The Digital Tachograph
Ernst Bovelandner

- Senior Security Consultant
- 15 years of experience in smart cards and PKI
- Projects for the government:
  - Multi functional smart card for the Dutch MoD
  - The Dutch passport
- Projects for financial world:
  - Visa
  - MasterCard
  - ABN-Amro
- PKI government
- SmartVision
The tachograph

Instrument for registration of driving and rest periods for trucks etc.
The Digital Tachograph

- European Council Regulation 2135/98
  - Technical Specification: Annex 1B (290 pages !!)
- Instrument for registration of driving and rest periods for trucks etc.
  - Replacement of the current, analogue tachograph
  - Improved security
  - Improved enforcement
- Technical implementation based on:
  - Smart cards for data storage
  - PKI for digital signatures
Digital Tachograph and Security

• Registration of driving and rest periods
  - Integrity (‘complete and accurate’)
  - Authenticity (‘personal’)
  - Availability

• Enforcement
  - Undisputable evidence (non-repudiation)
  - Efficient enforcement
Digital tachograph: functional

- Motion sensor
- Vehicle Unit
- Tachograph Card

- Digital Tachograph
- External Media

- Print
- Download

- Pulse generation
- Clock
- Driver identification

- Recording tachograph data
- Recording driver data
Security Mechanisms

- Secure Cryptographic Device
- Mutual Authentication
- Secure Messaging
- Pairing
- Digital Signature (signature + hash)

Motion Sensor
- Processor Security Components
- MS data

Vehicle Unit
- Processor Security Components
- VU data

Tacho Card
- Processor Security Components
- TC data

VU download
TC download

Digital Signature
(signature + hash)
Number of cards to be issued
Card Issuing Process

Card Stock

Card Personalisation

Member State Certification Authority (MSCA)

Public key MSCA

Public key Card

CHR EOV

Card Management System

Card Issue

Workflow Management System

Certificates

European Certification Authority (ERCA)

MS Certificate

Card distribution
How it all might work…
Tachograph Card Personalisation

Card Issuer

Personalisation bureau

Response file

Card Distribution

Personalisation

PIN Generation

Private key

PIN letter

Certificate Content

Public key

Card Certificate
MS Certificate
European Public Key

Nationale Certification Authority

Key Generation

Hardware Security Module

Card Issuer

Personalisation data

Certificate Content
Member State CA

- Separation of RA-tasks and CA-tasks
- Key generation for cards at personaliser
- Non-standard certificates
- What is the business model of existing CA’s
- Insourcing, outsourcing or what…?  
  - Buy a CA service
  - Buy a CA product
Organizational challenges

- European regulation, national implementation
  - Hierarchical PKI model
  - Harmonisation at member state level
- Taskforce PKIOverheid model
  - Building upon ‘existing’ card issuing infrastructure
- Very tight schedule
  - 12 months after publication: type approved cards
  - 21 months after publication: fully operational
- Complex project
  - Unique in size and nature
  - Interesting issues: legal implications, enforcement, cooperation with other member states etc.
Technical challenges

• Regulation based on non-standard security mechanisms
  – Non X.509 certificates

• Requirements in ‘Annex 1b’ are not always unambiguous or clearly formulated
  – ITSEC vs. CC

• And how about ‘new’ developments…?
  – GPS, GSM
  – Migration to standard certificate format
PKIgovernment model

- Organizational structure follows the requirements of the PKIgovernment
  - Separation of roles
  - CSP requirements
  - Card issuing processes

- Technical implementation differs with respect to:
  - The certificate format
  - One certificate for all purposes

- And we all know: PKI is only for 20% a technology issue!
Status and milestones

• EU Council Regulation
  - Publication: June 2002 (we hope!)
  - Type approval tachograph cards: 1 June 2003
  - Fully operational: 1 April 2004

• Tendering
  - Workflow and card management
  - Personalisation
  - Member State Certification Authority
  - Distribution

• Card Issuing organization
  - Organizational structure in place 2003
“The best way to escape from a problem is to solve it.”

Thank you for your attention!

For more information:

**Ernst Bovelerander**

e-mail: ernst.bovelander@solvision.nl

Phone: +31 (0)6 2954 5681