Zentrum für sichere Informationstechnologie – Austria
Secure Information Technology Center – Austria

A-SIT

Seidlgasse 22 / 9, 1030 Wien
Tel.: (+43 1) 503 19 63–0
Fax: (+43 1) 503 19 63–66

Inffeldgasse 16a, 8010 Graz
Tel.: (+43 316) 873-5514
Fax: (+43 316) 873-5520

http://www.a-sit.at
E-Mail: office@a-sit.at

DVR: 1035461
ZVR: 948166612
UID: ATU60778947

EINSATZ VON NFC IN EIDS IN AUSGEWÄHLTEN EU-LÄNDERN

Version 1.0 vom 29.12.2020
Alexander Marsalek – amarsalek@iaik.tugraz.at
Gerald Palfinger – gpalfinger@iaik.tugraz.at
Bernd Prünster – bpruenster@iaik.tugraz.at

Abstract/Zusammenfassung: In diesem Projekt werden ausgewählte NFC-fähige elektronische Authentifizierungslösungen verglichen. Es werden dazu die deutsche AusweisApp 2, die italienische Lösung SPID sowie die niederländische Lösung DigiD vorgestellt und verglichen. NFC wird typisch entweder zur Stärkung der Fern-Beantragung einer eID über das Auslesen eines herkömmlichen Ausweises verwendet (NL DigiD Substantieel, IT SPID) oder beim Online-Anmeldeprozess selbst (DE nPA mit AusweisApp 2, NL DigiD Hoog). Die vorgestellten Lösungen sind typische Vertreter der beiden Szenarien des NFC Einsatzes im Zuge der Ausstellung einer eID und des eID Einsatzes selbst.

Inhaltsverzeichnis

© A-SIT, Partner für Sicherheitsfragen

1. Einleitung

In dieser Kurzstudie werden die elektronischen Authentifizierungslösungen von Deutschland, Italien und Niederlande kurz vorgestellt und verglichen. Der Fokus wird dabei auf Near Field Communication-fähige (NFC-fähige) Ausweisdokumente gelegt, sowie auf Lösungen, welche eine Authentifizierung nach eIDAS Sicherheitsniveau *mittel* oder *hoch* erlauben. Im nächsten Abschnitt werden ausgewählte, vom deutschen Bundesamt für Sicherheit in der Informationstechnik (BSI) spezifizierte Protokolle vorgestellt. Abschnitt 3 stellt die niederländische Lösung DigiD vor. Abschnitt 4 behandelt die italienische Lösung SPID und Abschnitt 5 die deutsche Lösung AusweisApp 2. In Abschnitt 6 werden die Lösungen abschließend verglichen.

2. Hintergrundinformationen

In diesem Abschnitt werden die vom BSI spezifizierten Protokolle *PACE*, *Terminal Authentication Version 2* bzw. *Chip Authentication Version* 2 und die verschiedenen Terminaltypen vorgestellt.

2.1. Password Authenticated Connection Establishment (PACE)

PACE sorgt dafür, dass die Chip-Daten eines Ausweisdokumentes nicht ohne direkten Zugriff ausgelesen werden können [1]. Zudem wird sichergestellt, dass die Daten verschlüsselt mit dem Lesegerät ausgetauscht werden. Lesegeräte mit den richtigen Berechtigungszertifikaten können mittels MRZ oder CAN Nummer auf die Chip-Daten zugreifen. MRZ steht für Machine Readable Zone, CAN steht für Card Access Number. Diese Zugriffsnummern werden typischerweise auf das Ausweisdokument gedruckt. Solche Lesegeräte kommen typischerweise bei Grenzkontrollen vor. Bei anderen Lesegeräten wird die persönliche Geheimnummer benötigt, bevor die Daten ausgelesen werden können.

2.2. Terminal Authentication Version 2

Bei *Terminal Authentication Version 2* handelt es sich um ein Challenge-Response-Protokoll, welches die explizite einseitige Authentifizierung eines Terminals ermöglicht. Mittels dieses Protokolls kann ein eIDAS Token[1] überprüfen, ob das Lesegerät (Terminal) für den Zugriff auf sensible Daten berichtigt ist. Im Zuge der Terminal Authentifizierung werden folgende Schritte durchgeführt [2]:

1. Das Terminal sendet eine Zertifikatskette zum eIDAS Token. Das Root-Zertifikat der Kette kann mittels des auf dem eIDAS Token gespeicherten, öffentlichen Teil des CVCA[2] Schlüssels überprüft werden. Das andere Ende der Zertifikatskette bildet das Terminal-Zertifikat.
2. Der eIDAS Token überprüft die Zertifikatskette und extrahiert den öffentlichen Schlüssel des Terminals.
3. Im nächsten Schritt generiert das Terminal ein kurzlebiges (ephemeral) Diffie-Hellman Schlüsselpaar und sendet den komprimierten öffentlichen Teil des Schlüsselpaares zum eIDAS Token. Das Terminal kann in diesem Schritt auch weitere Hilfsdaten an den eIDAS Token schicken.
4. Der eIDAS Token generiert eine zufällige Challenge und sendet diese zum Terminal.
5. Als Antwort schickt das Terminal eine Signatur die mittels des im zweiten Schritt extrahierten Schlüssels überprüft werden kann. Die Signatur umfasst den in Schritt 4 übertragenen

[1] Der Begriff *eIDAS Token* wurde in einer von deutschen BSI und französischen ANSSI erstellten Spezifikation gewählt. Wenngleich diese auf die EU eIDAS Verordnung ausgerichtet ist, ist sie nicht als eine von den eIDAS Gremien (wie das Kooperationsnetzwerk) verabschiedete oder für eIDAS verbindliche Spezifikation zu verstehen, noch bedeutet dessen Einhaltung grundsätzlich eIDAS-Konformität. BSI TR-03110 versteht unter eIDAS Token alle Token, welche für die elektronische Identifizierung, Authentifizierung oder für Signaturen benutzt werden können.

[2] CVCA steht für Country Verifying Certificate Authority. Es handelt sich dabei um eine von einer staatlich betriebenen Wurzelzertifizierungsstelle, etwa dem BSI in Deutschland.

Zufallswert, den in Schritt 3 übertragenen komprimierten öffentlichen Teil des Schlüsselpaares, die Hilfsdaten, sofern vorhanden, sowie eine zuvor übertragene eIDAS Token Kennung.
6. Im letzten Schritt überprüft der eIDAS Token die Signatur mittels des in Schritt 2 extrahierten öffentlichen Schlüssels.

Alle Nachrichten müssen mittels *Secure Messaging*, im Verschlüsseln-Dann-Authentifizieren-(encrypt-then-authenticate) Modus übertragen werden. Dazu werden abgeleitete Sitzungsschlüssel aus PACE verwendet. Nach Terminal Authentication Version 2 muss *Chip Authentication* durchgeführt werden. Dieses Protokoll wird im nächsten Abschnitt beschrieben.

2.3. Chip Authentication Version 2

Mit diesem Protokoll kann der eIDAS Token authentifiziert werden. Dafür wird eine kurzlebige (ephemeral), statische Diffie-Hellman Schlüsselvereinbarung verwendet. Version 2 des Protokolls ermöglicht neben der Authentifizierung des eIDAS Tokens auch eine implizite Authentifizierung der gespeicherten Daten. Für die Kommunikation wird wieder Secure Messaging eingesetzt, allerdings mit neuen Sitzungsschlüsseln. Das Protokoll besteht aus den folgenden sechs Schritten [2]:

1. Der eIDAS Token schickt den öffentlichen Teil des statischen Diffie-Hellmann Schlüssels sowie die Domain-Parameter an das Terminal.
2. Das Terminal schickt den während der Terminal-Authentifizierung erstellten kurzlebigen öffentlichen Schlüssel an den eIDAS Token.
3. Der eIDAS Token errechnet den komprimierten öffentlichen Schlüssel und vergleicht den Wert mit dem während der Terminal-Authentifizierung (Schritt 3) empfangenen Wert.
4. Danach berechnen der eIDAS Token und das Terminal jeweils ein gemeinsames Geheimnis. Dazu verwenden beide jeweils ihren eigenen privaten Schlüssel, den öffentlichen Schlüssel des Gegenübers sowie die Domain-Parameter.
5. Danach generiert der eIDAS Token eine kryptografische Nonce und leitet davon mittels des zuvor berechneten gemeinsamen Geheimnisses einen Nachrichten-Authentifizierungsschlüssel sowie einen Verschlüsselungsschlüssel ab. Anschließend wird ein Nachrichtenauthentifizierungscode (Message Authentication Code, oder kurz MAC) über den soeben erstellten Nachrichten-Authentifizierungsschlüssel sowie den öffentlichen Schlüssel des Terminals erstellt und zusammen mit der Nonce zum Terminal geschickt.
6. Das Terminal errechnet aus der empfangenen Nonce und dem gemeinsamen Geheimnis ebenfalls den Nachrichten-Authentifizierungsschlüssel sowie den Verschlüsselungsschlüssel und überprüft damit die Gültigkeit des empfangenen Nachrichtenauthentifizierungscodes.

Aus Sicherheitsgründen muss vor der Chip-Authentifizierung eine passive Authentifizierung erfolgen.

2.4. Terminal Typen

Die technische Richtlinie TR-03129 [3] unterscheidet zwischen zwei Terminal-Typen. Terminals mit nur einem Lesegerät werden als integrierte Terminals bezeichnet und im nächsten Abschnitt beschrieben. Terminals mit mehreren Lesegeräten werden als verteilte Terminals bezeichnet. Diese werden in Abschnitt 2.4.2 beschrieben.

2.4.1. Integriertes Terminal

Integrierte Terminals haben nur ein Lesegerät. Der private Schlüssel des Terminals ist auf dem integrierten Hardware-Sicherheitsmodul (HSM) abgelegt, wodurch die Terminal-Authentifizierung offline durchgeführt werden kann. Eine Internetverbindung wird nur zum Aktualisieren von Zertifikaten benötigt. Der Nachteil dieser Architektur ist, dass die Terminals nach einem Diebstahl, bis zum Ablauf der hinterlegten Zertifikate weiterhin für Terminal Authentication verwendet werden können.

2.4.2. Verteiltes Terminal

Verteilte Terminals verfügen über mehrere Lesegeräte und werden von einem Terminal-Kontrollzentrum gesteuert. Das HSM befindet sich nicht im Lesegerät, sondern ist Teil des Kontrollzentrums. Aus diesem Grund benötigen die Lesegerate eine permanente (abgesicherte) Verbindung zum Kontrollzentrum. Das Kontrollzentrum muss auch sicherstellen, dass nur mit Lesegeräten, die unter der eigenen Kontrolle stehen, zusammengearbeitet wird. Das Kontrollzentrum kann, muss sich aber nicht in der Nähe des Terminals befinden.

Nachfolgend werden die Eigenschaften im Produktivbetrieb eingesetzter eID-Systeme unterschiedlicher Länder zusammengefasst. In Abschnitt 6 werden diese Lösungen einander gegenübergestellt.

3. Die Niederlande – DigiD

Bei DigiD wird NFC entweder im Zuge der Fern-Beantragung einer eID zur Bindung an die Person über Auslesen von Führerschein oder Personalausweis verwendet (Abschnitt 3.1 DigiD App mit ID-Prüfung (DigiD Substantieel)) oder bei der eID Nutzung selbst, wenn Führerschein oder Personal-ausweis Träger der eID sind und über ein NFC-fähiges Handy angesprochen werden (Abschnitt 3.2 Führerschein / Personalausweis (DigiD Hoog))

DigiD ermöglicht die digitale Identifizierung von Benutzerinnen bzw. Benutzern an öffentlichen niederländischen Services. DigiD wird von Logius [4] entwickelt und gewartet. Es handelt sich um ein zentrales Authentifizierungssystem welches derzeit vier verschiedene Anmeldeverfahren bei vier Konfidenzstufen (Basis, Midden, Substantieel, Hoog) unterstützt [5]:

1. Anmeldung mittels Benutzername und Passwort (DigiD Basis)
2. Anmeldung mittels Benutzername, Passwort und SMS (DigiD Midden)
3. DigiD App (DigiD Midden) und DigiD App mit ID-Prüfung (DigiD Substantieel)
4. Führerschein / Personalausweis (DigiD Hoog)

Tabelle 1 illustriert die Abbildung der vier verschiedenen niederländischen Konfidenzstufen auf die drei eIDAS-Sicherheitsniveaus.

DigiD	eIDAS-Sicherheitsniveau
Basis	Low
Midden	
Substantieel	Substantial
Hoog	High

Tabelle 1: Abbildung der DigiD Konfidenzstufen auf die eIDAS Stufen.

Ruft eine Benutzerin bzw. ein Benutzer ein öffentliches Service auf und möchte sich dort anmelden, leitet das Service die Benutzerin bzw. den Benutzer weiter zu DigiD. Nach der erfolgreichen Authentifizierung wird die Benutzerin bzw. der Benutzer wieder zum Service zurückgeleitet. Der Serviceanbieter erhält in diesem Schritt lediglich eine (verschlüsselte) Identifizierungsnummer (polymorph verschlüsselte Ableitung der „Burgerservicenummer" BSN), aber keine weiteren persönlichen Daten. Mittels des Identifikators kann der Serviceanbieter bei dem zentralen Register „Basisregistratie personen" (BRP), die persönlichen Daten abfragen. Für Abfragen zu Führer-scheinen wird das „Centraal Rijbewijsregister" (CRB) verwendet.

In den folgenden Abschnitten werden die beiden für diese Studie relevanten Authentifizierungsansätze „DigiD App mit ID-Prüfung“ im Zuge Beantragung einer eID und digitale Authentifizierung mit Führerschein oder Personalausweis betrachtet.

3.1. DigiD App mit ID-Prüfung (DigiD Substantieel)

Bei der Online-Aktivierung muss der Benutzer bzw. die Benutzerin die eigene Identität nachweisen. Dazu wird ein Reisepass, Führerschein oder Personalausweis benötigt. Nach Eingabe des Benutzernamens und Passwortes muss eine 5-stellige PIN gesetzt werden. Anschließend liest die App via NFC den Chip am Ausweis aus.

Technisch gesehen wird nach der PIN-Eingabe die PIN maskiert und verschlüsselt an die DigiD-Server übermittelt [5]. Danach ruft der Server die BSN aus den Registern BRP und CRB ab. Basierend auf den Daten wird eine Sitzung mit dem „Remote Document Authentication“ (kurz RDA) Server erstellt. Im nächsten Schritt scannt der Benutzer bzw. die Benutzerin das Identitätsdokument. Sobald dies geschieht, erstellt die DigiD-App einen Tunnel zwischen dem Identitätsdokument und dem RDA-Server. Über diesen Tunnel werden die Dokumentdaten geschickt und anschließend vom RDA-Server überprüft. Bei der Prüfung wird unter anderem sichergestellt, dass das Dokument physisch im Besitz der Bürgerin bzw. des Bürgers ist, nicht als gestohlen oder verloren gemeldet wurde, sowie dass die Gültigkeit nicht widerrufen wurde. Nach der erfolgreichen Prüfung informiert der RDA-Server den DigiD-Server und dieser aktiviert die App auf der Ebene „Substantial“. Anschließend kann sich die Benutzerin bzw. der Benutzer mittels App authentifizieren. Bei Anmeldung auf dem Smartphone geschieht die Authentifizierung direkt, bei der Anmeldung auf anderen Geräten muss ein QR-Code mit einem Kopplungscode gescannt werden.

Die NFC-Nutzung dient bei DigiD Substantieel also zur Bindung der App an die Person über ihr oder sein herkömmliches (NFC-fähiges) Ausweisdokument. Die PIN dient dem Schutz vor Missbrauch über Aktivierung durch Dritte, etwa wenn ein Ausweis zeitweise nicht in der Verfügungsgewalt der betroffenen Person ist.

3.2. Führerschein / Personalausweis (DigiD Hoog)

Die DigiD-App unterstützt auch die Identifizierung auf der eIDAS Stufe „hoch“. Dafür muss DigiD Hoog verwendet werden. Es werden Führerscheine mit dem notwendigen eID Applet, das PACE und Extended Access Control im Authentifizierungsprozess ausführen kann, seit 2018 an die niederländische Bevölkerung ausgerollt, der Start von DigiD Hoog selbst ist aber erst für Anfang 2021 geplant[3]. Anfang 2021 soll eine neue Identitätskarte herauskommen, welche DigiD Hoog unterstützt [6] [7]. Die Unterstützung des Führerscheins ist für die Zukunft geplant [8], Reisepässe werden jedoch nicht unterstützt [7]. Für DigiD Hoog wird das Ausweisdokument bei jeder Anmeldung benötigt. Auf dem Chip im Ausweisdokument ist hierfür ein spezielles eID-Applet installiert. Bei jeder Anmeldung wird der Besitz des Ausweises sowie die Kenntnis der dazugehörigen PIN überprüft.

Bei DigiD Hoog wird NFC im Zuge des Authentifizierungsvorgangs verwendet, der über das Applet des Ausweischips abläuft. Die DigiD-App dient mit dem Smartphone im wesentlichen als Kartenleser und zur PIN-Eingabe.

4. Italien – SPID

In Italien kann man mittels SPID auf über 5300 Dienste von öffentlichen Stellen und Behörden zugreifen. SPID steht für „Sistema Pubblico d’Identità Digitale”, oder (frei übersetzt) öffentliches System für digitale Identität. SPID bietet drei unterschiedliche Sicherheitsstufen [9]:

- Stufe 1 (Low) sieht den Einsatz von Benutzernamen und Passwort vor.

[3] u.a. Ankündigung niederländischer Gemeindeverband https://www.vngrealisatie.nl/producten/digid-hoog

- Stufe 2 (Substantial) benötigt zusätzlich einen zweiten Faktor; ein Einmalpasswort per SMS oder eine App.

- Stufe 3 (High) sieht den zusätzlichen Einsatz einer Sicherheitslösung (beispielsweise einer Smartcard) vor, auf der private Schlüssel sicher abgelegt werden können.

SPID ist ein Programm, mit einer Reihe von Identitätsprovidern, welche unterschiedliche Methoden zur Erlangung einer eID bzw. dessen Nutzung verwenden. Diese Studie beschränkt sich auf jene Anbieter und Varianten, in denen NFC-Funktionen des Smartphones verwendet werden. Dies ist im Zuge der Fern-Beantragung der eID möglich, wo über NFC ausgelesene Ausweisdaten die Videoidentifikation von Personen ergänzen.

Der Identitätsanbieter stellt eine App zur Verfügung, welche auf die Kamera des Smartphones zugreift und Fotos oder Videos aufnehmen kann. Zusätzlich kann die App mittels NFC mit der italienischen elektronischen ID-Karte sowie dem Reisepass kommunizieren. Dafür baut die App einen sicheren Kommunikationskanal zu den Servern des Identitätsanbieters auf.

Im Folgenden werden die Schritte des Identifizierungsprozesses für die Registrierung beim Anbieter PosteID beschrieben. PosteID [10] wurde als Beispiel herangezogen, da sonst kaum öffentliche Dokumentation verfügbar ist. Während des Identifizierungsprozesses werden folgende Schritte durchgeführt:

- Der Benutzer bzw. die Benutzerin muss die PosteID App auf einem NFC-fähigen Smartphone installieren und einen nach Oktober 2016 ausgestellten Reisepass oder die CIE 3.0 eID-Karte besitzen.

- Mittels der integrierten Kamera liest die App zuerst den aufgedruckten MRZ Code ein. Mittels dieses Codes kann die App per NFC mit dem Ausweisdokument kommunizieren.

- Zusätzlich muss noch ein Foto der Vorder- und Rückseite des Ausweisdokumentes sowie der Gesundheitskarte erstellt werden. Anschließend muss ein kurzes Video erstellt werden, welches den Benutzer oder die Benutzerin zeigt wie er oder sie einen kurzen von der App vorgegebenen Satz vorliest.

- Abschließend muss noch ein Porträtfoto aufgenommen werden, das abgesehen vom Gesicht auch den Ausweis beinhaltet.

Nach dieser ersten Phase, wird der Benutzer bzw. die Benutzerin aufgefordert, weitere Daten sowie Kontaktdetails anzugeben. Die übermittelten Daten werden dann von Mitarbeitern der Poste Italiane auf Korrektheit überprüft bzw. verglichen. Anschließend ist eine Authentifizierung auch mittels App möglich. Derzeit gibt es in Italien drei Anbieter, welche die höchste Authentifizierungsstufe unterstützen [11]. Diese drei Anbieter sind Aruba [12], PosteID [13] und Sielte [14].

Auf dem Reisepass sind neben dem Vor- und Nachnamen, dem Geburtsort und -datum, der Nationalität sowie der Steuernummer auch noch ein Bild sowie zwei Fingerabdrücke gespeichert [15] [16] [17]. Die Daten können bis auf die Fingerabdrücke von der App bzw. anderen Terminals ausgelesen werden. Dazu muss nur der MRZ Code bekannt sein. Der Zugriff auf die Fingerabdrücke ist zusätzlich abgesichert und nur speziellen Behörden gestattet.

Die Nutzung von NFC in SPID beschränkt sich vorerst also auf den Ausstellungsprozess einiger Identitätsprovider zur Ergänzung der Videoidentifikation über Prüfung von Ausweisen.

5. Deutschland - AusweisApp 2

In Deutschland war der neue Personalausweis (nPA) von Beginn der Ausgabe im Jahr 2010 ein NFC-fähiges Identitätsdokument und wurde für aus eIDAS Sicherheitsniveau hoch notifiziert. Zu

Beginn war dies auf die Nutzung am PC oder Laptop mit einem kontaktlosen Kartenleser ausgerichtet. Zur Nutzung der Online-Ausweisfunktion war am Gerät der Anwenderin oder des Anwenders eine sogenannte AusweisApp installiert, die die Kommunikation mit dem nPA initiiert und steuert. Mit der AusweisApp 2 wurde dies auf NFC-fähige Smartphones erweitert.

Die Online-Ausweisfunktion wird vom neuen Personalausweis oder dem Aufenthaltstitel unterstützt. Neben dem Besitz des Ausweises wird zusätzlich eine 6-stellige PIN benötigt um die Authentifizierung zu starten. Die Eingabe der PIN wird dabei als Zustimmung zur Authentifizierung gewertet. Auf dem Chip des Ausweises befindet sich ein eID-Applet, welches unter anderem den Vornamen, Nachnamen, Geburtstag und Geburtsort, sowie die Adresse, den Dokumententyp und einen kartenspezifischen Identifikator speichert.
Auf diese Daten kann erst nach einer erfolgreichen, wechselseitigen Authentifizierung von Chip und Gegenstelle zugegriffen werden. Zusätzlich muss die Gegenstelle gültige Zugriffsrechte nachweisen. Für die Übertragung wird ein Ende-zu-Ende gesicherter Kanal verwendet. Technisch baut die eID auf der eIDAS Token Spezifikation BSI TR-03110 [18] auf, wobei die Architektur in BSI TR-03127 [19] beschrieben ist. Für die wechselseitige Authentifizierung wird das Protokoll „Extented Access Control v2“ verwendet. Dieses Protokoll sieht zuerst die Authentifizierung des Dienstleisters mittels Terminal Authentication Version 2 (Abschnitt 2.2) vor. Dadurch kann der Dienstleister sich authentifizieren, sowie seine Zugriffsrechte nachweisen. Anschließend wird mittels passiver Authentifizierung die Echtheit der eID nachgewiesen. Dafür wird der vom Hersteller signierte öffentliche Schlüssel der Karte herangezogen. Im letzten Schritt wird die Echtheit des Ausweises sowie dessen Besitz mittels Chip Authentication Version 2 (siehe Abschnitt 2.3) nachgewiesen. Technisch wird hierfür der Besitz des privaten Teils des im vorherigen Schritt überprüften öffentlichen Schlüssels bewiesen.

Aus dieser Architektur ergeben sich mehrere Vorteile [20]. In der physischen Welt wird beim Vorzeigen eines Ausweises nur eine kurzfristige Identifizierung der Person erreicht. Weiteres kann ein Kontrolleur die Identität der bzw. des Überprüften nicht gegenüber einer weiteren Partei nachweisen. Dieses Prinzip verwendet die deutsche eID auch im Rahmen der elektronischen Identifizierung. Es wird nur eine temporäre Identifizierung ermöglicht, welche nicht benutzt werden kann, um die Identität gegenüber einer weiteren Partei zu beweisen. Daraus ergeben sich aus Sicht des Datenschutzes Vorteile. Technisch gesehen wird keine dauerhafte Identifizierung ermöglicht, da die Daten nicht signiert werden. Stattdessen wird die Echtheit der Daten durch den sicheren Übertragungskanal garantiert. Ein weiterer Vorteil ist, dass keine Drittparteien (z.B.: Identitätsprovider) während der Authentifizierung benötigt werden. Stattdessen wird nur der Dienstleister, der Ausweis, sowie die App benötigt. Dadurch werden zentrale Sicherheits-Hotspots und Tracking verhindert. Es ergibt sich auch eine höhere Ausfallsicherheit, da keine dauerhaften Verbindungen zum Identitätsanbieter benötigt werden. Stattdessen muss nur eine kurzzeitige Verbindung bestehen um die Zertifikate zu aktualisieren. Während der Authentifizierung ist keine Verbindung zum Identitätsanbieter notwendig.

6. Vergleich der Lösungen

Tabelle 1 zeigt einen Vergleich der verschiedenen eID Lösungen. Es wird verglichen um welchen eID-Typ es sich handelt, welche Daten auf der eID gespeichert sind, wie die MDS-Daten gesichert sind, ob NFC benötigt wird, ob das Ausweisdokument oder der Identitätsanbieter bei jeder Anmeldung notwendig ist, sowie das erreichte Authentifizierungslevel.

Tabelle 1: Vergleich der eID Lösungen.

	NL - DigiD		IT - SPID		DE - eID
	Substantieel	**Hoog**	**Stufe 2**	**Stufe 3**	**AusweisApp 2**
eID Typ	App	Ausweis	App bzw. Einmal-passwort	Ausweis	Ausweis
NFC genutzt für	Auslesen Ausweis bei Online-Beantragung	Authentifi-zierung über eID-Applet	nicht verwendet	Auslesen Ausweis bei Online-Beantragung (einige IdPs)	Authentifi-zierung über eID-Applet
MDS auf eID gespeichert?	Nein	Nein	Ja	Ja	Ja
MDS vor unberechtigten Zugriff geschützt	-	Zugriffscode benötigt	-	Aufgedruckter Zugriffscode benötigt	Explizite Zugriffsrechte notwendig
eIDAS Authentifizierungs-level	Substantial	High	Substantial	High	High
Ausweisdokument bei jeder Authentifizierung benötigt?	Nein	Ja	Nein	Nein	Ja
Identitätsanbieter bei jeder Anmeldung notwendig?	Ja	Ja	Ja	Ja	Nein

7. Fazit

In allen drei vorgestellten Ländern wird eine App und mindestens ein NFC-fähiges Ausweisdokument angeboten. Unterschiede gibt es beim Design der einzelnen Lösungen. So benutzen die Niederlande beispielsweise eine Identifizierungsnummer auf dem Ausweis um damit die MDS-Daten aus Registern zu beziehen, während Italien und Deutschland die MDS-Daten direkt elektronisch auf dem Ausweisdokument speichern. Auch die Leseberechtigungen werden unterschiedlich vergeben. Die Niederlande beziehen den Zugriffscode aus einem Register, Italien druckt ihn auf den Ausweis, während Deutschland explizite Zugriffsrechte vergibt. Auch in Puncto Architektur gibt es Unterschiede. Die italienischen und niederländischen Lösungen benötigen einen Identitätsanbieter während der Anmeldung, während die deutsche Lösung auch eine Authentifizierung ohne Einbindung des Identitätsanbieters erlaubt. Die Nutzung der NFC-Funktion ist entweder im Zuge der Online-Beantragung einer eID, um über gesichertes Auslesen eines Personalausweises o.ä. eine stärkere Bindung der eID an die Person zu erreichen (IT SPID und NL DigiD Substantieel), oder in der Verwendung der eID selbst, wo ein eID Applet am Chip des Ausweisdokuments genutzt wird.

Referenzen

[1] Bundesamt für Sicherheit in der Informationstechnik, „icherheitsmechanismen in elektronischen Ausweisdokumenten,“ [Online]. Available: https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/ElektronischeIdentitaeten/Sicherheitsmechanismen/sicherPACE/pace_node.html. [Zugriff am 23 12 2020].

[2] Bundesamt für Sicherheit in der Informationstechnik, „Technical Guideline TR-03110, Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token – Part 2: Protocols for electronic IDentification, Authentication and trust Services (eIDAS),“ 21 12 2016. [Online]. Available:

https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03110/BSI_TR-03110_Part-2-V2_2.pdf?__blob=publicationFile&v=3. [Zugriff am 10 12 2020].

[3] Bundesamt für Sicherheit in der Informationstechnik, „BSI-TR-03129 Technical Guideline PKIs for Machine Readable Travel Documents, v1.10," 09 11 2009. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG03129/BSI_TR_03129.pdf?__blob=publicationFile&v=2. [Zugriff am 10 12 2020].

[4] Logius, Ministerie van Binnenlandse Zaken en Koninkrijkrelaties, „DigiD: wie doet wat?," [Online]. Available: https://logius.nl/diensten/digid/wie-doet-wat. [Zugriff am 1 12 2020].

[5] Laura van Well, Logius, „Functionele beschrijving DigiD app," 10 6 2020. [Online]. Available: https://www.logius.nl/sites/default/files/bestanden/website/Functionele%20beschrijving%20DigiD%20app%20v0.2%20def_0.pdf. [Zugriff am 1 12 2020].

[6] Logius, Ministerie van Binnenlandse Zaken en Koninkrijkrelaties, „DigiD: hoe werkt het?," [Online]. Available: https://www.logius.nl/diensten/digid/hoe-werkt-het. [Zugriff am 22 12 2020].

[7] J. Huijbregts, „Identiteitskaart om in te loggen met DigiD-niveau 'hoog' verschijnt in januari," 2 10 2020. [Online]. Available: https://tweakers.net/nieuws/172916/identiteitskaart-om-in-te-loggen-met-digid-niveau-hoog-verschijnt-in-januari.html. [Zugriff am 22 12 2020].

[8] VNG Realisatie, „DigiD Hoog," 03 09 2020. [Online]. Available: https://www.vngrealisatie.nl/producten/digid-hoog. [Zugriff am 22 12 2020].

[9] Agenzia per l'Italia digitale, „Sistema Pubblico di Identità Digitale - General Information," 21 09 2017. [Online]. Available: https://ec.europa.eu/cefdigital/wiki/download/attachments/62885733/G.1%20-%20General%20information%2C%20v1.0.pdf?version=1&modificationDate=1531759224705&api=v2. [Zugriff am 14 12 2020].

[10] Poste Italiane, „Guida Utente PosteID abilitato a SPID - Sistema Pubblico di Identità Digitale," 18 01 2019. [Online]. Available: https://www.agid.gov.it/sites/default/files/repository_files/dto_spid_pi_004-allegato_guida_utente_v2.5.pdf. [Zugriff am 15 12 2020].

[11] Agenzia per l'Italia Digitale, „Richiedi SPID," 10 12 2020. [Online]. Available: https://www.spid.gov.it/richiedi-spid/. [Zugriff am 23 12 2020].

[12] Aruba, „ESecurity - Product choice," [Online]. Available: https://cart.aruba.it/ESecurity?workflowId=76e967a6-e0ca-4695-be2e-4ffbbbd36600. [Zugriff am 23 12 2020].

[13] PosteID, „PosteID abilitato a SPID," [Online]. Available: https://posteid.poste.it/. [Zugriff am 23 12 2020].

[14] Sielte SpA , „Registrati a SielteID," [Online]. Available: https://myid.sieltecloud.it/signup/. [Zugriff am 23 12 2020].

[15] Ministero dell'Interno, „Il microchip," [Online]. Available: https://www.cartaidentita.interno.gov.it/il-microchip/. [Zugriff am 15 12 2020].

[16] Ministero dell'Interno, „Caratteristiche del documento," [Online]. Available: https://www.cartaidentita.interno.gov.it/caratteristiche-del-documento/. [Zugriff am 15 12 2020].

[17] Thales Group, „The new Italian national eID card goes live (2020 update)," 2020. [Online]. Available: https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/customer-cases/new-national-identity-card-for-italy. [Zugriff am 15 12 2020].

[18] Bundesamt für Sicherheit in der Informationstechnik, „BSI TR-03110 Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS token," [Online]. Available: https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03110/TR-03110_node.html. [Zugriff am 21 12 2020].

[19] Bundesamt für Sicherheit in der Informationstechnik, „BSI TR-03127 eID-Karten mit eID- und eSign-Anwendung basierend auf Extended Access Control," [Online]. Available:

https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03127/TR-03127_node.html. [Zugriff am 21 12 2020].

[20] Federal Office for Information Security, „ German eID based on Extended Access Control v2 - Overview of the German eID system,“ 21 08 2017. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/EIDAS/German_eID_Whitepaper_final.pdf?__blob=publicationFile&v=6. [Zugriff am 21 12 2020].