Anlage 1

Technische Richtlinie BSI TR-03116-2 eCard-Projekte der Bundesregierung – Teil 2 – Hoheitliche Ausweisdokumente Version 2012 vom 16. Mai 2012

Inhaltsübersicht

1 Einleitung

Die Technische Richtlinie BSI TR-03116 stellt eine Vorgabe für die eCard-Projekte des Bundes dar. Die Technische Richtlinie ist in zwei Teile gegliedert:

- Teil 1 der Technischen Richtlinie beschreibt die Sicherheitsanforderungen für den Einsatz kryptographischer Verfahren im Gesundheitswesen für die elektronische Gesundheitskarte (eGK), den Heilberufeausweis (HBA) und der technischen Komponenten der Telematikinfrastruktur.
- Der vorliegende Teil 2 der Technischen Richtlinie beschreibt die Sicherheitsanforderungen für den Einsatz kryptographischer Verfahren in hoheitlichen Ausweisdokumenten, zur Zeit für den elektronischen Reisepass, den elektronischen Personalausweis und den elektronischen Aufenthaltstitel.

Die Vorgaben des vorliegenden Teil 2 der Technischen Richtlinie basieren auf Prognosen über die Sicherheit der in hoheitlichen Dokumenten verwendeten kryptographischen Verfahren über einen Zeitraum von 6 Jahren, zur Zeit bis zum Jahr 2018. Eine weitere Verwendung des Verfahrens über diesen Zeitraum hinaus ist nicht ausgeschlossen und wird mit 2018+ gekennzeichnet.

Da die Gültigkeit der hoheitlichen Dokumente i.d.R. über den Prognosezeitraum hinausgeht, besteht die Möglichkeit den elektronischen Teil bereits ausgegebener hoheitlicher Dokumente durch Rückruf des verwendeten Document Signer Zertifikates (vgl. Abschnitt 2.1) zu sperren. Das physikalische Ausweisdokument behält jedoch auch in diesem Fall seine Gültigkeit.

1.1 Hoheitliche Ausweisdokumente

Die Technische Richtlinie legt verbindlich die Vorgaben für den Einsatz von kryptographischen Verfahren basierend auf der TR-02102 [7] für folgende hoheitliche Ausweisdokumente fest:

- Elektronischer Reisepass
- Elektronischer Personalausweis
- Elektronischer Aufenthaltstitel

Abweichungen von den Empfehlungen aus TR-02102 werden in den einzelnen Abschnitten erläutert.

1.2 Kryptographische Verfahren und Standards

Hoheitliche Ausweisdokumente sind durch eine Reihe von internationalen, europäischen und nationalen Standards festgelegt. Tabelle 1 gibt einen Überblick über die kryptographischen Verfahren.

Standard	Kryptographisches Verfahren
ICAO Doc 9303	Basic Access Control
	Passive Authentisierung
	Aktive Authentisierung
ICAO TR-PACE	Password Authenticated Connection Establishment
BSI TR-03110, Parts 1-3	Extended Access Control Version 1 & 2 – Chip Authentisierung 1 & 2 – Terminal Authentisierung 1 & 2
	Password Authenticated Connection Establishment
	Restricted Identification

Tabelle 1: Kryptographische Verfahren

1.2.1 Internationale Reisedokumente

Der elektronische Reisepass und der elektronische Aufenthaltstitel (nach Vorgaben der EU-Kommission) sind internationale Reisedokumente.

Der internationale Standard für Reisedokumente wird von der ICAO in Doc 9303 festgelegt:

- Teil 1: Maschinenlesbare Reisepässe [16]
- Teil 2: Maschinenlesbare Visa
- Teil 3: Maschinenlesbare Identitätsdokumente [17]
- Technical Report: Supplemental Access Control for MRTDs [18][1].

Die von der ICAO standardisierten kryptographischen Verfahren sind:

- Password Authenticated Connection Establishment,
- Basic Access Control,
- Passive Authentisierung und
- Aktive Authentisierung.

[1] Das Verfahren Password Authenticated Connection Establishment (PACE) gemäß ICAO Technical Report [18] ist kompatibel zur Technischen Richtlinie BSI TR-03110 [8] und stammt ursprünglich aus einer älteren Version der BSI TR-03110.

1.2.2 Europäische Reisedokumente

Der elektronische Reisepass und der elektronische Aufenthaltstitel (nach Vorgaben der EU-Kommission) sind europäische Reisedokumente.

Die EU hat über die Verordnung (EC) No 2252/2004 [27] die Kommission mit der Standardisierung von zusätzlichen Verfahren zur Integration von Fingerabdrücken in Reisedokumente beauftragt. Die Technischen Spezifikationen sind in den Kommissionsentscheidungen C(2006) 2909 [13], C(2011) 5478 [14] und C(2011) 5499 [15] dargelegt und verweisen auf die Technische Richtlinie BSI TR-03110 und den ICAO Technical Report [18].

Folgende der in der Technische Richtlinie BSI TR-03110, Part 1 [8] spezifizierten kryptographischen Verfahren sind für europäische Reisedokumente relevant:

- Extended Access Control Version 1, d. h.
  - Chip Authentisierung Version 1
  - Terminal Authentisierung Version 1

Folgendes in der dem ICAO Technical Report [18] spezifizierten kryptographischen Verfahren sind für europäische Reisedokumente relevant:

- Password Authenticated Connection Establishment (kompatibel zu [8])

1.2.3 Nationale Ausweisdokumente

Nationale Ausweisdokumente sind nicht notwendigerweise konform zu den Spezifikationen für Reisedokumente. Der elektronische Personalausweis und der elektronische Aufenthaltstitel sind nationale Ausweisdokumente.

Folgende der in der Technischen Richtlinie BSI TR-03110, Part 2 [9] spezifizierten kryptographischen Verfahren sind für nationale Ausweisdokumente relevant:

- Extended Access Control Version 2, d. h.
  - Chip Authentisierung Version 2
  - Terminal Authentisierung Version 2
- Password Authenticated Connection Establishment
- Restricted Identification.

Verfahren	Algorithmus
Digitale Signatur	ECDSA [10]
Schlüsseleinigung	ECKA [10]
Blockchiffre	AES [24] – ECB-Mode [19] – CBC-Mode [19] – CMAC Mode [26]
	2 Key 3DES [25] – CBC-Mode [19] – Retail MAC [20]
Hash	SHA-1 und SHA-2 [23]

Tabelle 2: Kryptographische Algorithmen

1.3 Kryptographische Algorithmen

1.3.1 Basisverfahren

Tabelle 2 gibt einen Überblick über die in hoheitlichen Dokumenten verwendeten kryptographischen Basisverfahren. Das Verfahren 2 Key 3DES wird in der Technischen Richtlinie TR-02102 [7] nicht mehr empfohlen. Die Aufnahme dieses Verfahrens in dieser Technischen Richtlinie gilt nur für den elektronischen Reisepass und den elektronischen Aufenthaltstitel aufgrund der internationalen bzw. europäischen Standardisierung.

1.3.2 Domainparameter für Elliptische Kurven

Für Kryptographische Algorithmen basierend auf Elliptischen Kurven (d. h. ECDSA und ECKA) sind die Brainpool Domain Parameter [21] in den entsprechenden Bitlängen zu verwenden.

1.3.3 Zufallszahlengeneratoren

Für die Erzeugung von Zufallszahlen und kryptographischen Schlüsseln (inkl. ephemeralen Schlüsseln) sind in allen verwendeten kryptographischen Protokollen Zufallszahlengeneratoren aus einer der folgenden Klassen (siehe [1]) zu verwenden:

- DRG.3,
- DRG.4,

– PTG.2,
– PTG.3,
– NTG.1.

Bei der Verwendung von PTG.2 muss ggf. eine anwendungsspezifische kryptographische Nachbearbeitung der Zufallszahlen erfolgen, um eine mögliche Schiefe der Zufallszahlen zu verhindern. Es wird empfohlen einen Zufallszahlengenerator der Klasse PTG.3 zu verwenden.

1.3.3.1 PTG.2 Nachbearbeitung bei PACE

Bei PACE wird eine 128 Bit Zufallszahl s erzeugt und anschließend zu $z=E_K(s)$ verschlüsselt. Die Nachbearbeitung der Zufallszahl s muss konform zur Klasse DRG.3 erfolgen.

Alternativ kann folgende Variante des PACE-Algorithmus verwendet werden:

– Es werden zwei 128 Bit Zufallszahlen s_1 und s_2 mit einem Zufallszahlengenerator der Klasse PTG.2 erzeugt.
– Anschließend wird der Chiffretext $(c||s||z) = E_K(s_1||s_2||0)$ wie in Abbildung 1 dargestellt berechnet.
– Der Wert c wird verworfen, die Werte s und z ($=E_K(s)$) werden wie bisher verwendet.

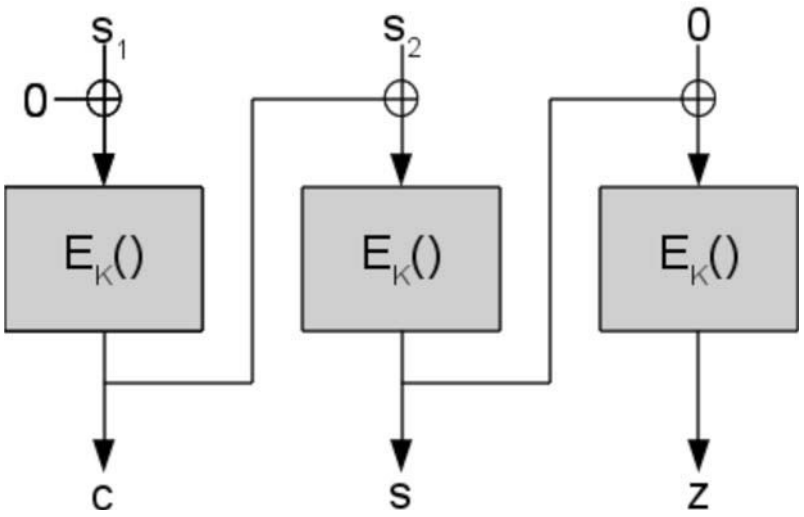

Abbildung 1: Alternative Verschlüsselung der PACE Nonce

Sofern eine andere Nachbearbeitung verwendet wird, muss diese mit dem BSI abgestimmt werden.

2 Public Key Infrastrukturen

Es werden zwei unterschiedliche Arten von Public Key Infrastrukturen verwendet:

– Eine Public Key Infrastruktur zur Überprüfung der Authentizität hoheitlicher Dokumente (Passive Authentisierung).
– Mehrere anwendungsspezifische Public Key Infrastrukturen zur Festlegung von Berechtigungen von Lesegeräten (Terminal Authentisierung).

2.1 Passive Authentisierung

Die Authentizität des elektronischen Teils hoheitlicher Dokumente kann durch die Passive Authentisierung (in Verbindung mit der Chip Authentisierung) geprüft werden. Die Passive Authentisierung basiert auf einer Public Key Infrastruktur bestehend aus einer *Country Signing Certification Authority* als nationale Wurzelinstanz und für jeden autorisierten Herausgeber des hoheitlichen Dokuments mindestens einem *Document Signer*.

Das Signaturverfahren mit der die X.509 Zertifikate signiert werden, wird durch die Country Signing Certification Authority festgelegt. Die Schlüssellängen sind jedoch u. U. unterschiedlich. Die Country Signing Certification Authority wird vom BSI betrieben.

Tabelle 3 legt die zu verwendenden kryptographischen Verfahren verbindlich fest. Die Verwendungszeiträume beziehen sich auf die Dokumentenproduktion.

Verfahren	Algorithmus	Länge	Verwendung von	Verwendung bis
Country Signing CA				
Signatur	ECDSA	256 384	2011	2011 2018+
Hash	SHA-2	256 384	2011	2011 2018+

Verfahren	Algorithmus	Länge	Verwendung von	Verwendung bis
Document Signer				
Signatur	ECDSA	224 256	2010	2010 2018+
Hash	SHA-2	224 256	2010	2010 2018+
Passive Authentisierung				
Hash von Datengruppen	SHA-1 SHA-2	160 256	2010	2010 2018+

Tabelle 3: Passive Authentisierung

2.2 Terminal Authentisierung

Die Berechtigung zum Lesen und Schreiben von bestimmten Daten auf dem Chip muss ein Lesegerät über die Terminalauthensierung nachweisen. Die Terminal Authentisierung basiert auf einer Public Key Infrastruktur bestehend aus einer *Country Verifying Certification Authority* als nationale Wurzelinstanz, einem *Document Verifier* für jeden Betreiber von Lesegeräten sowie den *Terminals*.

Das Signaturverfahren einschließlich der Schlüssellängen mit dem die kartenverifizierbaren Zertifikate (Card Verifiable Certificate) signiert werden, wird durch die Country Verifying Certification Authority festgelegt. Die Country Verifying Certification Authority wird vom BSI betrieben.

Tabelle 4 legt die zu verwendenden kryptographischen Verfahren verbindlich fest. Die Verwendungszeiträume beziehen sich auf die Zertifikatserzeugung.

Verfahren	Algorithmus	Länge	Verwendung von	Verwendung bis
Signatur	ECDSA	224 256	2010	2010 2018+
Hash	SHA-2	224 256	2010	2010 2018+

Tabelle 4: Terminal Authentisierung

3 Zugriffskontrolle und sichere Kommunikation

Alle auf dem Chip gespeicherten Daten (mit Ausnahme einiger administrativer Daten) sind mit einem Schutz gegen unberechtigten Zugriff zu versehen.

3.1 Basic Access Control

Basic Access Control ist ein von der ICAO [16], [17] standardisierter Zugriffsschutz. Dieses Verfahren basiert auf symmetrischer Kryptographie (die Schlüssel werden aus der optisch lesbaren maschinenlesbaren Zone erzeugt) und setzt keine Infrastruktur voraus. Basic Access Control ist für alle Reisedokumente zu implementieren. Langfristig ist es vorgesehen Basic Access Control durch PACE zu ersetzen, da PACE deutlich bessere kryptographische Eigenschaften besitzt.

Tabelle 5 legt die zu verwendenden kryptographischen Verfahren verbindlich fest.

Verfahren	Algorithmus	Länge	Verwendung von	Verwendung bis
Verschlüsselung	3DES CBC-Mode	112	Vorgegeben durch [16], [17].	
Integritätssicherung	3DES Retail MAC	112	Vorgegeben durch [16], [17].	

Tabelle 5: Basic Access Control

3.2 PACE

PACE (Password Authenticated Connection Establishment) [9], [18] ist ein kryptographisches Verfahren mit den gleichen Zielen wie Basic Access Control, basiert aber auch auf asymmetrischer Kryptographie und kann mit mehreren, auch kurzen Passwörtern (PINs) verwendet werden.

Tabelle 6 legt die zu verwendenden kryptographischen Verfahren verbindlich fest. Die Verwendungszeiträume beziehen sich auf die Dokumentenausstellung.

Verfahren	Algorithmus	Länge	Verwendung von	Verwendung bis
Schlüsseleinigung	ECKA	256	2010	2018+
Permutation	AES ECB-Mode	128	2010	2018+

Verfahren	Algorithmus	Länge	Verwendung von	Verwendung bis
Mapping	Generic ECKA	256	2010	2018+
Verschlüsselung	AES CBC-Mode	128	2010	2018+
Integritätssicherung	AES CMAC	128	2010	2018+

Tabelle 6: PACE

3.3 Extended Access Control

Extended Access Control [8], [9] ist ein PKI-basiertes Zugriffskontrollverfahren, das sich aus den Bestandteilen Chip Authentisierung (s. Abschnitt 4.2) und Terminal Authentisierung (s. Abschnitt 2.2) zusammensetzt.

4 Identifikation des Ausweisdokuments

Das Ausweisdokument kann über die Dokumentennummer, die Chip Authentisierung oder die Restricted Identification identifiziert werden.

4.1 Dokumentennummer

Die Dokumentennummer bietet eine eindeutige Identifizierung des Dokumententyps. Die Dokumentennummer ist eine 9-stellige alphanumerische, pseudozufällige Nummer. Sie ist aus folgenden Zeichen zu bilden: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, C, F, G, H, J, K, L, M, N, P, R, T, V, W, X, Y, Z. Die Dokumentennummer kann zentral (beim Produzenten) oder dezentral erzeugt werden. Es wird empfohlen, die Dokumentennummer durch das Warbler-Verfahren aus einer sequentiellen Nummer zu erzeugen [22].

4.2 Chip Authentisierung

Die Chip Authentisierung [8], [9] ist ein kryptographisches Verfahren, mit dem die Echtheit des Chips durch den Aufbau einer starken Sitzungsverschlüsselung und -integritätssicherung nachgewiesen wird. Bei der Chip Authentisierung in Version 1 muss das Schlüsselpaar chipindividuell erzeugt werden, ab der Version 2 kann ein Schlüsselpaar für alle Dokumente einer Generation verwendet werden. Für die hoheitliche Nutzung muss zusätzlich ein chipindividuelles Schlüsselpaar verwendet werden.

4.2.1 Nationale Vorgaben

Tabelle 7 legt die zu verwendenden kryptographischen Verfahren für Chip Authentisierung in Version 1 verbindlich fest. Die Verwendungszeiträume beziehen sich auf die Dokumentenausstellung.

Verfahren	Algorithmus	Länge	Verwendung von	Verwendung bis
Schlüsseleinigung	ECKA	256	2010	2018+
Verschlüsselung	3DES CBC-Mode AES CBC-Mode	112 128	2010 3. Quartal 2012	3. Quartal 2012 2018+
Integritätssicherung	3DES Retail MAC AES CMAC	112 128	2010 3. Quartal 2012	3. Quartal 2012 2018+

Tabelle 7: Chip Authentisierung in Version 1 (Nationale Anwendung)

Tabelle 8 legt die zu verwendenden kryptographischen Verfahren für Chip Authentisierung in Version 2 verbindlich fest. Die Verwendungszeiträume beziehen sich auf die Dokumentenausstellung.

Verfahren	Algorithmus	Länge	Verwendung von	Verwendung bis
Schlüsseleinigung	ECKA	256	2010	2018+
Verschlüsselung	AES CBC-Mode	128	2010	2018+
Integritätssicherung	AES CMAC	128	2010	2018+

Tabelle 8: Chip Authentisierung in Version 2 (Nationale Anwendung)

4.2.2 Europäische Vorgaben

Tabelle 9 stellt die zu verwendenden kryptographischen Verfahren nach übergeordneten EU-Vorgaben dar. Diese müssen für Chip Authentisierung in Version 1 für den elektronischen Reisepass und den elektronischen Aufenthaltstitel zusätzlich zu den nationalen Vorgaben implementiert werden.

Verfahren	Algorithmus	Länge	Verwendung von	Verwendung bis
Verschlüsselung	3DES CBC-Mode	112	Vorgegeben durch [13].	
Integritätssicherung	3DES Retail MAC	112	Vorgegeben durch [13].	

Tabelle 9: Chip Authentisierung (Europäische Vorgaben)

4.3 Restricted Identification

Die Restricted Identification [9] ist ein kryptographisches Verfahren zur Erzeugung von sektorspezifischen Kennungen.

Tabelle 10 legt die zu verwendenden kryptographischen Verfahren verbindlich fest. Die Verwendungszeiträume beziehen sich auf die Dokumentenausstellung.

Verfahren	Algorithmus	Länge	Verwendung von	Verwendung bis
Schlüsseleinigung	ECKA	256	2010	2018+
Hash zur Erzeugung von sektorspezifischen Kennungen	SHA-2	256	2010	2018+
Hash zur Erzeugung von Sperrsummen	SHA-2	256	2010	2018+

Tabelle 10: Restricted Identification

5 Qualifizierte elektronische Signatur

Sofern das Ausweisdokument eine Signaturfunktion unterstützt, muss diese als qualifizierte Signatur ausgestaltet sein. Es sind folgende Vorgaben einzuhalten.

5.1 Signaturerzeugung

Für die Signaturerzeugung sind die Vorgaben aus [12] einzuhalten. Tabelle 11 legt die zu verwendenden kryptographischen Verfahren darüber hinaus verbindlich fest. Die Verwendungszeiträume beziehen sich auf die Zertifikatsausstellung.

Verfahren	Algorithmus	Länge	Verwendung von	Verwendung bis
Signaturverfahren	ECDSA	256	2010	2018+
Hash	extern zu berechnen			

Tabelle 11: Signaturerzeugung

5.2 Kennzeichnung der kryptographischen Verfahren

Die eSign-Anwendung wird durch eine Cryptographic Information Application ergänzt, die über die Verwendbarkeit des Signaturschlüssels Auskunft gibt. Es müssen folgende Object Identifier nach TR-03111 [10] zur Kennzeichnung der Verfahren verwendet werden:

- Signaturverfahren: ecdsa-plain-signatures
- Schlüssel in X.509 Zertifikaten: id-ecPublicKey
- Schlüssel im TLV-Format: id-ecTLVPublicKey

Das Signaturverfahren wird ohne Angabe des extern zu erzeugenden Hashes angegeben. Die Signaturanwendungskomponente kann die von der Karte erstellte Signatur im plain-Format in das X9.62-Format (einschließlich des verwendeten Hashes) umwandeln.

6 Kartenprofile

6.1 Elektronischer Reisepass

Der elektronische Reisepass beinhaltet die ePass-Anwendung [16].

6.1.1 Unterstützte Verfahren

Der elektronische Reisepass unterstützt folgende kryptographische Verfahren:

- Passive Authentisierung
- Basic Access Control
- Extended Access Control Version 1
  - Chip Authentisierung 1
  - Terminal Authentisierung 1

Die zusätzliche Unterstützung von Password Authenticated Connection Establishment wird empfohlen. Ab 2013 muss PACE (gemäß [18]) vom elektronischen Reisepass unterstützt werden.

Die Absicherung der Kommunikation zwischen Chip und Lesegerät erfolgt über Secure Messaging, welches über Basic Access Control/Password Authenticated Connection Establishment und Chip Authentisierung vereinbart wird. Die Verwendung der Chip Authentisierung ist für den Leser nicht verpflichtend.

6.1.2 Nicht unterstützte Verfahren

Der elektronische Reisepass unterstützt keine Aktive Authentisierung.

6.2 Elektronischer Personalausweis

Der elektronische Personalausweis beinhaltet die folgenden drei Anwendungen: ePass [17], eID [9] und eSign [11].

6.2.1 Unterstützte Verfahren

Der elektronische Personalausweis unterstützt folgende kryptographische Verfahren:

- Passive Authentisierung
- Password Authenticated Connection Establishment (gemäß [9])
- Extended Access Control Version 2
  - Chip Authentisierung 2
  - Terminal Authentisierung 2
- Restricted Identification
- Qualifizierte elektronische Signatur

Die Absicherung der Kommunikation zwischen Chip und Lesegerät erfolgt über Secure Messaging, welches über Password Authenticated Connection Establishment und Chip Authentisierung vereinbart wird. Alle Chips einer Generation müssen das gleiche Schlüsselpaar für die Chip Authentisierung verwenden, zusätzlich müssen chipindividuelle Schlüssel vorhanden sein.

6.2.2 Nicht unterstützte Verfahren

Der elektronische Personalausweis unterstützt folgende kryptographische Verfahren nicht:

- Basic Access Control
- Extended Access Control Version 1
- Aktive Authentisierung

6.3 Elektronischer Aufenthaltstitel

Der elektronische Aufenthaltstitel beinhaltet die folgenden drei Anwendungen: ePass [16], [17], eID [9] und eSign [11].

6.3.1 Unterstützte Verfahren

Der elektronische Aufenthaltstitel unterstützt folgende kryptographische Verfahren:

- Passive Authentisierung
- Basic Access Control
- Password Authenticated Connection Establishment
- Extended Access Control (Version 1 und Version 2)
  - Chip Authentisierung 1 & 2
  - Terminal Authentisierung 1 & 2
- Restricted Identification
- Qualifizierte elektronische Signatur

Für den Zugriff auf die ePass-Anwendung kann Basic Access Control/Password Authenticated Connection Establishment (gemäß [18]) und bei Zugriff auf Fingerabdrücke Extended Access Control in Version 1 verwendet werden, für den Zugriff auf die eID- und eSign-Anwendung muss PACE (gemäß [9]) und Extended Access Control in Version 2 verwendet werden.

Alle Chips einer Generation müssen das gleiche Schlüsselpaar für die Chip Authentisierung verwenden, zusätzlich müssen chipindividuelle Schlüssel vorhanden sein.

6.3.2 Nicht unterstützte Verfahren

Der elektronische Aufenthaltstitel unterstützt keine Aktive Authentisierung.

7 Zertifizierung der Ausweisdokumente

Die hoheitlichen Ausweisdokumente müssen nach den Common Criteria zertifiziert sein. Das Zertifikat wird mit der Auflage erteilt, dass der Inhaber des Zertifikats für einen Zeitraum von neun Jahren, beginnend mit dem Zeitpunkt der Zertifizierung oder des jeweils letzten vollständig abgeschlossenen Re-Assessments, alle 18 Monate auf eigene Kosten eine Neubewertung des Prüfberichts auf Basis der aktuellen Bedrohungslage durchführen lässt und das Ergebnis dieser Neubewertung dem BSI zur Verfügung stellt.

Ferner wird dem Inhaber des Zertifikats aufgegeben, das BSI bei von diesem angeordneten weiteren Prüfungen des Zertifizierungsgegenstandes auf Kosten des BSI zu unterstützen, insbesondere geforderte Unterlagen herauszugeben.

Das Common Criteria Zertifikat muss einen Hinweis enthalten, dass bei der Evaluierung des hoheitlichen Ausweisdokumentes die Anforderungen dieser Technischen Richtlinie berücksichtigt wurden.

7.1 Elektronischer Reisepass

Im Rahmen der erforderlichen Zertifizierung muss die Konformität zu den Schutzprofilen BSI-CC-PP-0055-2009 [2], BSI-CC-PP-0056-V2-2012 [3] und sofern Password Authenticated Connection Establishment unterstützt wird, BSI-CC-PP-0068-V2-2011 [5] nachgewiesen werden. Bis zum Ende des 2. Quartals 2012 kann übergangsweise auch das Schutzprofil BSI-CC-PP-0069-2010 [6] für die Zertifizierung verwendet werden. In diesem Fall muss die Konformität zum Schutzprofil BSI-CCPP-0069-2010 sowie die nachträgliche Unterbindung des Zugriffs auf die eID- und die eSign-Anwendung nachgewiesen werden[2].

Die Bauteile der kontaktlosen Schnittstelle (z. B. Antenne) sind als sicherheitsrelevant eingestuft und daher im Zertifizierungsverfahren mit zu berücksichtigen. Die Produktionsschritte *Initialisierung, Pre-Personalisierung* und *Antennenmontage* sind Teil des zu zertifizierenden Lebenszyklusses des elektronischen Reisepasses.

Außerdem soll der Chip Maßnahmen vorsehen, so dass die Dauer eines erfolgreichen Brute-Force-Angriffs auf die MRZ im Durchschnitt 30 Tage nicht wesentlich unterschreitet.

7.2 Elektronischer Personalausweis

Im Rahmen der erforderlichen Zertifizierung muss die Konformität zum Schutzprofil BSI-CCPP-0061-2009 [4] nachgewiesen werden. Die Bauteile der kontaktlosen Schnittstelle (z. B. Antenne) sind als sicherheitsrelevant eingestuft und daher im Zertifizierungsverfahren mit zu berücksichtigen. Die Produktionsschritte *Initialisierung, Pre-Personalisierung* und *Antennenmontage* sind Teil des zu zertifizierenden Lebenszyklusses des elektronischen Personalausweises.

Die gespeicherten kryptographischen Schlüssel *Chip Authentication Private Keys, Restricted Identification Private Keys* und der *private Schlüssel für qualifizierte Signaturen* müssen durch geeignete Maßnahmen zusätzlich geschützt werden. Diese Maßnahmen sind im Einzelnen mit dem BSI abzustimmen.

Außerdem soll der Chip Maßnahmen vorsehen, so dass die Dauer eines erfolgreichen Brute-Force-Angriffs auf ein nicht-geheimes Passwort (MRZ, CAN) im Durchschnitt 30 Tage nicht wesentlich unterschreitet.

7.3 Elektronischer Aufenthaltstitel

Im Rahmen der erforderlichen Zertifizierung muss die Konformität zum Schutzprofil BSI-CC-PP-0069-2010 [6] nachgewiesen werden. Die Bauteile der kontaktlosen Schnittstelle (z. B. Antenne) sind als sicherheitsrelevant eingestuft und daher im Zertifizierungsverfahren mit zu berücksichtigen. Die Produktionsschritte *Initialisierung, Pre-Personalisierung* und *Antennenmontage* sind Teil des zu zertifizierenden Lebenszyklusses des elektronischen Aufenthaltstitels.

Die gespeicherten kryptographischen Schlüssel *Chip Authentication Private Keys, Restricted Identification Private Keys* und der *private Schlüssel für qualifizierte Signaturen* müssen durch geeignete Maßnahmen zusätzlich geschützt werden. Diese Maßnahmen sind im Einzelnen mit dem BSI abzustimmen.

Außerdem soll der Chip Maßnahmen vorsehen, so dass die Dauer eines erfolgreichen Brute-Force-Angriffs auf ein nicht-geheimes Passwort (MRZ, CAN) im Durchschnitt 30 Tage nicht wesentlich unterschreitet.

Literaturverzeichnis

[1] BSI AIS 20/31, A proposal for: Functionality classes for random number generators, Version 2.0, 2011

[2] BSI CC-PP-0055-2009, Common Criteria Protection Profile – Machine Readable Travel Document with „ICAO Application“ Basic Access Control Version 1.10, 2009

[3] BSI CC-PP-0056-V2-2012, Common Criteria Protection Profile – Machine Readable Travel Document with „ICAO Application“ Extended Access Control with PACE (PP-MRTD) Version 1.3, 2012

[4] BSI CC-PP-0061-2009, Common Criteria Protection Profile – Electronic Identity Card (ID_Card PP) Version 1.03, 2009

[5] BSI CC-PP-0068-V2-2011, Electronic Passport using Standard Inspection Procedure with PACE (ePass_PACE PP), 2011

[6] BSI CC-PP-0069-2010, Common Criteria Protection Profile Electronic Residence Permit Card (RP_Card PP), 2010

[7] BSI TR-02102, Kryptographische Verfahren: Empfehlungen und Schlüssellängen Version 1.0, 2008

[8] BSI TR-03110-1, Advanced Security Mechanisms for Machine Readable Travel Documents – Part 1, Version 2.1, 2012

[9] BSI TR-03110-2, Advanced Security Mechanisms for Machine Readable Travel Documents – Part 2, Version 2.1, 2012

[10] BSI TR-03111, Elliptic Curve Cryptography (ECC) Version 1.11, 2009

[11] BSI TR-03117, eCards mit kontaktloser Schnittstelle als sichere Signaturerstellungseinheit, 2009

[12] Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen – Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung, Geeignete Algorithmen, 2012

[13] EU Kommission, Technical specifications on the standards for security features and biometrics in passports and travel documents issued by Member States, Commission Decision C(2006) 2909, 28. Juni 2006

[2] Die Unterbindung wird nachträglich in der Phase der Personalisierung durchgeführt. Innerhalb der Produktzertifizierung muss die Wirksamkeit des dabei eingesetzten Mechanismus geprüft und bestätigt werden.

[14] EU Kommission, Technical specifications for the uniform format for residence permits for third country nationals, Commission Decision C(2011) 5478, 4. August 2011

[15] EU Kommission, Amendment to C(2011) 2909 laying down the technical specifications on the standards for security features and biometrics in passports and travel documents issued by member states, Commission Decision
C(2011) 5499, 4. August 2011

[16] ICAO Doc 9303, Specifications for electronically enabled passports with biometric identification capabilities, 6th Edition, 2006

[17] ICAO Doc 9303, Specifications for electronically enabled official travel documents with biometric identification capabilities, 3rd Edition, 2009

[18] ICAO Technical Report, Supplemental Access Control for Machine Readable Travel Documents, Version 1.00, 2010

[19] ISO/IEC 10116:2006, Information technology – Security techniques – Modes of operation for an n-bit block cipher, 2006

[20] ISO/IEC 9797-1:1999, Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher, 1999

[21] Lochter, Manfred; Merkle, Johannes RFC 5639, Elliptic Curve Cryptography (ECC) Brain-pool Standard Curves and Curve Generation, 2010

[22] Margraf, Marian, Beschreibung und Einsatz der Verschlüsselungsfunktion Warbler, 2006

[23] NIST FIPS PUB 180-2, Secure hash standard (and Change Notice to include SHA-224), 2002

[24] NIST FIPS PUB 197, Specification for the Advanced Encryption Standard (AES), 2001

[25] NIST FIPS PUB 46-3, Data Encryption Standard (DES), 1999

[26] NIST Special Publication 800-38B, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, 2005

[27] Rat der EU, Standards for security features and biometrics in passports and travel documents issued by Member States, Council Regulation (EC) No 2252/2004, 13. Dezember 2004