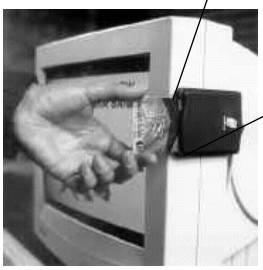
Väestörekisterikeskus
Population Register Centre

Finnish **E**lectronic **I**dentification

- Finnish Citizen Card -



Väestörekisterikeskus
Population Register Centre

Finnish **E**lectronic **Id**entification
and Supporting Technologies

General Issues

- **The amount of various transactions is increasing rapidly in Internet**
- **To make it safe we need:**
  - **both sides identification,**
  - **digital signature,**
  - **encrypted: - data**
    - data transfer
- **Field is developing rapidly**
- **Important part of the information society**

Väestörekisterikeskus
Population Register Centre

Finnish Electronic Identification
and Supporting Technologies

General Issues

- **The development of the infrastructure needed is a large operation demanding modern and safe technical solutions based on open standards**
- **There will be huge markets**
- **Finland: One of the leading countries in the field**

Väestörekisterikeskus
Population Register Centre

Finnish Electronic Identification
and Supporting Technologies

Identification, digital signatures and encryption will be based on:

- **open standards:**
  - **Public Key Infrastructure**
  - **chipcards and readers (ISO-standards)**
  - **X.509 v.3 certificates**
  - **X.500- and LDAP-directories**
  - **EID-application (FINEID S1=SEIS S1=SS614330=PKCS#15?)**
- **highly secured environments**
  - **key generation**
  - **face to face identification**
- **voluntary involvning**
- **cards and certificates valid for a certain time (3-5 years max.)**
- **EU-directive draft for digital signature**
- **legislation in Finland**

Väestörekisterikeskus
Population Register Centre

Finnish **E**lectronic **Id**entification
and Supporting Technologies

Population Register Centre will be the Certification Authority In Finland responsible for building up the infrastructure needed in administration:

- **the cards**
- **the keys**
- **the certificates**
- **directory services**
- **certificate revocation list-services**
- **timestamp-services**
- **help desk services**
- **the cerificate policy**
- **international collaboration**

- **New electronic ID-cards will be issued in 1999**
- **New services must be created for the citizens in 1999-2001**

Väestörekisterikeskus
Population Register Centre

Finnish **E**lectronic **Id**entification
and Supporting Technologies

How to do it ?

A joint project

- pilot projects (4 official)

Legislation

Financing

Everything must be ready during 1999 !

Väestörekisterikeskus
Population Register Centre

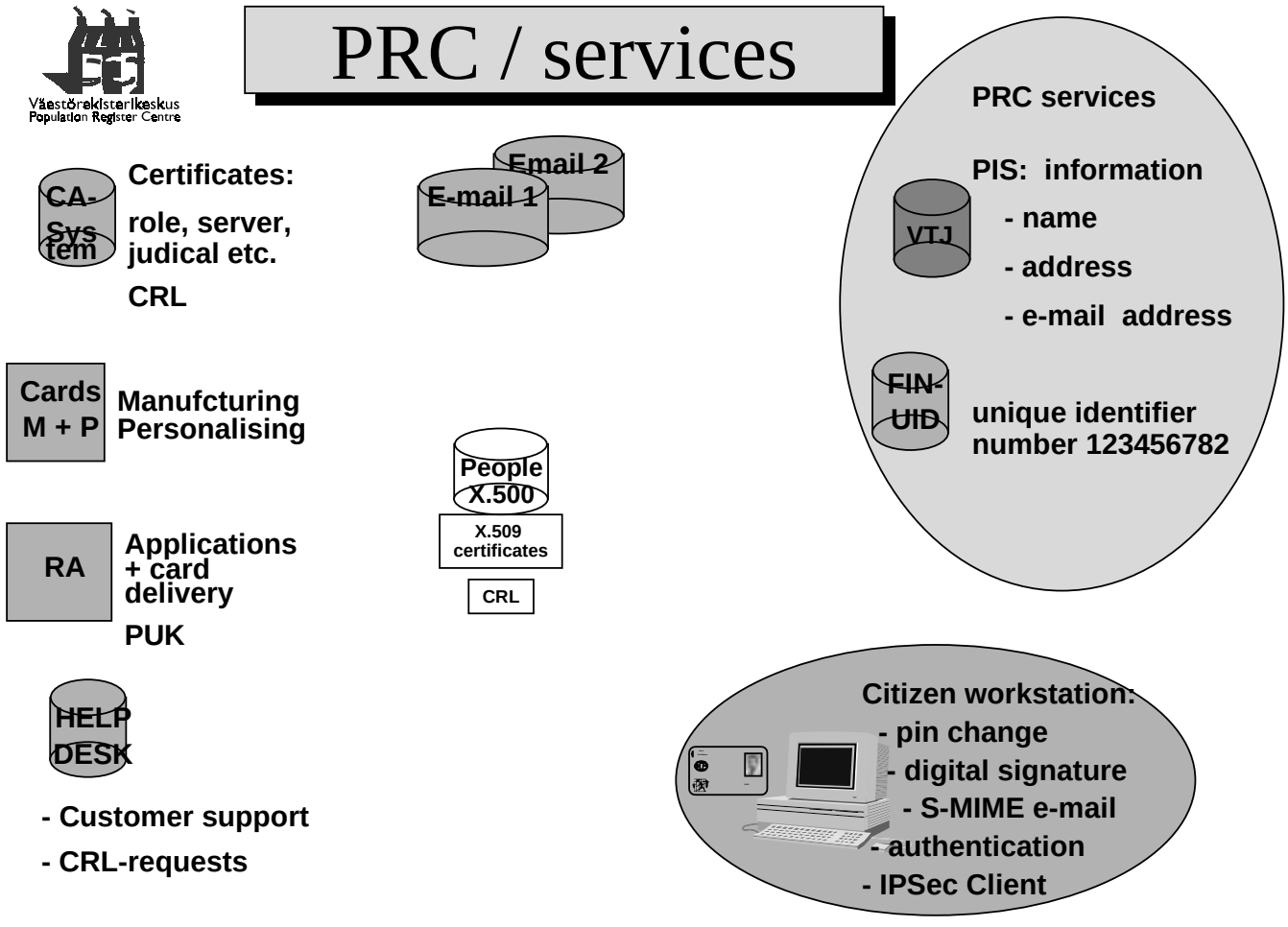
Finnish **E**lectronic **Id**entification
and Supporting Technologies

Pilots

- PRC - CA services, civil cervants
  - 7.9.1998
- FinnCity project: Espoo, Vantaa, Oulu ja Pori
  - december 1998
- Ministry of agriculture and forestry
  - 15.9.1998
- Ministry of Social Affairs and Health, ICT macro pilot in Finnish social care and health services 1998-2000
  - 1999
- Other minor pilots

Väestörekisterikeskus
Population Register Centre

PRC / services



Väestörekisterikeskus
Population Register Centre

Finnish **E**lectronic **Id**entification
and Supporting Technologies

FINEID SPECIFICATIONS

***AVAILABLE*: http://www.vaestorekisterikeskus.fi**

- **FINEID-S1: ELECTRONIC ID-APPLICATION**
- **FINEID-S3: CERTIFICATE SPECIFICATION**
- **FINEID-S4-1: IMPLEMENTATION PROFILE**
- **FINEID-S5: X.500 DIRECTORY SPECIFICATION AND CRL**
- **FINEID-P18: PILOT CARD AND CERTIFICATE SPECIFICATION**

FOR THE PILOT USE ONLY:

- **FINEID-S10: CERTIFICATE POLICY FOR THE PILOT**
- **FINEID-P11: GENERAL ISSUES OF FINEID**
- **FINEID-P12: FINNISH CITIZEN CARD CONTENTS**
- **FINEID-P13: CARD MANUFACTURING AND INVIDUALIZING**
- **FINEID-P14: CA SERVICES**
- **FINEID-P15: DUTIES OF THE REGISTRATION AUTHORITY**
- **FINEID-P16: TIME STAMPING**
- **FINEID-P17: HELP DESK SERVICES**
- **TELECOMMUNICATIONS SECURITY**
- **CPS**

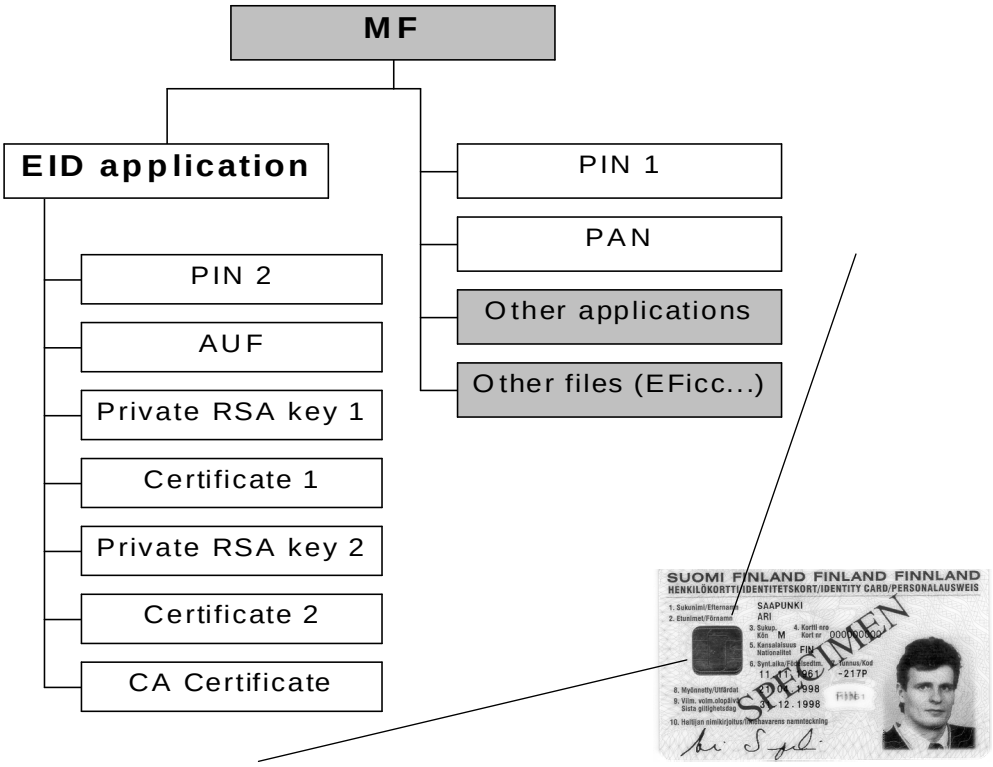
Väestörekisterikeskus
Population Register Centre

Technology elements: www.vaestorekisterikeskus.fi

- **Electronic ID-application**
  - **FINEID S1**
- **FINEID-certificate**
  - **FINEID S3**
- **FINEID-implementation profile**
  - **FINEID S4-1**
- **Directory and CRL**
  - **FINEID S5**
- **Pilot card**
  - **FINEID P18**

Väestörekisterikeskus
Population Register Centre

Finnish **E**lectronic **Id**entification
and Supporting Technologies



Väestörekisterikeskus
Population Register Centre

Finnish **E**lectronic **Id**entification
and Supporting Technologies

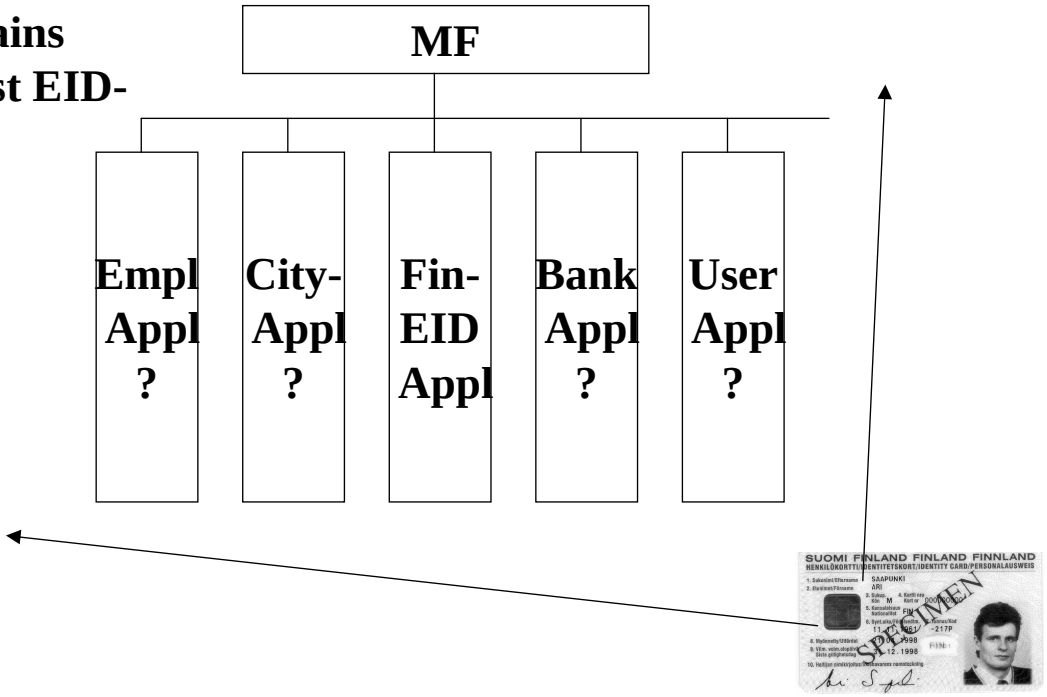
SS 61 43 30 (v0.7)
versus FINEID S1

- New Certificate Index File (CIF) added
  - for each private key there is a CIF-file (file ID told in the AUF file)
  - CIF file contains:
    - certificate label
    - path to certificate file or URL
- All labels is now BMPString
- CAKeyIdentifier added to the CAInfo (AUF)

Finnish Electronic Identification
and Supporting Technologies

Future Citizen Card possibly contains more than just EID-application

It allows wide range of usage with high security



Finnish Electronic Identification
and Supporting Technologies

Certificate

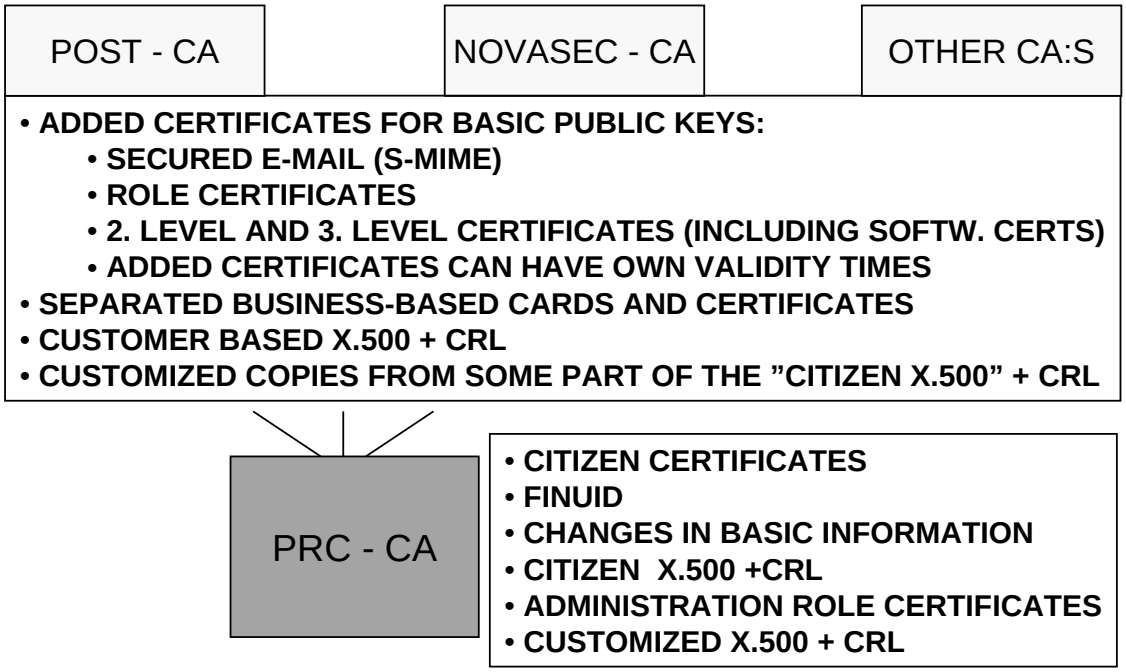
Basic fields: **Certificate**

- **version:** value 2 = x.509 v.3 certificate (Internet X.509 Public Key Infrastructure Certificate and CRL Profile“, IETF PKIX, ISO/IEC 9594-8: 1997 X.509)
- **serial number:** unique within an issuer
- **signature :** the algorithm identifier for the algorithm used by the CA to sign the certificate
- **issuer:** country = FI, organisation = 123456-1234 (unique within a country, CommonName = Väestörekisterikeskus
- **validity:** YYMMDDHHMMSSZ
- **subject:** country=FI, Surnamei=Meikäläinen, Given name=Maija, Finuid=123456786
- **subject public key:** The algorithm identifier of the subject’s public key

Extensions: Key usage , Certificate policies , Authority and Subject key identifier

Väestörekisterikeskus
Population Register Centre

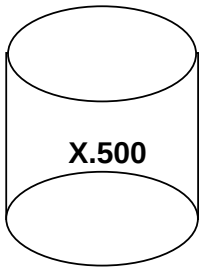
Finnish **E**lectronic **Id**entification
and Supporting Technologies



Väestörekisterikeskus
Population Register Centre

Finnish **E**lectronic **Id**entification
and Supporting Technologies

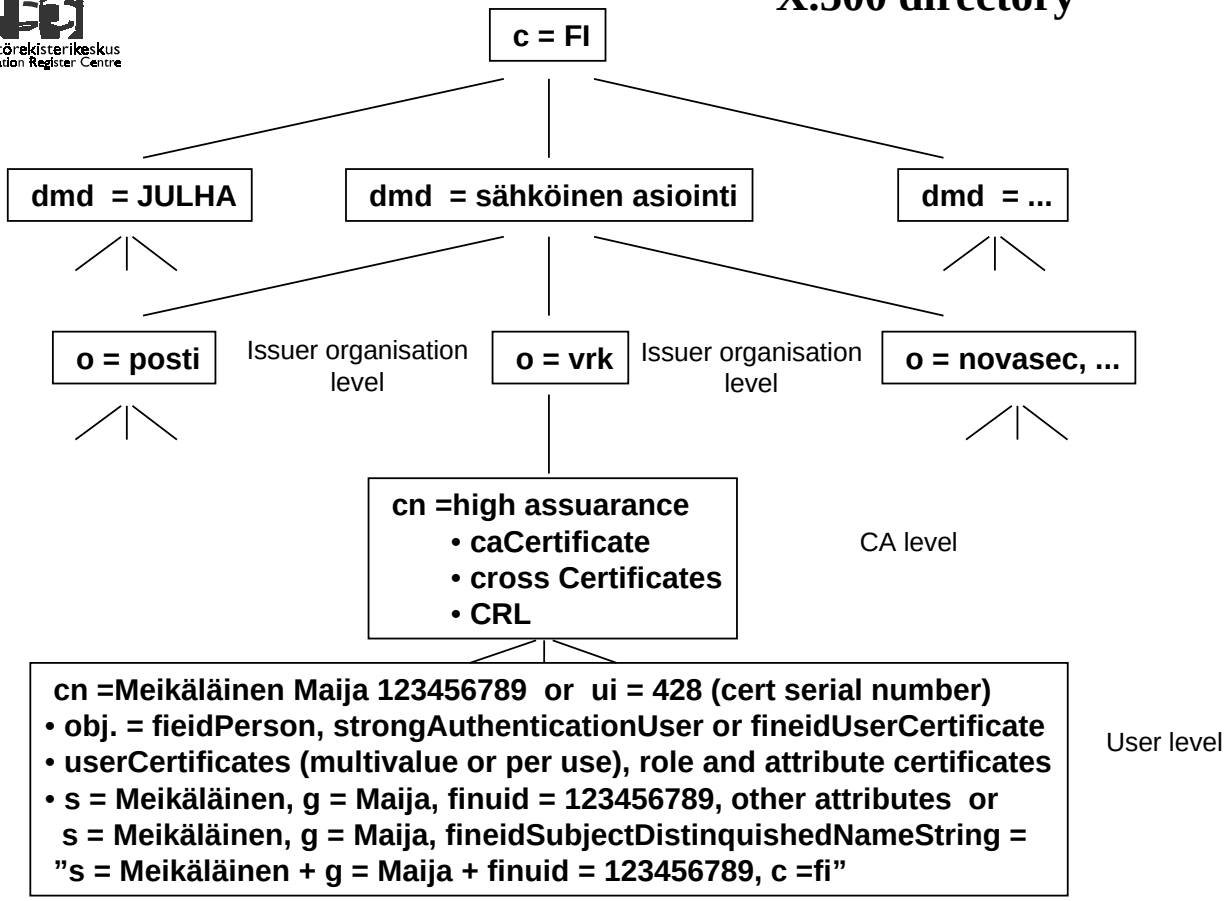
DIRECTORY SERVICE



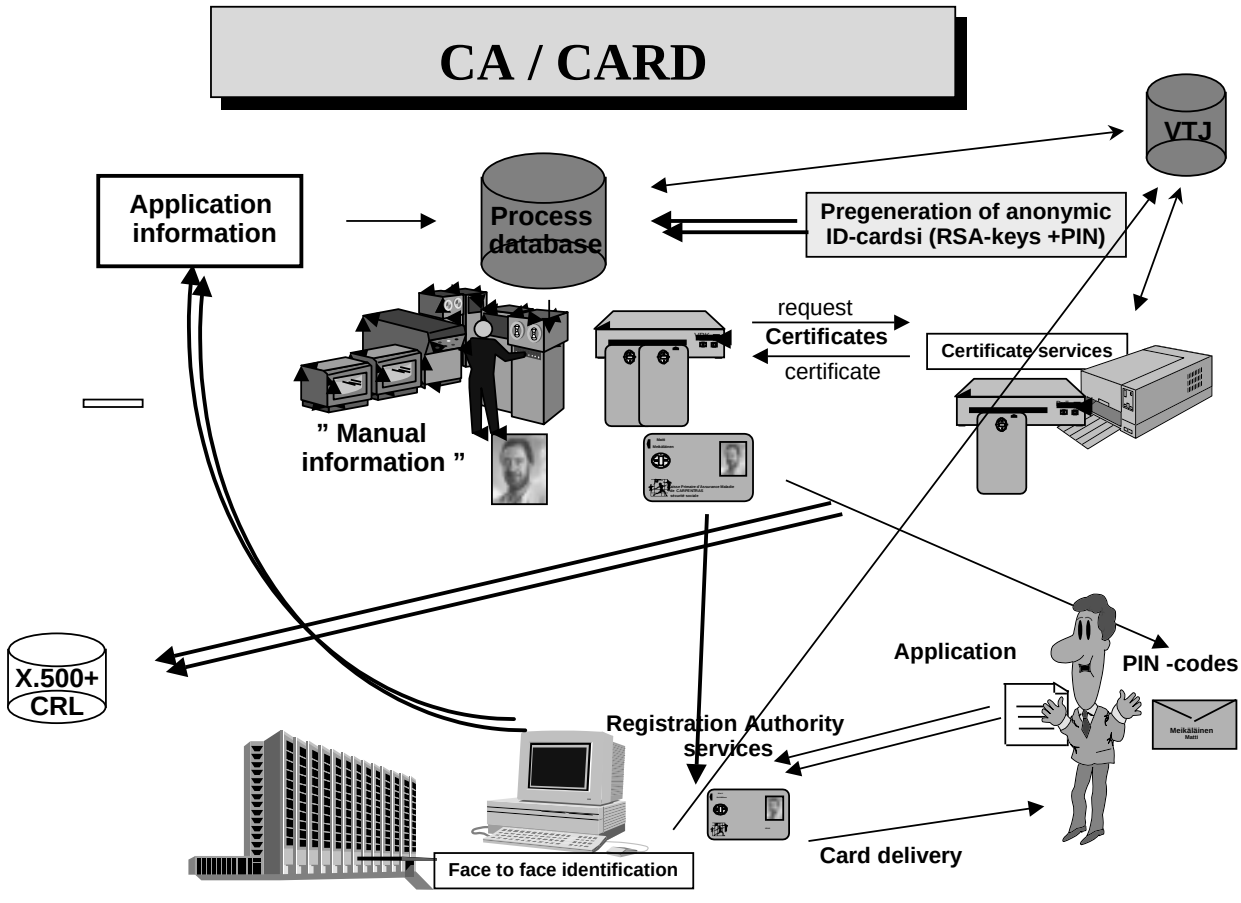
- **PEOPLE X.500, OPEN DIRECTORY SERVICE**
- **CLOSED ENVIRONMENTS -> CLOSED DIRECTORIES (LDAP ETC.)**
- **PERSONAL CERTIFICATES:**
  - **CERTIFICATE 1: AUTHENTICATION AND ENCRYPTION**
  - **CERTIFICATE 2: DIGITAL SIGNATURE**
- **JUDICAL AND SERVER CERTIFICATES**
- **CRL (Certificate Revocation List)**
- **DIRECTORY REQUESTS : LDAP V.2.0 OR 3.0**

Väestörekisterikeskus
Population Register Centre

X.500 directory



CA / CARD



Secured data transfer

- **secured data transfer based on open standards is needed**
- **you need to be able to use strong encryption with the partners who allows it and weaker where only weak encryption is available**
- **you should be able to use your electronic identity as a starting point, not ip-address of your terminal**

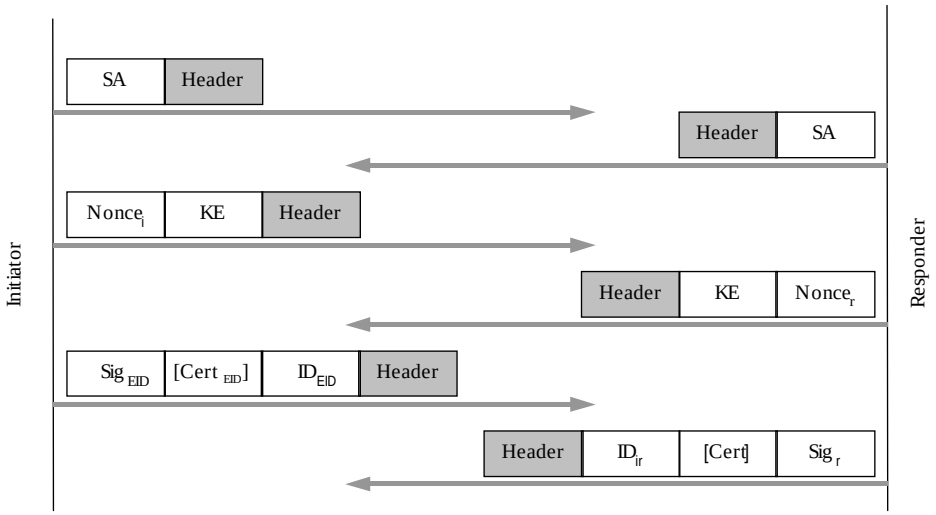
Väestörekisterikeskus
Population Register Centre

Finnish **E**lectronic **Id**entification
and Supporting Technologies

Secured data transfer

- **Asymmetric encyption provided by a ID-card is too ”heavy” to calculate when we are securing data transfer**
- **PKI solution with RSA encryption allows a good way of carrying the symmetric session time key**
- **What we need is a sort of X.509 certificate tool that includes all the necessary components required for checking:**
  - **the validity of a certificate,**
  - **requesting new certificates,**
  - **retrieving certificates from Certificate Authority directories,**
  - **and checking Certificate Revocation Lists**

IKE in Main Mode: EID and Service



Header - an ISAKMP header corresponding to the used mode
SA - the negotiated Security Association
Nonce - a random number sent for signing
KE - Key Exchange data for Diffie-Hellman key exchange
Sig - signature payload used for authentication
Cert - a certificate for the public key
ID - identity payload (ii is initiator and ir responder in phase I)

[] denotes an optional

This figure is based on authentication by using
The payloads are slightly different when other methods are used. The main difference is that the is replaced by a hash.

Väestörekisterikeskus
Population Register Centre

Finnish **E**lectronic **Id**entification
and Supporting Technologies

Secured data transfer

The ISAKMP/Oakley (=Internet Key Exchange Protocol IKE):

- **tool for negotiating the terms of the communication before the actual encryption and secure session can begin**

- **communication security parameters includes, for example:**
  - **which encryption algorithms to use**
  - **the lifetime of the encryption,**
  - **and the encryption keys themselves**
  - **negotiation process has to be made automatic and secure to allow scaling to the global Internet**

- **Summary : ISAKMP/Oakley with FINEID support is a one way to accomplishe the elements needed when securing data transfer**

Väestörekisterikeskus
Population Register Centre

Finnish Electronic Identification
and Supporting Technologies

Users

Finland

- **Public administration (100 ongoing projects)**
  - **State authorities and municipalities (0,5 mill. employees)**
- **Private sector**
  - **banks**
  - **telecommunication operators**
  - **large firms**
  - **commerce**
- **Citizens 5 millions**
- **Sweden SEIS interoperability, both public and private sector,**
- **Norway SEIS interoperability in administration, citizens**
- **Estonia ?, EU ?, PKCS#15 --> global market !**

Väestörekisterikeskus
Population Register Centre

Finnish Electronic Identification
and Supporting Technologies

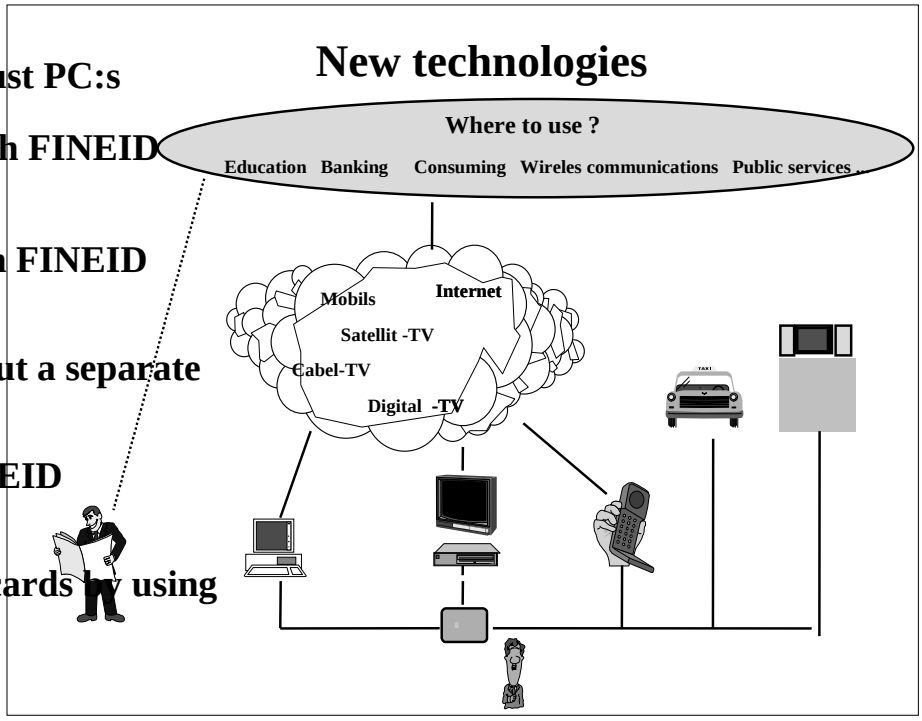
What is needed ?

- **Testing and evaluating of FINEID-products (starting project with SEIS)**
- **Software and a card reader package for end users**
- **New technical solutions for service providers**
- **Citizen terminals and kiosks**
- **Notariat and time stamp service**
- **The chains of certificates, role certificates, judical and service certificates**
- **New terminals**

Väestörekisterikeskus
Population Register Centre

Finnish **E**lectronic **Id**entification
and Supporting Technologies

- **We need more than just PC:s**
- **WWW-television with FINEID compatibility**
- **Digital television with FINEID compatibility**
- **GSM with and without a separate card reader**
- **Telephones with FINEID compatibility**
- **Identification to the cards by using biometrics**



Väestörekisterikeskus
Population Register Centre

Finnish **E**lectronic **Id**entification
and Supporting Technologies

Where to start?

- **www.vaestorekisterikeskus.fi**
- **ari.saapunki@vrk.intermin.fi**

Väestörekisterikeskus
Population Register Centre

- **www.seis.se**

SEIS

Väestörekisterikeskus
Population Register Centre

Finnish **E**lectronic **Id**entification
and Supporting Technologies

Endusers software package and smart card reader

- **S-MIME based e-mail client**
- **Software for digital signature**
- **Client software for authentication**
- **Secured data transfer client (IpSec, ISAKMP/Oakley)**
- **Encryption of files or data**
- **Certificate cheque (validity, CRL-cheque)**

Väestörekisterikeskus
Population Register Centre

Finnish **E**lectronic **Id**entification
and Supporting Technologies

End users basic software package and a card reader

- **Time Stamp client**
- **Software for changing PINs**
- **Client for reading open information from the card**
- **Card reader as a device or as a part of a computer (keyboard)**
- **Virusprotection, etc**

Citizen terminals and kiosks

- **We need proper terminals as many as possible**
- **We need them available**
- **There will be terminals in working places and in homes**
- **There will be terminals in libraries and other public buildings**
- **We need them available in the streets and other open environments**
- **We need kiosks: internet connection, videoconferencing etc.**

Väestörekisterikeskus
Population Register Centre

Finnish **E**lectronic **Id**entification
and Supporting Technologies

Notariat and time stamp service

- **We need the exact time for transactions coming from a reliable third party**
- **We need a system for maintaining the history of information**
- **So, there is a need for Notariat and time stamp service and**
- **there is a global market**

Chains of certificates, directory and crl

- **There is a need for full FINED interoperatibility and for added certificates, role, judical and server certificates**
- **That can mean chains of certificates based on same public keys**
- **We need a database maintaing information (cards, users and certificates**
- **We need support for different directory cervices (x.500, ldap)**
- **We need added services for existing softwares**

Väestörekisterikeskus
Population Register Centre

Finnish **E**lectronic **Id**entification
and Supporting Technologies

Softwares for service providers

- **New web-server services (electronic forms, IpSec, ldap etc.)**
- **Server end authentication, certificate- and CRL-cheque**
- **Connection to the existing databases**
- **Civil servant product for managing digitally signed forms**
- **Application to application connections etc.**

Employee usage

- **User authentication, SingleSignOn solutions**
- **Data and data transfer encryption**
- **Remote acces with FINEID-compatibility**
- **Workstation protection**
- **Application to application connections etc.**