Basic Access Control and Extended Access Control in ePassports

Tom Kinneging

ISO/IEC JTC1 SC17 WG3/TF5

New Technology Working Group (NTWG)
TAG/MRTD 18

18th Meeting of the Technical Advisory Group on Machine Readable Travel Documents

History

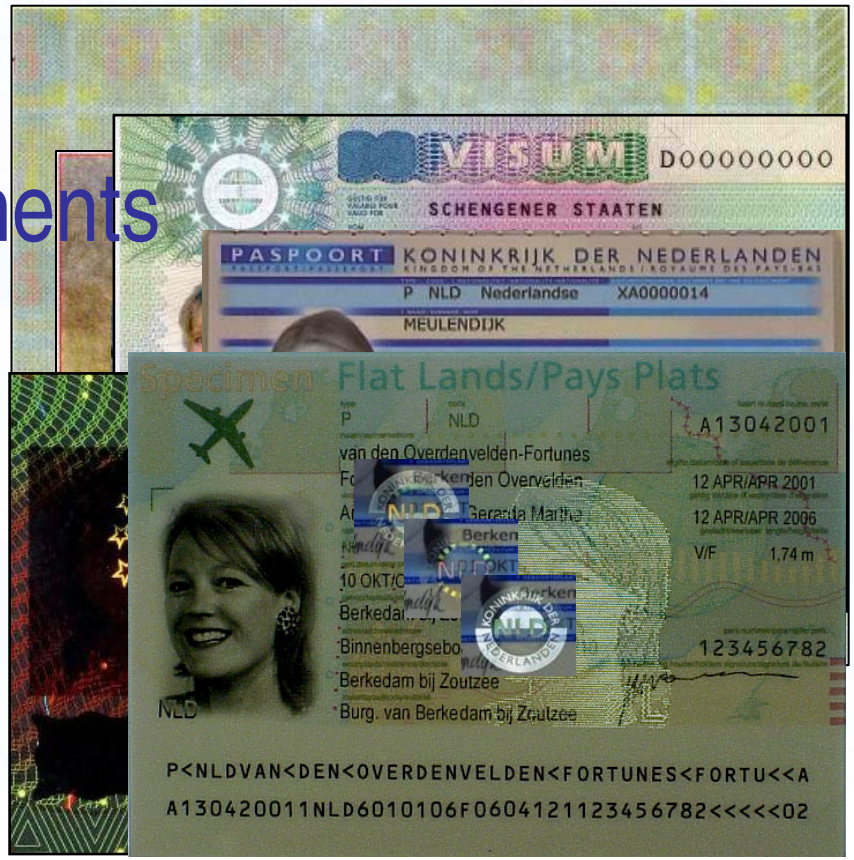
Rembrandt van Rijn

History

- Document as proof of identity
  - Protected against
    - Counterfeit
    - Manipulation
    - Copying and cloning
  - Physically
  - Electronically

Physical security

- Materials
- Security printing
- Optical variable elements
- Personalization



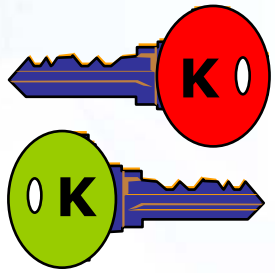
Electronic security

- Against counterfeit and manipulation
  - Passive Authentication
- Against copying and cloning
  - Active Authentication

Passive Authentication

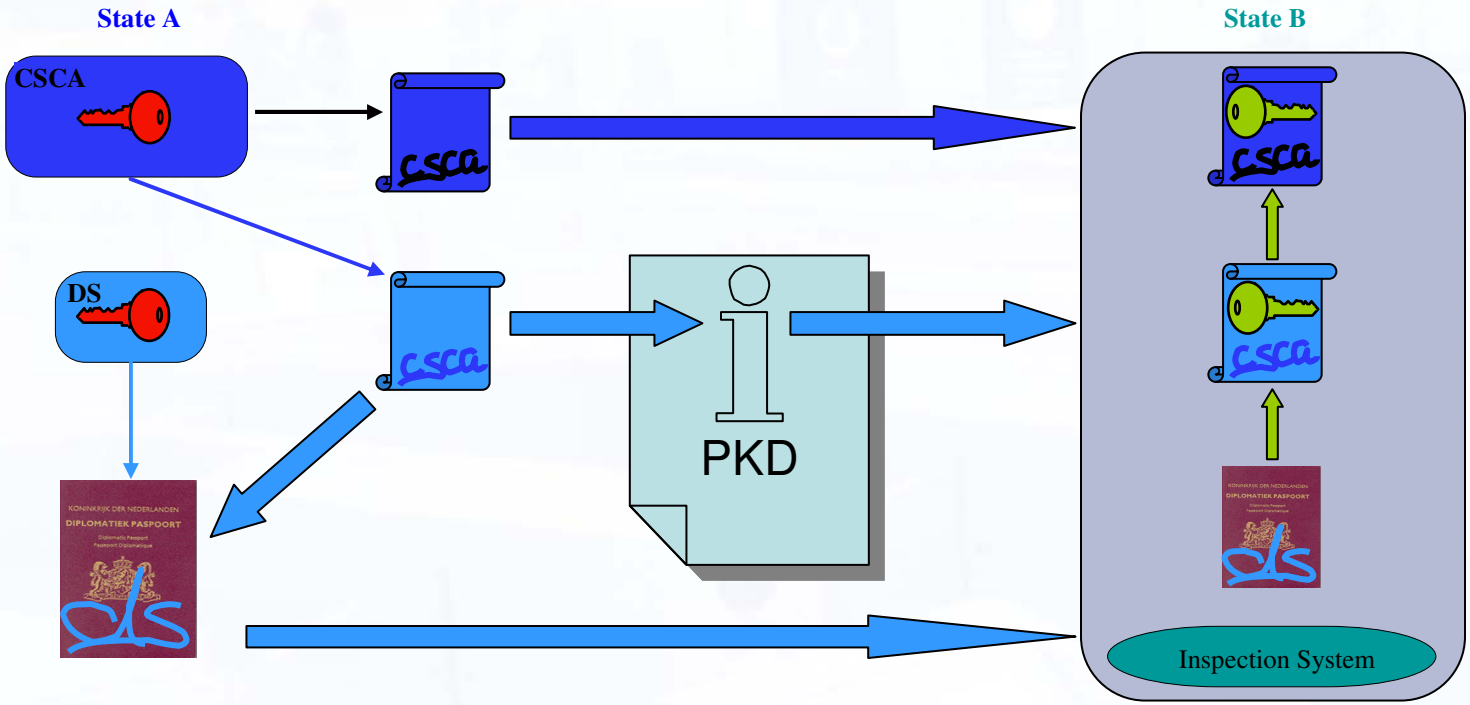
Against counterfeiting and manipulation

- Electronic signature
  - Chip data is authentic
  - Chip data has not been changed
- Cryptographic key pair
  - Private key for signing
  - Public key for verification



Passive Authentication

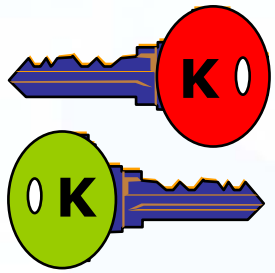
Key distribution



Active Authentication

Against copying and cloning

- Challenge response mechanism
  - Genuine combination chip and data
- Cryptographic key pair
  - Private key in chip's secure memory
  - Public key in Data Group 15



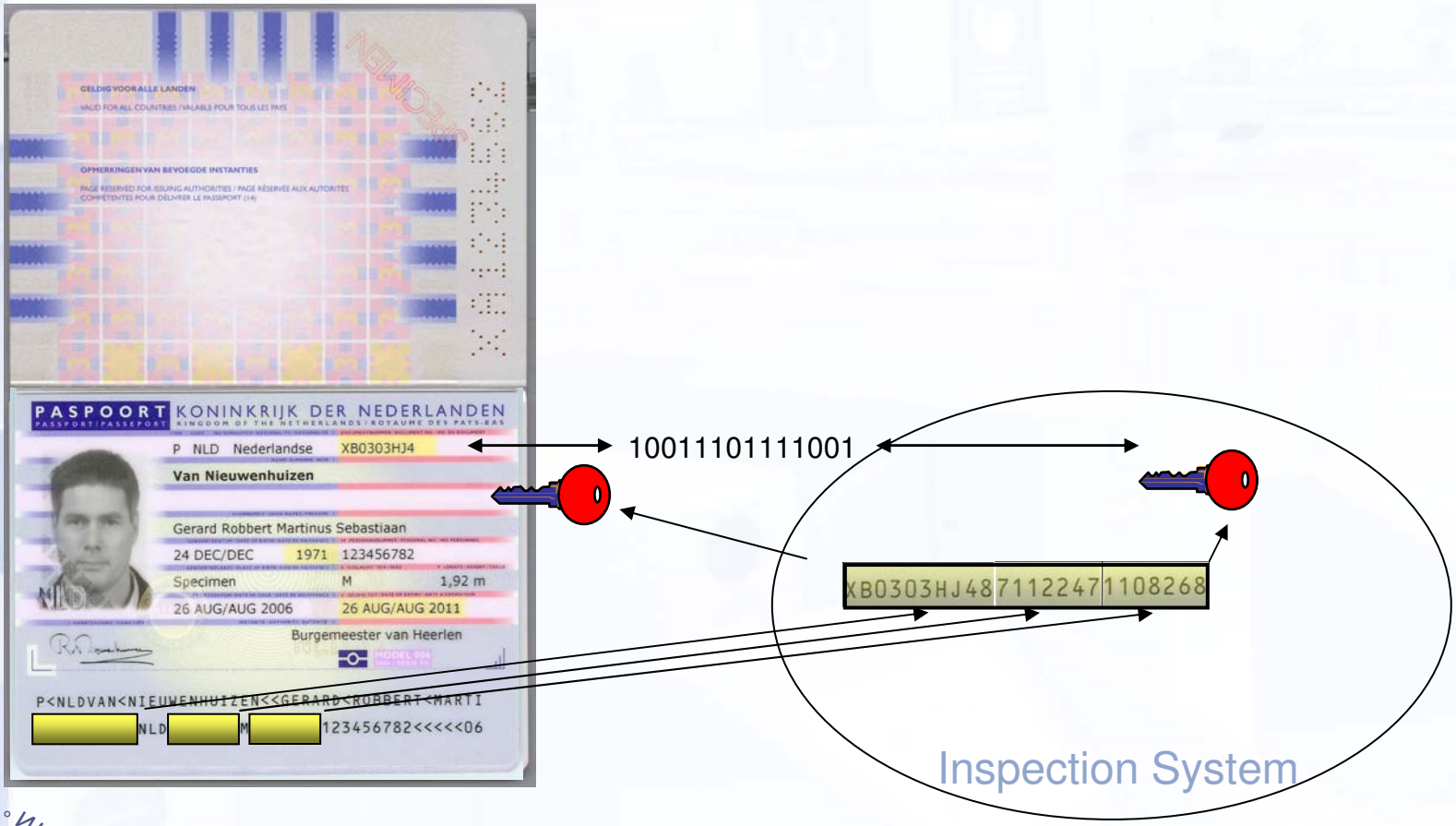
Privacy

- No problem for conventional passport
  - You cannot read a closed book
- Introduction RF chip
  - Skimming
    - Reading data from the RF chip
  - Eavesdropping
    - Reading along the chip-reader communications

Basic Access Control

Inspection System

Basic Access Control



Basic Access Control

- Strong or weak?
  - Skimming no problem
  - Eavesdropping risks can be diminished
    - Random document number
- Lifetime
  - Computer power increases
  - Planned evaluation, investigate successor

Extended Access Control

- Doc 9303 recommends a more strict protection of sensitive data
  - Finger print
  - Iris
- To be realized
  - At a national or bilateral level
  - Through Encryption or Extended Access Control

Extended Access Control

- Two protocols
  - Chip Authentication
  - Terminal Authentication

Chip Authentication

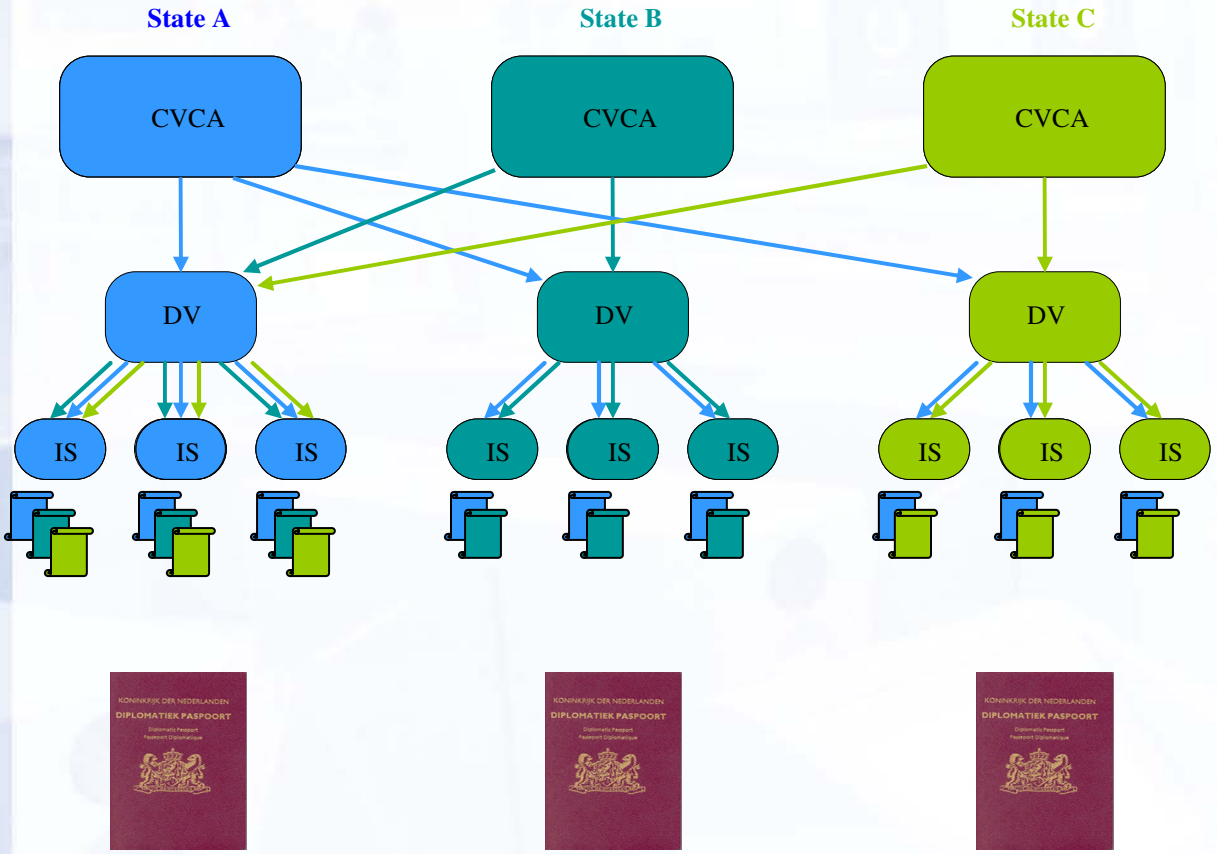
- Strong secure communications
  - First BAC
  - Replace BAC keys
- Implicit verification of genuine chip
  - Like Active Authentication
- Can be used on its own

Terminal Authentication

- After Chip Authentication
- MRTD chip verifies access rights
  - Verify certificates present in I.S.
  - Grant access to sensitive data
- Certificate issued by MRTD issuer

Terminal Authentication

Certificate distribution



Terminal Authentication

- Opens up other possibilities
  - Access rights verification for
    - Updating chip contents
    - Writing visa information
    - Writing travel records

Summary

- Passive authentication
  - Enables the inspection system to verify that
    - The chip contents is authentic
    - The chip contents has not been altered
- Active authentication
  - Enables the inspection system to verify that
    - The chip contents is not a copy
    - The authentic chip is in the document

Summary

- Basic Access Control
  - Enables the chip system to verify that
    - The passport is opened for inspection
- Extended Access Control
  - Enables the chip to verify that
    - The inspection system is authorized to read sensitive data

Summary

- Chip Authentication
  - Can be used on its own for
    - Strong secure communications
    - Alternative to Active Authentication
- Terminal Authentication
  - Authorized access
    - Acces to sensitive data
    - Writing and updating chip contents

Working Paper 6

- Action by the TAG
  - Investigate BAC successor
  - Continue study to global standard for EAC
    - based on implementation experiences in Europe
  - Recognize Chip Authentication
    - as stand-alone protocol
  - Recognize Terminal Authentication
    - as general authentication mechanism

Thank you
for your attention

Tom Kinneging

ISO/IEC JTC1 SC17 WG3/TF5

New Technology Working Group (NTWG)
TAG/MRTD 18

18th Meeting of the Technical Advisory Group on Machine Readable Travel Documents