MoA

MRTD online Authentication

Machbarkeitsstudie V2.0

Institut für ICT-Based Management der Berner Fachhochschule

Autoren:
Dr. Annett Laube-Rosenpflanzer
Gerhard Hassenstein
Severin Hauser
Co-Autoren:
Dr. Rolf Haenni
Reto Koenig

17. Dezember 2013

Berner Fachhochschule
Technik und Informatik

Inhaltsverzeichnis

Änderungskontrolle

Version	Datum	Autor	Bemerkung
0.1	24.08.2013	Gerhard Hassenstein Severin Hauser	Anfangsdokument vor erstem internem Review
0.2	26.08.2013	Gerhard Hassenstein	Version nach 1. Review
1.0	30.08.2013	Annett Laube-Rosenpflanzer	Fertigstellung Version 1.0
2.0	16.12.2013	Gerhard Hassenstein	Überarbeitete Version nach Präsentation PoC vom 12.12.2013 beim Fedpol

Management Summary

Dieses Dokument enthält eine technische Machbarkeitsstudie zu der Variante 2 der ‚Konzeptstudie elektronischer Identitätsnachweis' des FedPol, die mögliche Realisierungs-Varianten eines elektronischen Identifikationsmittels beschreibt, welche zusammen mit der neuen schweizerischen Identitätskarte oder anderen staatlichen Ausweisen umgesetzt werden sollen.

Dieses Dokument beschreibt eine starke elektronische Authentisierung gegenüber einem Online-Dienstanbieter mittels der standardisierten Funktionen eines elektronischen ICAO-Reisedokumentes realisiert. Dabei soll ein möglichst handelsübliches Lesegerät (z.B. ein Smartphone mit eingebautem NFC-Reader) zusammen mit einer speziellen, darauf laufenden Anwendung (lokale Leseapplikation, LLA) dafür sorgen, dass sich das Reisedokument gegenüber einem Dienstanbieter im Internet wie ein normales elektronisches Identifikationsmittel verhält.

Im Dokument werden die einzuhaltenden Standard der ICAO und die Erweiterungen für Reise-dokumente mit biometrischen Daten der EU identifiziert. Die für diese Studie massgeblichen kryptographischen Verfahren werden beschrieben und die einzelnen Schritte eines für heutige schweizerische Reisedokumente gültigen Zugriffsprozesses werden aufgezeigt.

Der Kern dieser Studie ist der *MRTD online Authentication Process (MoA),* der aufzeigt, wie ein Standard ICAO-Reisedokumentes verwendet wird, um sich sich gegenüber einem Online-Dienst stark zu authentisieren. Dabei muss sich ein Online-Dienst von der Echtheit und Präsenz des Reisedokuments überzeugen. Das wird durch eine direkte Chip- und Passive-Authentication zwischen dem ICAO-Chip des Reisedokuments und dem Online-Dienst erreicht. Die Anwendung (LLA) auf dem Smartphone dient dabei nur zum Aufbau eines sicheren Kommunikationskanals.

Der MoA-Prozess besteht aus zwei Teilen:
- der initialen Registrierungsphase, bei welcher der Inhaber des Reisedokuments, ein Zertifikat erlangt, das für eine starke 2-Faktor-Authentisierung erforderlich ist,
  und
- der eigentlichen Authentisierung.

Zur einmaligen Registrierung erhält der rechtmässige Inhaber des Reisedokumentes ein persönliches Einmal-Passwort per Post. Dieses gibt er zusammen mit der MRZ des Reisedokuments in die lokale Leseapplikation ein. Die LLA liest die notwendigen Daten aus dem Chip des Reisedokumentes aus und schickt eine Registrierungsnachricht an den Federal Registration Service (FRS). Dieser überprüft per direkter Chip- und Passive-Authentication, die Präsenz des Reisedokumentes und liest die zur Überprüfung notwendigen Daten (Security Objekt und DG14) aus. Nach erfolgreicher Überprüfung der Zugehörigkeit des aktuellen Benutzers zum Reisedokument, erhält der Benutzer ein Zertifikat, das PIN-geschützt auf dem Smartphone abgelegt wird.

Auch bei der Authentisierung gegenüber einem Online-Dienst wird die Präsenz des Passes durch direkte Chip- und Passive-Authentication überprüft. Zusätzlich muss sich der Benutzer per Zertifikat authentisieren, das er in der Registrierungsphase erlangt hat. Dieses ist durch eine, nur dem rechtmässigen Inhaber des Reisedokumentes bekannte PIN geschützt. Die verwendeten Verfahren erlauben zudem, dass die LLA die zwischen Online-Dienst und Chip übertragenen Daten kontrolliert und damit vor unerlaubtem Zugriff schützen kann.

MoA kann für verschiedene Anwendungsszenarien eingesetzt werden. Neben der direkten Anwendung von MoA gegenüber speziell dafür erweiterten Online-Diensten, werden Szenarien mit einen Federal Authentication Service (FAS) vorgestellt. Letztere bieten - aufgrund der Ähnlichkeit der Architektur zur SuisseID-Infrastruktur - Vorteile bezüglich der Integration in bestehende Anwendungen, Datenschutz und Vereinfachung der Prozesse bei der Erneuerung von Reisedokumenten oder Zertifikaten. Es wird aber auch aufgezeigt, dass es nicht möglich ist einen MRTD-Chip als einfaches Identifikationstoken für eine zertifikatsbasierte 2-Faktor-Authentisierung gegenüber einem SSL/TLS-Webserver einzusetzen, da dies Änderungen der ICAO-Standardisierung auf Seiten Chip bedingen würde.

In diesem Dokument wird gezeigt, dass mit einem schweizerischen Standard-ICAO-Reisepass eine sichere Authentifizierung möglich ist. Das gilt für Dokumente basierend auf den heutigen Standards (BAC, EACv1), aber auch für zukünftige Varianten (z.B. mit SAC oder EACv2).

Verglichen mit anderen Lösungen für staatliche, elektronische Identitäten im europäischen Umfeld, handelt es sich bei MoA um eine alternative, innovative Herangehensweise, die sich auch in europäische eID-Infrastrukturen, wie STORK, integrieren lässt.
Die aktuellen europäischen Lösungen enthalten zumeist drei Funktionalitäten: ePass (Identifikation), eID-Applikation (Authentisierung) und eSign (Signaturdienste). Die hier vorgestellte Lösung basierend auf MoA kann zwei dieser Funktionalitäten abdecken. Die Bereitstellung von Signaturdiensten kann aber im Rahmen eines Ökosystems umgesetzt werden.
Die Studie hat dargelegt, was mit einem MRTD-Chip bezüglich online Authentisierung maximal möglich ist. Gleichzeitig werden aber auch die Grenzen des ICAO Standards aufgezeigt. Je nach Authentisierungsmethode des zweiten Faktors (Benutzer) sind grosse Unterschiede beim Handling festzustellen. Die einfachste Benutzerauthentisierungsmethode (mit einem Passwort) bringt zwar einige Einschränkungen in der Sicherheit mit sich, weist aber umgekehrt bezüglich Einfachheit und Handhabung einige Vorteile auf. Integriert in ein bestehendes Identitätsprotokoll (wie zum Beispiel SAML) kann MoA als 2-Faktorenauthentisierungsverfahren durchaus als ernstzunehmende Lösungsvariante angesehen werden.

1. Einführung

Das vorliegende Dokument wurde im Auftrag des Bundesamtes für Polizei (Fedpol) im Rahmen der ‚Konzeptstudie elektronischer Identitätsnachweis' als zusätzliche Machbarkeitsstudie erstellt. Die FedPol-Konzeptstudie umfasst eine übergreifende Sicht auf die Ziele und Anforderungen sowie mögliche Realisierungs-Varianten für ein elektronisches Identifikationsmittel, das zusammen mit der neuen schweizerischen Identitätskarte oder anderen staatlichen Ausweisen, z.B. dem Ausländerausweis, zukünftig bezogen werden soll.
Es werden in der Studie unterschiedliche Lösungsansätze mit ihren Vor- und Nachteilen gegenübergestellt und daraus vier verschiedene Varianten extrahiert:

- Variante 1: Private eID mit staatlicher Identifikation und Regulierung
- Variante 2: Identitätsnachweis mit der ICAO-ePass-Funktion
- Variante 3: Klassische staatliche Mainstream-ECC-eID
- Variante 4: eID-Lösung nach deutschem Vorbild

Für weitere Informationen über die Ziele und Anforderungen, sowie die Gegenüberstellung der einzelnen Varianten wird auf die Konzeptstudie [1] verwiesen.

1.1 Ziel der Studie

Dieses Dokument beinhaltet das Konzept für die technische Umsetzung der Variante 2. Ziel dieser Variante ist eine starke elektronische Authentisierung mittels standardisierter Funktionen eines elektronischen ICAO-Reisedokumentes. Es soll gezeigt werden, wie mit einem Standard-ICAO-Reisedokument und dessen kryptographischen Mitteln eine sichere Online-Authentisierung realisiert werden kann. Damit wäre die neue schweizerische Identitätskarte mit ePass-Chip, wie auch der bisher ausgestellte biometrische Pass und der neue Ausländerausweis, als elektronisches Identifikationsmittel einsetzbar.

1.2 Struktur des Dokuments

- In Kapitel 2 werden einführend die geltenden internationalen Standards der ICAO, sowie die Erweiterungen für Reisedokumente mit biometrischen Daten der EU zusammengefasst. Zusätzlich werden die für diese Studie massgeblichen kryptographischen Verfahren kurz vorgestellt. Im Anschluss daran werden die einzelnen Schritte eines für heutige schweizerische Reisedokumente gültigen Zugriffsprozesses aufgezeigt. Basierend auf diesen standardisierten Verfahren und den Standards beinhaltet dieses Kapitel damit die Rahmenbedingungen zu dieser Studie.
- In Kapitel 3 wird der *MRTD online Authentication Process (MoA)* als Kern der Lösung vorgestellt. Mit diesem Prozess lässt sich ein Reisedokument dazu verwenden, sich gegenüber einem Online-Dienst stark zu authentisieren. Der gesamte Prozess besteht aus zwei Teilen, einer initialen Registrierungsphase und dem eigentlichen Laufzeitprozess, worin sich der Eigentümer eines elektronischen Reisedokuments authentisiert.
- MoA kann für verschiedene Anwendungsszenarien eingesetzt werden. Diese Anwendungen werden in Kapitel 4 beschrieben. Wir zeigen hier grundsätzlich drei Hauptanwendungen auf: (1) wie man MoA für eine Authentisierung direkt gegenüber einem speziell dafür erweiterten Online-Dienst einsetzen kann und wie MoA zusammen mit einem Federal Authentication Service (FAS) indirekt für andere lokale Applikationen (2) oder auch in bestehende Protokolle (wie beispielsweise SAML) (3) integriert werden kann.
- In Kapitel 5 findet sich ein kurzer Ausblick über aktuelle internationale Entwicklungen und Bestrebungen, um die Nachhaltigkeit von MoA aufzuzeigen.
- Das letzte Kapitel 6 beinhaltet eine Gegenüberstellung der einzelnen Anwendungsszenarien wobei Vor- und Nachteile aufgezeigt und diskutiert werden. Daneben werden zu klärende Punkte und Prozesse identifiziert, die im Detail untersucht werden sollten, um ein vollständiges Bild des Einsatzes von MoA als schweizerisches Identifikationsmittel zu bekommen.
- Im Anhang A (Kryptographische Verfahren) sind die für diese Studie relevanten Algorithmen und Prozesse zusammengestellt.

2. Ausgangslage

Die Machbarkeitsstudie hat das Ziel einen Lösungsweg aufzuzeigen, wie die im biometrischen Pass enthaltenen Funktionen und Verfahren für eine starke Authentisierung des Inhabers gegenüber einem Online-Dienstanbieter genutzt werden können. Dabei soll ein möglichst handelsübliches Lesegerät (z.B. ein Smartphone mit eingebautem NFC[1]-Reader) und eine spezielle, lokale Anwendung dafür sorgen, dass sich das Reisedokument gegenüber einem Dienstanbieter im Internet wie ein normales elektronisches Identifikationsmittel verhält. Der Dienstanbieter muss sich davon überzeugen können, dass nur der Inhaber des Dokuments dieses als elektronisches Identifikationsmittel verwendet.
Um die in Frage kommenden Funktionen und Verfahren genau eingrenzen zu können, ist zunächst eine Übersicht der bestehenden internationalen und europäischen Standards unumgänglich.

2.1 Standards

Ein Reisedokument hat eine Lebensdauer von 5 bis 10 Jahren. Dies gilt ebenso für Reisedokumente mit Chip auf welchen persönliche Daten des Inhabers sicher gespeichert werden müssen. Deshalb müssen Sicherheitsbestimmungen und -mechanismen laufend überarbeitet und weiterentwickelt werden. Es erstaunt deshalb nicht, dass auf internationaler Ebene elektronische Reisedokumente unterschiedliche Sicherheitslevels implementiert haben und es deshalb auch standardisierende Dokumente gibt.

2.1.1 Internationale Standards

Die internationale Grundlage aller elektronischer Reisedokumente sind die MRTD[2]-Anforderungen der ICAO[3] in DOC 9303 [2]. Es ist eine Spezifikation, welche in erster Linie für elektronische Reisepässe gedacht ist, und diese vereinheitlichen soll.

Der internationale Standard für Reisedokumente wird von der ICAO in den folgenden Dokumenten festgelegt:

DOC 9303	Inhalt
Part 1 [3] [4]	Volume 1 beschreibt den Reisepass (im ID-3 Format) ohne Chip. Volume 2 spezifiziert den kontaktlosen Chip, welcher das Dokument zu einem eigentlichen MRTD macht, dessen kryptographischen Verfahren und die Kommunikation mit diesem.
Part 2	Part 2 befasst sich mit maschinenlesbaren Visa und ist deshalb für diese Studie nicht von Bedeutung
Part 3 [5] [6]	Part 3 beschreibt Ausweise, die als Reisedokument verwendet werden können, aber nicht unbedingt das Format eines Reisepasses haben (z.B. eine ID-Karte). Volume 1 beschreibt die veränderte Form der maschinenlesbaren Zone, Volume 2 den Chip (dieser kann auch kontaktbehaftet sein).
ICAO-TR 2010 [7]	Technical Report, welcher die Sicherheitserweiterungen der Zugriffkontrolle eines Lesers durch den MRTD-Chip beschreibt.

Tabelle 1: ICAO DOC 9303 Standards

[1] Near Field Communication
[2] Machine Readable Travel Documents
[3] International Civil Aviation Organization

2.1.2 Europäische Standards

2006 wurden in der EU alle Mitglieder verpflichtet auf dem MRTD-Chip zusätzlich zu den in ICAO DOC 9303 spezifizierten Daten biometrische Informationen zu speichern. Dies hatte zur Folge, dass weitere Sicherheitsverfahren notwendig wurden, um diese sensitiven Daten vor unberechtigtem Zugriff möglichst gut zu schützen. Diese erweiterten Verfahren wurden vom BSI[4] in den folgenden Technischen Richtlinien [8] zusammengefasst:

BSI Dokumente	Inhalt
TR-03110-1 [9]	Erweitert in erster Linie die in Doc 9303 Part 1 Volume 2 spezifizierten Sicherheitsmechanismen, welche für europäische Reisedokumente vorgeschrieben sind.
TR-03110-2 [10]	Erweitert die in Doc 9303 Part 3 Volume 2 spezifizierten Sicherheitsmechanismen und Funktionen für Identitätskarten und elektronische Reisepässe.
TR-03110-3 [11]	Enthält weitere Spezifikationen der in TR-03110-1 und -2 verwendeten Verfahren und definiert die notwendigen Public Key Infrastrukturen.

Tabelle 2: BSI Technische Richtlinien

2.2 Kryptographische Verfahren

Tabelle 3 enthält eine Übersicht der kryptographischen Verfahren und deren Quellen. Die mit **Fettschrift** versehenen Verfahren und Referenzen sind für diese Studie massgeblich.

Kryptographische Verfahren	Abkürzung	Anhang	Referenz
1. Basic Access Control **2. Passive Authentication** 3. Active Authentication	**BAC** **PA** AA	**7.1** **7.3** 7.4	**ICAO DOC 9303 Part 1- Volume 2**
4. Supplemental Access Control basierend auf Password Authenticated Connection Establishment	SAC PACE	7.2	ICAO-TR 2010 BSI TR-03110-1/3
5. Extended Access Control Version 1 **a. Chip Authentication Version 1** b. Terminal Authentication Version 1	EACv1 **CAv1** TAv1	 **7.6.1** 7.6.2	**BSI TR-03110-1/3**

Tabelle 3: Kryptographische Verfahren und Referenzen

Im Anhang A auf Seite 34 sind die kryptografischen Verfahren näher beschrieben, welche in den schweizerischen Reisedokumenten (ePass-10) heute verwendet werden und welche im Zusammenhang mit dieser Studie von Bedeutung sind.

[4] Bundesamt für Sicherheit in der Informationstechnik

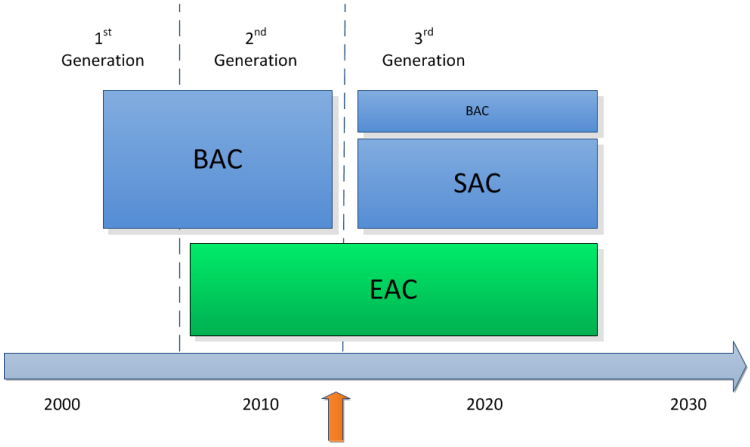


Abbildung 1: Entwicklung der MRTD-Standards

Der ICAO Technical Report welcher Supplemental Access Control (SAC) spezifiziert, ist für die Machbarkeitsstudie nur am Rand von Bedeutung. SAC stellt ein zu BAC zusätzliches Zugriffskontrollverfahren dar, welches voraussichtlich ab Ende 2013 in den schweizerischen Reisedokumenten eingeführt wird. Dadurch wird nebst BAC auch das SAC Verfahren künftig unterstützt werden. Abbildung 1 zeigt eine Übersicht der MRTD- und BSI-Standards in der zeitlichen Entwicklung.

2.3 Zugriffsrechte auf MRTD-Chip Datengruppen

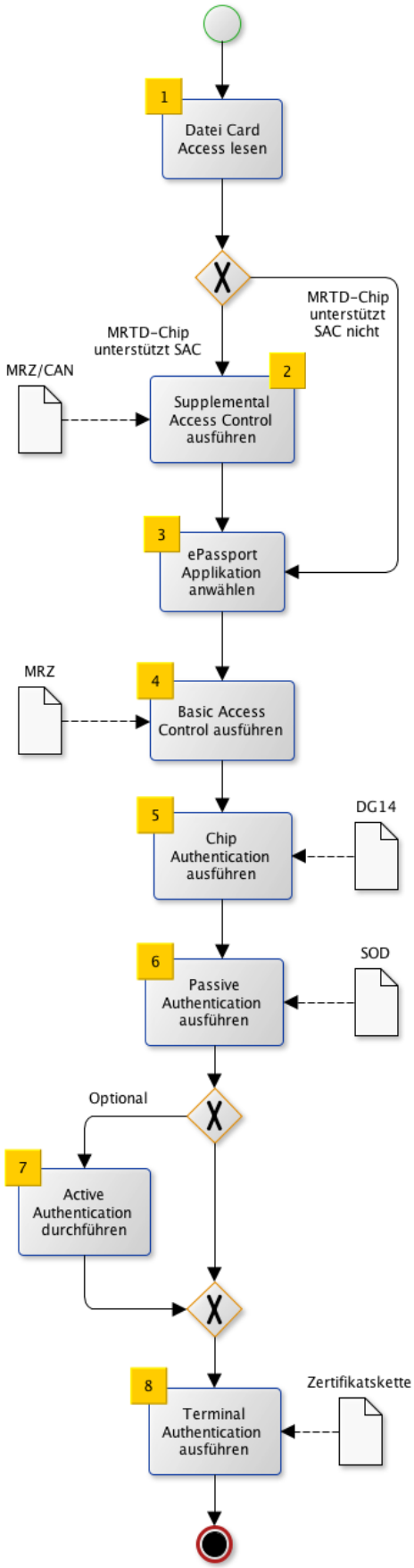
In Abhängigkeit der Zugriffsverfahren kann ein Lesegerät auf bestimmte Datengruppen zugreifen. An dieser Stelle (Tabelle 4) werden die für diese Studie benötigten Datengruppen aufgelistet, sowie die Zugriffsverfahren anhand der ICAO-MRTD bzw. BSI TR-03110-1/3 Spezifikationen.

DG	Inhalt	Zugriff mit	
		BAC/PACE	EACv1
DG1	Maschinenlesbare Zone (wie auf dem Dokument aufgedruckt)	x	x
DG2	Digitales Foto (identisch mit dem aufgedruckten Bild)	x	x
DG3	Digitale Fingerabdrücke	-	x
DG4	Digitale Iris	-	x
...		x	x
DG11	Detailinformationen zur Person	x	x
DG14	SecurityInfos	x	x
DG15	Active Authentication	x	x
DG16	...	x	x
SO_D	Document Security Object	x	x

Tabelle 4: ePassport Datengruppen und Zugriffrechte

2.4 MRTD-Chip Zugriffsprozess

Die im Anhang beschriebenen kryptographischen Verfahren dienen als Bausteine, um daraus einen Prozess zur Überprüfung des MRTD-Chips zusammenzusetzen. Im einfachsten Fall führt das Prüfgerät (Terminal) nur eine passive Authentifizierung durch (das in der MRTD-Spezifikation einzig verpflichtete Verfahren). Im Fall eines Zugriffs auf biometrische Daten hingegen ist der Prozess umfangreicher. In der für Europa gültigen Spezifikation TR-03110-1 wird zwischen einer ‚*Standard Inspection Procedure*' und zwischen einer ‚*Advanced Inspection Procedure*' unterschieden. Die Standardprozedur beinhaltet keine Authentisierung des Chips und ist von daher für diese Studie nicht von Bedeutung. Die in Abbildung 2 dargestellte und beschriebene ‚*Advanced ePassport Inspection*' beinhaltet alle möglichen Varianten, welche der Standard vorgibt. Die Schritte 1, 3, 4, 5 und 6 sind für die Machbarkeitsstudie notwendig und müssen von Chip bzw. Terminal durchgeführt werden, um zu den ICAO-MRTD- und BSI TR-03110-1/3-Spezifikationen kompatibel zu sein.



1. Lesen der Datei EF.CardAccess um die Sicherheitsparameter des Chips zu erfassen.

2. Wenn MRTD-Chip Supplemental Access Control (SAC) unterstützt, wird die MRZ optisch eingelesen oder die CAN eingegeben. SAC wird durchgeführt (s. Abschnitt 7.2). Nach erfolgreicher Autorisierung des Terminals wird Secure Messaging (SM_{SAC}) gestartet. Der MRTD-Chip gewährt Zugriff auf DG1, DG2, DG14, DG15 und EF.SOD.

3. Wenn MRTD-Chip nur Basic Access Control (BAC) unterstützt, wird die ePassport Applikation direkt angewählt.

4. Die MRZ wird optisch gelesen und BAC wird ausgeführt (s. Abschnitt 7.1). Nach erfolgreicher Autorisierung des Terminals wird Secure Messaging (SM_{BAC}) gestartet. Der MRTD-Chip gewährt Zugriff auf DG1, DG2, DG14, DG15 und EF.SOD.

5. Für eine ‚Advanced Inspection Procedure' sind die Schritte 4, 5 und 7 zwingend auszuführen, um Zugriff auf Datengruppen mit biometrischen Informationen zu gewähren. DG14 (beinhaltet öffentlicher Schlüssel für Chip Authentisierung) wird gelesen und Chip Authentication Version 1 (s. Abschnitt 7.6.1) wird ausgeführt. Secure Messaging (SM_{CA}) wird neuem Schlüsselmaterial neu gestartet. Zugriff auf DG1, DG2, DG14, DG15 und EF.SOD wird wiederum gewährt.

6. Das Terminal muss für jegliche Prüfvorgänge eine Passive Authentication durchführen. Dazu wird die Datei EF.SOD gelesen und die Signatur des *Document Security Object* geprüft (s. Abschnitt 7.3).

7. Active Authentication ist optional (s. Abschnitt 7.4).

8. Der wichtigste Schritt für den Zugang auf sensitive Daten ist die Authentifizierung des Terminals. Dazu wird von diesem die Zertifikatskette an den Chip übertragen und dieser führt die Terminal Authentication Version 1 durch (s. Abschnitt 7.6.2). Danach gewährt der Chip zusätzlichen Zugriff auf sensitive Datengruppen (DG3 und DG4), wobei die Kommunikation durch SM_{CA} geschützt ist.

Abbildung 2: MRTD Advanced Inspection Procedure

2.5 Anforderungen an die Lösung

Ausgehend von den gesteckten Zielen und Rahmenbedingungen der ‚Konzeptstudie elektronischer Identitätsnachweis' [1] des FedPol sowie basierend auf allgemeinen Sicherheitsüberlegungen und Datenschutzrichtlinien muss die angestrebte Lösung bestimmte Anforderungen erfüllen. Diese sind in Tabelle 5 zusammengetragen:

Anf.	Beschreibung	Quelle
A1	*Kompatibilität* Der MRTD-Chip verfügt über ICAO-MRTD-Standard.Funktionen nach DOC-9303 [4], sowie über erweiterte Funktionen nach BSI TR-03110-1 [9]. Es soll damit möglich sein, dass jedes schweizerische Reisedokument eID-fähig gemacht werden kann. Die Grundfunktionen (als international einsetzbares elektronisches Reisedokument) müssen dabei aber erhalten bleiben.	• Konzeptstudie elektronischer Identitätsnachweis [1]
A2	*Zwei-Faktor-Authentifizierung (2FA)* Die zu authentifizierende Person (Inhaber des Reisedokuments) muss sich gegenüber einem authentifizierenden Dienst mindestens mit 2-Faktoren authentisieren. Der authentifizierende Dienst muss sicherstellen, dass die Gegenstelle im Besitz des Reisedokuments ist und gleichzeitig beweisen kann, dass sie in Kenntnis eines Geheimnisses ist, welches sie berechtigt das Reisedokument zur Authentifizierung zu nutzen.	• Konzeptstudie elektronischer Identitätsnachweis [1] • Allgemeine Sicherheits-anforderungen
A3	*Sicherer Kommunikationskanal* Die Kommunikation zwischen MRTD-Chip und authentifizierendem Dienst muss gegen Abhörangriffe geschützt sein.	• Allgemeine Sicherheits- und Datenschutz-anforderungen
A4	*Man-in-the-Middle Resistenz* Ein authentifizierender Dienst muss sich von der Echtheit und der Präsenz des MRTD-Chips direkt überzeugen können. Es muss verhindert werden, dass ein Intermediär (lokale Applikation) gegenüber dem authentifizierenden Dienst korrekte Informationen eines bereits verwendeten aber nicht mehr verfügbaren Reisedokuments wiedereinspielen kann.	• Allgemeine Sicherheits- und Datenschutz-anforderungen
A5	*Informationelle Selbstbestimmung* Ein authentifizierender Dienst darf keine Personendaten aus dem MRTD-Chip ohne Einverständnis des Inhabers lesen.	• Allgemeine Sicherheits- und Datenschutz-anforderungen
A6	*Informationelle Selbstbestimmung* Weder ein Intermediär (lokale Applikation) noch ein authentifizierender Dienst dürfen biometrische Daten aus dem Reisedokument lesen.	• ICAO-MRTD 9303 [4] • BSI TR-03110-1 [9]

Tabelle 5: Anforderungskatalog

2.6 Lösungsansätze

Zur Authentifizierung des Reisenden an der Grenzkontrolle setzt man bei Reisedokumenten auf eine starke 2-Faktor-Authentisierung. Erstens das Dokument selbst (*something you have*) und zweitens biometrische Merkmale (*something you are*), welche je nach Überprüfungsverfahren gegenüber dem aufgedruckten Foto oder den gespeicherten Daten übereinstimmen müssen.

Diese Vergleiche sind einfach zu machen, wenn die Person physisch anwesend ist. Dafür wurde der MRTD-Chip mit seinen Funktionen ausgelegt. Für eine Authentisierung gegenüber einem Online-Dienst, lässt sich dies aber kaum oder gar nicht überprüfen.
Aus diesem Grund müssen als Lösungsansatz die biometrischen Merkmale durch ein asymmetrisches Schlüsselpaar (*something you have*) mit PIN gesichertem Zugriff (*something you know*) ersetzen werden.
Dazu sind zwei Lösungsansätze möglich:

1. Der private Schlüssel des asymmetrischen Schlüsselpaars wird auf dem Chip generiert und der Zugriff auf den privaten Schlüssel durch eine PIN geschützt. Im Fall eines MRTD-Chips könnte dieser so über die NFC-Schnittstelle von einer Applikation als sicheres Hardware-Authentisierungstoken verwendet werden. Das hätte den Vorteil, dass der Chip zur gegenseitigen zertifikatbasierten SSL/TLS-Authentifizierung nach RFC2246 [12] gegenüber einem Standard SSL/TLS-Webserver oder -Webservice eingesetzt werden kann. Die Verwendung des privaten Schlüssels auf dem MRTD-Chip ist aber nicht PIN geschützt, und dies wird sich nach ICAO-und BSI-Richtlinien auch nicht ändern. Der Zugriff durch Passport-Prüfgeräte wird auch in Zukunft nur durch die Eingabe einer MRZ bzw. CAN geschützt sein. Damit musste dieser Ansatz im Vornherein verworfen werden.

2. Das asymmetrische Schlüsselpaar auf dem MRTD-Chip wird nur dafür verwendet, wozu es konzipiert wurde, nämlich für die Authentisierung des Reisedokuments selbst. Darum muss ein zweites Authentifizierungsmerkmal (Credential) ausserhalb des Chips für den rechtmässigen Inhaber generiert und über einen Registrierungsdienst mit dem MRTD-Chip nachträglich gekoppelt werden.

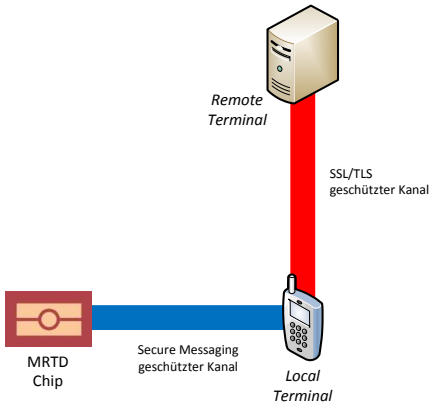
3. MRTD online Authentication (MoA)

Das MRTD online Authentication Verfahren ist der Kern der Machbarkeitsstudie. In diesem Kapitel werden zunächst Aufbau und Anordnung der Komponenten aufgezeigt. In den darauf folgenden Abschnitten werden Beispiele möglicher Registrierungs- und Authentisierungsprozesse eingehender beschrieben.

Die hier beschriebenen Prozesse stellen jeweils den positiven Ablauf dar. Fehler- und Ausnahmesituationen der dargestellten Prozesse wurden an dieser Stelle bewusst nicht berücksichtigt.

3.1 MoA Setup

Die Vorgaben der Konzeptstudie erfordern, dass sich ein Benutzer mit seinem Reisedokument nicht gegenüber einem lokalen Prüfgerät, sondern gegenüber einem entfernten Dienst authentisiert. In der Folge wird dieser Online-Dienst allgemein als Remote Terminal (RT) bezeichnet.



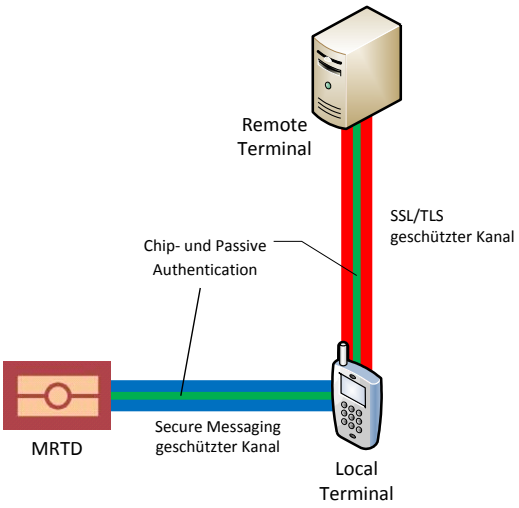
Der MRTD-Chip muss dazu über ein lokales Gerät mit diesem entfernten Authentisierungsdienst verbunden werden. Dies kann nur über einen lokalen Leser erfolgen, welcher als Intermediär wirkt.
Es wird deshalb zwischen einem Local Terminal und einem Remote Terminal unterschieden. Die Kommunikationsverbindungen zwischen MRTD-Chip, Local Terminal (LT) und Remote Terminal (RT) müssen gemäss Anforderung A3 gegen Abhörangriffe geschützt werden. Dies ist zwischen MRTD-Chip und Lesegerät durch den ICAO Standard (Secure Messaging) gewährleistet. Zwischen LT und RT wird die Kommunikation mittels SSL/TLS abgesichert.

Abbildung 3: MoA Setup

MRTD-Chip	Local Terminal (LT)	Remote Terminal (RT)
Ein auf dem Reisedokument eingebauter Chip mit RFID-Schnittstelle.	Zum Beispiel ein Smartphone mit NFC-Schnittstelle, welche die Kommunikation mit dem Chip ermöglicht. Das Local Terminal beinhaltet die Funktion der lokalen Leseapplikation (LLA). Diese bildet die Schnittstelle zum Benutzer, dem MRTD-Chip sowie dem Remote Terminal und kontrolliert die Kommunikation zwischen diesen beiden Endpunkten.	Das RT authentisiert direkt den MRTD-Chip. Das RT ist ein Web Service, welcher SSL/TLS unterstützt mit einer Softwarekomponente welche den MRTD Chip direkt über Chip- und Passive Authentication authentisieren kann.

Tabelle 6: MoA Komponenten

Direkte Chip- und Passive Authentication:



Wie die Anforderung A4 aufzeigt, muss sich das Remote Terminal von der Echtheit, sowie von der Präsenz der Karte überzeugen können.
Diese Sicherheitsvorgabe kann nur dann erfüllt werden, wenn das Remote Terminal eine direkte Chip- und Passive-Authentication mit dem MRTD-Chip durchführen kann.
In dieser Phase der Authentifizierung des MRTD-Chips darf es einem Schadprogramm auf dem Local Terminal nicht möglich sein, die Identität der Karte zu fälschen bzw. deren Präsenz gegenüber dem prüfenden Dienst vorzutäuschen.

Abbildung 4: direkte Chip- und Passive Authentication

Dieses Remote Authentisierungsverfahren des MRTD-Chips durch ein Remote Terminal, kann als Teilprozess zur Registrierung eines Benutzers, wie auch zur regelmässigen Authentisierung eingesetzt werden. Bei der Registrierung wird die *direkte Chip- und Passive Authentication* verwendet, um ein persönliches Authentifizierungsmerkmal (Credential) an den MRTD-Chip zu koppeln, um dann diese beiden Mittel als Zweifaktor-Authentisierung verwenden zu können.

3.2 Authentifizierungsmittel

Die Art eines persönlichen Authentisierungsmerkmals (Credentials) ist dabei nicht zwingend vorgegeben. Es sind unterschiedliche Merkmale und Verfahren möglich. In einem Registrierungsprozess wird ein Authentisierungsmittel an den MRTD-Chip geknüpft. Es ist denkbar, dass ein Benutzer auch mehrere Credentials an seinen MRTD-Chip binden lässt. In diesem Dokument werden beispielshaft die Registrierungs- und Authentisierungsprozesse von drei verschiedenen Benutzerauthentisierungsverfahren aufgezeigt:

1. Authentisierung mit Benutzerzertifikat (MoA-Cert)
2. Authentisierung mit Passwort (MoA-PW)
3. Authentisierung mit MSS (MoA-MSS)

Hinweis
In Ergänzung zu diesem Dokument wird von der BFH als ‚Proof-of-Concept' ein Prototyp mit MOA-Cert (Zertifikat) umgesetzt.

3.3 Registrierung

In der Registrierungsphase von MoA wird der MRTD Chip mit einem persönlichen Credential des Inhabers über das Smartphone logisch verbunden. Unabhängig vom verwendeten Credential wird diese Verbindung auf einem staatlich kontrollierten Federal Registration Service (FRS) vorgenommen. Dieser Registrierungsserver prüft zunächst die Zusammengehörigkeit von Chip und Inhaber. Um sicher zu stellen, dass nur der rechtmässige Inhaber des Reisedokuments sich mit Hilfe seines MRTD-Chips registrieren kann, wird diesem vom FRS per eingeschriebenen Brief ein Code PW_{INIT} in Form eines QR-Codes oder eines Einmal-Passwortes zugestellt.
Für alle Authentisierungsmethoden gilt, dass die MoA-LLA in der Registrierungsphase überprüfen kann, dass es sich bei der Gegenstelle um den staatlichen Registrierungsserver (FRS) handelt. Deshalb muss dieser über ein vertrauenswürdiges SSL/TLS-Zertifikat verfügen.

3.4 Authentisierung

Zur Authentisierung gegenüber einem online Service kann der Benutzer das zuvor registrierte persönliche Authentisierungsmittel zusammen mit dem MRTD-Chip einsetzen. Je nach Credential sind unterschiedliche Online Services möglich. Mit MoA-Cert (Benutzerzertifikat) kann auch ein eGovernment oder privatwirtschaftlicher Webservice die direkte Authentifizierung des Benutzers vornehmen, da er die Zusammengehörigkeit des MRTD-Chip zum Benutzerzertifikat selbst prüfen kann. Bei MoA-PW (Passwort) und MoA-MSS (Mobile ID) kann dies nur ein staatlicher Authentisierungsserver, welcher auf die Informationen des Registrierungsserver (FRS) zugreifen kann.

3.5 Authentisierung mit Benutzerzertifikat (MoA-Cert)

Diese Methode wird stellvertretend für die Methoden MoA-PW und MoA-MSS in detaillierter Form dargestellt und beschrieben, da diese Methode auch im Proof-of-Concept umgesetzt wurde.

3.5.1 Registrierung

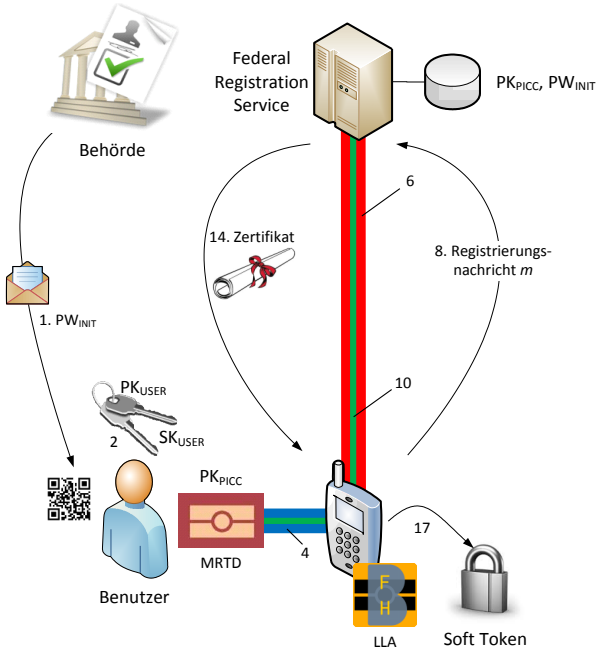


Abbildung 5 zeigt den Registrierungsprozess in einer Übersicht. Der Einfachheit halber sind nur die wichtigsten Schritte nummeriert. Die vollständige Beschreibung kann der folgenden Tabelle 7 entnommen werden.

Abbildung 5: Registrierung mit Benutzerzertifikat

Detaillierter Prozessablauf:

MRTD-Chip	LLA/Benutzer	Federal Registration Service (FRS)
	1. Der Benutzer erhält per Post von der zuständigen Bundesstelle einen persönlichen Code PW_{INIT} als QR-Code oder Einmal-Passwort. Dieses liest oder tippt er über die LLA in sein Smartphone ein.	
	2. Auf der LLA des Smartphones wird ein zufälliges, asymmetrisches Schlüsselpaar erzeugt mit einem öffentlichen Schlüssel PK_{USER} und einem privaten Schlüssel SK_{USER}.	

MRTD-Chip	LLA/Benutzer	Federal Registration Service (FRS)
	3. Der Benutzer liest einmalig die MRZ[5] mit seiner Smartphone-Kamera ein, oder gibt die *Dokumentennummer*, sein *Geburtsdatum* und das *Ablaufdatum* des Reisedokuments von Hand ein.	
4. Der Benutzer bringt sein Reisedokument mit dem Smartphone zusammen. Das Smartphone wird sich mittels BAC gegenüber dem Chip autorisieren und es wird ein Secure Messaging Kanal (SM_{BAC}) aufgebaut.		
➔ ➔ ➔	5. Die LLA liest die für die Chip Authentication benötigten Daten[6] ($DOMAIN_{PICC}$, PK_{PICC}) aus DG14 aus.	
	6. Die LLA baut eine SSL/TLS-Verbindung zum FRS auf.	
	7. Die LLA verifiziert das FRS Serverzertifikat anhand der Zertifizierungskette zum vertrauenswürdigen CSP.	
	8. Die LLA sendet eine Registrierungsnachricht[7] $m:= h(PW_{INIT}) \mid enc_{PW_{INIT}}[CSR(PK_{USER}, DOMAIN_{PICC}, PK_{PICC})]$ an den FRS. ➔ ➔ ➔	
		9. Der FRS entschlüsselt die Nachricht mit PW_{INIT} und kontrolliert die Signatur des CSR.
10. Der FRS baut über das Smartphone eine Verbindung zum MRTD-Chip auf, wobei die LLA die Nachrichten mittels SM_{BAC} verschlüsselt und authentisiert. Der FRS stösst eine Chip Authentication an. MRTD-Chip und FRS führen einen DH-Key Exchange durch und errechnen die SM_{CA} Session-Schlüssel K_{ENC} und K_{MAC}.		
11. Der FRS sendet die Befehle zum Auslesen des Security Objects (SO_D) und der Datengruppe DG14 an den MRTD-Chip, um eine Passive Authentication durchzuführen. Die LLA leitet die Befehle zwischen FRS und Chip weiter, ohne diese zu verändern.		
		12. Der FRS überprüft die Authentizität der erhaltenen Daten und damit des MRTD-Chips. Der FRS verfügt redundant über alle notwendigen Daten, um die Zusammen-gehörigkeit des Reisedokuments (PK_{PICC}) zum rechtmässigen Inhaber (PW_{INIT}) herstellen zu können.

[5] Mit Einführung von SAC kann hier auch die CAN verwendet werden.

[6] $Domain_{PICC}$ sind die Domainparameter für den Diffie-Hellman Key Exchange. PK_{PICC} ist der öffentliche Schlüssel des MRTD-Chip. Der Begriff PICC wird hier wie in BSI TR-03110 verwendet und steht für Proximity Integrated Circuit Chip.

[7] bestehend aus dem Hashwert von PW_{INIT}, verkettet mit einem mit PW_{INIT} verschlüsselten Certificate Signing Request (nach PKCS#10 Standard [17]) welcher mit SK_{USER} signiert wurde.

MRTD-Chip	LLA/Benutzer	Federal Registration Service (FRS)
		13. Sind alle Daten korrekt, erstellt der FRS auf Basis seiner Informationen ein Zertifikat für den Benutzer, welches dessen Chip mit dem zufälligen Schlüsselpaar aus Schritt 2 koppelt. Dazu wird als *CommonName* im *Subject DN*[8] des Zertifikats ein komprimiertes Abbild von PK_{PICC} verwendet.
	← ← ←	14. Der FRS sendet das von ihm ausgestellte Zertifikat an die LLA.
	15. Die LLA lässt den Benutzer eine PIN[9] wählen.	
	16. Die LLA verschlüsselt den privaten Schlüssel SK_{USER} mit der gewählten PIN.	
	17. Die LLA speichert das Zertifikat und den verschlüsselten SK_{USER} lokal auf dem Smartphone (letzterer in einem Soft-Token).	

Tabelle 7: Prozessablauf Registrierung mit Zertifikat

Ergebnis der Registrierungsphase mit Benutzerzertifikat

Nach erfolgter Registrierung hat der Benutzer ein - von staatlicher Stelle - beglaubigtes Zertifikat, womit er gegenüber einem Authentication Service seine Identität zusammen mit seinem Reisedokument beweisen kann. Nur der Benutzer, welcher Kenntnis der PIN hat, kann sich gegenüber einem Authentication Service authentisieren. Insgesamt sind also drei Faktoren zur Authentifizierung notwendig:

1. Reisedokument mit MRTD-Chip,
2. Schlüsselpaar auf Smartphone,
3. PIN um auf privaten Schlüssel zugreifen zu können.

3.5.2 Authentisierung

Der folgende Authentisierungsprozess beinhaltet die Schritte, in welchen eine Authentifizierung des MRTD-Chips und des Benutzers gegenüber einem Authentication Server erfolgen. Die Authentisierung des Benutzers erfolgt im SSL/TLS 2-way Handshake Protokoll. In diesem Protokoll wird ebenfalls das Benutzerzertifikat übertragen.

Bedingung für diese Form der Authentisierung ist die vorgängige Implementierung der MoA-Middleware (MoA-MW) auf dem Authentication Server.

[8] Subject Distinguished Name nach RFC5280 [24,22]

[9] Personal Identification Number

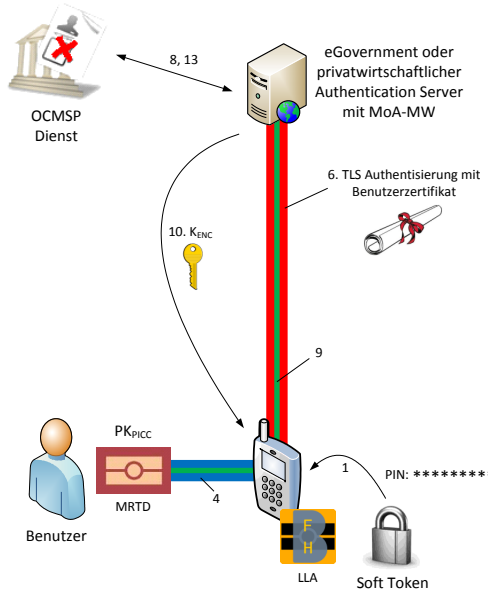


Abbildung 6 zeigt den Authentisierungsprozess im Überblick. Der Einfachheit halber sind nur die wichtigsten Schritte nummeriert. Die vollständige Beschreibung kann der folgenden Tabelle 8 entnommen werden.

Abbildung 6: Authentisierung mit Zertifikat

Detaillierter Prozessablauf:

MRTD-Chip	LLA/Benutzer	Authentication Service (AS)
	1. Der Benutzer gibt seine PIN ein, um der LLA den Zugriff auf den privaten Schlüssel zu geben.	
	2. Die LLA entschlüsselt den privaten Schlüssel SK_{USER}.	
	3. Falls die LLA die MRZ des Reisedokuments aus der Registrierungsphase nicht bereits gespeichert hat, muss der Benutzer die MRZ mit seiner Smartphone-Kamera einlesen, oder die *Dokumentennummer*, sein *Geburtsdatum* und das *Ablaufdatum* des Reisedokuments von Hand eingeben.	
4. Der Benutzer bringt sein Reisedokument mit dem Smartphone zusammen. Das Smartphone wird sich mittels BAC gegenüber dem Chip autorisieren und es wird ein Secure Messaging Kanal (SM_{BAC}) aufgebaut.		
➔ ➔ ➔	5. Die LLA liest die für die Chip Authentication benötigten Daten ($DOMAIN_{PICC}$, PK_{PICC}) aus DG14 aus.	
	6. Die LLA baut eine SSL/TLS-Verbindung zum Remote Terminal auf. Dieser verlangt eine zertifikatbasierte Authentifizierung des Benutzers SSL/TLS Handshake-Protokoll [12]. Die LLA verwendet dabei SK_{USER} um den Benutzer gegenüber dem Remote Terminal zu authentisieren.	

MRTD-Chip	LLA/Benutzer	Authentication Service (AS)
		7. Der Authentication Service verifiziert das von der LLA im SSL/TLS Handshake-Verfahren erhaltene Benutzerzertifikat, indem er die Zertifizierungskette bis zur vertrauenswürdigen Root-CA (CSP, welcher in der Registrierungsphase das Zertifikat des Benutzers ausgestellt und signiert hat) bildet.
		8. Der Authentication Service kann den Revokations-Status des Benutzerzertifikats über einen ‚Online Certificate- and MRTD-Status Protocol' Dienst (s. Kapitel 3.8) prüfen.
9. Der Authentication Service baut über das Smartphone eine Verbindung zum MRTD-Chip auf, wobei die LLA die Nachrichten mittels SM_{BAC} verschlüsselt und authentisiert. Das Remote Terminal initiiert dabei eine Chip Authentication. MRTD-Chip und Remote Terminal führen einen DH-Key Exchange durch und errechnen dabei die SM_{CA} Session-Schlüssel K_{ENC} und K_{MAC}.		
	← ← ←	10. Das Remote Terminal überträgt den Session-Schlüssel K_{ENC} (nicht aber K_{MAC}) an die LLA. Mit K_{ENC} kann die LLA jeglichen Verkehr zwischen Chip und Remote Terminal mithören, selbst aber keine gültigen Nachrichten generieren, da ihr der dazu notwendige Session-Schlüssel K_{MAC} fehlt.
11. Das Remote Terminal sendet die Befehle zum Auslesen des Security Objects (SO_D) und der Datengruppe DG14 um eine Passive Authentication durchzuführen. Die LLA entschlüsselt die Befehle mit K_{ENC} und kontrolliert, dass der Authentication Service des RT keine weiteren Daten anfordert. Die LLA sendet die Befehle an den Chip und die resultierenden Daten zurück an das Remote Terminal - ohne diese zu verändern.		
		12. Der Authentication Service überprüft die Authentizität der erhaltenen Daten und damit des MRTD-Chips.
		13. Der Authentication Service kann den Revokations-Status eines Reisedokuments online prüfen, sofern der OCMSP (s. Kapitel 3.8) eine Statusabfrage von MRTD's anbietet.
		14. Der Authentication Service vergleicht den aus DG14 gelesenen PK_{PICC} und vergleicht ihn mit der komprimierten Version im *Subject DN* des Benutzerzertifikats.

MRTD-Chip	LLA/Benutzer	Authentication Service (AS)
		15. Sind alle Daten korrekt, ist der Authentisierungsvorgang damit abgeschlossen.

Tabelle 8: Prozessablauf Authentisierung mit Zertifikat

Ergebnis der Authentisierungsphase

Nach erfolgter Authentisierung kann ein Remote Terminal verifizieren, dass sich ein Benutzer auf seinem Dienst angemeldet hat,

1. welcher gerade jetzt ein Reisedokument bei sich hat, welches von der schweizerischen Eidgenossenschaft ausgestellt wurde;
2. welcher im Besitz eines Schlüsselpaars ist, welches mit diesem Reisedokument von einer vertrauenswürdigen, staatlichen Stelle assoziiert wurde;
3. welcher in Kenntnis einer PIN ist, um auf den privaten Schlüssel zugreifen zu können.

Das Remote Terminal hat aber keine Informationen darüber, ***wer*** dieser Benutzer ist. Ausser es verfügt bereits über Informationen über den Benutzer und hat diese vorgängig mit dem Identifikator PK_{PICC} verbunden.

3.6 Authentisierung mit Passwort (MoA-PW)

Die zweite Methode zur Benutzerauthentisierung sieht vor, den MRTD-Chip über ein Benutzerpasswort auf dem Federal Registration Service zu koppeln. Damit wird auf ein Soft-Token im Smartphone verzichtet.

3.6.1 Registrierung

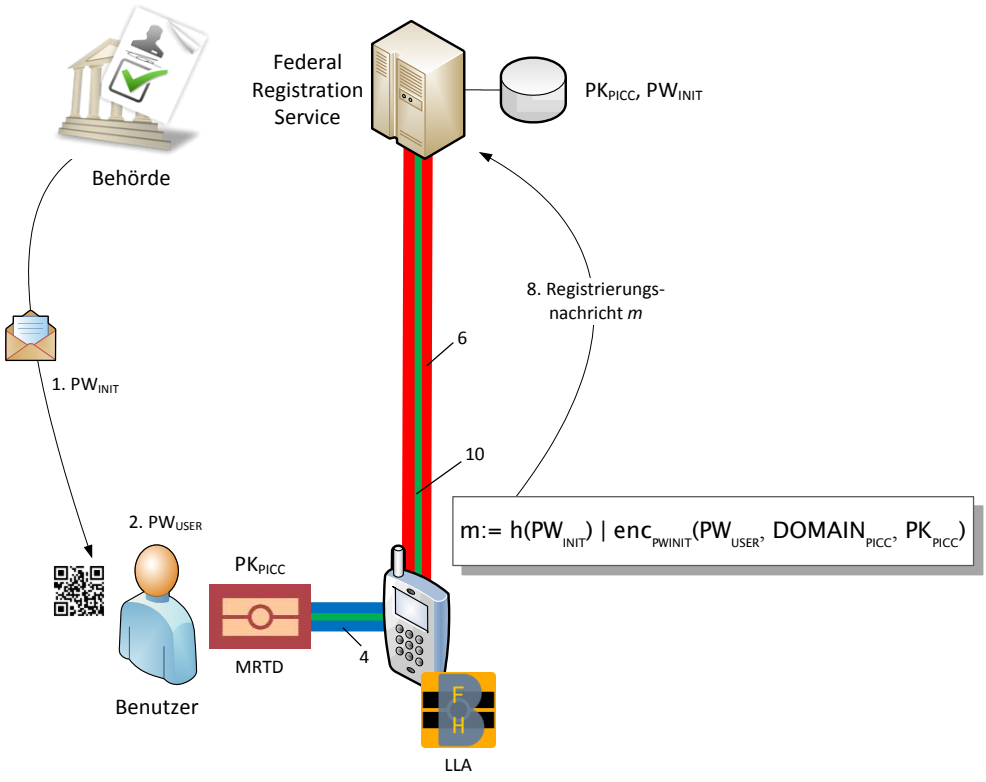


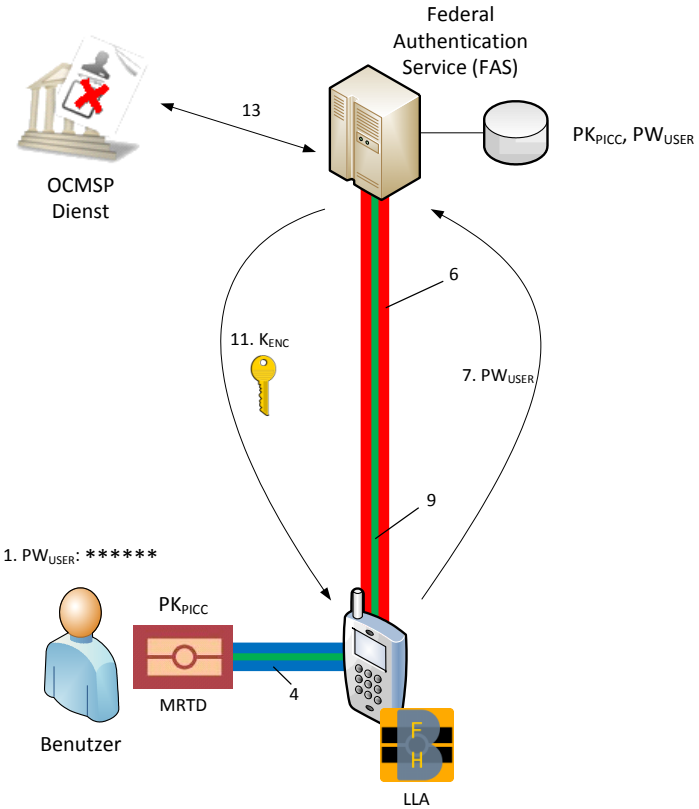
Abbildung 7: Registrierung mit Passwort

Dieser Lösungsansatz hat den Vorteil, dass der Authentisierungsvorgang unabhängig vom verwendeten Smartphone ist. Nur die LLA muss installiert sein und die MRZ muss auf einem Smartphone einmalig eingelesen werden. Damit kann sich ein Benutzer mit MRTD und Passwort gegenüber dem FAS authentisieren.

Im Gegensatz zur Registrierung mit Benutzerzertifikat, muss bei dieser Methode das Credential (Benutzerpasswort) auf dem Server abgelegt werden. In Schritt 2 gibt der Benutzer auf der LLA sein frei gewähltes Passwort PW_{USER} ein. Als Registrierungsnachricht in Schritt 8 wird PW_{USER} verschlüsselt in $m := h(PW_{INIT}) \mid enc_{PWINIT}(PW_{USER}, DOMAIN_{PICC}, PK_{PICC})$ zum Server übertragen. Die Schritte, in welchen der FRS ein Zertifikat für den Benutzer erstellt und übermittelt, sowie der Schritt, in welchem die LLA ein PKCS#12 Softtoken auf dem Smartphone speichert, entfallen.

3.6.2 Authentisierung

Die Authentisierung mit Passwort kann nur gegenüber einem Online Service erfolgen, welcher ebenfalls in Besitz des gemeinsamen Geheimnisses (Passwort des Benutzers) ist. Damit entfallen bei dieser Methode alle eGovernment und privatwirtschaftlichen Authentication Services. Die Authentisierung kann nur gegenüber einem Federal Authentication Service (FAS) erfolgen.



Das Verfahren zu dieser Methode der Authentisierung entspricht mehrheitlich der Beschreibung in Tabelle 8 mit folgenden Unterschieden:

- Im Gegensatz zur PIN- Eingabe in Schritt 1, muss hier der Benutzer sein Passwort eingeben.
- Anstelle der SSL/TLS Benutzer-authentifizierung in Schritt 6, wird diese hier in Schritt 7 gemacht, indem das Passwort in der SSL/TLS Verbindung geschützt übertragen wird und in Schritt 8 der FRS das PW_{USER} prüft.

Abbildung 8: Authentisierung mit Passwort

3.7 Authentisierung mit MSS (MoA-MSS)

Die dritte Methode zur Benutzerauthentisierung verbindet den MRTD-Chip mit einem externen Authentisierungsdienst eines Mobiltelefon Anbieters, welcher *Mobile Signature Services* (MSS) nach ETSI TS 102 204 (V1.1.4) [13] unterstützt. In der Schweiz ist das zum jetzigen Zeitpunkt die Swisscom mit der *Mobile ID* [14]. Diese Methode wird hier aufgeführt, um aufzuzeigen, dass ganz unterschiedliche Benutzerauthentisierungsverfahren an MoA gekoppelt werden können.
Auf technische und kommerzielle Vorbedingungen zur Nutzung dieses Services durch den FAS wird an dieser Stelle verzichtet. Auf Benutzerseite wird vorausgesetzt, dass er in seinem mobilen Gerät eine SIM-Karte der neusten Generation verwendet. Diese SIM-Karte verfügt über eine Mobile ID App,

sowie über einen benutzerspezifischen privaten Schlüssel und ermöglicht die Ver- und Entschlüsselung von SMS-Nachrichten und die Signierung von Nachrichten.
Als Identifikator auf Seiten FRS wird in diesem Beispiel die MSISDN (Mobilnummer des Benutzers) verwendet. Es wäre auch möglich das X.509-Zertifikat der Mobile ID anstelle der MSISDN zu verwenden.

3.7.1 Registrierung

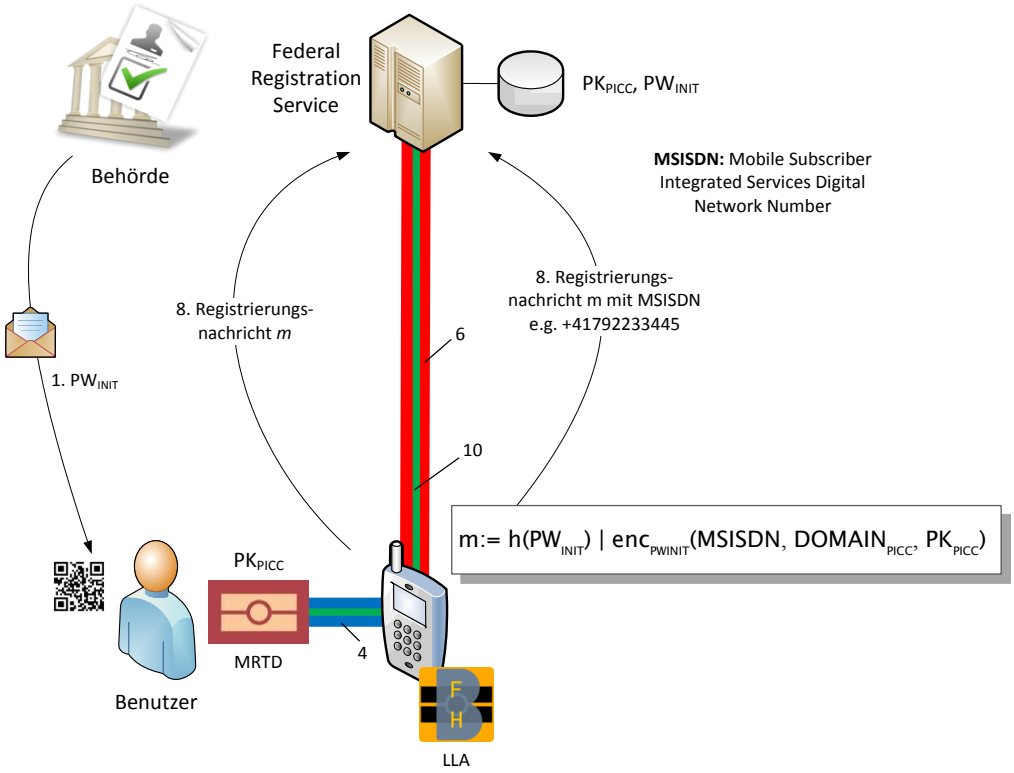


Abbildung 9: Registrierung mit Mobile Nummer

Im Gegensatz zur Registrierung mit Passwort, muss in dieser Methode die MSISDN (Mobilenummer) auf dem Server abgelegt werden. Diese kann durch die LLA aus dem Smartphone ausgelesen werden. Als Registrierungsnachricht in Schritt 8 wird die MSISDN verschlüsselt in m:= $h(PW_{INIT})$ | enc_{PWINIT}(MSISDN, $DOMAIN_{PICC}$, PK_{PICC}) zum Server übertragen. Der Benutzer muss kein Passwort eingeben, er wählt zur Registrierung in der LLA einfach die Mobile ID an.

3.7.2 Authentisierung

Eine Authentisierung mit MSS in Kombination mit MoA wird sinnvollerweise in Kombination mit dem Federal Authentication Service (FAS) eingesetzt, nachdem eine Registrierung der MSISDN stattgefunden hat, wie sie im vorhergehenden Kapitel beschrieben wurde.

Das Verfahren läuft in vereinfachter Form folgendermassen ab (vgl. dazu Abbildung 10):

- Die MSISDN zu einem MRTD-Chip ist bereits auf dem FAS registriert.
- Bei einem Loginversuch gegenüber dem FAS laufen dieselben Schritte ab, wie bei der Authentisierung mit Passwort (vgl. Kapitel 3.6.2). Anstelle der Eingabe eines Passworts in Schritt 1 stösst die LLA gegenüber dem FAS direkt eine Mobile-Signatur Authentisierung an.
- Der FAS sendet (7) eine Signaturanfrage (zufälliger Text) mit den Angaben der Mobile Nummer der SIM-Karte an den MSS Dienst des Providers.
- Der MSS überprüft bei der eigenen CA, ob das Zertifikat des Mobile Kunden mit dieser Nummer noch gültig ist. Der MSS sendet den Signaturanfragetext per SMS an die SIM-Karte. Optional kann der Benutzer den Text mit demjenigen vergleichen, der ihm von der LLA angezeigt wird.

- Durch Eingabe seiner PIN (8) auf dem mobilen Gerät bestätigt der Benutzer die Freigabe zur Signatur des Textes durch die SIM-Karte. Die signierte Antwort wird zum MSS zurückgesendet und von diesem geprüft.
- Der MSS sendet eine Meldung an den FAS, um die Authentisierung zu bestätigen.
- Die restlichen Schritte entsprechen wiederum dem Standard MoA Verfahren.

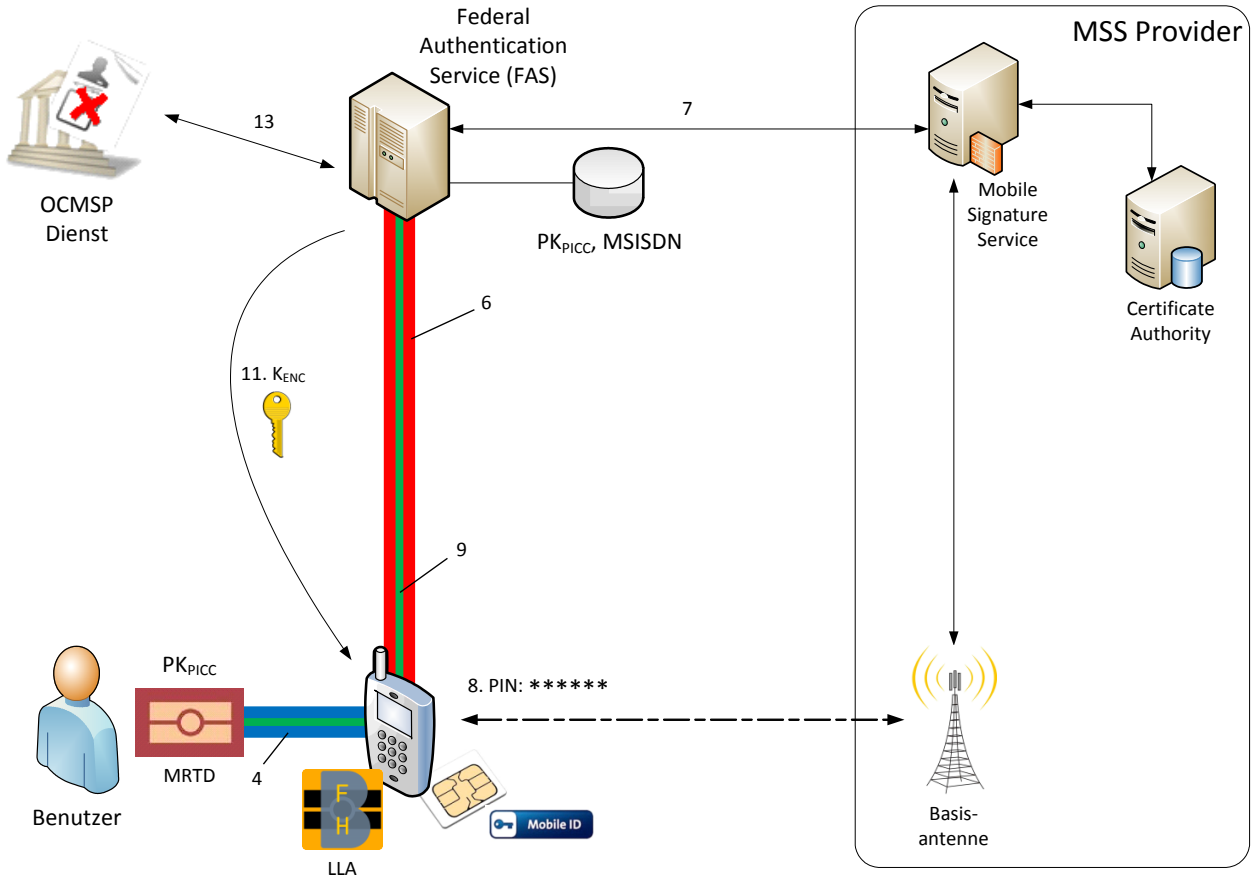


Abbildung 10: Authentisierung mit MSS

Denkbar wäre auch der Einsatz von MoA-MSS mit einem privatwirtschaftlichen Authentisierungsdienst. Dazu muss dieser Service als *Application Provider* gegenüber dem MSS Provider agieren können und zusätzlich die MoA Middelware implementiert haben. Anstelle der MSISDN müsste aber für das Identity Mapping ein MoA-basierender Identifikator verwendet werden. Für einen privatwirtschaftlichen Authentisierungsdienst hätte dies den Vorteil den Mobile Signature Service mit einer staatlich beglaubigten Identität kombinieren zu können. Diese Form der Authentisierung ist sicherlich nicht zu Ende gedacht. Sie wird hier dennoch aufgeführt, um als Anregung für eine weitere mögliche Anwendungsform von MoA zu dienen.

3.8 Online Certificate- and MRTD-Status Protocol Service (OCMSP)

Um den aktuellen Status eines eID-fähigen Reisedokuments und optional eines Benutzerzertifikats (nur bei MoA-Cert) überprüfbar zu machen, bedarf es eines offiziellen Online-Dienstes. Einem Authentication Service muss die Möglichkeit geboten werden den aktuellen Zustand zeitnah abzufragen.
Die Prozesse zum Sperren eines Reisedokuments bei Verlust sind heute klar geregelt und für den Inhaber einfach durchführbar. Soll das Reisedokument künftig über eine eID-Funktion verfügen, kommt eine Revokation der Schlüssel hinzu. Ein Authentication Service (ob privatwirtschaftlich oder FAS) muss in der Lage sein automatisch den aktuellen Staus eines MRTD-Chips überprüfen zu können. Analog verhält es sich mit dem X.509 Benutzerzertifikat. Für diese Zertifikate besteht mit dem Online Certificate Status Protocol (OSCP) [15] eine standardisierte Lösung, welche für die Abfrage von MRTD-Chips erweitert werden müsste.

3.9 Übersicht der Komponenten

Local Terminal (LT): Das LT ist ein netzwerkfähiges Gerät, welches über eine NFC-Schnittstelle nach ISO 14443 [16] verfügt. Auf dem LT ist die Lokale Leseapplikation (MoA-LLA) installiert, welche die Logik und Kommunikation zwischen ICAO-MRTD und Remote Terminal übernimmt. Dies kann ein PC mit einem RFID Leser (über USB-Schnittstelle) sein, oder ein NFC-fähiges Smartphone/Tablet[10].

Remote Terminal (RT):
Das RT ist ein Webservice, welcher über die MoA-Middleware (MoA-MW) verfügt. Dieser Webservice führt die Authentifizierung des Benutzers mittels MRTD-Chip und Authentisierungsmerkmal durch. Ein RT kann drei Ausprägungen haben:

1. *Federal Registration Service (FRS):* Ein Service, über welchen der Inhaber eines Reisedokuments die eID-Funktion aktivieren kann, indem er sich auf diesem Service registriert. Die zuständige Bundesstelle gibt den persönlichen Initial Code (PW_{INIT}) zur Registrierung aus.

2. *Federal Authentication Service (FAS*): Ein spezieller Authentication Service ist der FAS, welcher redundant (wie der FRS auch) über die Personendaten des Inhabers eines Reisedokuments verfügt. Der FAS kann anderen Applikationen Identitätsinformationen (z.B. Meldeadresse) über ein entsprechendes Identitätsprotokoll strukturiert zur Verfügung stellen.

3. *Authentication Service (AS):* Hierbei handelt es sich um eine web-basierte E-Government Applikation oder um eine Applikation des privatwirtschaftlichen Bereichs, bei welcher der Zugriff auf eine Ressource durch MoA geschützt ist. Der Benutzer kann sich gegenüber einem AS nur mit MoA-Cert (Zertifikat) authentisieren. Der AS verfügt in der Regel über keine weiteren Informationen des Inhabers des Reisedokuments.

[10] wird z. Zt. nur von Android unterstützt

4. Integration von MoA

In Abhängigkeit der Kopplung eines Authentisierungsmerkmals an den MRTD-Chip kann MoA in verschiedenen Szenarien zur sicheren Benutzerauthentifizierung eingesetzt werden. In diesem Kapitel werden mögliche Szenarien aufgezeigt. Wir unterscheiden dabei zwischen direkter und indirekter Anwendung von MoA. Letztere ist eine Integration von MoA in ein bestehendes Identitätsprotokoll, wobei der MRTD-Chip und das Credential über einen zweiten Kanal zur Benutzerauthentifizierung verwendet werden.

4.1 Direkte Anwendung mit MoA-Service Anbieter

Eine Anwendung von MoA mit einem eGovernment oder privatwirtschaftlichen Service Anbieter ist nur möglich, wenn zur Authentisierung des Benutzers MoA-Cert verwendet wird.

Wie in Kapitel 3.5.2 aufgezeigt, kann der Service Anbieter selbst die Zusammengehörigkeit des Benutzerzertifikats mit dem öffentlichen Schlüssel des MRTD prüfen, da diese Verbindung im Benutzerzertifikat fälschungssicher hinterlegt werden kann. Damit weiss der authentifizierende Dienst, dass sich der Inhaber mit den Faktoren Reisedokument, privater Schlüssel + PIN authentisiert hat. Somit kann diese Methode gegenüber MoA-fähigen Servern als vertrauenswürdiges 2FA-Token[11] eingesetzt werden.

4.1.1 Anwendungsszenario

Ein Benutzer registriert in einem ersten Schritt den Identifikator seines Reisedokuments (PK_{PICC}) auf einer kommerziellen Web Applikation für künftige Anmeldevorgänge (ähnlich wie dies heute mit der SuisseID üblich ist). Die Web Applikation legt einen neuen Benutzer mit diesem Identifikator an, oder verbindet PK_{PICC} mit einem bereits bestehenden Benutzeraccount. Die Web Applikation kann mit MoA den Benutzer authentifizieren, kann aber ohne Erweiterungen nicht die Identität des Benutzers feststellen (vgl. dazu Kasten ‚Resultate Authentisierungsverfahren' auf Seite 21). Um die erfolgte Authentifizierung für seine Anwendung sinnvoll einsetzen zu können, benötigt die Web Applikation weitere Personendaten, wie Name, Vorname, usw. aus dem Chip. Wie im nächsten Kapitel beschrieben, kann diese Funktion durch MoA ebenfalls zur Verfügung gestellt werden, wenn auch mit bestimmten Einschränkungen.

4.1.2 Auslesen von Personendaten mit MoA

Durch die Übergabe von K_{ENC} an die lokale Leseanwendung (LLA) kann sichergestellt werden, dass nach der Authentifizierung des Chips ein Authentication Service keine persönlichen Informationen (DG2 und DG11) unbemerkt auslesen kann. Nach erfolgtem Schritt 9 im Authentisierungsablauf muss in Schritt 10 K_{ENC} zwingend übertragen werden. Erfolgt dieser Schritt nicht wie vorgesehen, bricht die LLA das Authentisierungsverfahren ab. Der Authentication Service kann damit nur die Präsenz und Authentizität des MRTD-Chips überprüfen. Das Lesen weiterer Daten wird von der LLA unterbunden.

Nach einer erfolgreichen Chip Authentication ist von Seiten Chip der Authentication Service berechtigt weitere Datengruppen mit Personendaten (DG1, DG2 und DG11) direkt aus dem MRTD-Chip auszulesen. Als kleinste Einheit können dabei aber nur komplette Datengruppen gelesen werden. Da die LLA über K_{ENC} verfügt, kann sie das Auslesen dieser Datengruppen kontrollieren aber nicht fälschen, da sie nicht über K_{MAC} verfügt. Damit ist es möglich auf dem Local Terminal dem Benutzer eine Einverständniserklärung abzufordern falls das RT weitere Datengruppen auslesen möchte.

4.2 Indirekte Anwendung über zweiten Kanal

MoA lässt sich auch einfach in ein bestehendes Identitätsprotokoll integrieren. Über einen zweiten Kanal kann die LLA dazu verwendet werden, den Benutzer beim Federal Authentication Service (FAS) zu authentisieren. Bei diesem Szenario können alle drei MoA Authentisierungsmethoden zur Kopplung des Benutzers an den MRTD-Chip verwendet werden.

[11] 2-Faktoren Authentisierung

4.2.1 MoA als lokale Authentisierungs-App

Die LLA wird in diesem Szenario indirekt als Authentisierungsmittel für andere lokale Applikationen eingesetzt. Die LLA hat dabei keinen direkten Kontakt zur Web-Applikation und agiert als Vermittler zwischen dem Federal Authentication Service und einer Local Terminal Application (LTA). Der Benutzer muss sich in diesem Szenario nicht gegenüber der Web-Applikation, sondern gegenüber dem zentralen Federal Authentication Service (FAS) ausweisen. Dies bringt einige Vorteile, da die Kommunikation zwischen der lokalen Applikation (App oder Browser) und der Web Applikation nicht verändert wird. In der folgenden Abbildung 11 wird die indirekte Authentisierung für eine Applikation auf dem Local Terminal dargestellt.

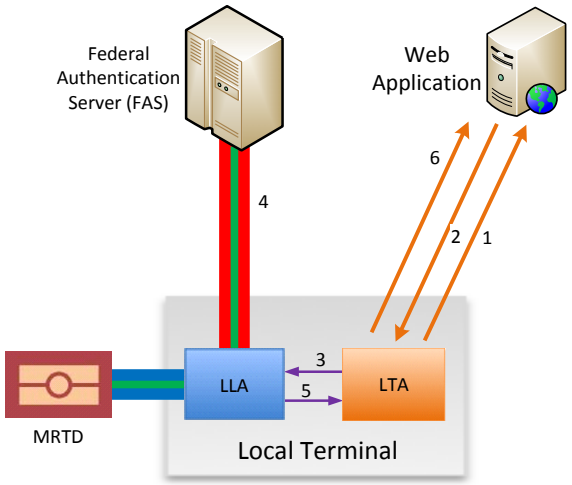


Abbildung 11: MoA für Local Terminal Applikationen

1. Ein Benutzer will von einer Local Terminal Application (LTA) auf eine Web Application zugreifen.
2. Die Web Applikation verlangt eine Authentifizierung des Benutzers.
3. Die LTA sendet einen *Authentication Request* an die LLA.
4. Die LLA führt das MoA Verfahren gegenüber dem FAS durch. Der FAS gibt in Schritt 14 des Authentisierungsprozesses (vgl. Seite 20) zusätzlich ein *Authentication Statement* für den Benutzer aus und sendet dieses an die LLA. In diesem Statement bestätigt der FAS der anfragenden Applikation (LTA), dass er den Benutzer authentifiziert hat. Im Gegensatz zur Erweiterung in Kapitel 4.1 kann hier die Web Applikation einzelne Attribute des Benutzers anfragen und der FAS kann die Attributwerte in diesem Statement an Stelle kompletter Datengruppen zurückgeben.
5. Da die Übermittlung der Personendaten über die LLA abgewickelt wird, kann diese dem Benutzer die verlangten Attribute einzeln zur Bestätigung vorlegen und der LTA zurückgeben.
6. Die LTA kann die Authentifizierungsbestätigung und die evtl. angeforderten Attribute der Web Applikation weiterleiten.

Wie dieses Szenario zeigt, ist ein Lösungsansatz mit einem zentralen Federal Authentication Service um einiges flexibler, da dieser redundant über Personendaten des sich authentifizierenden Benutzers verfügt. Hinzu kommt, dass der MoA-Authentisierungsprozess im Fall eines FAS etwas einfacher gestaltet werden kann. Der FAS verfügt redundant bereits über alle notwendigen Daten, um die Zusammengehörigkeit von MRTD-Chip und Zertifikat überprüfen zu können. Insofern muss er PK_{PICC} nicht aus dem *Subject Name* im Zertifikat (s. Tabelle 8, Schritt 14) prüfen.

4.2.2 MoA mit SAML

Als weitere Anwendung kann MoA auch als Authentisierungstoken für Applikationen dienen, welche auf Rechnern ohne NFC-Schnittstelle ausgeführt werden (z.B. ein Notebook oder Tablet, usw.). Wie in Abbildung 12 dargestellt, wird das Smartphone nur als Lesegerät und Kommunikationsmittel zum FAS verwendet. Ein Benutzer greift mit seinem Notebook (z.B. mit Browser) auf eine Web-Applikation zu. Die Web-Applikation agiert als SAML Service Provider und der FAS ist zusätzlich zum MoA-Endpunkt auch SAML Identity und Attribut Provider.

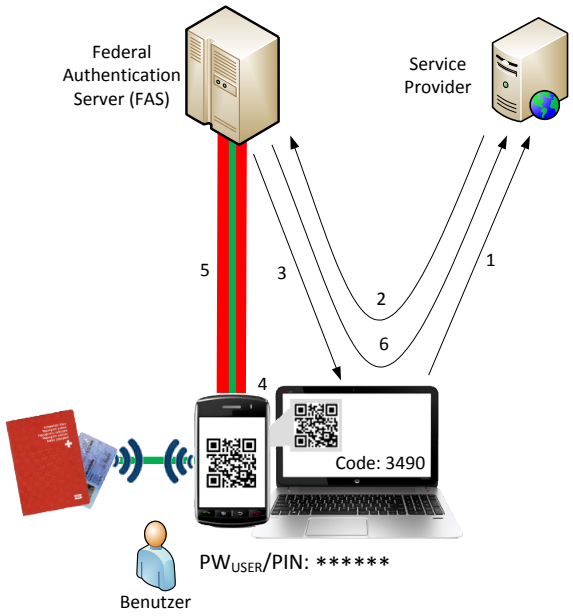


Abbildung 12: MoA mit SAML

1. Ein Benutzer öffnet mit seinem Browser (oder einer dedizierten App) eine Verbindung zu einer Web-Applikation (z.B. ein Webshop).
2. Die Web-Applikation (Service Provider) leitet den Benutzer zwecks Authentifizierung zum Federal Authentication Service (FAS), welcher als SAML [22] Identity Provider (IdP) agiert. Der FAS kann den Benutzer mittels MoA authentifizieren und verfügt nebst den auf dem Chip gespeicherten Personendaten evtl. noch über weitere Informationen (z.B. die Meldeadresse des Benutzers).
3. Der FAS stellt dem Benutzer eine Challenge als QR-Code und als Zahlencode auf dem Bildschirm dar.
4. Der Benutzer liest den QR-Code mit der LLA vom Bildschirm ein (oder gibt den Zahlencode über die Tastatur ein).
5. Die LLA führt das MoA-Verfahren mit dem FAS durch, wobei in diesem Fall die LLA die Challenge in Schritt 6 dem FAS mitgibt. Dadurch ist der FAS in der Lage die bestehende SAML-Session mit dem MoA-Authentisierungsvorgang zu verbinden.
6. Nach erfolgter MoA-Authentisierung gibt der FAS eine SAML-Assertion mit einem Authentication Statement und den angeforderten Attributen an den Webshop zurück. Bei diesem Verfahren kann der FAS dem Benutzer die vom Webshop verlangten Attribute einzeln zur Bestätigung vorlegen.

5. Internationale Entwicklungen

Auf internationaler Ebene, insbesondere in Europa geht die Entwicklung der elektronischen Reisedokumente weiter. Die deutsche eID Infrastruktur mit eID-Server und Ausweis-App für den neuen Personalausweis (nPA) ist eine nationale Lösung. Die Entwicklung und Standardisierung einer European Citizen Card (ECC) wurde gestoppt. Diese beiden Systeme verfolgen aber einen etwas anderen Weg, als die MRTD online Authentication:

- Der neue deutsche Personalausweis [17] hat gegenüber einem internationalen Reisedokument erweiterte Funktionen. Die Daten auf dem Personalausweis werden in drei Anwendungen aufgeteilt:
  1. ePass-Applikation: wie der ICAO Standard, aber nur mit PACE[12] als Access Control Protocol (BAC wird nicht mehr unterstützt).
  2. eID-Applikation: optionale Anwendung, welche eine Online-Authentisierung gegenüber einem eID-Server ermöglicht. Der eID-Server kann darauf auf bestimmte demographische Daten in einem vom ICAO Standard unabhängigen Satz von Daten zugreifen. Der Zugriff auf die eID-Applikation kann nur über PACE und PIN erfolgen. Speziell autorisierte Lesegeräte können bestimmte Datengruppen (z.B. Adresse und Wohnort) wieder-beschreiben.
  3. eSign-Applikation: Eine CSP kann ein Signaturzertifikat[13] auf dem Chip aktivieren und der Benutzer kann damit qualifiziert signieren.
- Die European Citizen Card (ECC) Spezifikation [18] hat ebenfalls drei Basisprofile für Identifikations-, Authentifikations- und Signaturdienste ähnlich dem deutschen Personalausweis beinhaltet. Das Projekt wurde in den letzten Jahren aus politischen Gründen nicht weiterverfolgt. Es ist offen, was aus dem nPA und aus der ECC-Spezifikation von der EU übernommen wird, um eine multifunktionelle eID-Karte in Zukunft zu standardisieren.
- Das Anwendungsszenario, wie es in Kapitel 4.2.2 „MoA mit SAML“ beschrieben wurde, kann problemlos auch für STORK[14] [19] eingesetzt werden. STORK basiert grundsätzlich auf SAML und ist demnach mit dieser Implementierung kompatibel. Der FAS wäre in diesem Fall der staatlich autorisierte Identity Provider.

Unabhängig von diesen Entwicklungen treibt die EU die Spezifikation von Reisedokumenten mit biometrischen Daten voran. Es besteht die Möglichkeit, dass die ‚General Authentication Procedure' in EACv2 aus BSI TR-03110-2 [10] für Reisedokumente mit biometrischen Daten als verbindlich erklärt wird. Der Grund liegt darin, dass für EACv1 bereits einige Schwachstellen aufgezeigt wurden, welche in EACv2 behoben sind. EACv2 hat gegenüber EACv1 einen entscheidenden Unterschied. BSI TR-03110-2 empfiehlt auch für die ePassport Anwendung die ‚General Authentication Procedure' einzusetzen, welche folgenden Ablauf zwingend vorschreibt:

1. PACE mit (MRZ oder CAN)
2. Terminal Authentication (Version 2)
3. Passive Authentication
4. Chip Authentication (Version 2)

Mit der Terminal Authentisierung in Schritt 2 kann der MRTD-Chip sicherstellen, dass er mit einem berechtigten Terminal und nicht mit einem Angreifer kommuniziert. Erst nach diesem Schritt muss der MRTD-Chip - auf Grund bestimmter Attribute im Terminalzertifikat - Zugriff auf Datengruppen gewähren. Dies betrifft auch die Standard ICAO Datengruppen mit Personendaten (DG1, DG2 und DG11). Mit der Passive Authentication wird in Schritt 3 die Echtheit des Chips durch das Terminal verifiziert, um dann über die bestehende Verbindung eine Chip Authentisierung durchzuführen, womit zum Schluss neue starke Sitzungsschlüssel etabliert werden.
Die Wahrscheinlichkeit, dass EACv2 in dieser Form als verbindlich erklärt wird, ist sehr gering, da der Chip erst Zugriff auf Daten erlaubt, nachdem er die Berechtigung des Terminals geprüft hat. Dies stellt eine unüberwindbare Inkompatibilität mit dem heutigen internationalen Standard dar. Dennoch könnte eine modifizierte Version von EACv2 künftig in Betracht gezogen werden, welche nur die Reihenfolge zwischen TAv2 und CAv2 ändert. In dieser Form wurde dies bereits im ECC-Standard mit

[12] Password Authenticated Connection Establishment

[13] nach RFC 5280 und RFC 3739 (Qualified Certificates Profile)

[14] Secure idenTity acrOss boRders linKed

modular Extended Access Control (mEAC) vorgeschlagen. Bereits dieser Wechsel würde einige Sicherheitsmängel eliminieren. Damit müsste aber auch MoA nachziehen und die Terminal Authentication *vor* der Chip Authentication durchführen, was aber aus heutiger Sicht kein Problem darstellen würde.
Ein Wechsel auf EACv2 hat aber dennoch Auswirkungen auf das MoA System:

- Eine direkte Anwendung von MoA zu einem nicht staatlich kontrollierten Authentication Service - wie sie in Kapitel 4.1 beschrieben wurde – dürfte nicht mehr so einfach möglich sein, da das Remote Terminal sich zuerst als autorisiertes Prüfgerät gegenüber einem EACv2 kompatiblen MRTD-Chip ausweisen muss. Dazu müsste der Staat Terminal-Zertifikate für Remote Terminals mit eGovernment oder privatwirtschaftlichen Authentication Services ausstellen, was sehr unwahrscheinlich ist.
- Anders dürfte dies für einen Federal Authentication Service (FAS) aussehen. Dieser Dienst wird von staatlicher Stelle betrieben. Somit sollte es möglich sein, für diesen Dienst ein Terminal-Zertifikat auszustellen, um auch EACv2 mit MoA zu ermöglichen.

Es ist absolut möglich, dass auch auf internationaler Ebene in Zukunft der Zugriff auf Personendaten aus Datenschutzgründen eingeschränkt wird. Eine solche Entwicklung würde zwar einige, wenige Einschränkungen mit sich bringen, die Grundfunktion von MoA aber nicht beeinträchtigen.

6. Fazit und Ausblick

Wie in Kapitel 4 beschrieben, sind mit dem MoA-Verfahren verschiedene Anwendungsszenarien möglich. Es konnte aufgezeigt werden, dass ein Standard ICAO-MRTD-Reisedokument als eID-Token eingesetzt werden kann. Eine direkte Anwendung von MoA zu einem nicht-staatlichen Authentication Service, wie in Kapitel 4.1 beschrieben, macht aus mehreren Gründen dennoch wenig Sinn:

1. Bei einer Erneuerung eines Reisedokuments ändert sich PK_{PICC}. Damit muss ein Benutzer seinen Identifikator bei jeder registrierten Web-Applikation wechseln. Es gibt auf dem Standard ICAO MRTD-Chip keinen verwendbaren, anonymen Identifikator, welcher nach einer Erneuerung des Reisedokuments gleich bleibt (ausser Personendaten, auf welche die Web Applikation aber ohne Einverständnis des Benutzers nicht zugreifen darf).
2. Die Web Applikation erhält vom MRTD-Chip immer denselben Identifier PK_{PICC}. Damit besteht die Gefahr einer Profilebildung im Backend verschiedener Web-Applikationen.
3. Die Web-Applikation kann optional auch Personendaten aus dem Chip lesen, es ist aber nur möglich den kompletten Satz und nicht nur einzelne Attribute auszulesen. Damit wird das ‚need-to-know' Prinzip aus technischen Gründen verletzt.
4. Eine privatwirtschaftliche oder eGovernment Web-Applikation muss über die MoA-Middleware verfügen. Diese bedingt die Ausgabe, den Support und den Unterhalt einer entsprechenden Softwarekomponente.

Eine indirekte Anwendung von MoA zu einem zentralen Federal Authentication Service, wie es im Kapitel 4.2 beschrieben ist, weist demgegenüber die folgenden Vorteile auf:

1. Das Protokoll zwischen der lokalen Applikation (App oder Browser) und der Web-Applikation wird nicht tangiert. Die Web Applikation benötigt keine zusätzliche Softwarekomponente.
2. Der FAS kann Benutzer und MRTD-Chip über einen eigenen sicheren Kanal authentifizieren.
3. Der FAS kann dem anfragenden System ein Authentication Statement zurückgeben, welches auch einzelne Personendaten als Attribute beinhalten kann. Falls der FAS noch über weitere Informationen als diejenigen im Reisedokument des Benutzers verfügt, so kann er diese zum Attributset hinzufügen.
4. Der FAS kann anstelle von PK_{PICC} einen pseudonymen Identifikator zurückgeben, womit der Schutz der Privatsphäre des Benutzers gegenüber der anfragenden Stelle besser gewahrt werden kann. Dieser pseudonyme Identifikator kann auch bei Erneuerung des Reisedokuments auf dem FAS beibehalten werden. Nur der FAS muss den neuen PK_{PICC} kennen.

<u>Nächste Schritte:</u>

Im Rahmen dieser Machbarkeitsstudie sind einige Fragen und noch zu definierende Prozesse aufgetaucht. Diese betreffen in erster Linie die Benutzerfreundlichkeit und das Handling der MoA-Lösung. Folgende Punkte müssen noch eingehender behandelt werden (insbesondere, wenn diese Lösung weiter verfolgt werden sollte):

Offene Punkte	Problembeschreibung	Lösung
Kopplung des Private Key SK_{USER} an ein Smartphone	Softtoken wird vom Handy gestohlen. Wenn zusätzlich eine Kopplung zwischen Smartphone und FRS bei der Registrierung gemacht wird, würde damit die Sicherheit erhöht werden. Ein Schlüsselpaar kann nur von genau einem registrierten Smartphone aus verwendet werden. Beim Wechsel eines Smartphones müsste dieses beim FRS neu registriert werden. Damit wird das alte automatisch überschrieben.	Um die Sicherheit des 2. Faktors zu erhöhen, wäre es denkbar die Identität des Smartphones (IMEI-Nummer[15]) oder des Netzteilnehmers (IMSI[16]-Nummer) auf dem FRS mit zu registrieren.

[15] *International Mobile Equipment Identity* ist eindeutig pro Gerät, aber mit entsprechender Software überschreibbar

[16] *International Mobile Subscriber Identity* ist ein eindeutiger Identifikator des Netzteilnehmers

Offene Punkte	Problembeschreibung	Lösung
Neues Smartphone	Ein Benutzer erhält vom Provider ein neues Smartphone. • Wie kann er sein Soft-Token und sein Zertifikat auf das neue Teil übertragen? • Wie kann er seine LLA Einstellungen (z.B. gespeicherte MRZ/CAN) übertragen?	• Wenn beide Smartphones parallel betrieben werden können, so wäre eine Key-Move/Copy-Funktion denkbar. • Grundsätzlich wäre auch ein Cloud-Service möglich (durch den Staat betrieben?), auf welchem Soft-Token, Zertifikat und Einstellungen der LLA in einem verschlüsselten Container abgelegt werden. Damit kann der Benutzer jederzeit die lokalen MoA-Parameter wiederherstellen.
Smartphone ist defekt, kein Backup vorhanden	Das Soft-Token und das Zertifikat sind unwiederbringlich weg.	• Der FRS bietet einen Online-Zertifikatsrevokationsdienst an. Der Benutzer installiert die LLA aus dem App-Store neu und authentisiert sich nur mit seinem MRTD (CAv1). Er beantragt damit automatisch ein neues PWINIT direkt an seine Meldeadresse und kann den Registrierungsprozess durchlaufen.
Normaler Ablauf der Gültigkeit eines Zertifikats	Ein vom FRS ausgestelltes Zertifikat hat eine begrenzte Gültigkeitsdauer. Max. Lifetime: 1-3 Jahre. Wie sieht der Erneuerungsprozess aus?	• Der FRS bietet einen Online-Zertifikatserneuerungsdienst an. Mit dem alten Zertifikat kann er sich mit MoA authentisieren. Der MoA-Registrierungsprozess wird durchlaufen und ein neues Schlüsselpaar wird erstellt und auf dem Smartphone installiert.

Tabelle 9: Offene Punkte

Nebst den in Tabelle 9 aufgeführten Themen, welche eher das Handling eines Smartphones im Zusammenhang mit MoA betreffen, stellen sich auch infrastrukturelle, semantische und rechtliche Fragen. Die folgenden Fragen sollen als Anregung dienen und müssen gesondert behandelt werden. Wenn MoA dazu verwendet wird den Inhaber eines Reisedokuments durch einen Federal Authentication Service (FAS) authentisieren zu lassen;

1. um darüber weitere behördliche oder privatwirtschaftliche elektronische Identitätsmittel (z.B. SuisseID, eSign, e-Voting Card, MobileID, usw.) beziehen zu können,
2. oder einfach um eine anfragende Applikation mit bestimmten Personeninformationen zu beliefern,

so stellen sich in diesem Zusammenhang folgende Fragen (keine abschliessende Liste):

- Wie soll eine solche Infrastruktur (Ökosystem) aufgebaut werden?
- Wie werden die Vertrauensbeziehungen zwischen den Parteien etabliert?
- Welche Attribute einer Person können/dürfen von einer Applikation abgefragt werden?
- Wie sind Syntax und Semantik dieser Personeninformationen definiert (Attribute-Metadaten)?
- Wie kann der FAS auf die Passdaten und evtl. andere vorhandene Personeninformationen zugreifen (Backend-Infrastruktur, Sicherheitszonen)?
- Welche rechtliche Grundlagen und Einschränkungen bestehen bezüglich Ausgabe von Passinformation in elektronischer Form an Dritte?

Abschliessend lassen sich die im vorliegenden Dokument vorgestellten drei Authentisierungsmethoden gegenüberstellen und mit einigen in der Studie diskutierten Kriterien in einer Übersichtstabelle zusammenfassen und vergleichen.

Kriterien	MoA Authentisierungsmethoden		
	Zertifikat	Passwort	Mobile Signature
Sicherheit des Verfahrens	**Gross,** 2-FA 1-Channel, MRTD und Token/PIN	**Gut,** 2-FA 1-Channel, MRTD und Passwort	**Sehr Gross,** 2FA 2-Channel, MRTD, SIM-Karte + PIN über zweiten Kanal
Angriffspotenzial auf Server bzw. Kanal	**Gering,** da Server kein Credential des Benutzers speichert und 2-way SSL/TLS Handshake	**Gross,** da Passwort in SSL/TLS Kanal übermittelt und auf Server gespeichert wird	**Gering,** Authentisierung über zweiten Kanal
Angriffspotenzial auf Gerät (Smartphone)	**Mittel,** Softtoken wegkopieren, PIN ausspionieren	**Gering,** Password ausspionieren	**Gering,** PIN ausspionieren
Abhängigkeit von Gerät (Smartphone)	**Mittel,** Softtoken kann auch auf anderem Gerät parallel eingesetzt werden	**Keine**	**Gross,** Token ist an SIM-Karte gebunden
Abhängigkeit von zusätzlichen Infrastrukturen (ausgenommen FRS, FAS und OCMSP)	**Mittel,** Lösung benötigt PKI vom Bund für Benutzer-zertifikate	**Keine**	**Gross,** Infrastruktur eines MSS Providers, spezielle SIM-Karte, Vertrag und Registrierung des FAS als MSS-Applikation
Benutzerfreundlichkeit (Authentisierung)	**Gross,** Eingabe PIN	**Gross,** Eingabe Passwort	**Gross,** Eingabe PIN
Benutzerfreundlichkeit (Credential Handling)	**Mittel,** Softtoken selbst sichern, auf neues Gerät kopieren, auf altem Gerät löschen	**Gross,** nur Passwort	**Gross,** gekoppelt an SIM Karte
Integration in bestehende Authentisierungsinfra-strukturen (z.B. SAML)	**Möglich**	**Möglich**	**Möglich**
Anwendbarkeit auf staatlichen Authentisierungsdienst	**Möglich,** da FAS in jedem Fall über Verbindung PK_{PICC} zu Credential des registrierten Benutzers verfügt		
Anwendbarkeit auf eGovernment oder privatwirtschaftlichen Authentisierungsdiensten	**Möglich,** da Public Key des Chip in Benutzerzertifikat enthalten	**Nicht möglich,** Benutzer teilt kein Geheimnis mit Server	**Nicht möglich,** Identity Mapping zwischen Mobile ID und MRTD Chip fehlt

Tabelle 10: Vergleich MoA-Authentisierungsmethoden

7. Anhang A (Kryptographische Verfahren)

Dieser Anhang beinhaltet die kryptografischen Verfahren, welche in den schweizerischen Reisedokumenten (ePass-10) verwendet werden und welche in Zusammenhang mit dieser Studie von Bedeutung sind.

7.1 Basic Access Control (BAC)

Bei Verwendung einer kontaktlosen Schnittstelle ist es nötig, sicherzustellen, dass die Nutzung der Karte nur durch berechtigte Terminals möglich ist. Das Basic Access Control Verfahren steht also am Anfang der Kommunikation zwischen Lesegerät und MRTD-Chip. Es soll sicherstellen, dass nur mit Einverständnis des Inhabers der Zugriff auf bestimmte Datengruppen auf dem Chip ermöglicht wird. Das Ziel von BAC ist es einerseits Skimmingangriffe[17] zu verhindern und andererseits die Kommunikation über die Luftschnittstelle gegen Abhörangriffe Dritter abzusichern. Mit BAC kann die Echtheit des MRTD-Chips nicht geprüft werden. BAC ist daher kein Werkzeug, um eine Fälschung oder widerrechtliche Kopie (Cloning) eines Reisedokuments feststellen zu können. Es verhindert lediglich, dass ein Reisedokument, welches in einer Tasche liegt, unbemerkt ausgelesen werden kann. BAC basiert auf symmetrischen Algorithmen und benötigt daher einen gemeinsamen geheimen Schlüssel. Auf der Seite des MRTD-Chips ist dieser Schlüssel fest gespeichert und auf Seiten Lesegerät kann der Schlüssel aus der MRZ[18] gebildet werden (dazu muss der Inhaber den Pass öffnen und auf den Scanner des Lesegerätes legen).
BAC ist zwar heute internationaler Standard und in den meisten internationalen Reisedokumenten aktiv, hat aber einige gravierende Nachteile:

- Das gemeinsame Geheimnis (die MRZ) und die damit abgeleiteten Schlüssel zur Absicherung der Luftschnittstelle haben eine zu niedrige Entropie[19].
- Für jede Sitzung werden immer dieselben Schlüssel berechnet.
- BAC ist gemäss ICAO-Spezifikation nicht zwingend vorgeschrieben

Für weitere Informationen zu BAC wird an dieser Stelle auf ICAO DOC 9303 Part 1- Volume 2 [4] verwiesen.

7.2 Supplemental Access Control (SAC)

Langfristig ist es vorgesehen Basic Access Control durch Supplemental Access Control (SAC), wie in ICAO-TR 2010 [7] spezifiziert, zu ersetzen, da dieses Verfahren deutlich bessere kryptographische Eigenschaften besitzt. SAC basiert auf PACE[20] und stellt ebenso sicher, dass nur autorisierte Terminals (Lesegeräte) mit dem MRTD-Chip kommunizieren können. SAC kann als gemeinsames Geheimnis nebst der MRZ auch eine auf der Karte aufgedruckte Zahl CAN[21] verwenden. Dieses gemeinsame Geheimnis wird nun aber nicht zur Schlüsselerzeugung verwendet, sondern dient nur zur Authentifizierung der beiden Partner. Die für die sichere Kommunikation verwendeten Schlüssel werden mittels Diffie-Hellman Key Exchange Verfahren für jede Sitzung neu gebildet. So werden starke, zufällige Sitzungsschlüssel etabliert, da die Generierung der Schlüssel nicht auf der Entropie des gemeinsamen Geheimnisses basiert und die Nutzung eines Sitzungsschlüssels ist auf eine Sitzung begrenzt.

Der Unterschied zwischen BAC und SAC wird hier nicht weiter diskutiert, da die beiden Verfahren zum gleichen Endresultat führen, wenn auch mit sehr unterschiedlichen Sicherheitseigenschaften. Für diese Studie sind diese Unterschiede zweitrangig.

[17] Unbemerktes Auslesen eines Chips über die Luftschnittstelle
[18] Machine Readable Zone
[19] Mass der Zufälligkeit eines Schlüssels
[20] Password Authenticated Connection Establishment
[21] Card Access Number

7.3 Passive Authentication (PA)

Für die passive Authentisierung erstellt der Dokumentenherausgeber zum Zeitpunkt der Ausgabe des Reisedokuments eine elektronische Signatur über die notwendigen Datengruppen auf dem MRTD-Chip. Die Integrität dieser Daten kann nun zu jedem Zeitpunkt durch die Prüfung der Signatur, die in einem Datenobjekt auf der Karte abgelegt wird (EF.SOD), verifiziert werden. Dabei kann ein verifizierendes Gerät feststellen, dass das Dokument durch den Dokumentenhersteller erstellt wurde und die gelesenen Daten Integer sind. Dazu laufen folgende Schritte ab:

1. Das *Document Security Object (SOD)* wird gelesen.
2. Der *Document Signer (DS)* wird aus dem *Document Security Object* gelesen.
3. Mit Hilfe des Public Keys des *Document Signers* wird verifiziert, dass die Signatur des *Document Security Objects* korrekt ist.
4. Mit Hilfe des Public Keys des entsprechenden *Country Signing CSP*[22] wird verifiziert, dass die Signatur des *Document Signer* Zertifikates korrekt ist, somit ist der *Document Signer* eine gültige Signaturinstanz.
5. Die relevanten Datengruppen werden aus dem MRTD-Chip gelesen.
6. Die Hash-Werte der relevanten Datengruppen werden berechnet.
7. Die Hash-Werte werden mit denen im *Document Security Object* verglichen. Sind diese korrekt, kann davon ausgegangen werden, dass die Daten in den Datengruppen nicht verändert wurden und authentisch sind.

Für weitere Informationen zu PA wird an dieser Stelle auf ICAO DOC 9303 Part 1- Volume 2 [4] verwiesen. PA ist gemäss Spezifikation für alle Reisedokumente zwingend vorgeschrieben.

7.4 Active Authentication (AA)

Die Active Authentication ist ein kryptographisches Verfahren, welches das Kopieren (Cloning) eines MRTD-Chips verhindern soll. Es basiert auf einem asymmetrischen Challenge-Response Verfahren, wobei der private Schlüssel auf dem Chip nicht auslesbar gespeichert wird. Jeder MRTD-Chip erhält so einen eigenen Schlüssel, wodurch der Chip und damit auch das Reisedokument eindeutig identifizierbar werden. AA ist in ICAO DOC 9303 Part 1 – Volume 2 [4] spezifiziert und ist optional. Da AA nicht resistent gegen Man-in-the-Middle Angriffe ist und weitere Bedenken bezüglich semantischer Angriffe mittels Challenge festgestellt und publiziert wurden (vergleiche dazu BSI TR-03110-1 [9] Appendix B ‚Challenge Semantics'), wird der Einsatz von AA auch von der ICAO nicht mehr empfohlen. Das FedPol hat im aktuell ausgestellten ePass-10 die AA-Funktion deaktiviert.

7.5 Secure Messaging

Nach Bildung eines gemeinsamen Sitzungsschlüssel (sei es nach BAC, SAC oder CA) wird Secure Messaging gestartet. Secure Messaging ermöglicht einfach die abgesicherte (verschlüsselte) Kommunikation zwischen Lesegerät und dem MRTD-Chip. Die Luftstrecke wird dabei einerseits durch einen symmetrischen Verschlüsselungsalgorithmus (z.B. AES[23]) gegen Abhörangriffe geschützt und durch einen MAC[24] gegen Manipulationen geschützt.

7.6 Extended Access Control (EACv1)

Extended Access Control ist ein PKI-basiertes Zugriffskontrollverfahren, das sich aus den Bestandteilen Chip Authentisierung (s. Abschnitt 7.6.1) und Terminal Authentisierung (s. Abschnitt 7.6.2) zusammensetzt. EACv1 führt zusätzlich die Schlüsselvereinbarung mittels Diffie-Hellman auf Elliptic Curve Cryptography ECDH [20] basierend ein.

[22] Certification Service Provider

[23] Advanced Encryption Standard

[24] Message Authentication Code

7.6.1 Chip Authentisierung (CAv1)

Die Chip Authentisierung (spezifiziert in BSI TR-03110-1 [9]) dient analog der Active Authentication (s. Abschnitt 7.4) dem Nachweis, dass der Chip in Besitz eines privaten Schlüssels ist. Zusätzlich wird innerhalb der Chip Authentisierung aber auch noch ein neues Schlüsselpaar ausgehandelt. Der dazu vom MRTD-Chip verwendete öffentliche Schlüssel befindet sich in der Datengruppe (DG 14). In Verbindung mit der Passiven Authentisierung (s. Abschnitt 7.3) wird damit die Echtheit des Chips und damit auch der auf dem Chip gespeicherten Daten nachgewiesen. Die Chip Authentisierung verhindert also das Kopieren eines Chips.
Weiter dient die Chip Authentisierung dem Aufbau eines sicheren Kanals zwischen Terminal bzw. Dienstanbieter und Chip.
Bei der Chip Authentisierung laufen folgende Protokollschritte ab:

1. Der MRTD-Chip sendet seinen statischen Diffie-Hellman (DH) Public Key (PK_{CHIP}) und die zu dessen Erzeugung verwendeten DH-Parameter zum Lesegerät.
2. Das Lesegerät seinerseits erzeugt ein zufälliges DH-Schlüsselpaar und sendet seinen öffentlichen Teil (PK_{TERM}) dem MRTD-Chip zurück.
3. Beide Parteien berechnen mittels DH-Verfahren den gemeinsamen Schlüssel K.
4. Beide leiten aus K einen gemeinsamen MAC-Schlüssel K_{MAC} und einen Verschlüsselungsschlüssel K_{ENC} ab.
5. Beide Parteien komprimieren und speichern PK_{TERM}. für die folgende Terminal Authentication.

Da das Lesegerät nicht über ein Zertifikat des Chips verfügt, worüber es den öffentlichen Schlüssel bis zu einer vertrauenswürdigen CSP validieren könnte, muss zur Prüfung der Authentizität dieses Schlüssels eine Passive Authentication (s. Abschnitt 7.3) erfolgen*.
Nach erfolgreicher Chip Authentication wird Secure Messaging neu gestartet, wobei nun die abgeleiteten Schlüssel K_{ENC} und K_{MAC} verwendet werden.

* **Wichtig:** Der Standard schreibt an dieser Stelle eine Passive Authentication zwingend vor. Nur durch eine Kombination von Chip Authentication zusammen mit einer Passive Authentication kann die Echtheit eines MRTD-Chips geprüft werden.

7.6.2 Terminal Authentisierung (TAv1)

Die Terminal Authentisierung (spezifiziert in BSI TR-03110-1 [9]) dient dem Nachweis der Zugriffsrechte eines Lesegerätes (Terminals) bzw. eines Dienstanbieters. Damit kann der MRTD-Chip prüfen, ob der Partner den notwendigen Nachweis der Zugriffsrechte erbringen kann, um auf biometrische Daten im MRTD-Chip zugreifen zu können. Die Zugriffsrechte des Terminals werden an die in der Chip Authentisierung ausgehandelten Sitzungsschlüssel gebunden, d.h. die Rechte des Terminals können nur innerhalb des durch die Chip Authentisierung aufgebauten verschlüsselten Kanals ausgeübt werden. Die Terminal Authentisierung kann pro Sitzung nur einmal durchgeführt werden. Eine neue Sitzung wird durch Abbau des verschlüsselten Kanals (und damit verbunden Löschen der Sitzungsschlüssel und Zurücksetzen aller Zugriffsrechte) gestartet.
Die Rechte des Terminals werden über eine Zertifikatskette vergeben. Diese besteht aus:

- Der RootCA (Country Verifying Certification Authority, kurz CVCA)
- der Document Verifier Sub CAs (kurz DV)
- dem Zertifikat des Terminals bzw. des Dienstanbieters

Die Zertifikate für die Terminal Authentisierung sind CV-Zertifikate (Card Verifiable Certificates) nach ISO/IEC 7816 [21], Teil 6 und BSI-TR-03110 [8].
Folgende Protokollschritte werden in der Terminal Authentisierung durchgeführt:

1. Das Terminal sendet seine gesamte Zertifikatskette zum MRTD-Chip, beginnend mit dem CVCA Zertifikat (welches zwecks Verifikation schon bei der Ausgabe des Chips auch auf diesem selbst gespeichert ist) allen intermediären Document Verifier (DV) bis hin zum Terminalzertifikat.
2. Der MRTD-Chip verifiziert die Zertifikatskette und extrahiert den öffentlichen Schlüssel des Terminals (PK_{PCD}) aus dessen Zertifikat.

3. Der MRTD-Chip berechnet eine Nonce[25] und sendet diese an das Terminal bzw. an den Dienstanbieter.
4. Das Terminal signiert (mit seinem privaten Schlüssel) die Nonce zusammen mit der ID[26] des Reisedokuments und dem aus der Chip Authentisierung gespeicherten komprimierten öffentlichen Wert PK_{TERM} und sendet das Resultat an den Chip zurück.
5. The MRTD-Chip verifiziert die Signatur mit dem öffentlichen Schlüssel PK_{PCD} und erteilt dem Terminal Zugriff auf die gesicherten Datengruppen.

[25] Number used once (einmalig verwendete Zufallszahl)

[26] Im Falle von BAC wird die ID aus der MRZ berechnet.

8. Anhang B (Verzeichnisse)

8.1 Terminologie und Abkürzungen

Begriff	Beschreibung
AS	eGovernment oder privatwirtschaftlicher Authentication Service
BAC	Basic Access Control
BSI	Bundesamt für Sicherheit in der Informationstechnik
CA	Chip Authentication
CSR	Certification Signing Request gemäss RFC2986 [22]
EAC	Extended Access Control
ECC	European Citizen Card
eIDM	Elektronisches Identifikationsmittel
FAS	Federal Authentication Service
FRS	Federal Registration Service
ICAO	International Civil Aviation Organization
LLA	-> MoA-LLA
LT	Local Terminal
MoA	MRTD online Authentication
MoA-MW	Serverseitige MoA Softwarekomponente
MoA-LLA	Lokale Leseapplikation (LLA) auf Smartphone
MoA-Cert	MoA Authentisierungsmethode mittels Benutzerzertifikat
MoA-PW	MoA Authentisierungsmethode mittels Passwort
MoA-MSS	MoA Authentisierungsmethode über Mobile Signature Service (Mobile ID)
MRTD	Machine Readable Travel Documents
MSISDN	Mobile Subscriber Integrated Service Digital Service Number
MSS	Mobile Signature Service
NFC	Near Field Communication
PACE	Password Authenticated Connection Establishment
RFID	Radio Frequency Identification
RT	Remote Terminal
SAC	Supplemental Access Control
SM_{BAC}	Secure Messaging mit Schlüsselmaterial aus BAC
SM_{CA}	Secure Messaging mit Schlüsselmaterial aus CA
TA	Terminal Authentication

8.2 Abbildungsverzeichnis

8.3 Tabellenverzeichnis

8.4 Literaturverzeichnis

[1] Bundesamt für Polizei (fedpol), "Konzeptstudie elektronischer Identitätsnachweis," Eidg. Justiz- und Polizeidepartement EJPD, Bern, Konzeptstudie 2013.

[2] ICAO. DOC 9303 - Machine Readable Travel Documents. [Online]. http://www.icao.int/publications/pages/publication.aspx?docnum=9303

[3] ICAO. (2006) DOC 9303 MRTD Part 1 / Volume 1. [Online]. http://www.icao.int/publications/Documents/9303_p1_v1_cons_en.pdf

[4] ICAO. DOC 9303 MRTD Part 1 / Volume 2. [Online]. http://www.icao.int/publications/Documents/9303_p1_v2_cons_en.pdf

[5] ICAO. DOC 9303 MRTD Part 3 / Volume 1. [Online]. http://www.icao.int/publications/Documents/9303_p3_v1_cons_en.pdf

[6] ICAO. DOC 9303 MRTD Part 3 / Volume 2. [Online]. http://www.icao.int/publications/Documents/9303_p3_v2_cons_en.pdf

[7] ICAO. (2010, November) Supplemental Access Control for MRTD (Technical Report). [Online]. http://www.icao.int/Security/mrtd/Downloads/Technical%20Reports/Technical%20Report.pdf

[8] BSI. Technical Guideline Advanced Security Mechanisms for Machine Readable Travel Documents. [Online]. https://www.bsi.bund.de/EN/Publications/TechnicalGuidelines/TR03110/BSITR03110.html

[9] BSI. TR-03110-1 (Advanced Security Mechanisms for Machine Readable Travel Documents). [Online]. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03110/TR-03110_v2.1_P1pdf.pdf?__blob=publicationFile

[10] BSI. TR-03110-2 (Advanced Security Mechanisms for Machine Readable Travel Documents). [Online]. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03110/TR-03110_v2.1_P2pdf.pdf?__blob=publicationFile

[11] BSI. TR-03110-3 (Advanced Security Mechanisms for Machine Readable Travel Documents). [Online]. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03110/TR-03110_v2.1_P3pdf.pdf?__blob=publicationFile

[12] IETF. RFC 2246 The TLS Version 1.0. [Online]. http://www.ietf.org/rfc/rfc2246.txt

[13] European Telecommunications Standard Institute (ETSI). (2003, Aug.) ETSI TS 102 204. [Online]. http://docbox.etsi.org/EC_Files/EC_Files/ts_102204v010104p.pdf

[14] Swisscom. Mobile ID. [Online]. http://www.swisscom.ch/de/business/mobile-id

[15] IETF. X.509 Internet Public Key Infrastructure Online Certificate Status Protocol (OSCP). [Online]. http://www.ietf.org/rfc/rfc2560.txt

[16] ISO. (2001) ISO/IEC 14443 Identification Cards - Contactless Integrated Circuit(s) Cards -

Proximity Cards.

[17] BSI. Funktionen des neuen Personalausweis. [Online]. https://www.bsi.bund.de/DE/Themen/ElektronischeAusweise/Personalausweis/Funktionen/Funktionen_node.html

[18] Comité Européen de Normalisation (CEN). (2007) TS 15480/1-3.

[19] STORK. STORK - Secure idenTity acrOss boRders linKed 2.0. [Online]. https://www.eid-stork2.eu

[20] Certicom Research. (2000) SEC1: Elliptic Curve Cryptography. [Online]. http://www.secg.org/secg_docs.htm

[21] ISO/IEC. ISO 7816 - Identification cards – Integrated circuit cards.

[22] IETF. PKCS #10: Certification Request Syntax Specification. [Online]. http://tools.ietf.org/html/rfc2986

[23] Swiss Federal Office of Police. Official Swiss Passport Site. [Online]. http://www.schweizerpass.admin.ch/pass/de/home.html

[24] IETF. (1997) www.ietf.org. [Online]. http://www.ietf.org/rfc/rfc2119.txt

[25] OASIS. (2005, March) Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0. [Online]. http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf

[26] OASIS Standard. OASIS Standard.

[27] IETF. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. [Online]. http://www.ietf.org/rfc/rfc5280.txt

[28] OASIS. (2005) OASIS Standard. [Online]. http://oasis.org