



Extended Access Control: Infrastructure and Protocol

Interop-Test, Berlin 2006

Dennis Kügler
Federal Office for Information Security

2006-06-01

Goals of Extended Access Control

- **Fingerprints are sensitive Data**
 - Basic Access Control is not sufficient
- **Requirements**
 - Strong session encryption
 - *Chip Authentication*
 - Access restricted to authorized terminals
 - *Terminal Authentication*
- **Extended Access Control**
 - Chip Authentication + Terminal Authentication



Chip Authentication



- **Copy protection**
 - Chip-individual key pair
 - Implicit authentication of the chip
 - Strong encryption/integrity protection
- **Add-on to Basic Access Control**
 - BAC protection against skimming: **good**
 - BAC protection against eavesdropping: **sufficient**
 - BAC + CA = strong encryption

- **Ephemeral-Static (EC)-Diffie-Hellman**
 - **Chip:** Chip-individual static key pair
Public Key stored in the LDS (signed)
Private Key stored in secure memory
 - **Terminal:** Ephemeral key pair
dynamically chosen by the terminal
 - ECDH (224 Bit) asymmetric key agreement
 - 3DES (112 Bit) symmetric encryption/integrity protection
- **Implicit Authentication of the chip**
 - Only a genuine chip is able to communicate securely

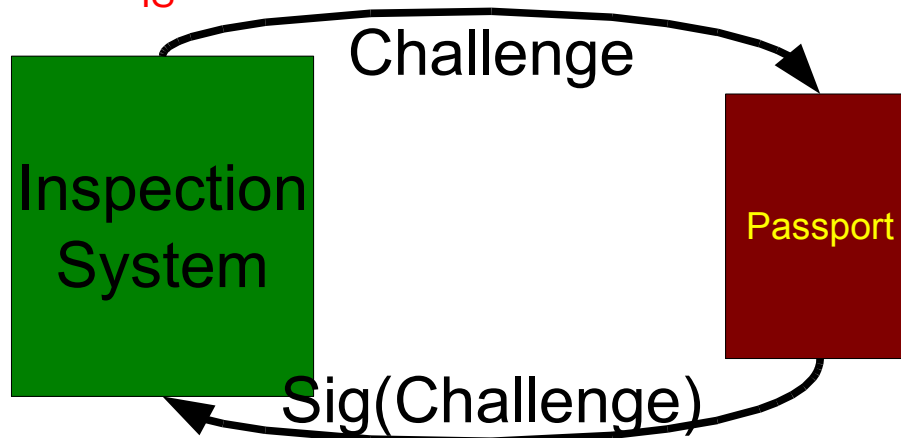
Comparison

- **Passive Authentication**
 - Static signature over all passport data
 - **Problem:** Signature can be copied
- **Active Authentication**
 - Explicit authentication of the chip
 - Chip-individual key pair used for Challenge-Response
 - **Problem:** Challenge Semantics
- **Chip Authentication**
 - Implicit authentication of the chip
 - Chip-individual key pair used for Key Agreement

- Active Authentication

- An inspection system can assign its challenges a “hidden semantic”
- Signature issued by the chip is transferable

Challenge =
 $H(\text{Sig}_S(\text{MRZ}, \text{Time}, \text{Location} \dots))$





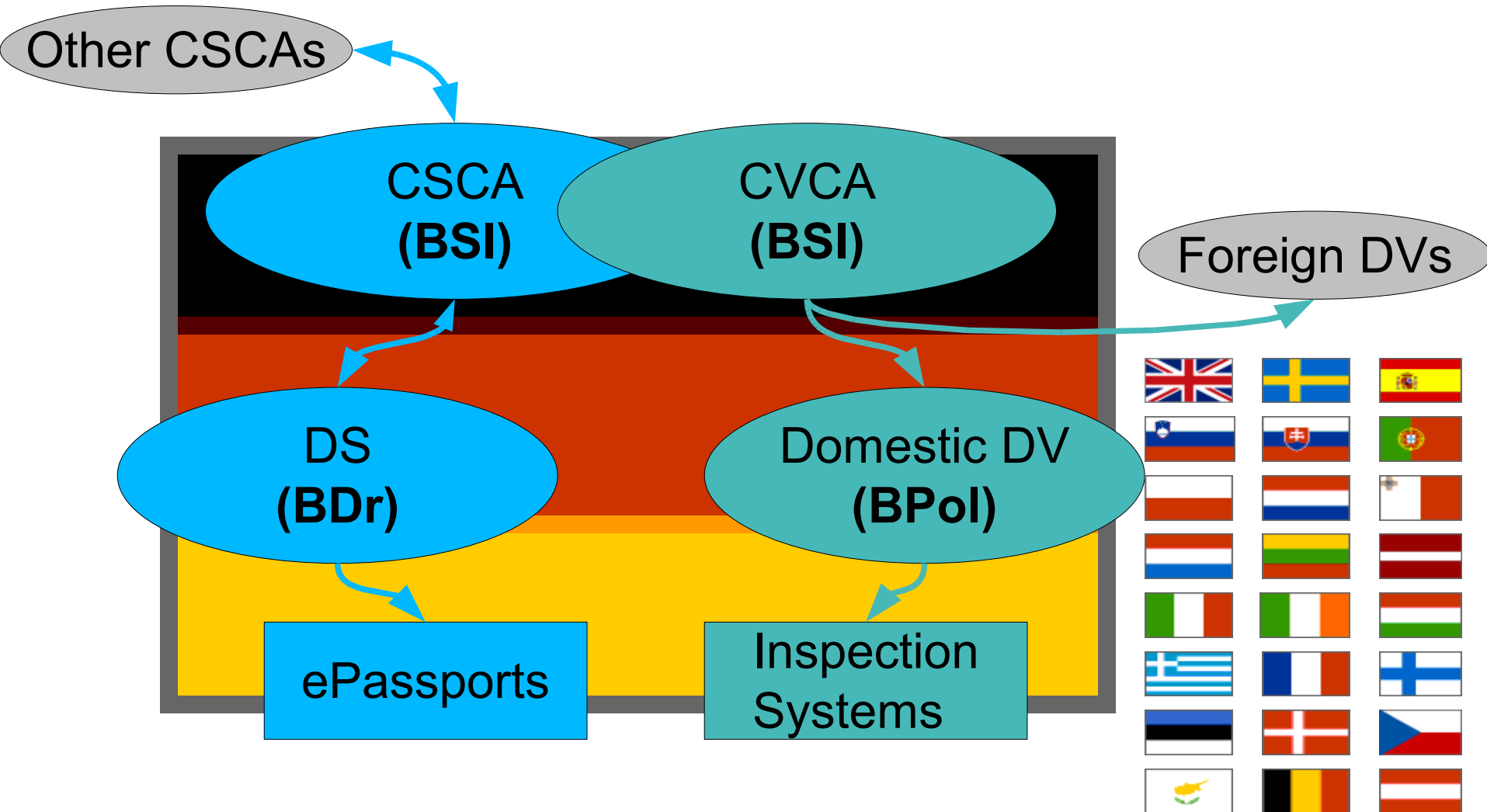
Terminal Authentication



- **Authentication of Inspection Systems**
 - Inspection System-individual key pair
 - *Card-Verifiable Certificate* indicates access rights
- **Lost and stolen Inspection Systems**
 - Revocation of CV Certificates is impossible
 - **Problem:** Chip would have to access & check CRLs
 - Alternative: Short validity periods
 - **Problem:** Chip has no source of time

- **Issuance of ePassports**
 - Goal: Protection against counterfeiting
 - Passive Authentication
 - Document Signer digitally signs stored data
 - Signature is checked by Inspection Systems
- **Verification of ePassports**
 - Goal: Protection against unauthorized access
 - Terminal Authentication
 - CV-Certificates / Challenge-Response
 - Certificate chain etc. is checked by the chip

ePassport Public Key Infrastructure(s) in Germany



Card Verifiable Certificates

- Data contained in a certificate
 - Certification Authority Reference
 - Public Key
 - Certificate Holder Reference
 - Certificate Holder Authorization
 - Certificate Effective Date
 - Certificate Expiration Date
 - ...
 - Signature

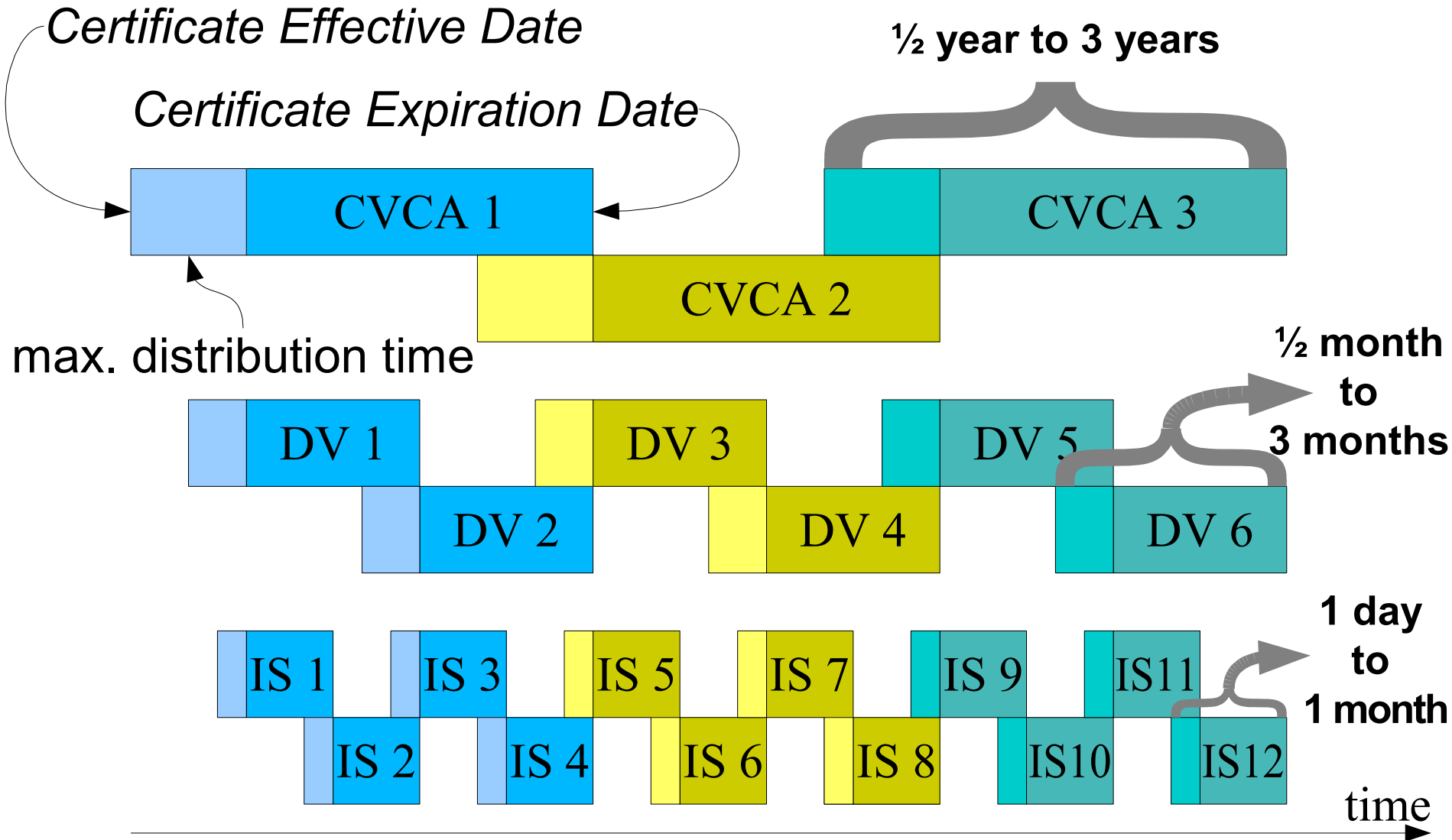
Generate your own certificates online!
<http://www.flexsecure.eu:7755>

Encoding of Access Rights


7	6	5	4	3	2	1	0	
xx	-----							Role
11	-----							CVCA
10	-----							DV domestic
01	-----							DV foreign
00	-----							IS
--	xxxxxxx							Access Rights
--	0000--							Reserved
--	-----1-							Read access to iris data
--	-----1							Read access to finger print data

Logical "and" of relative rights	
11000011	CVCA
01000001	DV
<u>00000011</u>	IS
00000001	<i>effective rights</i>

CV Certificate Scheduling



Inspection Procedure (EU)

- 
- Basic Access Control
 - Secure Messaging is started (**weak encryption**)
 - **Access rights:** “less-sensitive data“
 - **Read Chip Public Key (DG 14)**
 - Chip Authentication
 - Secure Messaging is restarted (**strong encryption**)
 - **Read Document Security Objects**
 - Chip is genuine
 - **Read less-sensitive Data (e.g. MRZ, facial image)**
 - Terminal Authentication
 - **Access rights:** “sensitive data (according to certificate chain)”
 - **Read sensitive Data (e.g. fingerprints)**

Contact

Federal Office for Information Security
(BSI)
Section 314

Dr. Dennis Kügler
Godesberger Allee 185-189
53175 Bonn, Germany

Tel: +49-1888-9582-183
Fax: +49-1888-9582-90-183

dennis.kuegler@bsi.bund.de

<http://www.bsi.bund.de>

