1.2.246.517.1.10
        X509v3 Basic Constraints:        FALSE
    Signature Algorithm: md5WithRSAEncryption
        a2:29:f6:d7:c5: ... :f4:82:64:79:0f
```


Certification authority (CA)

- "E-Identity provider" -



Files

Hardware token

Smart Card

Certificate Practice Statement (CPS)

- the cornerstone of trust -

- Defines the operating principles and security policies of a CA, for example:
  - How are users authenticated in practice?
  - How is the CA private key protected?
  - How often are CRLs generated?
  - How is the certificate revocation service organised?
  - How is access to the certificates and CRLs guaranteed?

Qualified certificate

- Directive 1999/93/EC -

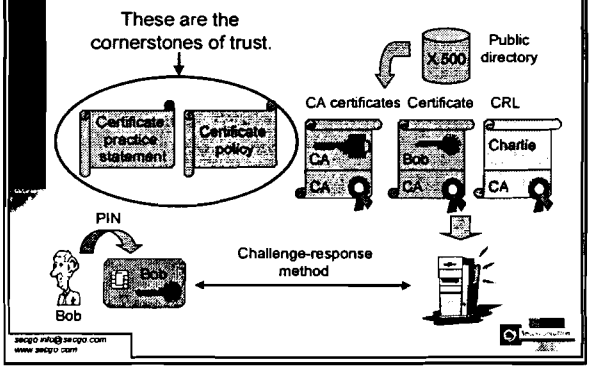
- Issued by a qualified Certification Authority (CA).
- The certificate contains the data as specified in the EU-directive (Annex 1)
- Required for secure/advanced digital signatures.
- See: "Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures"

Agenda

- Julkisen avaimen infrastuktuuri (PKI)
- **Käyttäjän todentaminen**
- Sähköinen allekirjoitus
- Yhteenveto

User authentication with PKI

- What do you need for authentication? -

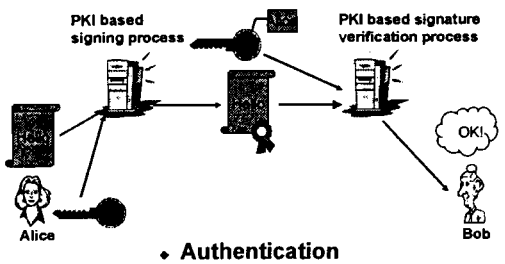


Agenda

- Julkisen avaimen infrastuktuuri (PKI)
- Käyttäjän todentaminen
- **Sähköinen allekirjoitus**
- Yhteenveto

Digital Signature

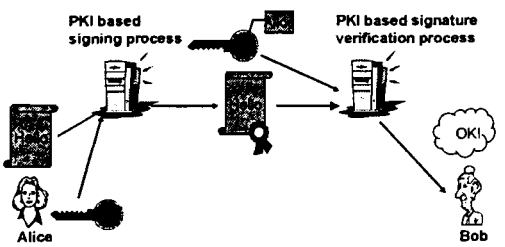
- Technical overview, a simple approach -



- **Authentication**
- **Integrity**
- **Non-repudiation**

Digital Signature

- Technical overview, open questions -



- **When was the document signed?**
- **Archiving?**

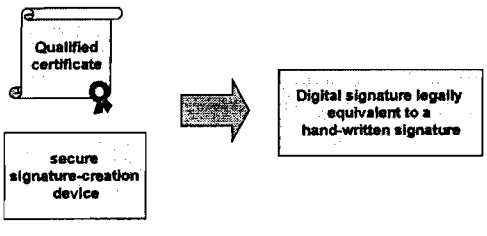
Digital Signature

- Security is as strong as the weakest link -

- CA/PKI level security
  - Certificate practice statement, certificate policy
- Application level implementation
  - How is the certificate's validity verified, how to ensure the correct time?
  - How is the signature verified, how are the documents stored?
- Users:

Digital Signature

- The legal point of view -



Agenda

- Julkisen avaimen infrastuktuuri (PKI)
- Käyttäjän todentaminen
- Sähköinen allekirjoitus
- **Yhteenveto**

Summary

- Secure user authentication and digital signatures are essential steps towards "truly electronic" patient records.
- PKI offers a comprehensive platform for user authentication, data encryption and digital signatures.
- User authentication and digital signature - security is as strong as the weakest link.
  - PKI/CA level security, qualified certificates
  - Application level implementation
  - Users

Where to find more information:

Cryptography books:
B.Schneier, *"Applied Cryptography, 2nd Ed."*, John Wiley & Sons, 1996
PKI:
http://www.fineid.fi/
http://www.cca.gov.sg/guidelines/info.html
http://www.tbg.com/public/samples/home.asp?docid=39
http://www.verisign.com/whitepaper/enterprise/pki/index.html

User authentication:
http://www.rsasecurity.com/rsalabs/faq/2-2-2.html

Digital signature:
http://europa.eu.int/eur-lex/fi/lif/dat/1999/fi_399L0093.html
http://finlex.edita.fi/dynaweb/stp/1999sd/@ebt-link?showtoc=false;target=IDMATCH(id,19991318.sd)

SecGo Solutions

SecGo Solutions Oy
Kuokkamaantie 4
P.O. Box 128
FIN-33800 TAMPERE
Finland

Tel +358 3 3138 5800
Fax +358 3 3138 5810
www.secgo.com
secgo.info@secgo.com