

Konzept und Status der Extended Access Control (EAC) PKI

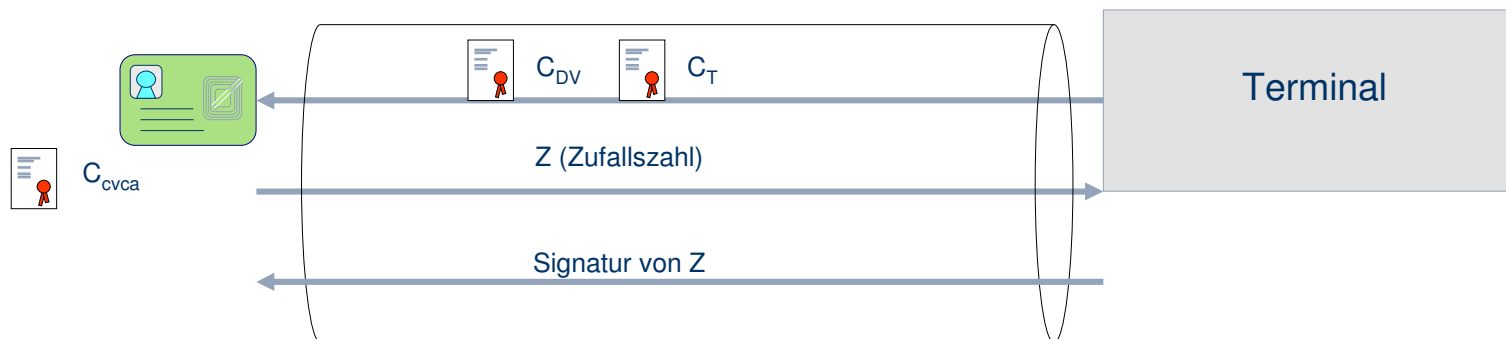
Andrea Klenk, media transfer AG

CAST Forum "Public-Key-Infrastrukturen"
28.01.2010

- ICAO Doc 9303: internationaler Standard für Reisedokumente, 3 Teile (maschinenlesbare Reisepässe, Visa und Identitätsdokumente)
 - BAC: Basic Access Control (opt.)
 - Passive Authentisierung
 - Aktive Authentisierung (opt.)
- BSI TR-03110 : nationaler und Europäischer Standard für erweiterte Sicherheitsmechanismen bei maschinenlesbaren Reisedokumenten
 - EAC: Extended Access Control V1/V2
 - Chip Authentisierung
 - Terminal Authentisierung
 - Grundlagen der EAC PKI
 - PACE: Passwort Authenticated Connection Establishment
 - RI: Restricted Identification
- BSI TR-03117 : eCards mit kontaktloser Schnittstelle als sichere Signaturerstellungseinheit
- CSN 36 9791: tschechischer und Europäischer Standard
 - CVCA Key Management Protocol for SPOC (Single Point of Contact)

- Elektronischer Reisepass (ePass):
 - internationales und europäisches Reisedokument
 - ICAO Doc 9303 Teil 1 (BAC, Passive Auth.)
 - BSI TR-03110 (EAC V1)
 - SPOC
 - beinhaltet nur eine Anwendung: ePass
- Elektronischer Personalausweis (ePA)
 - nationales Ausweisdokument
 - ICAO Doc 9303 Teil 3 (Passive Auth.)
 - BSI TR-03110 (EAC V2, PACE, RI)
 - BSI TR-03117
 - beinhaltet drei Anwendungen: ePass, eID, eSign
- Elektronischer Aufenthaltstitel (eAT) (in Planung)
 - internationales und europäisches Reisedokument und nationales Ausweisdok.
 - ICAO Doc 9303 Teil 1 und 3 (BAC, Passive Auth.)
 - BSI TR-03110 (EAC V1 und V2, PACE, RI)
 - BSI TR-03117
 - beinhaltet drei Anwendungen: ePass, eID, eSign

Prinzip der EAC Terminal Authentisierung



Ziel: verlässliche Authentisierung des Terminals gegenüber Ausweis/Bürger
Festlegung der konkreten Zugriffsrechte auf die Anwendungen des Ausweises

- ePass Anwendung (Reisepass und Personalausweis, in unterschiedlicher Ausprägung)
 - MRZ
 - Biometrische Merkmale (Gesicht, Fingerabdruck, Iris)
- eID Anwendung (Personalausweis und Aufenthaltstitel)
 - Vor-, Nachname, Künstlername, Titel
 - Adresse, Geburtsdatum / -ort
 - Nationalität, Geschlecht
 - Gültig bis
 - Gemeindekennzahl
- eSign Anwendung (Personalausweis und Aufenthaltstitel)
 - Schlüsselpaar und Zertifikat für QES

- Inspection Systems (Reisepass)
 - hoheitliche Anwendungen (Grenzkontrolle, national und international)
 - lesender Zugriff auf ePass Anwendung
 - 2 Klassen:
 - basic inspection system gemäß ICAO (BAC, Zugriff auf MRZ und Gesichtsbild)
 - extended inspection system: „advanced authentication procedure“ gemäß TR 3110 (Zugriff auf weitere biom. Daten)

- Inspection Systems (ePA)
 - hoheitlichen Anwendungen (Identitätsfeststellung)
 - lesender Zugriff auf ePass Anwendung, lesender Zugriff auf alle Daten der eID Anwendung
 - „general authentication procedure“ gemäß TR 3110

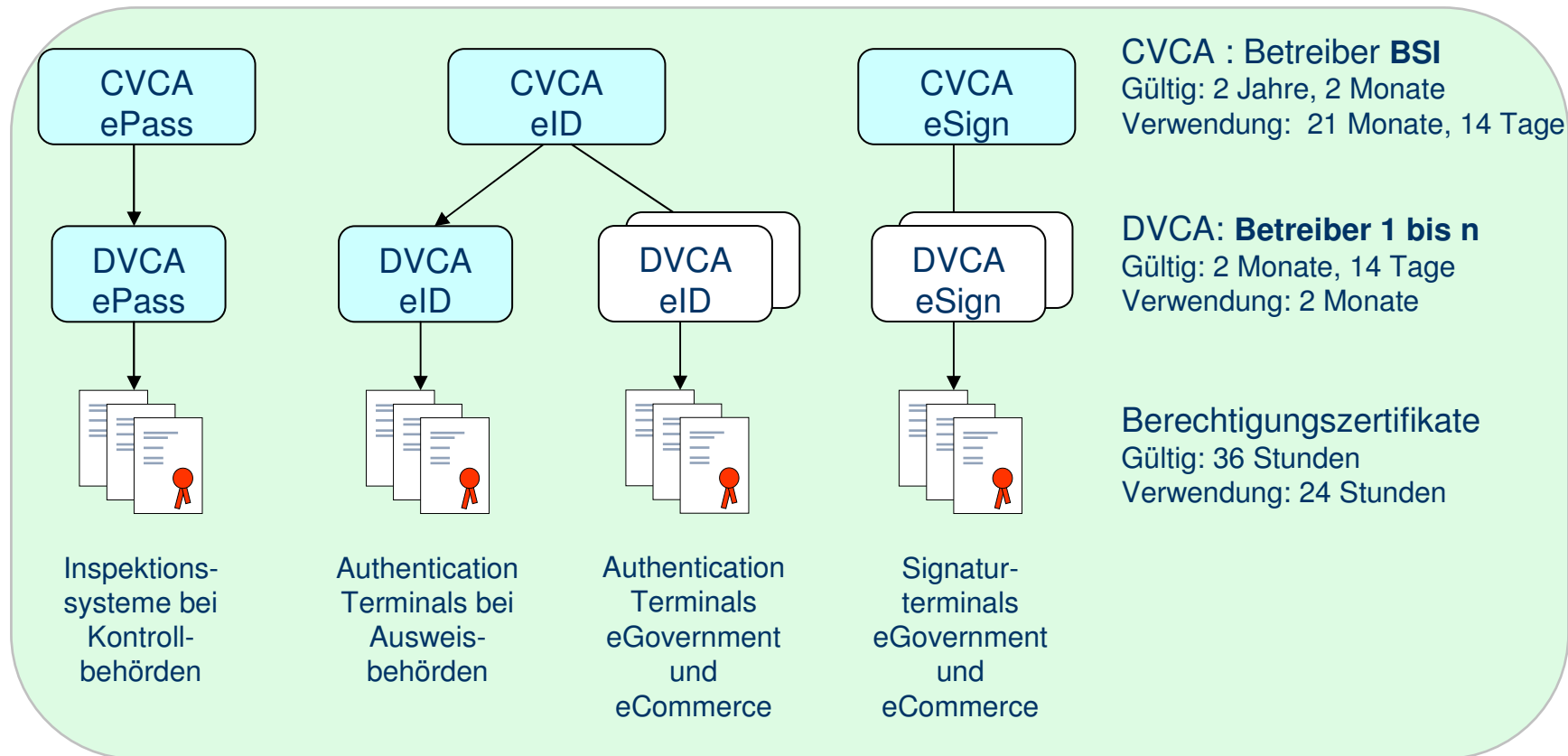
- Authentication Terminals
 - Lesender und/oder schreibender Zugriff auf Datengruppen der eID Anwendung
 - schreibender Zugriff auf eSign Anwendung
 - Terminals bei Ausweisbehörden, eCommerce und eGovernment
 - „general authentication procedure“ gemäß TR 3110

- Signature Terminals
 - Zugriff auf eSign Anwendung zur Erzeugung QES
 - Terminals in eCommerce und eGovernment
 - „general authentication procedure“ gemäß TR 3110

Einsatzbereiche und Zugriffsrechte auf Anwendungen

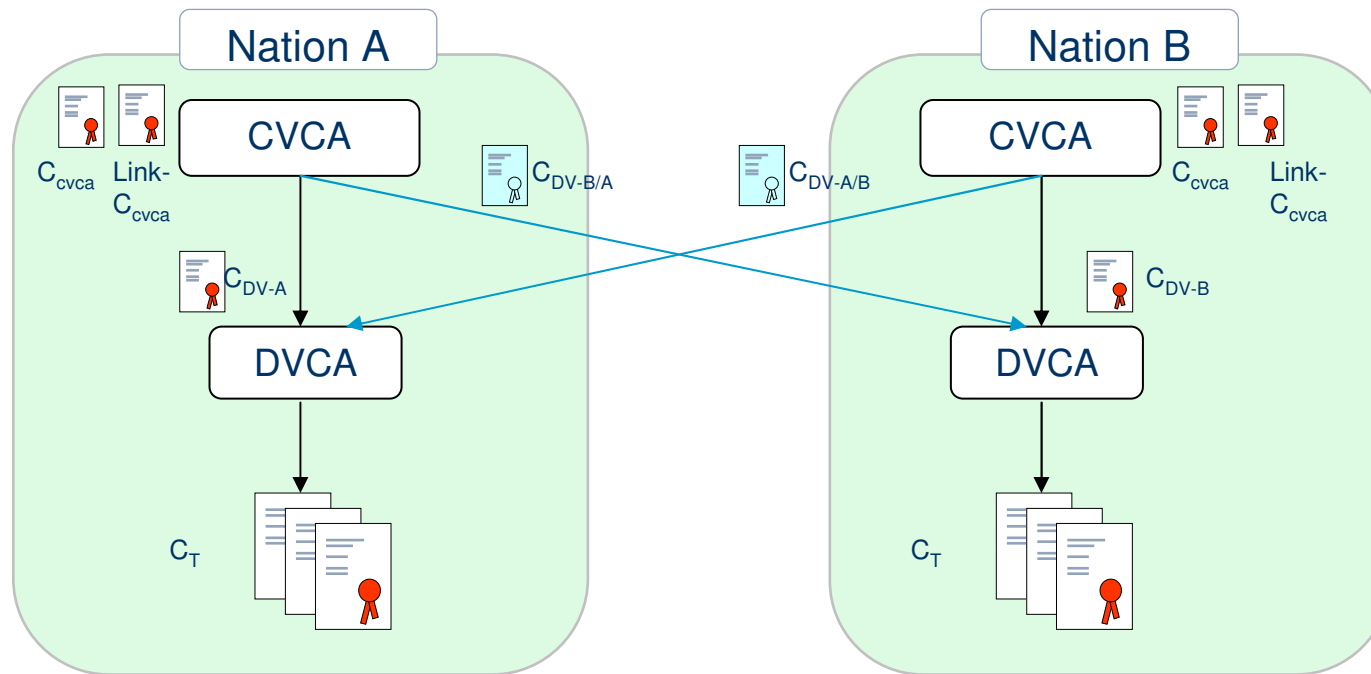
Einsatzbereich		Anwendung	lesend	Schreibend
Hoheitlich	Ausweisbehörden	ePass	QS bei Ausgabe	-
		eID	Auskunfts- begehren	Adresse, Gemeindeschl. PIN-Managem.
		eSign	-	-
	Kontrollbehörden	ePass	Identitätsfest- stellung	-
		eID	inklusive Adresse	-
		eSign	-	-
Nicht-hoheitlich	Online Terminal	ePass	-	-
		eID	Identitätsnachweis Altersverifikation	-
		eSign	qual. Signatur	Schlüsselgenerierung Zertifikatsspeicherung

Struktur der nationalen EAC PKI



 hoheitlich

- Certificate Body
 - Certificate profile identifier: Version 1
 - Certification authority reference: identifiziert den PK der ausgebenden CA
 - Country code
 - Holder Mnemonic (variable Länge, max. 9 byte)
 - Sequence number (5 byte)
 - Public key
 - Certificate holder reference: identifiziert den PK des Zertifikats
 - Certificate holder authorization template
 - Object id: Terminaltyp und Format der nachfolgenden Daten
 - Datenobjekt, das die Rolle in der Hierarchie und die konkreten Zugriffsrechte kodiert
 - Certificate effective date: Generierungsdatum
 - Certificate expiration date
 - Certificate extensions (opt.)
 - Certificate description
 - Terminal sector
- Signature



 $C_{DV-B/A}$ Von A ausgestelltes Cross- Zertifikat für DVCA von B

 $C_{DV-A/B}$ Von B ausgestelltes Cross- Zertifikat für DVCA von A

- Brussels Interoperability Group (BIG):
 - Technische Arbeitsgruppe der EU Mitgliedsstaaten und Staaten des Schengener Abkommens
 - Ziel: einheitliche Interpretation der EU Richtlinien und Herstellung von Interoperabilität bei europ. Reisedokumenten
 - Durchführung von Test Events bzgl. Konformität und Interoperabilität zu den internat. und europäischen Standards für Reisedokumente (Berlin 2006, Prag 2008)
 - u.a. Erarbeitung des SPOC Konzepts, das in CSN 36 9791 beschrieben ist
- SPOC (Single Point of Contact):
 - Komponente, die verantwortlich ist für EAC PKI Key Management Operationen zwischen Nationen
 - Jeweils bilateral zwischen zwei Nationen

- Teilnehmer an PKI Interop Tests beim Event Prag 2008:
 - Tschechien
 - Deutschland
 - Spanien
 - Groß Britanien
 - Österreich
 - Slovenien
 - Hongkong
 - Schweiz
 - Macao
 - Portugal
 - Niederlande
 - Schweden

Vielen Dank für Ihre Aufmerksamkeit.

Andrea Klenk

media transfer AG (mtG)

Dolivostraße 11

64293 Darmstadt

www.mtg.de

Tel. 06151 819313

aklenk@mtg.de