Schweizer Pass
cnlab Herbsttagung 2021

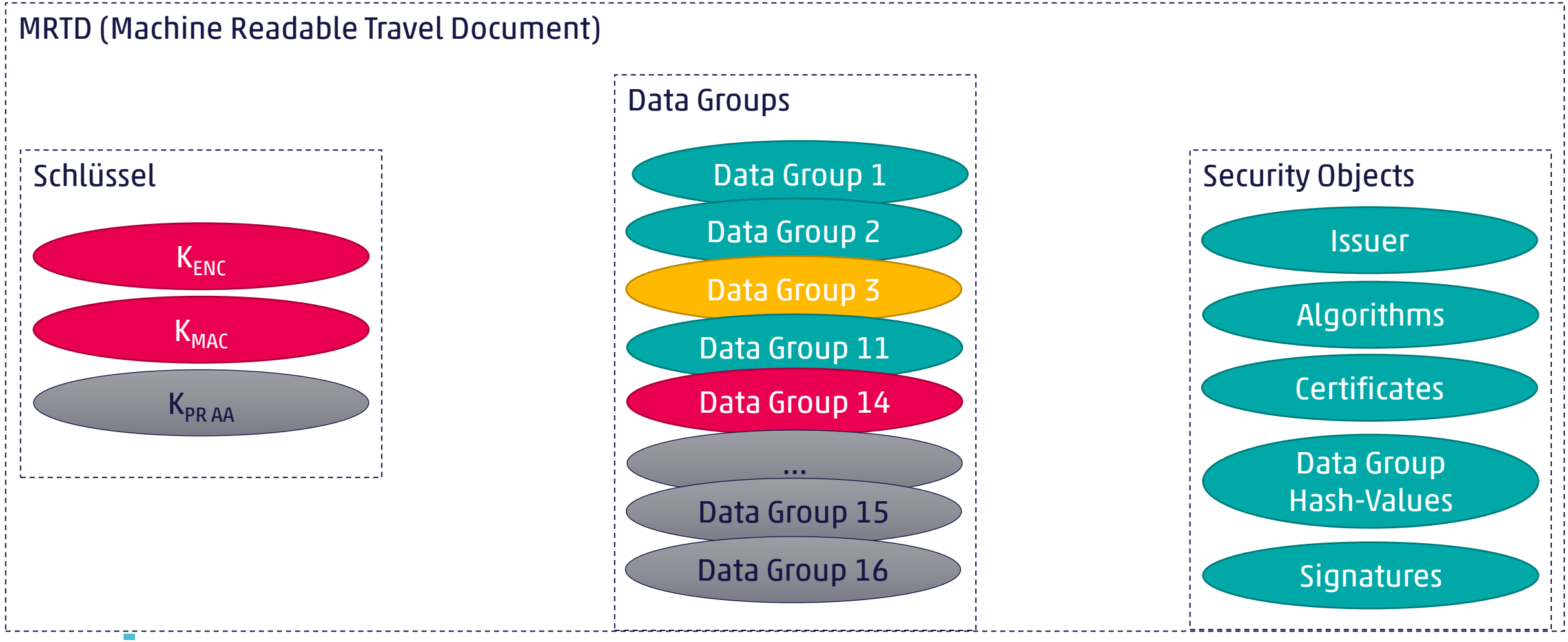
Dominic Peisker
Kosmos, 8. September 2021

cnlab

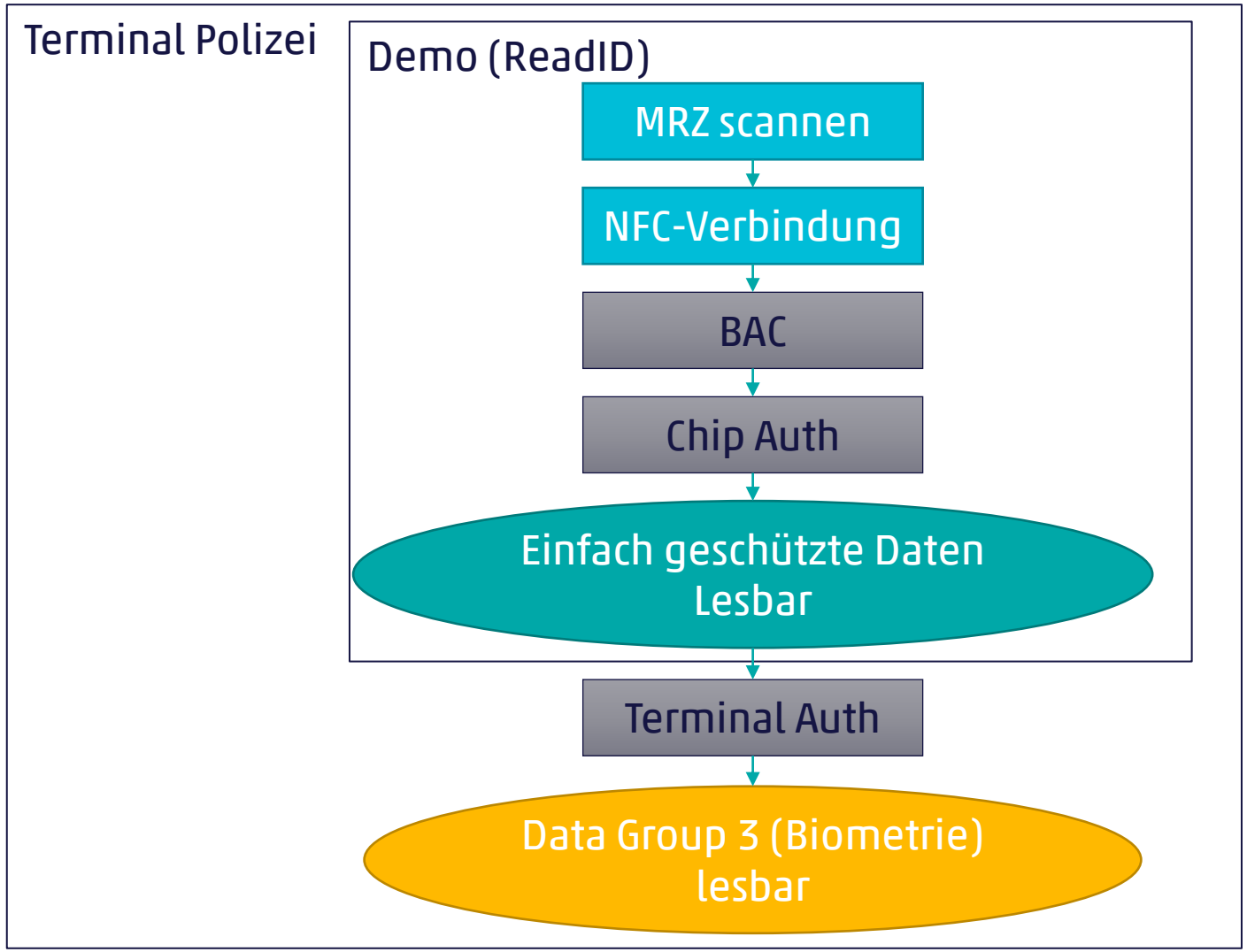
Der Schweizer Pass

- Aktuelle Version (Pass 10) wird seit Januar 2010 herausgegeben
- Pass enthält einen Chip, der via NFC ausgelesen werden kann
- Auf dem Chip enthalten sind
  - Optisch sichtbare Informationen
    - Foto und Textangaben
  - Fingerabdrücke (Biometrie)
  - Sicherheitsdaten (Schlüssel, Zertifikate, Signaturen)
- In der MRZ (Machine Readable Zone) sind Angaben zu Pass und Person codiert.

Daten auf dem Schweizer Pass



Lesevorgang



Demo

Vielen Dank für Ihre Aufmerksamkeit_

Dominic Peisker

info@cnlab-security.ch
+41 55 214 33 40

cnlab security AG
Obere Bahnhofstrasse 32b
CH-8640 Rapperswil-Jona
Switzerland

cnlab

Der Schweizer Pass - Zusatzinfos

- MRZ-Check Digits
  - Es gibt je eine Prüfziffer für Document ID, Geburtsdatum, Ablaufdatum und die gesamte 2. Zeile der MRZ.
  - Prüfziffern werden wie folgt berechnet:

A special check digit calculation has been adopted for use in MRTDs. The check digits shall be calculated on modulus 10 with a continuously repetitive weighting of 731 731 ..., as follows.

Step 1. Going from left to right, multiply each digit of the pertinent numerical data element by the weighting figure appearing in the corresponding sequential position.

Step 2. Add the products of each multiplication.

Step 3. Divide the sum by 10 (the modulus).

Step 4. The remainder shall be the check digit.

For data elements in which the number does not occupy all available character positions, the symbol < shall be used to complete vacant positions and shall be given the value of zero for the purpose of calculating the check digit.

When the check digit calculation is applied to data elements containing alphabetic characters, the characters A to Z shall have the values 10 to 35 consecutively, as follows:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35

Schutz der Daten

- Daten sind gespeichert in 16 Data Groups
- Zusätzliche Sicherheitsdaten (Zertifikate, Schlüssel, Signaturen)
- Die Hash-Werte der Data Groups sind mit einem Zertifikat (Document Signer) signiert abgelegt.
- Das Document Signer Zertifikat ist von der Country Signing CA (CSCA) signiert
- Zugang zu den Data Groups ist unterschiedliche eingeschränkt.
  - Sichtbare Daten (z.B. Foto, MRZ, Angaben zu Person und Dokument) sind allgemein lesbar
    - Basic Access Control (BAC)
    - Password Authenticated Connection Establishment (PACE) → In dieser Demo nicht behandelt.
  - Fingerprints sind zusätzlich geschützt
    - Extended Access Control (EAC)
- Schutz der Integrität der Daten
  - Schutz durch Passive Authentication

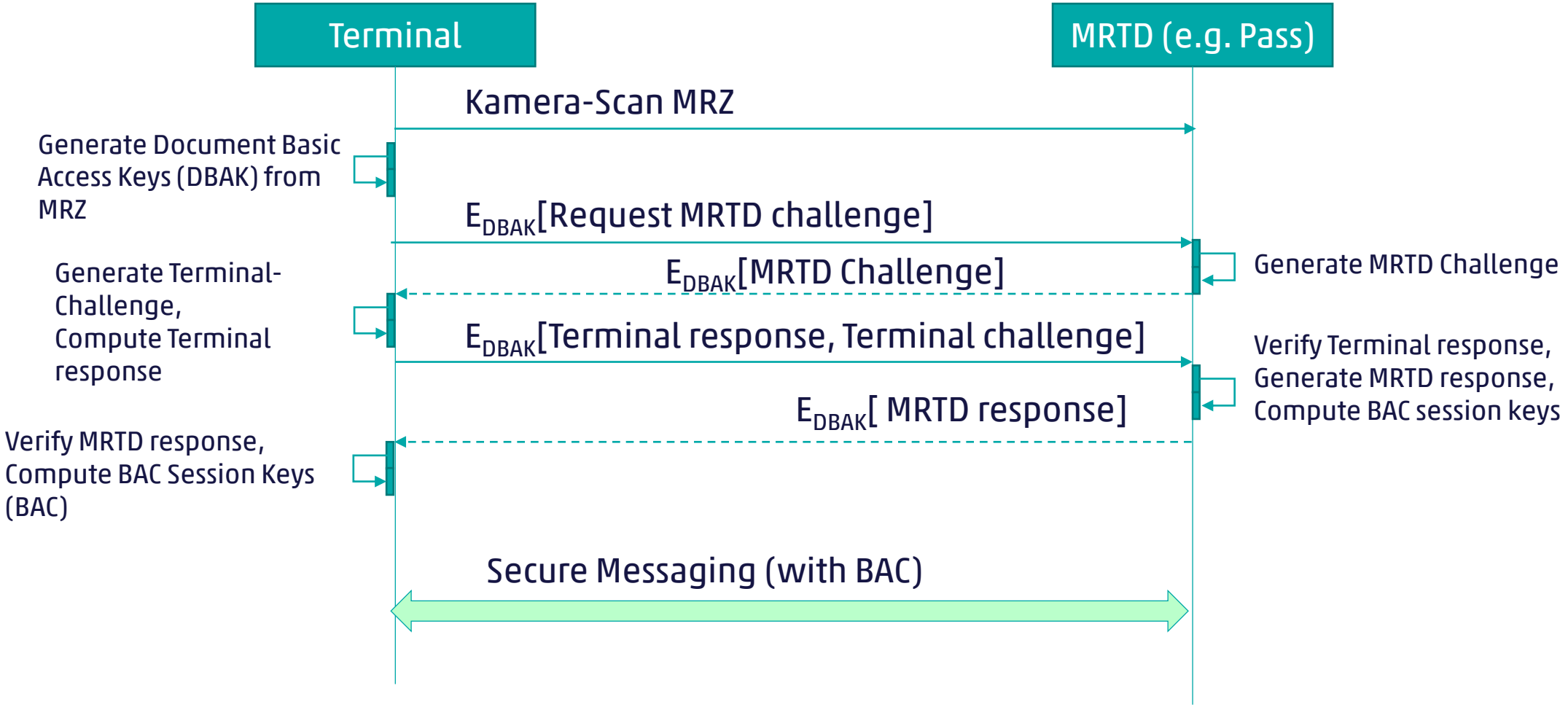
Data Groups

- **Gruppe 1**: MRZ
- **Gruppe 2**: Gesicht (Foto des Ausweises)
- **Gruppe 3**: Fingerprint (Geschützt mit EAC)
- Gruppe 4: Iris
- Gruppe 5: Foto (zusätzliche)
- Gruppe 6: Reserviert
- Gruppe 7: Unterschrift
- Gruppe 8 bis 10: Noch nicht definierte Elemente
- **Gruppe 11**: Angaben zur Person
- Gruppe 12: Zusätzliche Angaben
- Gruppe 13: Optionale Details
- **Gruppe 14**: Security Optionen
- Gruppe 15: Active Authentication Public Key Information
- Gruppe 16: Notfallkontakte
- Nur Gruppe 1 und 2 müssen vorhanden sein (Mandatory)

Schutz der Daten – Basic Access Control (BAC)

- Schutz vor Skimming (Auslesen der Daten, online) und Eavesdropping (Abhören, offline)
- Sicherheit basiert auf der MRZ
  - Optischer Zugang zur MRZ ist erforderlich
    - Aber: Brute-Force, tiefe Entropie der MRZ
  - Kenntnis der MRZ gibt Zugang zu den nicht speziell geschützten Daten auf dem Chip
- Verfahren
  - Aus der MRZ werden initiale symmetrische Schlüssel abgeleitet (Document Basic Access Keys)
    - Document ID, Geburtsdatum, Ablaufdatum
    - Wird für die Verschlüsselung des folgenden Challenge-Response Verfahrens verwendet.
  - Mittels Challenge-Response Verfahren werden die Session-Keys generiert
  - Je ein Schlüssel für Verschlüsselung und Berechnung des MAC (Message Authentication Code)
  - Basiert auf 3DES

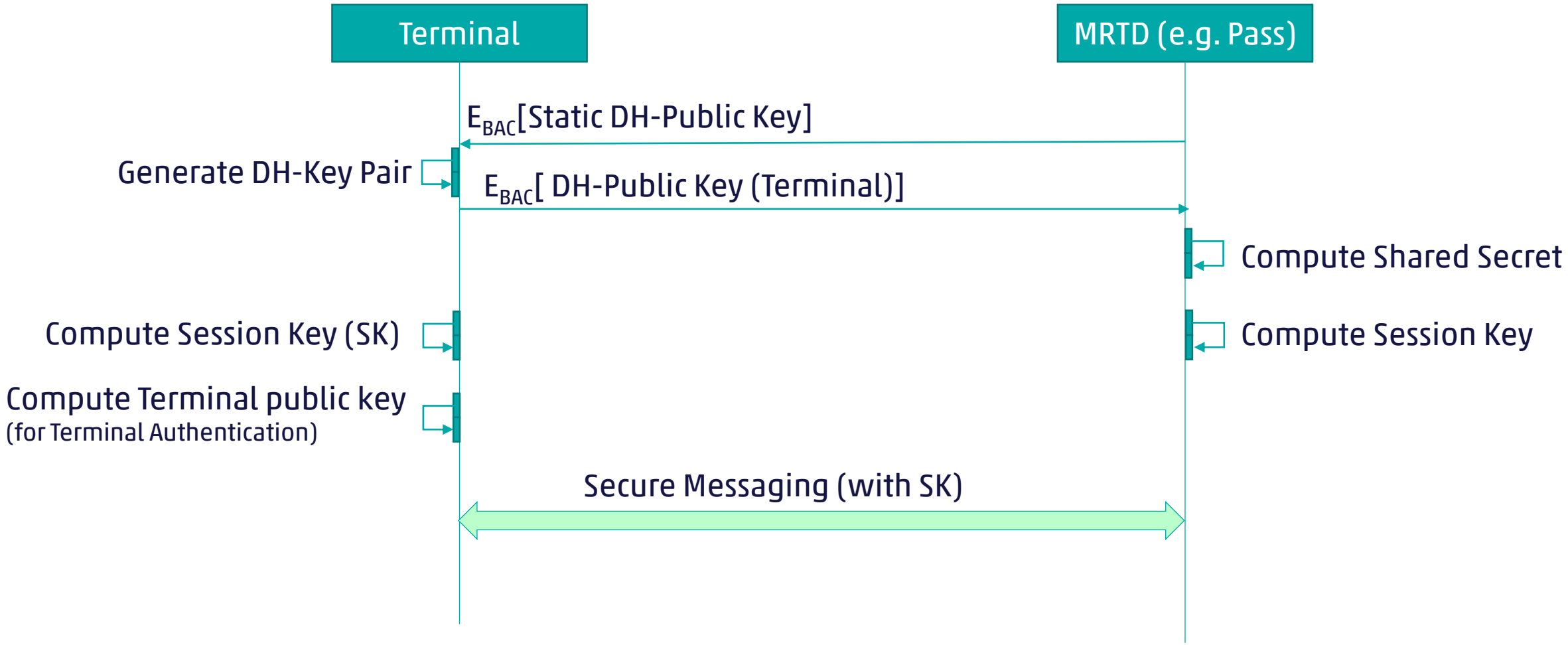
Basic Access Control (vereinfachte Darstellung)



Chip Authentication

- Wird für die Authentisierung des Chip sowie für den Aufbau einer sicheren Verbindung zwischen MRTD und Terminal genutzt
  - Verfahren basiert auf DHE
  - Statisches Key-Pair ist auf dem MRTD (Machine Readable Travel Document) gespeichert
    - In Data Group 14
      - Zugriff ist nach erfolgreicher BAC erlaubt
    - Authentizität wird über Passive Authentication geprüft
- Nach erfolgter Chip Authentication werden zukünftige Messages mit dessen (starkem) Key verschlüsselt

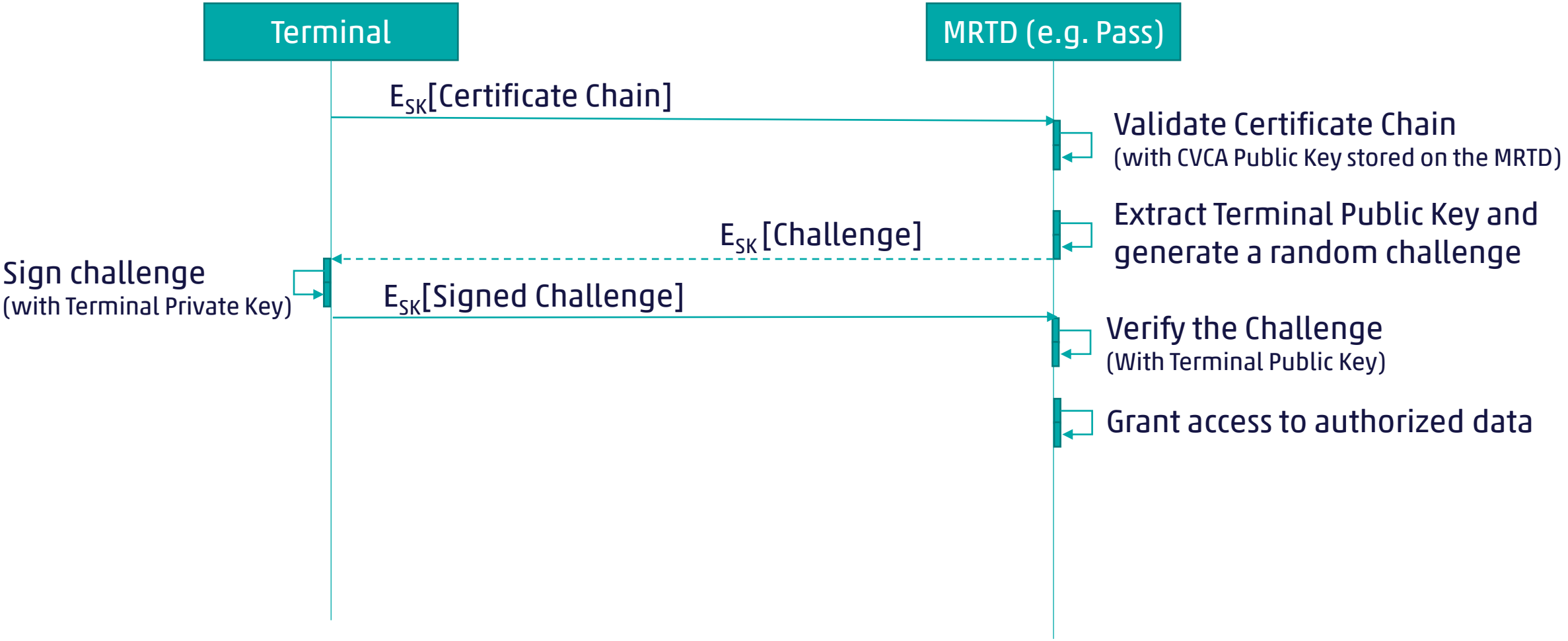
Chip Authentication (Version 1, vereinfachte Darstellung)



Schutz der Daten – Extended Access Control (EAC)

- Spezifiziert in BSI TR-03110
- Zusätzlich zur Chip Authentication wird eine Terminal Authentication durchgeführt
- Terminal Authentication
  - Setzt erfolgreiche Chip Authentication voraus
    - Zugriffsrechte des Terminals werden durch das MRTD an den bei der Chip Authentication ausgehandelten Key gebunden
  - Zugriffe auf geschützte Daten werden auf berechtigte Terminals eingeschränkt (über PKI)
    - Certificate Chain des Terminals muss mit dem CVCA public key des MRTD verifiziert werden können
    - Ausländische Behörten erhalten Zugriff, indem deren Zertifikat mit der CH-CVCA signiert wird.
  - Nach erfolgreicher Terminal Authentication erlaubt das MRTD den Zugriff auf mittels EAC geschützte Daten
    - Data Group 3 (Fingerprints)

Terminal Authentication (Version 1, vereinfachte Darstellung)



Schutz der Daten – Passive Authentication

- Passive Authentication wird vom Terminal ausgeführt
  - Verifizierung der Certificate Chain des MRTD (Machine readable travel document)
  - Verifizierung der Hash-Werte der einzelnen Data Groups
- Dient der Sicherstellung der Integrität der Daten.

Passive Authentication