Elektronische Identifizierung und vertrauenswürdige Dienste

Nicolas Buchmann · Harald Baier

da/sec – Biometrics and Internet Security Research Group
Hochschule Darmstadt
{firstname.lastname}@h-da.de

Zusammenfassung

Im Oktober 2013 hat der Ausschuss des Europäischen Parlaments für Industrie, Forschung und Energie (engl. ITRE) damit begonnen die Regulierung und Harmonisierung der elektronischen Identifikation, Authentisierung und vertrauenswürdige Dienste (engl. eIDAS) zwischen den EU-Mitgliedsstaaten einzuleiten. Die bevorstehende EU-Verordnung wird Kompatibilität und gegenseitige Akzeptanz der elektronischen Identifizierung über Grenzen hinweg sichern, was eine einmalige Gelegenheit bietet um vertrauenswürdige, elektronisch authentisierte Transaktionen im einheitlichen Euro-Zahlungsverkehrsraum (engl. SEPA) einzuführen. Der wissenschaftliche Beitrag dieses Artikels ist wie folgt: Zuerst diskutieren wir die Anwendung des eIDAS Standards für vertrauenswürdige Banken Transaktionen und heben die sich daraus ergebenden Vorteile für Sicherheit und Privatsphäre hervor. Des Weiteren präsentieren wir die erste Erweiterung des eIDAS Standards um Privatsphäre konforme, biometrisch authentisierte Transaktionen, durch das BioPACE Protokoll welche den Benutzerkomfort, Vertrauen und Zuversicht gegenüber E-Banking und E-Business verbessern. Im Gegensatz zu den wenigen vorhanden wissenschaftlichen Vorschlägen Biometrie mit Bankentransaktionen zu verknüpfen basiert unser Vorschlag auf Standards, Sicherheitsprotokollen, Infrastruktur und Technologien, die sich in anderen Bereichen bewährt haben, was aus unserer Sicht für eine vertrauenswürdige Bankenanwendung essenziell ist. Basierend auf unserer umfangreichen Diskussion und Beschreibungen der einzelnen Systemkomponenten kommen wir zu dem Schluss, dass unser konzipiertes System eine Verbesserung des Benutzerkomforts, Vertrauen und Zuversicht gegenüber E-Banking und E-Business leistet.

1 Einleitung

Aktuell bearbeiten die 33 SEPA Länder über 80 Milliarden elektronische Zahlungstransaktionen im Jahr [Euro13]. Ein Sicherheitsprotokoll zum Schutz einer solch enormen Anzahl an Transaktionen mit sensiblen Daten sollte auf einem Standard basieren, welcher sich in der Praxis als sicher und anwendbar erwiesen hat. Diese Voraussetzungen sind für den eIDAS Standard gegeben. Daraus ergibt sich die Möglichkeit die beiden Technologien (eIDAS und SEPA) zu verbinden, und dabei einen gegenseitigen Vorteil für beide Technologien zu erlangen.

- Einerseits wird der noch andauernde Prozess der eIDAS Standardisierung durch einen Millionen von Bürgern betreffenden Anwendungsfall gestärkt, z.B. sicheres Home Banking und der Schutz vor Skimming an Geldautomaten. Dies ist im Hinblick auf die schwache Akzeptanz der eID Funktion des deutschen Personalausweises ein nicht zu unterschätzender Faktor, denn nur durch Bürger relevante Anwendungsfälle kann wirkliches

P. Schartner · K. Lemke-Rust · M. Ullmann (Hrsg.) · D•A•CH Security 2015 · syssec (2015) 49-60.

und nachhaltiges Interesse für die elektronische Identifikation beim Bürger geweckt werden.

- Andererseits können SEPA Transaktionen durch Standards, welche sich in einer anderen Hochsicherheitsbranche bewährt haben gesichert werden.

Eine Studie in 2010 identifizierte die Harmonisierung der verschiedenartigen regulatorischen Vorschriften als eine der größten Hürden für den Gewinn von grenzüberschreitenden Finanzdienstleitungen [AhGa10]. Auch wenn eIDAS ein erst frischer Standard ist, welcher die genannten Hindernisse beseitigt, setzt dieser auf vorhandene Infrastruktur. Neun EU-Mitgliedsstaaten betreiben bereits eID Systeme und drei weitere haben angekündigt in nächster Zeit ein eID System aufzubauen [Trac12]. Die Harmonisierung dieser eID Systeme durch die EU mit eIDAS birgt somit ein hohes Potenzial und ein neues Level an Sicherheit für E-Banking im einheitlichen Euro-Zahlungsverkehrsraum. Die zusätzliche Integration von biometrischen Sicherheitsmerkmalen bietet Schutz gegen Phishing, E-Banking Betrug und Identitätsdiebstahl. Biometrische Merkmale, welche aus biometrischen Charakteristiken extrahiert wurden, bieten im Regelfall eine höhere Entropie als eine gewöhnliche numerische PIN, die im aktuellen Standard verwendet wird.

2 System Architektur

Unser vorgeschlagenes System setzt sich aus vier definierten Prozessen zusammen und verbindet drei Kernkomponenten:

1. Die elektronische Identifizierung und vertrauenswürdige Dienste (eIDAS) welche gerade durch die EU standardisiert und harmonisiert werden,
2. biometrische Authentisierung und
3. das BioPACE Protokoll.

Diese drei Komponenten bilden in Kombination einen vertrauenswürdigen Dienst mit elektronischer Identifizierung und biometrischen authentisierten Transaktionen.

Die vier Prozesse, welche diese drei Komponenten verwenden sind:

1. eIDAS Token Registrierung und Ausstellung
2. eIDAS Provider Aktivierung
3. Gegenseitige Authentisierung: Token und Lesegerät
4. Gegenseitige Authentisierung: Token und Service Provider

Um eine eIDAS unterstützende eBanking Anwendung verwenden zu können benötigt der Benutzer entsprechende Hardware. Ein Großteil der Benutzer besitzt bereits einen Teil der benötigten Hardware. Das Primärgerät ist im Regelfall ein Notebook, Smartphone oder Tablet mit einem Browser und Zugriff auf das Internet. Es wird angenommen, dass dieses Gerät nicht von Malware befallen ist und eine Kamera besitzt. Letzteres ist gängig für alle drei Gerätefamilien. Ein eIDAS Token kann entweder kontaktbasiert oder kontaktlos sein, durch die einfachere Benutzung und den geringeren Abrieb gehen wir davon aus, dass die meisten eIDAS Tokens kontaktlos sein werden. Bei einem Smartphone oder Tablet wird die Near Field Communication (NFC) Schnittstelle benötigt um mit einem kontaktlosen eIDAS Token zu kommunizieren. Wenn der Benutzer einen Laptop verwendet benötigt er sehr wahrscheinlich ein externes eIDAS Lesegerät oder ein Laptop mit NFC Unterstützung. Um das biometrische Merkmal des Benutzers zu lesen, wird entweder ein Gerät mit einem bereits integrierten biometrischen Lesegerät

benötigt oder ein externes Gerät, welches z.B. Teil der Funktionalität des eIDAS Lesegerätes sein kann. Wenn eIDAS sich verbreitet wird der Benutzer bereits eGovenment Dienste damit nutzen und somit auch schon die entsprechende Hardware besitzen.

Im Folgenden beschreiben wir diese vier Prozesse:

2.1 eIDAS Token Registrierung und Ausstellung

Innerhalb des vorgeschlagenen Systems ist ein Nutzer dazu angehalten ein eIDAS Token zu besitzen, welches ein separates Token sein kann, oder im Regelfall eher die integrierte Funktionalität, einer nationalen Identitätskarte. Ein Bürger bekommt seine Identitätskarte mit eIDAS Funktionalität, indem er ein älteres Dokument beim Bürgeramt präsentiert und dabei eine beaufsichtigte biometrische Erfassung durchführt. Abbildung 1 zeigt einen Überblick über die Erstellung und Personalisierung des eIDAS Dokuments.

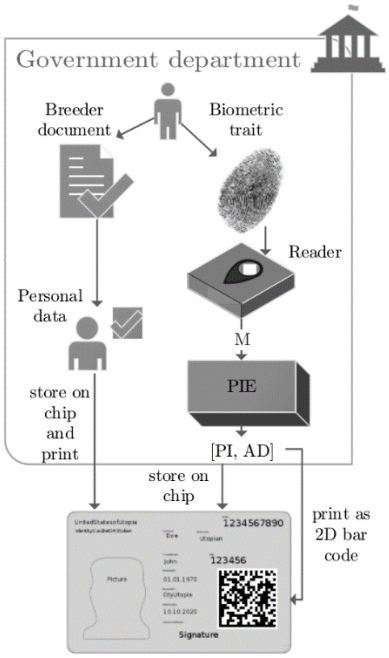

Abb. 1: eIDAS Token Registrierung und Ausstellung

Bei der biometrischen Registrierung präsentiert ein Bürger ein biometrisches Merkmal, z.B. einen Fingerabdruck oder die Iris. Basierend darauf werden biometrische Daten extrahiert. Durch die Biometrie wird eine starke Bindung zwischen dem Benutzer und dem eIDAS Token erzeugt. Es ist zu beachten, dass aktuelle biometrische Erfassungsgeräte eine Lebenderkennung besitzen, die Attacken wie z.B. Fingerattrappen verhindert [Comm13]. Die extrahierten biometrischen Daten M dienen als Eingabe für ein biometrisches Template Protection Verfahren [CaSt09a], welches die Privatsphäre des Benutzers schützt in Konformität mit der ISO/IEC IS 24745 [CaSt09b] für biometrischen Informationsschutz. Bei dieser standardisierten Architektur generiert ein Pseudonymous Identifier Encoder (PIE) aus M, während der eIDAS Token Registrierung, einen Pseudonymous Identifier (PI) und Auxiliary Data (AD), [PI,AD] = PIE(M). PI repräsentiert dabei eine geschützte Identität eines Benutzers und AD die Benutzer spezifischen Daten, welche dabei helfen PI beim Authentisierungsprozess zu reproduzieren.

In dem von uns vorgesehen System wird AD als ein 2D Barcode auf dem eIDAS Token gespeichert. PI hingegen wird im internen Speicher des eIDAS Token Chips gespeichert, ist nur für

den Chip selbst verfügbar und die ungeschützten extrahierten Merkmale M werden nach der Registrierung gelöscht.

2.2 eIDAS Provider Aktivierung

Der eIDAS Provider (z.B. eine Bank) benötigt Zugriff zur sogenannten „Signing Public Key Infrastructure (PKI)“ [ICAO06] damit dieser die Echtheit des vom Benutzer verwendeten eIDAS Tokens prüfen und um die Authentizität und Integrität der persönlichen Daten, welche vom eIDAS Token gelesen werden zu gewährleisten. Zusätzlich registriert der eIDAS Provider seinen Dienst bei der zuständigen Regierungsbehörde welche Zugriff auf die sogenannte Verifying PKI [BSI13c,NORM09] hat, um ein Zertifikat für den Dienst zu erhalten. Dieses Dienstezertifikat kann vom eIDAS Token verifiziert werden und beinhaltet außerdem die Zugriffsrechte des eIDAS Providers. Im speziellen enthält das Zertifikat die Zugriffsrechte auf welche Datengruppen das eIDAS Token dem eIDAS Provider Zugriff gewährt. Abbildung 2 zeigt den Ablauf der eIDAS Provider Aktivierung.

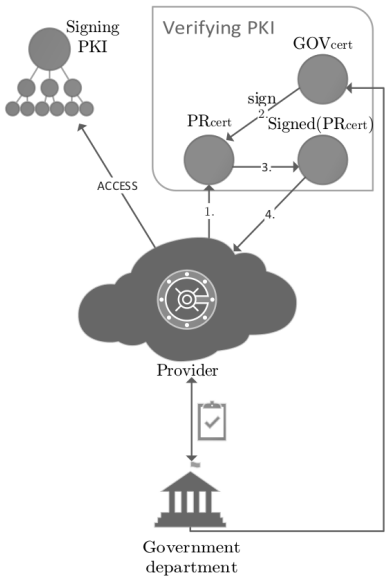

Abb. 2: eIDAS Provider Aktivierung

2.3 Gegenseitige Authentisierung: Token und Lesegerät

Während der Authentisierung präsentiert der Benutzer sein biometrisches Merkmal und sein eIDAS Token, welches AD in Form eines 2D Barcodes enthält, seinem Benutzer Gerät mit integriertem Lesegerät. Der Pseudonymous Identifier Recorder (PIR) nutzt die gelesenen biometrischen Daten M^* und AD als Eingabe und berechnet den Pseudonymous Identifier PI^*, $PI^* = PIR(M^*, AD)$. Dieses PI^* wird innerhalb des BioPACE-Protokolls [BRBP13] vom Lesegerät zum eIDAS Token übertragen. Dieses Protokoll führt auch den Vergleich der beiden geschützten Templates durch. Bei einem gewöhnlichen biometrischen Template Protection Scheme vergleicht der Pseudonymous Identifier Comparator (PIC) PI^* mit dem gespeicherten PI, $v = PIC(PI, PI^*)$. Abhängig vom verwendeten PIC ist das Vergleichsergebnis v entweder eine harte Entscheidung (ja/nein) oder ein Ähnlichkeitscore v, welcher dann mit einem Schwellwert t verglichen werden muss, um eine binäre Entscheidung zu erhalten. Basierend auf diesem statischen

gemeinsamen Geheimnis PI, einigen sich das eIDAS Token und das eIDAS Lesegerät auf ein flüchtiges gemeinsames Geheimnis welches mit PI, während dem BioPACE-Protokoll authentisiert wird. Mit diesem gemeinsamen Geheimnis bauen die beiden Entitäten einen sicheren kryptografischen Kanal auf, welcher Authentizität, Integrität und Vertraulichkeit für die übertragenen Daten gewährleistet welche darüber gesendet werden, wie in Abbildung 3 dargestellt.

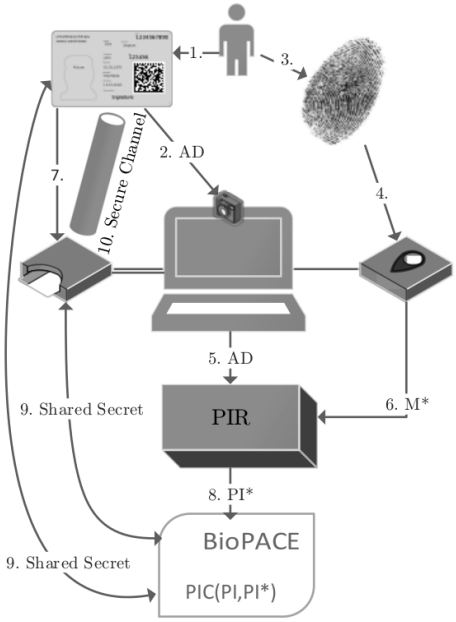

Abb. 3: Gegenseitige Authentisierung: Token und Lesegerät

2.4 Gegenseitige Authentisierung: Token und Provider

Nachdem der sichere kryptografische Kanal zwischen eIDAS Token und eIDAS Lesegerät aufgebaut wurde, müssen nun der eIDAS Service Provider und das eIDAS Token sich gegenseitig authentisieren. Dies erfolgt mithilfe der eIDAS Protokolle, der Signing PKI und der Verifying PKI. Im Falle dass dieser Schritt erfolgreich durchgeführt wird, sind folgende Zusicherungen gewährleistet:

1. Das eIDAS Token kommuniziert mit einem vertrauenswürdigen eIDAS Provider und kennt dessen Zugriffsrechte.
2. Der eIDAS Provider kommuniziert mit einem authentischen eIDAS Token.
3. Zwischen eIDAS Token und eIDAS Provider besteht ein sicherer kryptografischer Kanal.

Darauf folgend kann der eIDAS Provider nun über den sicheren kryptografischen Kanal auf die Daten des eIDAS Tokens zugreifen und den Benutzer authentisieren. Da nun beide Entitäten komplett authentisiert sind, kann der Benutzer eine Online Banking Transaktion durchführen. Diese Transaktion ist Zwei-Faktor authentisiert, da einerseits der Benutzer bewiesen hat, dass er ein gültiges eIDAS Token besitzt indem er es vor die Kamera hält und danach auf das Lesegerät legt. Andererseits wird ein biometrisches Merkmal des Benutzers überprüft. Durch die Separierung des Besitzes (eIDAS Token) und sein (biometrisches Merkmal) kann der eIDAS Provider sicher sein, dass der Benutzer die Transaktion selbst durchgeführt hat. Der gesamte Prozess ist in Abbildung 4 abgebildet.

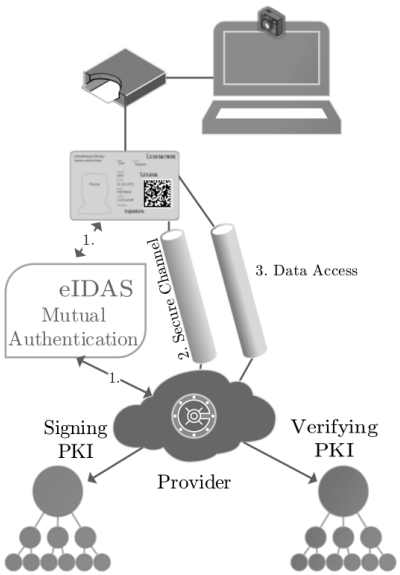

Abb. 4: Gegenseitige Authentisierung: Token und Provider

3 Integration der Biometrie

Der Begriff Biometrie ist definiert als „automated recognition of individuals based on their behavioural and biological characteristics“(ISO/IEC JTC1 SC37). Physiologische sowie verhaltensbiometrische Merkmale werden erhalten durch die Anwendung von entsprechenden Sensoren und markante Merkmale werden davon extrahiert, um ein biometrisches Template zu erzeugen. Während der biometrischen Verifikation oder Identifikation verarbeitet das System eine neue biometrische Eingabe, welche mit dem gespeicherten Template verglichen wird und entweder akzeptiert oder abgelehnt wird [JaRo04]. Die meiste Besorgnis gegenüber Privatsphäre und Datenschutz bei Biometrie ist in der Speicherung und dem Missbrauch der Daten begründet. Biometrische Template Protection [RaUh11], welche als biometrische Kryptosysteme [ViBB84] und Cancellable Biometrics [RaCB01] unterteilt werden, adressieren diese Besorgnis und verbessern das öffentliche Vertrauen und die Akzeptanz gegenüber Biometrie.

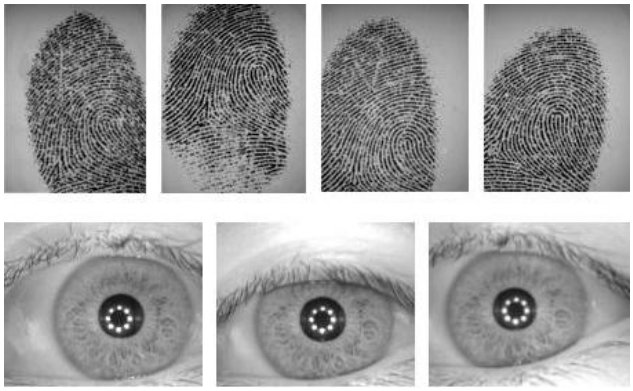

Abb 5: Biometrische Varianz (Bilder entnommen aus FVC’04, CASIAv3 Datenbank)

Beide Technologien sind in der Lage AD und PI aus einer biometrischen Eingabe M zu erzeugen. Wenn PI weiterverwendet wird z.B. für Verschlüsselung, muss gewährleistet sein, dass es ausreichend Entropie aufweist. Die Entropie der biometrischen Eingabe M wirkt sich direkt aus

auf die Entropie für das entsprechende PI. Verschiedene Techniken um die Entropie von biometrischen Merkmalen zu messen wurden vorgeschlagen.

Bei biometrischen Merkmalen kann nicht davon ausgegangen werden, dass diese komplett unabhängig voneinander sind, z.B. ein Fingerabdruck hat bestimmte charakteristische Strukturen. Für die Speicherung von Biometrie ist die binäre Darstellung der Template die favorisierte Darstellung, da diese wenig Speicher verbraucht und schnelle Vergleiche ermöglicht. Es wurden bereits zahlreiche Ansätze vorgestellt um binäre Merkmalsvektoren aus biometrischen Merkmalen, zu extrahieren. Wir beschränken unsere Analyse der Entropie deshalb auf die der biometrischen Daten in binärer Repräsentation.

Die übliche Methode um die durchschnittliche Entropie (Anzahl der gegenseitig unabhängigen Bits) von biometrischen Merkmalsvektoren abzuschätzen, ist die sogenannten „degrees-of-freedom“ zu messen. Diese sind definiert als $d = p(1-p)/o^2$, wobei p die mittlere Hamming Distance (HD) und o^2 die entsprechende Varianz zwischen verglichenen Paaren von biometrischen Merkmalsvektoren ist. Entropie Werte entnommen aus wissenschaftlicher Literatur sind in Tabelle 1 für die relevanten biometrischen Merkmale zusammengefasst. Die Abgeschätzte kann direkt auf AD bzw. PI übertragen werden, welche für weitere Anwendungen wie Verschlüsselung verwendet werden. Die resultierende Entropie kann jedoch verringert werden durch Verfahren der geschützten Templates, welche Varianzen kompensieren.

Tab. 1: Entropie für verschiedene biometrische Modalitäten

Biometric characteristic	Feature extractor	Entropy (in Bits)	Reference
Fingerprint	Minutia-based	84	[RaCB01]
Iris	2D Log-Gabor wavelets	249	[Daug06]
Face	Fusion of FLD and PCA	56	[AdYL06]

FLD = Fisher linear discriminant, PCA = Principal component analysis

4 BioPACE

Das Password Authenticated Connection Establishment (PACE) Protokoll wurde zuerst im neuen deutschen Personalausweis eingesetzt und standardisiert vom Bundesamt für Sicherheit in der Informationstechnik (BSI). Es ist inzwischen ein internationaler Standard in Form des PACE basierenden Supplemental Access Control (SAC) [ICAO10], welches seit Ende 2014 als ein ergänzendes Zugriffsprotokoll zu Basic Access Control (BAC) integrierst wird. Ab 2018 soll es BAC ersetzen [ICAO13]. Das BioPACE-Protokoll benutzt PACE als Basis, aber ersetzt das wissensbasierte Geheimnis durch ein biometrisches Geheimnis.

Die Idee von BioPACE wurde zuerst vorgestellt in [DMDK13] und später erweitert in [BRBP13] in Form von BioPACE Version 2. Da Version 2 eine Tracking Schwäche behebt und weitere nützliche Sicherheitseigenschaften erweitert, die für den eIDAS Kontext relevant sind, werden wir in dieser Arbeit BioPACE Version 2 als BioPACE bezeichnen.

Bei eIDAS wird das PACE-Protokoll für die gegenseitige Authentisierung zwischen eIDAS Token und eIDAS Token Lesegerät verwendet. Zusätzlich wird ein sicherer kryptografischer Kanal aufgebaut der Authentizität, Integrität und Vertraulichkeit der darüber transferieren Daten sicherstellt. Das Sub-Protokoll, welches für den Datentransfer über den sicheren Kanal zuständig ist wird als Secure Messaging bezeichnet.

BioPACE ist ein Vorverarbeitungsschritt für das PACE-Protokoll, welches das gewöhnliche wissensbasierte Geheimnis durch ein biometrisches Geheimnis ersetzt. In [DMDK13] wird die Idee biometrische Templates basierend auf dem ISO/IEC 24745 Standard für biometrischen Informationsschutz eingeführt. BioPACE favorisiert keine bestimmte biometrische Modalität, dass bedeutet BioPACE kann z.B. mit Gesicht, Fingerabdruck oder Iris implementiert werden. Das BioPACE-Protokoll besteht aus zwei Phasen:

1. Die Initialisierungsphase
2. Die Phase der regelmäßigen Anwendung

Für jedes eIDAS Token muss die Initialisierungsphase durchgeführt werden, bevor der Hersteller das Token personalisieren kann. Während der Beantragung eines eIDAS Tokens wird ein biometrisches Merkmal von einem Benutzer gelesen und Merkmale aus den gelesenen Daten extrahiert. Diese extrahierten Daten ergeben die biometrische Referenz des Benutzers welche aus dem Pseudonymous Identifier PI und der Auxiliary Data AD besteht.

Nach der biometrischen Registrierung wird AD in Form eines 2D Barcode auf das eIDAS Token gedruckt, dies ist in Abbildung 6 zu sehen.

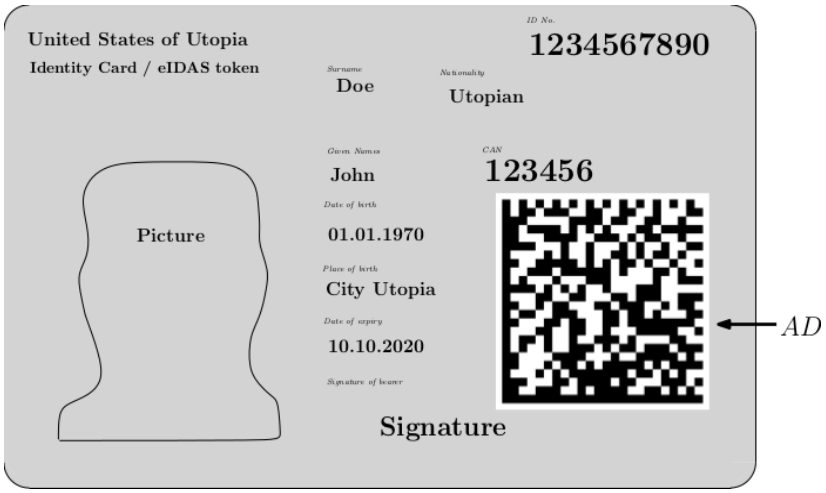

Abb. 6: Das eIDAS Token mit AD als Data Matrix Code

PI ist nicht öffentlich verfügbar, sondern ist im internen Speicher des eIDAS Tokens gespeichert und deshalb nur für den Chip des Tokens selbst verfügbar und nicht für das eIDAS Token Lesegerät.

Nach der einmaligen Initialisierung ist BioPACE bereit für die Phase der regelmäßigen Anwendung welche aus einer neuen Extrahierung der Merkmale aus neu gelesenen biometrischen Daten des Benutzers und dem optischen Lesen des vorherig erzeugten AD besteht. Ein eIDAS Token Lesegerät benötigt optischen Zugriff auf das eIDAS Token um den 2D Barcode zu lesen, da AD benötigt wird, um PI^* zu berechnen, welches nur dem initialen PI entspricht, wenn es sich um die gleiche Person handelt, welche auch die biometrischen Daten während der Registrierung bereitgestellt hat und deshalb eine biometrische Übereinstimmung gefunden wird. Diese Phase ist in Abbildung 7 dargestellt.

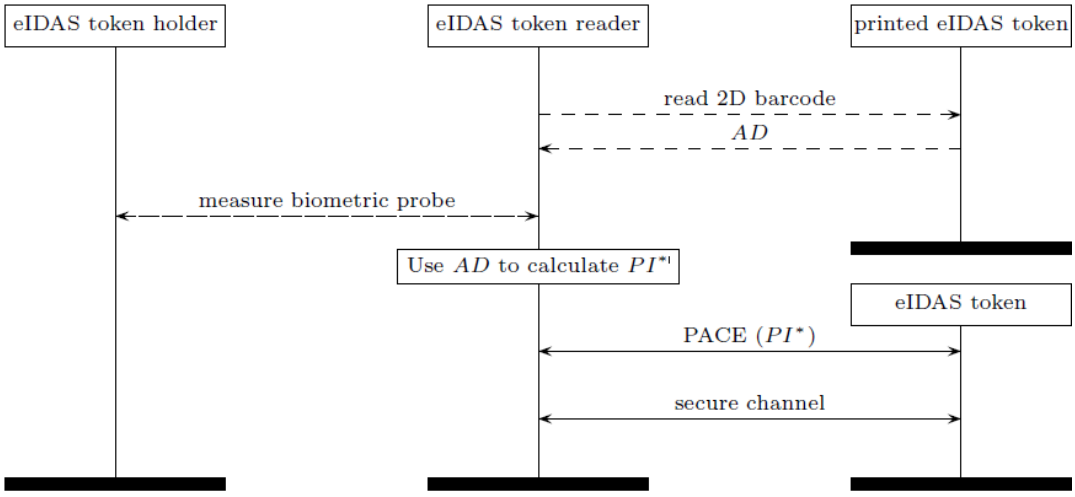

Abb. 7: Das BioPACE-Protokoll

Nach diesem Vorverarbeitungsschritt wird PI* als Eingabe für das PACE-Protokoll genutzt. PI* wird dabei implizit mit PI verglichen durch die Durchführung des PACE-Protokolls. Sollten PI* und PI nicht übereinstimmen, schlägt das PACE-Protokoll fehl. Hinsichtlich der Entropie (Tabelle 1) bietet PI hinreichend Entropie im Vergleich zu der bei PACE verwendeten sechsstelligen nummerischen PIN, $\log_2(10^6) \approx 20$ Bits Entropie.

5 eIDAS

eIDAS basiert stark auf den Protokollen und der Infrastruktur die auch bei elektronischen maschinenlesbaren Reisedokumenten (eMRTD) zum Einsatz kommt [BSI12]. Aktuell existiert die eIDAS Token Funktionalität nur als Zusatzfunktionen nationaler ID Karten. Dennoch muss ein eIDAS Token nicht zwangsläufig ein eMRTD sein, sondern kann auch ein eigenständiges Token sein oder z.B. Teil eines Führerscheins.

5.1 eIDAS Sicherheitsziele

Zwischen zwei Entitäten (z.B. einem Benutzer und einer Bank mit einem eID nutzenden Dienst) bietet eIDAS gegenseitige Authentisierung und Schlüsselvereinbarung, um einen sicheren kryptografischen Kanal aufzubauen. Einerseits kann dadurch der Benutzer sicher sein, dass er mit seiner Bank kommuniziert und die Bank kann sich sicher sein dass sie mit einem Benutzer kommuniziert der ein gültiges eIDAS Token besitzt. Andererseits einigen sich Benutzer und Bank während dem eIDAS Verfahren auf ein gemeinsames flüchtiges Geheimnis um einen sicheren Kanal zwischen den beiden Parteien aufzubauen um jegliche weitere Kommunikation abzusichern.

5.2 eIDAS Provider Authentisierung

Die eIDAS Provider Authentisierung entspricht dem Terminal Authentication (TA) Protocol aus dem eMRTD Bereich. Nach der Durchführung des TA-Protokolls kann sich der eIDAS Token Besitzer sicher sein über die Authentizität des eID Service Providers, mit dem er kommuniziert, und kennt auch dessen Zugriffsrechte. Zusätzlich erhält er einen authentischen, flüchtigen öffentlichen Schlüssel des eIDAS Providers. Das TA Protokoll ist in Abbildung 8 abgebildet. Nachdem das TA-Protokoll erfolgreich durchgeführt wurde, wird der Name des

eIDAS Providers aus dessen Zertifikat extrahiert und dem Benutzer präsentiert. Dies kann entweder durch ein separates Display am eIDAS Token Lesegerät erfolgen oder am Benutzerendgerät selbst. Der Benutzer muss nun aktiv bestätigen, dass er seine persönlichen Daten mit dem Provider entsprechend dessen Zugriffsrechte teilen möchte. Dies kann z.B. durch das Drücken eines Knopfes am eIDAS Token Lesegerät erfolgen oder dialoggeführt auf dem Benutzerendgerät.

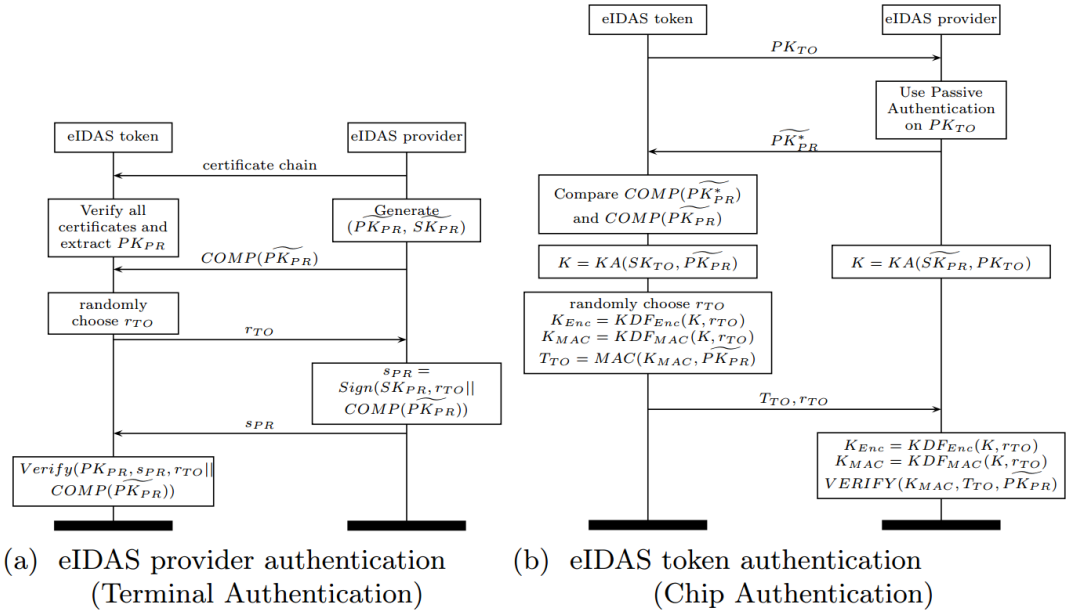

Abb. 8: Die eIDAS Protokolle

5.3 eIDAS Token Authentisierung

Das Protokoll Chip Authentication (CA) wird dazu verwendet um die Echtheit des eIDAS Tokens gegenüber dem eIDAS Service Provider sicherzustellen. Während dem CA-Protokoll werden Sitzungsschlüssel zwischen dem eIDAS Token und dem eIDAS Service Provider ausgehandelt. Um seine Echtheit zu beweisen, verfügt jedes eIDAS Token über einen statischen Diffie-Hellmann Schlüsselpaar wovon der private Schlüssel sicher im Speicher des nicht zugreifbaren Bereichs des eIDAS Tokens gespeichert ist. Der öffentliche Schlüssel wurde durch den eIDAS Token Hersteller während der Personalisierung signiert. Dies bedeutet dass der öffentliche Schlüssel mithilfe der Signing PKI und dem Passive Authentication Protokoll überprüft werden kann. Das CA Protokoll ist in Abbildung 8 dargestellt.

5.4 eIDAS Datenzugriff und Benutzer Authentisierung

Beide Parteien starten das Secure Messaging Protokoll neu mit den nun ausgehandelten Sitzungsschlüsseln. Der eIDAS Service Provider kann sich nun sicher sein, dass er mit einem echten eIDAS Token kommuniziert, aber er kann den Benutzer noch nicht eindeutig identifizieren. Dies liegt daran, dass der statische Diffie-Hellmann Schlüssel des eIDAS Tokens nicht eindeutig zwischen verschiedenen eIDAS Tokens ist. Das Mehrfachvorhandensein von eIDAS Token Schlüsseln ist Absicht, um zu verhindern, dass damit ein Tracking auf Basis der CA

Schlüssel durchgeführt wird. Um den eIDAS Token Benutzer eindeutig zu identifizieren werden im letzten Schritt vom eIDAS Service Provider die eigentlichen Chip Daten über den sicheren kryptografischen Kanal gelesen.

6 Fazit

In dieser Arbeit wurde der eIDAS Standard, welcher im Oktober 2013 durch ITRE harmonisiert wurde, adaptiert für vertrauenswürdiges eBanking und eBusiness, und erweitert um Privatsphäre konforme biometrisch authentisierte Transaktionen. Das vorgestellte System basiert vollständig auf standardisierten und beweisbar sicheren Protokollen, Infrastruktur und Technologien, was essenziell ist für jede Banken Transaktion Anwendung. Basierend auf der detaillierten Beschreibung und Nachforschungen um die beschriebenen Systemkomponenten, identifizieren wir eine signifikante Verbesserung des Benutzerkomforts und des Vertrauens gegenüber eBanking und eBusiness. Im Vergleich zu anderen Systemen sind die geschätzten Kosten vernachlässigbar für beide Parteien. Benutzer können größtenteils auf vorhandene Hardware zurückgreifen und Service Provider könnten auf eine bereits etablierte Infrastruktur zugreifen und zusätzlich Kosten für Hardware Support an Regierungsbehörden delegieren. Basierend auf den präsentierten Nachforschungen identifizieren wir eIDAS als einen Gewinn für zukünftige eBanking Dienste.

Literatur

[BSI13a] BSI: Technical Guideline TR-03110-2 Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token – Part 2 – Protocols for electronic IDentification, Authentication and trust Services (eIDAS), 2.20 beta edn. (9 2013)

[BSI13b] BSI: Technical Guideline TR-03110-4 Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token – Part 4 – Application and Profiles, 2.20 beta edn. (9 2013)

[BSI13c] BSI: Technical Guideline TR-03139 Common Certificate Policy for the Extended Access Control Infrastructure for Passports and Travel Documents issued by EU Member States, 2.1 edn. (5 2013)

[BSI12] BSI: Technical Guideline TR-03110-1 Advanced Security Mechanisms for Machine Readable Travel Documents – Part 1 – eMRTDs with BAC/PACEv2 and EACv1, 2.10 edn. (3 2012)

[AhGa10] S. Ahlswede, J. Gaab: eIDS in Europe – Not (yet) yielding profits for the cross-border financial services sector (9 2010), Deutsche Bank Research

[Trac12] Tractis – Negonation: World Map of eID deployments. *https://www.tractis.com/help/?p=3670* (12 2012)

[Comm13] Committee on Industry, Research and Energy: EU e-signature plan to make electronic deals safer and easier. *http://www.europarl.europa.eu/pdfs/news/expert/infopress/20131014IPR22239/20131014IPR22239_en.pdf* (10 2013)

[CaSt09a] A. Cavoukian, A. Stoianov: Biometric encryption: The new breed of untraceable biometrics. In: Biometrics: fundamentals, theory, and systems. Wiley (2009)

[CaSt09b] A. Cavoukian, A. Stoianov: Biometric encryption. In: Encyclopedia of Biometrics. Springer Verlag (2009)

[BRBB14] N. Buchmann, C. Rathgeb, H. Baier, C. Busch: Towards Electronic Identification and Trusted Services for Biometric Authenticated Transactions in the Single Euro Payments Area. In: Privacy Technologies and Policy. pp 172-190 (2014)

[ICAO06] ICAO: Doc 9303 Part 1 Machine Readable Passports Volume 2 Specifications for Electronically Enabled Passports with Biometric Identification Capability. International Civil Aviation Organization (ICAO), sixth edition edn. (2006)

[NORM09] C.T. NORMA: CSN 36 9791 ed. A – Information technology - Country Verifying Certification Authority Key Management Protocol for SPOC (12 2009)

[Euro13] European Payments Council (EPC): SEPA - Key Figures. *http://www.europeanpaymentscouncil.eu/* (10 2013)

[JaRo04] A.K. Jain, A. Ross, S. Prabhakar: An introduction to biometric recognition. IEEE Trans. on Circuits and Systems for Video Technology 14, 4–20 (2004)

[RaUh11] C. Rathgeb, A. Uhl: A survey on biometric cryptosystems and cancelable biometrics. EURASIP Journal on Information Security 2011(3) (2011)

[ViBB84] R. Viveros, K. Balasubramanian, N. Balakrishnan: Binomial and negative binomial analogues under correlated bernoulli trials. The American Statistician 48(3), 243–247 (1984)

[RaCB01] N.K. Ratha, J.H. Connell, R.M. Bolle: Enhancing security and privacy in biometrics-based authentication systems. IBM Systems Journal 40, 614–634 (2001)

[ICAO10] ICAO: Supplemental Access Control for Machine Readable Travel Documents. International Civil Aviation Organization (ICAO), 1.01 edn. (11 2010)

[ICAO13] ICAO: SUPPLEMENT to Doc 9303. International Civil Aviation Organization (ICAO), 13 edn. (10 2013)

[DMDK13] B. Deufel, C. Mueller, G. Duffy, T. Kevenaar: BioPACE – Biometric passwords for next generation authentication protocols for machine-readable travel documents. Datenschutz und Datensicherheit - DuD 37(6), 363 – 366 (2013)

[BRBP13] N. Buchmann, R. Peeters, H. Baier, A. Pashalidis: Security considerations on extending PACE to a biometric-based connection establishment. In: Biometrics Special Interest Group (BIOSIG), 2013 International Conference of the. pp. 1–13 (2013)

[RaCB01] N. Ratha, J. Connell, R. Bolle: An analysis of minutiae matching strength. In: Audio- and Video-Based Biometric Person Authentication, vol. 2091, pp. 223–228. Springer (2001)

[Daug06] J. Daugman: Probing the uniqueness and randomness of iriscodes: Results from 200 billion iris pair comparisons. Proc. of the IEEE 94(11), 1927–1935 (2006)

[AdYL06] A. Adler, R. Youmaran, S. Loyka: Towards a measure of biometric information. In: Canadian Conference on Electrical and Computer Engineering, (CCECE'06). pp. 210–213 (2006)