Neue Sicherheitsmechanismen und Profile der European Citizen Card

Dr. Gisela Meister, Dr. Henning Daum

Giesecke & Devrient GmbH
Prinzregentenstraße 159
81667 München
gisela.meister@gi-de.com
henning.daum@gi-de.com

Abstract: Nach der beschlossenen und weitgehend bereits umgesetzten Novellierung der Reisepässe ist eine Überarbeitung der nationalen Ausweisdokumente wie des deutschen Personalausweises absehbar. Diese können zusätzlich IT-Dienste beispielsweise zur Authentisierung und Autorisierung für eGovernment-Anwendungen erlauben. Für diese Dienste ist es jedoch notwendig, neue Sicherheitsmechanismen zu entwickeln und die vorhandenen anzupassen. Da diese Ausweise im europäischen Raum als grenzüberschreitende Reisedokumente akzeptiert werden, ist eine Harmonisierung dieser Bestrebungen im europäischen Rahmen sinnvoll. Dies erfolgt in der europäischen Spezifikation CEN prTS 15480 zur European Citizen Card. Diese beschreibt in Teil 1 die physikalischen Eigenschaften und in Teil 2 die logischen Datenstrukturen und Kartendienste. In Teil 4 werden diese zu derzeit zwei Applikationsprofilen zusammengesetzt: Einem Profil für eine ID-Karte mit eID-, ICAO- und einer optionalen Signatur-Applikation sowie einer reinen ESIGN-Karte mit optionaler Signaturfunktion als zweitem Profil.

1 Einführung

Nachdem der Reisepass den Schritt vom reinen Papierdokument zu einem elektronischen Ausweis durchgeführt hat, ist abzusehen, dass auch die europäischen Personalausweise und ID-Karten sich entsprechend weiterentwickeln. Nicht zuletzt weil diese Dokumente innerhalb der Schengen-Staaten als Reisedokument akzeptiert werden, ist es wünschenswert, die Daten und Anwendungen dieser zukünftig elektronischen Dokumente auf einer Smartcard interoperabel und kompatibel zu gestalten, wie dies für die Reisepässe geschehen ist.

Aus diesem Grund wird die europäische Spezifikation CEN prTS 15480 [ECC05] entwickelt die entsprechende Rahmenbedingungen für eine europäische Bürgerkarte (European Citizen Card, ECC) festlegt. Diese enthält vier Teile:

- Teil 1: Physikalische, elektrische Eigenschaften und Transportprotokolle

- Teil 2: Logische Datenstrukturen und Kartendienste
- Teil 3: Middleware und Interoperabilität
- Teil 4: Applikationsprofile

Physikalisch gesehen beschreibt die Spezifikation den Ausweis als eine Chipkarte nach ISO/IEC 7186-1 und -2 für die Kontaktschnittstelle bzw. ISO/IEC 14443 für die kontaktlose Schnittstelle. Die üblichen Transportprotokolle T=0 oder T=1 können verwendet werden, wobei auch eine Verbindung über USB bereits vorgesehen ist.

Hinsichtlich der Kartendienste besteht der Wunsch vieler Staaten, dem Karteninhaber neben der reinen Personenidentifikation zur Nutzung als Reisedokument und zum Nachweis des Wohnsitzes, auch IT-Zusatzfunktionen für den elektronischen Geschäftsverkehr anzubieten. Die Intention für die Unterstützung elektronischer Dienste zur Identifikation, Authentisierung und Signaturerstellung (IAS-Dienste) ist hierbei, die elektronische Handlungsfähigkeit des Bürgers zu erweitern und so neue Angebote zum Nutzen von Bürgern, Wirtschaft und Verwaltung beispielsweise durch eGovernment-Anwendungen zu ermöglichen. Daher wird neben der reinen Kartenspezifikation auch eine Middleware beschrieben, die eine sichere Online-Nutzung des Ausweises ermöglicht.

Die einzelnen Kartenkomponenten wie Schnittstellen, Transferprotokolle und Dienste werden abschließend im letzten Teil der Spezifikation zu sinnvollen Applikationsprofilen für bestimmte Einsatzzwecke gebündelt.

2 IAS-Dienste der ECC

Neben der reinen Personenidentifikation kann eine European Citizen Card auch erweiterte Dienste zur Identifikation, Authentisierung und Signaturerstellung (IAS-Dienste) unterstützen. Diese basieren meist auf Public-Key-Verfahren, überwiegend auf dem RSA-Verfahren wie es z. B. die deutsche Gesundheitskarte eGK und die französische Identitätskarte INES verwenden. Jedoch ist die Nutzung elliptischer Kurven auf dem Vormarsch, so wurde der europäische Standard CEN prEN 14890 zur sicheren Signaturerstellung [SSCD06] Mitte 2005 entsprechend erweitert. Dabei wurde besonderes Augenmerk auf Kompatibilität zur ECC-Spezifikation CEN prTS 15480 gelegt, so dass die IAS-Dienste auch auf Basis von elliptischen Kurven genutzt werden können. In den folgenden Abschnitten werden die wichtigsten IAS-Dienste der ECC vorgestellt.

2.1 Passive Authentisierung

Für die passive Authentisierung erstellt der Dokumentenherausgeber zum Zeitpunkt der Ausgabe der ECC eine Signatur über die Dokumentendaten oder Teilen davon. Meist werden hier nur die weniger sensitiven Daten mit kleinem Datenumfang (z. B. Personendaten, aber keine biometrischen Merkmale) als Grundlage verwendet. 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 wird nebenläufig festgestellt, dass das Dokument durch den Dokumentenhersteller erstellt wurde und ist somit passiv authentisiert.

Die passive Authentisierung ist jedoch nur für unveränderliche Daten sinnvoll, da ansonsten für jede Namens- oder Adressänderung eine aufwendige Aktualisierung der Signatur nötig wäre.

2.2 Basic Access Control (BAC)

Bei Verwendung einer kontaktlosen Schnittstelle ist es nötig, sicherzustellen, dass die Nutzung der Karte nur dann und durch solche Terminals möglich ist, denen der Inhaber zustimmt. Daher werden die maschinenlesbaren Daten des Ausweises optisch erfasst und daraus ein Schlüssel abgeleitet, der der Karte bereits bekannt ist. Mit diesem Schlüssel wird dann eine symmetrische Verschlüsselung gestartet. Nachteilig ist die beschränkte Entropie der zur Schlüsselableitung genutzten Daten sowie die Tatsache, dass ein und derselbe Schlüssel für alle Sitzungen genutzt wird.

2.3 Modular Extended Access Control (mEAC)

Wie der Name schon nahelegt, basiert die Modular Extended Access Control (mEAC) auf dem für den Reisepass entwickelten EAC-Protokoll. Übernommen wurden die Module Chip- und Terminalauthentisierung, jedoch werden diese in einer veränderten Reihenfolge genutzt. Zusätzlich gibt es ein neues Modul zur Prüfung der Benutzerpräsenz, das konditional zuerst ausgeführt wird. Dies kann bei kontaktorientierter Anwendung über die übliche Benutzerverifikation mittels PIN erfolgen, für kontaktlose Kommunikation kommt das PACE-Verfahren zum Einsatz (s. u.). Anschließend wird die Terminalauthentisierung angestoßen, bei der die Karte sicherstellt, dass sie mit einem berechtigten Terminal und nicht mit einem Angreifer kommuniziert.

Nun kann ein Hintergrundsystem über die bestehende Verbindung eine Chipauthentisierung durchführen und so die Echtheit der Karte feststellen (siehe Abbildung 1). Dabei werden über eine Diffie-Hellman-Schlüsselvereinbarung auch starke Sitzungsschlüssel etabliert, die im Anschluss für Aufbau eines vertrauenswürdigen Kanals mit Secure Messaging genutzt werden.

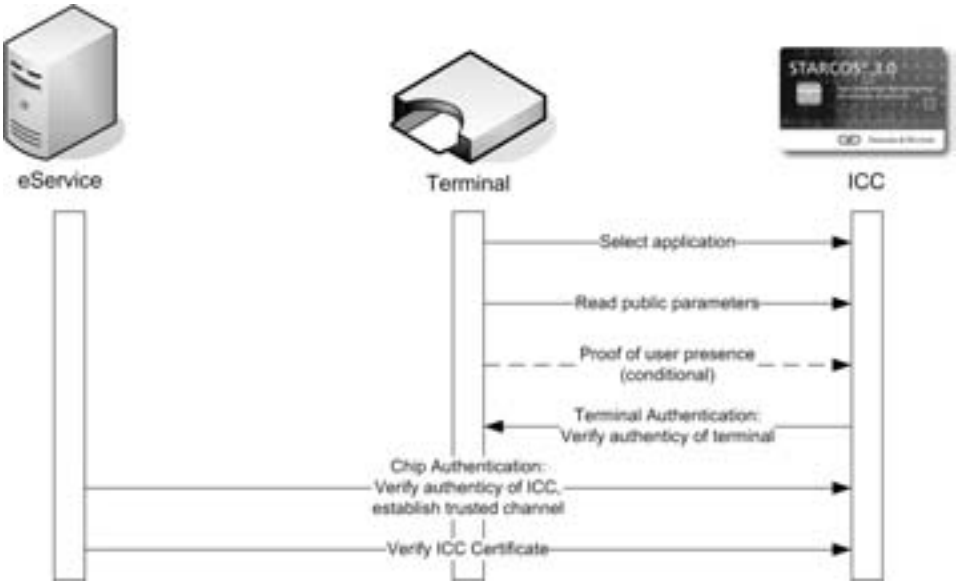

Abbildung 1: Ablauf Modular Extended Access Control

2.3 Password Authenticated Connection Establishment (PACE)

Dieses neue Protokoll bietet sich als Ersatz für das o. g. BAC-Protokoll an. Es stellt ebenso sicher, dass nur autorisierte Terminals mit der Karte kommunizieren können. Hierfür wird eine PIN verwendet, aus der ein gemeinsames Geheimnis abgeleitet wird. Auf dessen Basis wird anschließend eine Diffie-Hellman-Schlüsselvereinbarung durchgeführt. So werden starke Sitzungsschlüssel etabliert, da die Generierung der Schlüssel nicht auf der Entropie der Authentisierungsdaten basiert, wie es bei BAC der Fall ist. Darüber hinaus wird durch die Flüchtigkeit der Schlüssel für jede Sitzung ein anderer Schlüssel vereinbart.

2.4 Signaturdienst

Ein wichtiger Basisdienst ist der Signaturdienst, der zur Erstellung qualifizierter, elektronischer Signaturen in die ECC integriert werden kann. Für die derzeitigen Profile ist vorgesehen, dass der Signaturdienst auf der Karte vorhanden ist, jedoch zunächst keine entsprechenden Zertifikate und Schlüssel installiert werden. Dies erfolgt erst auf Wunsch des Benutzers nachträglich.

2.2 Verschlüsselung

Für verschlüsselte E-Mail-Kommunikation oder zur verschlüsselten Übertragung von Dokumenten ist ein Encryption-Key-Decipherment-Dienst vorgesehen. Hierbei wird die E-Mail bzw. das Dokument mit einem symmetrischen Verfahren verschlüsselt und der Nachrichtenschlüssel mittels eines asymmetrischen Verfahrens mit dem öffentlichen Schlüssel des Empfängers verschlüsselt. Der zugehörige geheime Schlüssel ist auf der Karte abgelegt, die nach entsprechender Authentisierung den Nachrichtenschlüssel entschlüsselt, der dann außerhalb der Karte zur Entschlüsselung der E-Mail verwendet werden kann.

3 Anwendungsprofile der ECC

Die in Teil 1 der Spezifikation CEN prTS 15480 der ECC beschriebenen Schnittstellen und Transportprotokolle sowie die in Teil 2 beschriebenen Dienste werden im Teil 4 zu Anwendungsprofilen zusammengesetzt. Ziel ist es, für festgelegte Anwendungen einheitliche, interoperable Karten zu spezifizieren, deren Sicherheitsfunktionen, Schnittstellen und Verhalten allgemein gleich ist.

Die Profile werden nach einem festen Schema definiert, das zum einen eine leichte Lesbarkeit und Vergleichbarkeit sicherstellt und darüber hinaus sicherstellt, dass alle notwendigen Angaben und Informationen enthalten sind. Der Schema-Aufbau ist auch in Teil 4 von CEN prTS 15480 festgelegt.

Derzeit sind zwei Profile festgelegt, wobei zu erwarten ist, dass bis zur Verabschiedung der Spezifikation weitere hinzugefügt werden.

3.1 Profil 1: ID-Karte (eID/ICAO/optional SIG)

Dieses Profil beschreibt eine Karte, die als Personaldokument genutzt wird. Für alle Anwendungen wird alleinig eine kontaktlose Schnittstelle nach ISO/IEC 14443 als verpflichtend festgelegt. Folgende drei Applikationen sind auf der Karte vorgesehen:

- eID: Diese Anwendung realisiert den elektronischen Ausweis. Die Daten des Karteninhabers (entsprechend den Daten der aktuellen Personaldokumente) werden in verschiedenen Datengruppen abgelegt. Der Zugriff auf die Datengruppen wird durch im Zertifikat des Lesers festgelegt Rechte feingranular abgestuft kontrolliert. Einzelne Datengruppen können für bestimmte Rollen schreibbar sein: So könnte beispielsweise nach entsprechender Authentisierung ein Meldeamt die Adresse aktualisieren, sodass die Karte bei einem Umzug nicht ersetzt, sondern nur aktualisiert werden muss. Für die eID-Anwendung sind Geräteauthentisierung und Secure Messaging verpflichtend zu unterstützen.

- ICAO: Da die Personalausweise innerhalb der Schengen-Staaten als Reisedokument akzeptiert werden, ist in diesem Profil eine MRTD-Anwendung (Machine Readable Travel Document) entsprechend den ICAO-Vorgaben enthalten, vergleichbar mit dem Reisepass. Als Kartendienste sind passive Authentisierung, BAC, EAC-Chip- und Terminal-Authentisierung sowie Secure Messaging für die ICAO-Applikation vorgeschrieben.

- SIG: Optional darf eine Karte nach Profil 1 eine Signatur-Applikation nach dem Standard CEN prEN 14890 (ESIGN) enthalten.

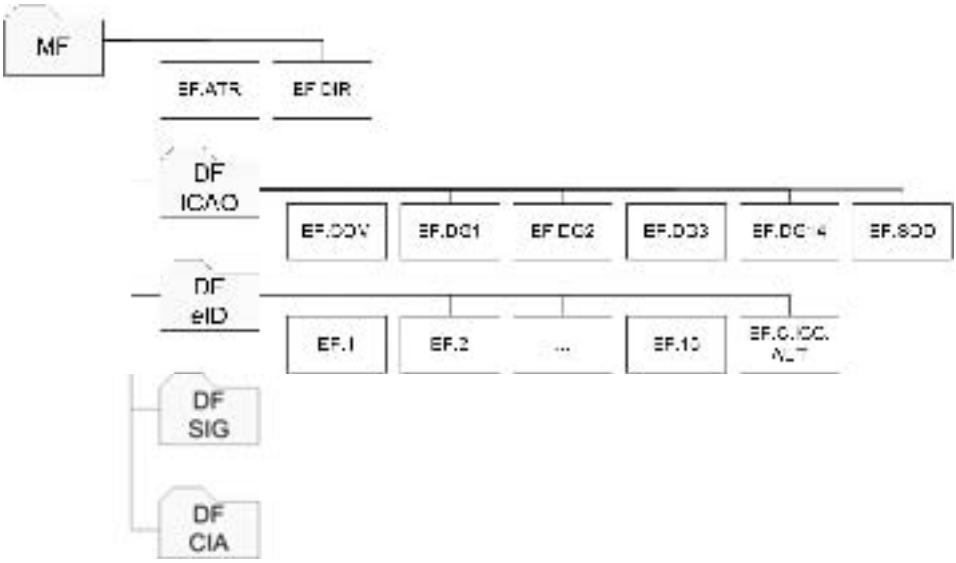

Abbildung 2: Datenstruktur des Profils 1

Profil 1 wurde im Rahmen des Deutschen Industrieforums (DIF AG 1) in Zusammenarbeit mit dem BSI erstellt, um eine Kompatibilität zu dem zukünftigen deutschen Personalausweis sicherzustellen.

Insbesondere folgende Kartendienste sind im Profil 1 vorgesehen:

- Passive Authentisierung:
- Basic Access Control (BAC)
- Modular Extended Access Control (EAC)
- Password Authenticated Connection Establishment (PACE)
- Secure Messaging
- Signaturdienst

Als Format der kartenprüfbaren Zertifikate (CV-Zertifikate) wird für die MRTD-Applikation das Format nach TR-03110 [EAC06] und für die eID- sowie die Signaturapplikation das Format nach prEN 14890 [prEN14890] festgelegt. Ergänzend wird die Struktur in den Zertifikaten enthaltenen CHAT-Datenobjekts spezifiziert, das die mit dem Zertifikat verbunden Zugriffsrechte festlegt.

3.2 Profil 2: ESIGN

Dieses Profil beschreibt eine Karte mit einer ESIGN-Applikation mit optionaler Ergänzung um eine Funktionalität für digitale Signaturen. Im Gegensatz zum ersten Profil ist eine kontaktorientierte Schnittstelle nach ISO/IEC 7816-3 mit dem Transportprotokoll T=1 vorgeschrieben. Das Profil basiert auf der Spezifikation der deutschen Gesundheitskarte (eGK). Die im Profil 2 genutzten Protokolle, Dienste und Formate basieren weitestgehend auf dem Standard prEN 14890 [SSCD06].

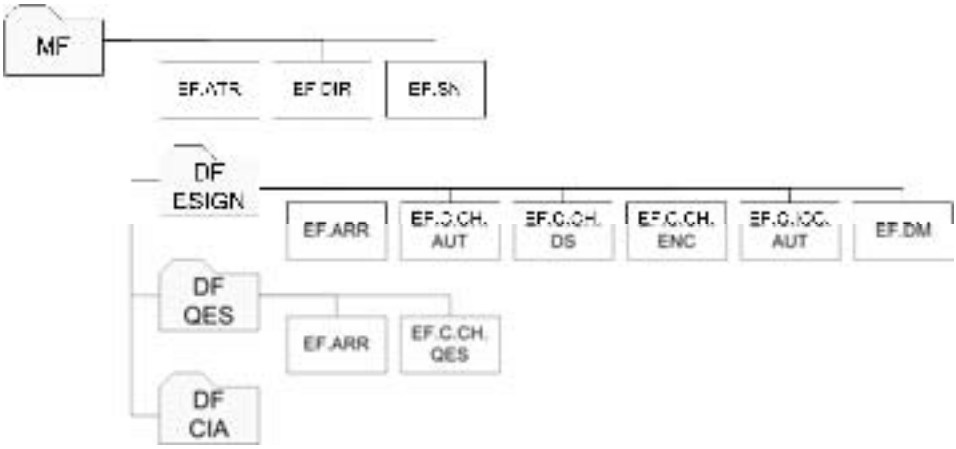

Abbildung 3: Datenstruktur des Profils 2

Folgende Kartendienste sind im Profil enthalten:

- Kartenidentifikation mittels PAN (Primary Account Number)
- Benutzerverifikation
- Geräteauthentisierung, Key Transport Protocol nach CEN prEN 14890
- Secure Messaging
- Client-Server-Authentisierung: Die Karte fungiert hierbei als krytographisches Werkzeug zum Aufbau gesicherter Verbindungen, z. B. zwischen einem Heimrechner und einem entfernten Server.
- Encryption-Key-Decipherment-Dienst
- Signaturdienst

3.3 Weitere Profile

Zurzeit enthält der aktuelle Entwurf des Teils 4 der Spezifikation prTS 15480 keine weiteren Profile. Bis zur Verabschiedung ist jedoch die Aufnahme weiterer Profile zu erwarten. Auch nach der Verabschiedung kann die Spezifikation über die entsprechende Arbeitsgruppe CEN TC224 WG 15 um neue Profile erweitert werden.

Um den Entwurf neuer Profile zu erleichtern, wurde ein entsprechendes Profil-Template integriert. Dieses stellt darüber hinaus sicher, dass die Profile identische Strukturen haben und so einfacher lesbar und vergleichbar sind, darüber hinaus wird einem Profil-Autor so Hilfestellung gegeben, welche Angaben in einem Profil benötigt werden.

Literaturverzeichnis

[EAC06] Technical Guideline, Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Version 1.01, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2. November 2006, siehe http://www.bsi.de/fachthem/epass/EACTR03110_v101.pdf

[ECC05] CEN prTS 15980 Identification card systems – European Citizen Card, CEN TC224 WG15, Draft November 2005

[ICAO04] ICAO TR PKI, Technical Report, PKI for Machine Readable Travel Documents offering ICC Read-Only Access, ICAO, Version 1.1, 1st October 2004, siehe http://www.icao.int/mrtd/download/documents/TR-PKI%20mrtds%20ICC%20read-only%20access%20v1_1.pdf

[ISO11770] ISO/IEC 11770 Information technology – Security techniques – Key management – Part 4: Mechanisms based on weak secrets, 2006

[ISO7816] ISO/IEC 7816 Identification cards – Integrated circuit cards, Part 4: Organization, security and commands for interchange, 2004, Part 8: Commands for security operations, 2004, Part 11: Personal verification through biometric methods, 2004, Part 13: Commands for application management in multi-application environment, FCD, 2006

[Kügl06] PACE: Password Authenticated Connection Establishment, Dennis Kügler, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2006

[RFC2631] Diffie Hellman Key Agreement Method, RFC 2631, E. Rescorla, June 1999, siehe http://www.ietf.org/rfc/rfc2631.txt

[SSCD06] CEN prEN 14890 Application Interface for Smartcards used as Secure Signature Creation Devices, CEN TC224 WG16, Part 1: Basic Services, draft, 17th July 2006, Part 2: Additional Services, draft, 17th July 2006