

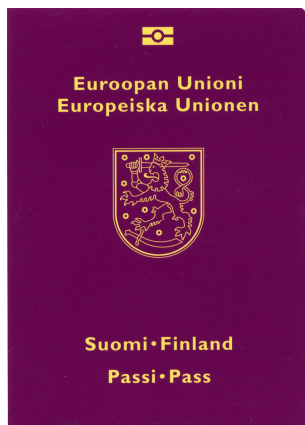


SISÄASIAINMINISTERIÖ  
INRIKESMINISTERIET

POLIISIOSASTO



# Älykortit ja tunnistautuminen Passi ja ajokortti 23.9.2009



Kehittämispäällikkö  
Mika Hansson  
Sisäasiainministeriö  
Poliisiosasto





## Biometriahanke

- Biometriahankkeen I vaihe
  - 2003-2006
  - Uusi passiversio elokuussa 2006
    - Siru
    - Biometria: kasvokuva
- Biometriahankkeen II vaihe
  - 2007-
  - Uusi passiversio kesäkuussa 2009
    - Sirulle sormenjäljet
  - Henkilökortit, oleskeluluvat
  - Sirun ja biometrian hyödyntäminen



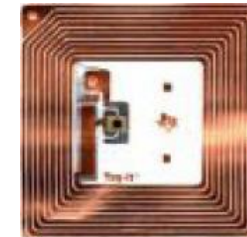
# Määritykset

- ICAO
  - International Civil Aviation Organization
  - Sirullisen passin minimivaatimukset ja valinnaiset ominaisuudet
- EU
  - Täsmentää mitkä ICAO:n valinnaiset ominaisuudet on otettava käyttöön
  - Sormenjäljet ja niiden suojaus
  - Siru myös oleskelulupiin



## Sivu

- RFID
- Standardi: ISO 14443 (tyypilliset toimikortit)
- Taajuusalue 13,56 Mhz
- Lukuetäisyys
  - 0-10 cm (standarditoteutus)
  - 1m (huippulaitteet labrassa)





## ICAO:n määrittelemät turvamekanismit

1. Passiivinen todennus (Passive Authentication, PA)
  - Pakollinen
2. Aktiivinen todennus (Active Authentication, AA)
  - Vapaavalintainen
3. Peruspääsynvalvonta (Basic Access Control, BAC)
  - Vapaavalintainen



## Euroopan unionin määritykset

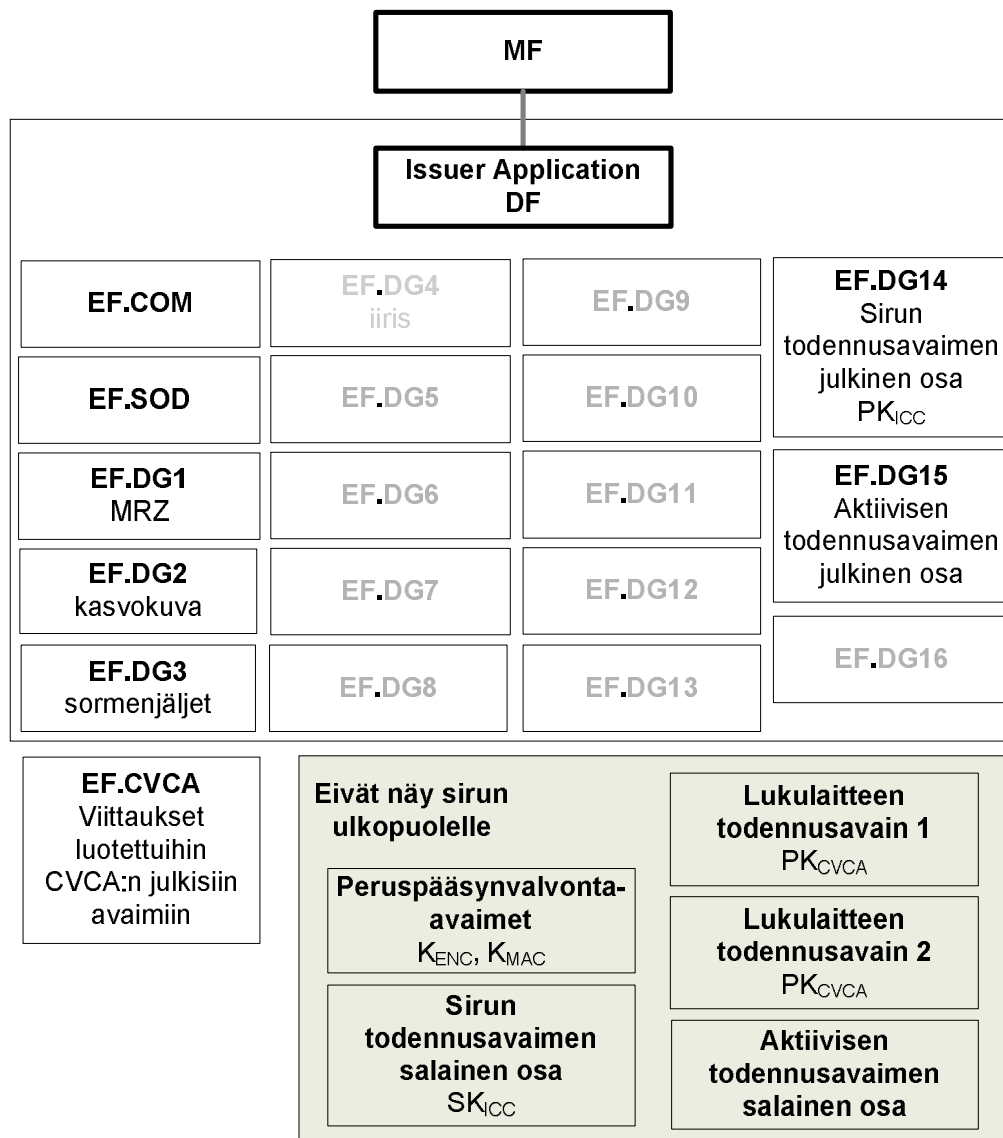
- Peruspääsynvalvonta pakollinen
  - Mahdollistaa sirulla olevien tietojen lukemisen
  - Ei anna kuitenkaan oikeutta lukea sormenjälki- tai iiristietoja
- Laajennettu pääsynvalvonta pakollinen biometrisiin lisätunnisteisiin
  - Sormenjäljet tulivat pakolliseksi kesäkuun 2009 jälkeen myönnettyissä passeissa
  - Iiriskuva



POLIISIOSASTO



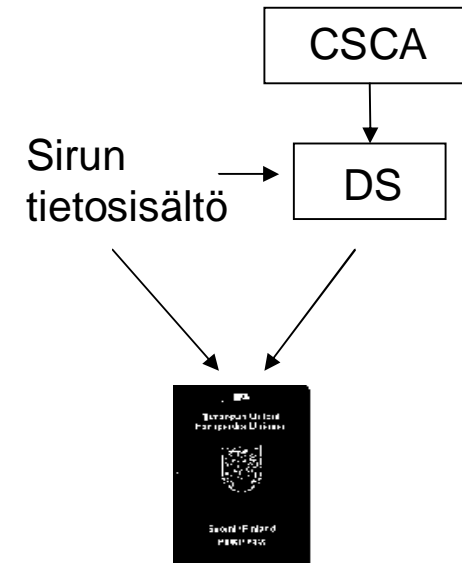
# Sirun tietosisältö





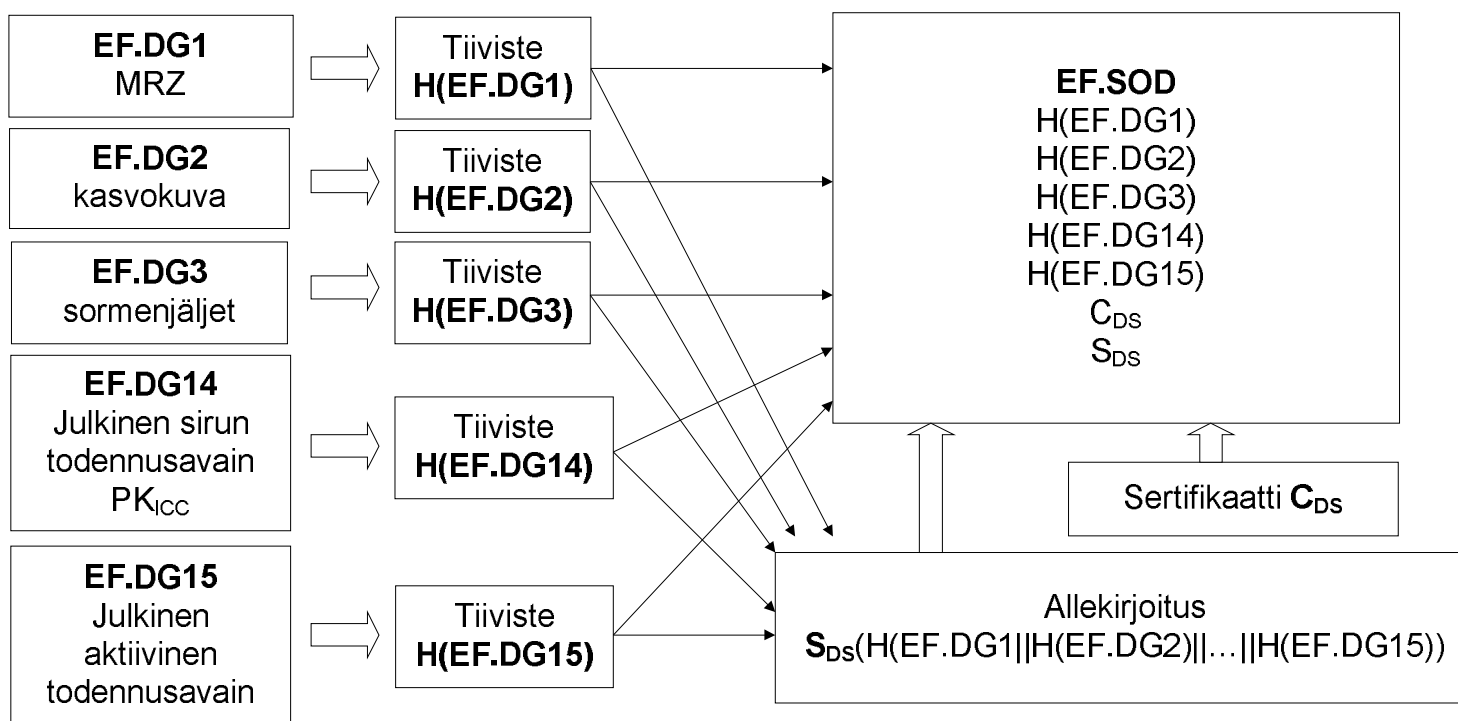
# Passiivinen todennus

- Passive Authentication (PA)
- ICAO: Pakollinen turvamekanismi
- Sirun tietosisältö allekirjoitetaan
- Julkisen avaimen järjestelmä
  - CSCA, Country Signing CA
  - DS, Document Signer
- EF.SOD:
  - EF.DG -tiedostojen tiivisteet
  - DS-varmenne
  - Allekirjoitus tiivisteistä
- Todentaa sirun tietosisällön alkuperän ja eheyden
- Ei estä kopiointia tai sirun vaihtamista





# Passiivinen todennus





## Aktiivinen todennus

- Active Authentication (AA)
- ICAO: valinnainen turvamekanismi
- Haaste-vaste -menetelmä perustuen RSA-algoritmin käyttöön
- Avainpituus 1024 bittiä
- Järjestelmä varmistuu sirun aitoudesta
- Estää sirun kopioimisen ja vaihtamisen
- Ei estä tietoliikenteen salakuuntelua



# Peruspääsynvalvonta

- BAC (Basic Access Control)
- Pakollinen (EU)
- Onnistuneen protokollan jälkeen
  - Sirulta voidaan lukea kaikki muut tiedot (EF.DGx) paitsi sormenjäljet ja iiriskuva
  - Tietoliikenteen eheys ja luottamuksellisuus varmistetaan sessioavainten avulla
    - Kaikki liikenne lukulaitteiston ja sirun välillä salataan ja jokaiseen viestiin lisätään salattu tiiviste (MAC)
- Konelukukentän tietävä pystyy tekemään onnistuneen peruspääsynvalvonnan



## Laajennettu pääsynvalvonta

- EU: pakollinen menetelmä sormenjälki- ja/tai iiristietojen lukemiseen
- Varmistaa sirun aitouden
- Estää sirun kopioimisen ja vaihtamisen
- Estää salakuuntelun
- Laajennettu pääsynvalvonta  $\approx$  Sirun todennus + Lukulaitteen todennus



## Sirun todennus

- Estää sirun kopioimisen ja vaihtamisen
- Sirun todennuksen jälkeen on käytössä kryptografisesti paljon vahvemmat avaimet liikenteen luottamuksellisuuden ja eheyden varmistamiseen
- Algoritmina DH tai ECDH
- Estää sirun kopioimisen

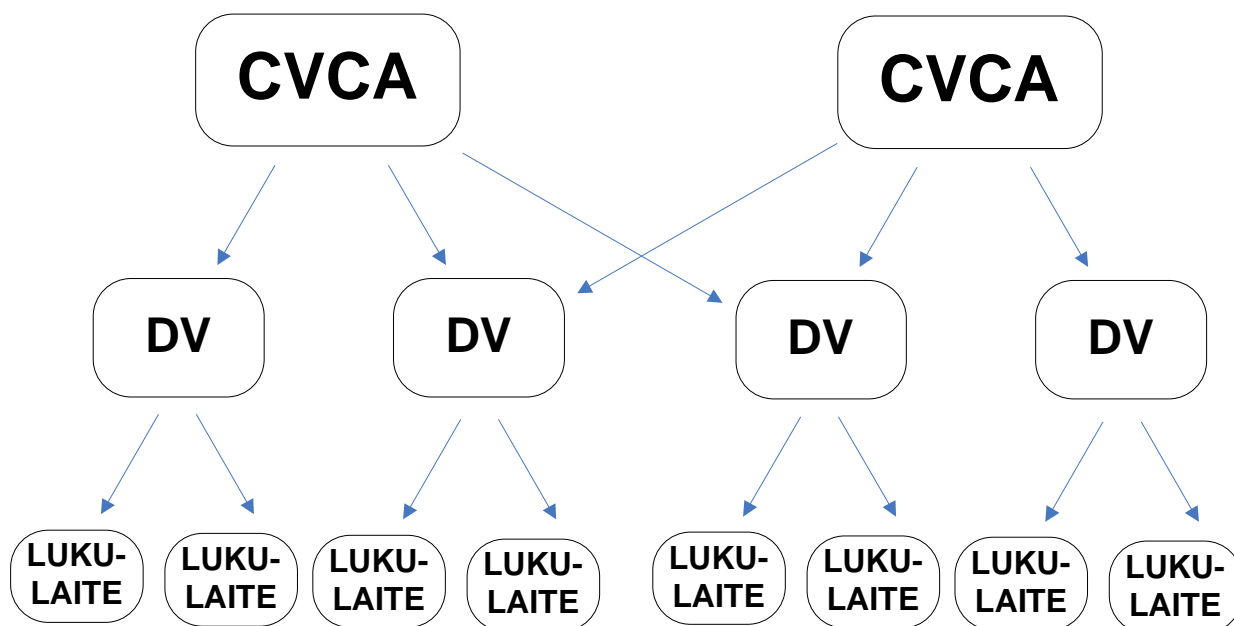


## Lukulaitteen todennus

- Lukulaitteen todennuksessa lukulaite osoittaa sirulle oikeutensa sormenjälkitietojen lukemiseen sirulta
- Sirulle on tallennettu tieto myöntäjään juurivarmenteesta (CVCA)
- Sirulle esitetään varmenneketju, joka alkaa passin myöntäneen maan juurivarmenteesta ja päättyy lukulaitteen omaan varmenteeseen
- Jos siru tarkistaa varmenneketjun onnistuneesti, niin se lähettää lukulaitteelle haasteen, jonka lukulaite allekirjoittaa varmennetta vastaavalla salaisella avaimella



# Laajennettu pääsynvalvonta





# Lukulaitteen todennus

- Algoritmivaihtoehdot
  - RSA
    - 1024, 1280, 1536, 2048 tai 3072 bittiä
    - SHA-1, SHA-256
  - ECDSA
    - SHA-1, SHA-224, SHA-256
- Jokainen maa päättää oman maansa passien lukuoikeuksien myönnöstä
- EU:n yhteinen varmennepolitiikka
  - Minimivaatimukset
  - Komissiolle kansallinen varmennepolitiikka ja auditointiraportti
- Hallinnollisen päätöksen jälkeen lukuoikeuden myöntö tapahtuu käytännössä varmenteen myöntämisellä



## Laajennettu pääsynvalvonta

- Laajennettu pääsynvalvonta edellyttää onnistunutta Lukulaitteen todennusta
- Lukulaitteen todennus edellyttää onnistunutta Sirun todennusta
- Sirun todennus edellyttää onnistunutta Peruspääsynvalvontaa
- Millään näistä ei ole mitään merkitystä, jos Passiivista todennusta ei tehdä kunnolla!



## Passijärjestelmän turvallisuus

- Turvallisuus muodostuu kokonaisuudesta
- Turvallinen asiakirja on vain yksi tekijä
- Myöntöprosessi
- Valmistusprosessi
- Käyttövaihe
  - Dokumentin tarkastaminen
  - Henkilöllisyyden varmistaminen



## Passisiru murrettu?

- Julkisuuteen tulleet väitteet passin murtamisesta perättömiä
- Passisirun voi kukin tehdä itselleen julkisten standardien mukaisesti
- Lukulaite, joka tarkistaa sirun turvamekanismit, paljastaa väärennöksen
- Kaikkein tärkeintä on passiivisen todennuksen tekeminen



# Ajokortti ja älykortti

- EU-direktiivi
  - Siru on vapaavalintainen
  - Sirun määrittelyt ovat vielä kesken
- Suomessa ei ole vielä päätöstä sirun käyttöönotosta (LVM)
- eReg
  - Association of European Vehicle and Driver Registration Authorities



## Sirun tietosisältö

- EReg Topic Group VIII
  - ISO/IEC 18013 perustaksi
  - Kolmenlaista tietoa
    - Pakolliset (EU)
    - Vapaavalintaiset (EU)
    - Kansalliset ratkaisut



## Sirun tietosisältö (eReg Topic Group VIII)

- DG1, pakollinen: kaikki ajokorttiin liittyvät perustiedot
- DG2, vapaavalintainen, lisätietoa kuljettajasta
- DG3, vapaavalintainen, lisätietoa myöntäjästä
- DG4, vapaavalintainen, kasvokuva
- DG5, vapaavalintainen, allekirjoitus
- DG6, vapaavalintainen, kasvokuvatunniste
- DG7, vapaavalintainen, sormenjälkitunniste
- DG8, vapaavalintainen, iiristunniste
- DG9, vapaavalintainen, joku muu biometrinen tunniste
- DG10, RFU
- DG11, vapaavalintainen kansallinen käyttötarkoitus



# Sirun mahdollistamat hyödyt

- Turvallisuuden parantuminen
  - Väärentäminen vaikeutuu
  - Kuljettajan luotettavampi todentaminen
- Automaation lisääminen
- Lisätietojen tallennuspaikka
- Kansalliset käyttötarkoitukset
- Sähköinen tunnistaminen



## Viitteet

- *Technical Guideline – Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Version 1.01, TR-03110*
- *MRTD Technical Report, PKI for Machine Readable Travel Documents Offering ICC Read-Only Access, International Civil Aviation Organization, Version 1.1, October 01 2004*
- *MRTD, Technical Report, Development of a Logical Data Structure - LDS for Optional Capacity Expansion Technologies, International Civil Aviation Organization, LDS 1.7 -2004-05-18, Revision 1.7, May 18 2004*
- *Machine Readable Travel Documents, Part 3 Machine Readable Official Travel Documents, Volume 2 Specifications for electronically Enabled Official Travel Documents with Biometric Identification Capability, Doc 9303, International Civil Aviation Organization, Third Edition - 2007*
- *Komission päätös 28/VI/2006 jäsenvaltioiden myöntämien passien ja matkustusasiakirjojen turvatekijöitä ja biometriikkaa koskevien vaatimusten teknisistä eritelmistä*

No, Huh  
Huh!

PASILA

