EGIZ

www.egiz.gv.at
E-Mail: post@egiz.gv.at
Telefon: ++43 (316) 873 5514
Fax: ++43 (316) 873 5520
Inffeldgasse 16a / 8010 Graz / Austria

Evaluierung mobiler Signaturlösungen auf Smartphones

Version 1.4, 24. April 2012

Thomas Zefferer, Peter Teufl – {thomas.zefferer, peter.teufl}@egiz.gv.at

Zusammenfassung: In Österreich ist zur mobilen Signaturerstellung seit einigen Jahren die Handy-Signatur erfolgreich im Einsatz und erfreut sich stetig wachsender Verbreitung und Beliebtheit. Durch die raschen Fortschritte mobiler Technologien sind auch die im Rahmen der Handy-Signatur zum Einsatz kommenden mobilen Endgeräte der Benutzerinnen und Benutzer einer ständigen Weiterentwicklung unterworfen. Daraus ergeben sich neue Möglichkeiten und Herausforderungen, die in Zukunft für Verfahren der mobilen Signaturerstellung – und damit auch für die österreichische Handy-Signatur – von Bedeutung sein können.

Im Rahmen dieser Studie soll ein Überblick über existierende mobile Signaturverfahren erarbeitet und mögliche zukünftige Entwicklungen skizziert werden. Dies soll in Ergänzung zur Handy-Signatur einen Überblick über den aktuellen Stand der Technik und über aktuelle internationale Lösungen geben. Für einen umfassenden Überblick wird zunächst die Relevanz mobiler Signaturlösungen motiviert und ein kurzer historischer Überblick über die Entwicklung von Verfahren zur Erstellung mobiler elektronischer Signaturen gezeigt. Da im Laufe der Jahre unterschiedliche Ansätze der mobilen Signaturerstellung entwickelt wurden, existieren verschiedene Möglichkeiten vorhandene Verfahren zu klassifizieren. Einige in der Literatur verwendete Ansätze werden in dieser Studie ebenfalls vorgestellt.

Aktuelle Implementierungen mobiler Signaturlösungen folgen einer Reihe von Standards und Spezifikationen. Die wichtigsten dieser Dokumente werden in dieser Studie überblickmäßig beschrieben und deren Relevanz für mobile Signaturlösungen diskutiert. Um einen Überblick über die aktuelle Verbreitung mobiler Signaturlösungen in Europa zu schaffen, werden im Folgenden verschiedene in Europa zur Anwendung kommende Verfahren beschrieben und diskutiert. Die beiden aktuell vorherrschenden Ansätze – die österreichische Handy-Signatur und Verfahren, die auf dem von ETSI spezifizierten Mobile Signature Service (MSS) Standard beruhen – werden näher analysiert und miteinander verglichen. Besonderes Augenmerk wird dabei auf eine Verwendbarkeit der verschiedenen Ansätze auf aktuellen Smartphone-Plattformen gelegt. Diese bieten einerseits neue Möglichkeiten der mobilen Signaturerstellung, können unter Umständen aber auch die Sicherheit bestehender Ansätze gefährden. Um eine sichere Verwendung mobiler Signaturlösungen auch auf Smartphones zu gewährleisten, werden in dieser Studie verschiedene Möglichkeiten diskutiert bestehende Signaturlösungen zu adaptieren um diese für einen sicheren zukünftigen Einsatz zu wappnen.

Inhaltsverzeichnis:

Abbildungsverzeichnis

Revision History

Version	Datum	Autor(en)	
0.1	02.12.2011	Thomas Zefferer	Dokumentstruktur
0.2	21.12.2011	Thomas Zefferer	Draft
0.3	30.12.2011	Peter Teufl	Überarbeitung
1.0	03.01.2012	Thomas Zefferer	Finalisierung
1.1	10.01.2012	Herbert Leitold	Review
1.2	12.01.2012	Peter Teufl, Thomas Zefferer	Überarbeitung
1.3	29.03.2012	Thomas Zefferer	Korrektur Layout
1.4	24.04.2012	Thomas Zefferer	Korrektur Nummerierung

1 Einleitung

1.1 Motivation

Mobilfunktechnologien haben in den letzten Jahren ein beeindruckendes Wachstum erfahren und erfreuen sich nach wie vor außerordentlicher Beliebtheit. Mobiltelefone haben sich mittlerweile zu einem ständigen Begleiter und hilfreichem Werkzeug in vielen Situationen des täglichen Lebens entwickelt. Neben dem privaten Sektor, welcher die anhaltende Popularität mobiler Technologien hauptsächlich zur Umsatzsteigerung zu nutzen versucht, setzt in zunehmenden Maße auch der öffentliche Bereich auf mobile Ansätze. Die Popularität und Vertrautheit mobiler Technologien soll dabei einerseits die Effizienz und Benutzerfreundlichkeit von E-Government-Verfahren steigern, andererseits soll durch den Einsatz mobiler Lösungen auch die Sicherheit von E-Government Anwendungen weiter erhöht werden.

Im Bereich des M-Government – dieser Begriff umfasst die Verwendung mobiler Technologien in E-Government Anwendungen – ist vor allem die sichere Erstellung von elektronischen Signaturen von zentraler Bedeutung. Mobiltelefone schienen für diese Aufgabe von jeher geeignet, da sie einerseits einen zusätzlichen Kommunikationskanal zu Benutzern ermöglichen und andererseits potentiell in der Lage sind sichere Signaturerstellungseinheiten in Form von Secure Elements zu integrieren. Aufgrund dieser Vorteile waren Verfahren zur Erstellung elektronischer Signaturen unter Verwendung mobiler Endgeräte bereits früh verfügbar.

Ein erster rudimentärer Überblick über vorhandene Verfahren und Technologien für bzw. konkrete Umsetzungen von mobilen Signaturlösungen wurde bereits im Rahmen des EGIZ Projekts „Grundsatzpapier Mobile Signatur“ [1] erarbeitet. Im Rahmen des EU LSP STORK wurden ebenfalls mobile eID und Signaturlösungen verschiedener europäischer Länder diskutiert [23]. Seitdem fanden auf dem mobilen Sektor zahlreiche neue Entwicklungen statt, die unter anderem zum Ausbau leistungsfähiger mobiler Kommunikationsnetze und zur Einführung leistungsstarker mobiler Endgeräte führten. Die Entwicklung leistungsfähiger Handhelds wurde anfangs vor allem von Apple[1] durch die Markteinführung des Apple iPhone[2] vorangetrieben. Die Kombination aus Funktionsvielfalt und Benutzerfreundlichkeit trug hauptsächlich zum Erfolg dieses Produkts und des generellen Konzepts Smartphone bei und zwang die Mitbewerber zur Entwicklung konkurrenzfähiger Produkte. Heute teilen sich mehrere Anbieter den umkämpften Smartphone-Markt und tragen durch laufende Innovationen zur rasanten Weiterentwicklung aktueller Smartphone-Plattformen bei.

Existierende mobile Signaturlösungen beruhen zumeist auf relativ einfachen GSM basierten Technologien. Obwohl diese natürlich bei einer Verwendung von Smartphones weiterhin verfügbar sind, können sich durch die besonderen Eigenschaften von Smartphones vor allem in Hinblick auf Sicherheitsanforderungen neue Herausforderungen ergeben. Im Rahmen dieser Studie sollen daher zunächst aktuelle Verfahren zur Erstellung elektronischer Signaturen recherchiert werden. Dabei sollen sowohl bereits in produktiver Anwendung befindliche Lösungen, als auch im Rahmen von wissenschaftlichen Publikationen vorgestellte Verfahren berücksichtigt werden. Die gesammelten Verfahren werden im Anschluss verglichen und analysiert, wobei besonderes Augenmerk auf deren Verwendbarkeit auf Smartphone-Plattformen gelegt wird. Für die gefundenen Probleme werden entsprechende Lösungsvorschläge erarbeitet.

[1] http://www.apple.com/

[2] http://www.apple.com/iphone/

1.2 Rückblick

Die Aussicht auf diverse Anwendungsgebiete für mobile Signaturlösungen löste in den Anfängen der Mobilfunkära einen beachtlichen Hype aus. Um das Jahr 2000 formierten sich zahlreiche Organisationen und Gruppierungen, in denen zumeist Repräsentanten der Privatwirtschaft vertreten waren, die zum Ziel hatten, gemeinsame Interessen bei der Entwicklung mobiler Signaturlösungen zu vertreten. Eine Übersicht über Aktivitäten in diesem Zeitraum findet sich im TÜViT-Arbeitspapier „Mobile elektronische Signaturen“ [2]. Folgende Organisationen versuchten in den Anfängen der mobilen Signatur initiativ zu werden und entsprechende Standards zu etablieren.

- **mSign Konsortium:** Das mSign Konsortium setzte sich aus über 50 Unternehmen der IT- und Telekommunikationsbranche zusammen und verfolgte das Ziel einer Standardisierung von mobilen Signaturlösungen. Die vom mSign Konsortium definierten Standards sehen die SIM-Karte des mobilen Geräts als Signaturerstellungseinheit vor. Die Kommunikation mit zentralen Komponenten basiert auf dem WAP-Protokoll. Der vom mSign Konsortium definierte Standard zielte vor allem auf eine Verwendung im Bereich des e-Commerce ab [4].

- **MoSign:** Die Initiative zum MoSign Projekt ging vom Bankensektor aus [3]. Involviert waren unter anderem die Deutsche Bank, Commerzbank AG, Dresdner Bank AG und HypoVereinsbank AG. Ziel war die Nutzung von Bankkarten als sichere Signaturerstellungseinheiten im Rahmen mobiler Signaturerstellungsvorgänge. Als mobiles Endgerät war ein Siemens IC35 Organizer mit integriertem WAP Browser und Kartenlesegerät vorgesehen.

- **MeT:** Die Mobile electronic Transaction (MeT) Initiative hatte zum Ziel die Entwicklungen des m-Commerce Marktes zu homogenisieren. Damit sollte für Benutzer eine einigermaßen einheitliche Bedienung verschiedener m-Commerce Lösungen erreicht werden. Die MeT Initiative ging hauptsächlich von führenden Herstellern von Mobiltelefonen aus. MeT hatte unter anderem das Ziel das mobile Gerät in ein sogenanntes Personal Trusted Device (PTD) überzuführen.

Die anfängliche Euphorie für mobile Signaturlösungen wich bald darauf einer Phase der Ernüchterung. Geringe Benutzerakzeptanz und komplexe sicherheitstechnische Vorgaben trugen dazu bei, dass zunächst nur wenige Vorhaben tatsächlich in die Praxis umgesetzt wurden. Erste praktische Erfahrungen mit mobilen Signaturlösungen wurden mit den folgenden Projekten gewonnen.

- **BankID:** In Norwegen entwickelte der Mobilfunkbetreiber Telenor[3] bereits in den Jahren 2000 und 2001 eine mobile Signaturlösung. Diese basierte auf speziellen von Gemalto[4] und Giesecke & Devrient[5] hergestellten SIM-Karten, die in der Lage waren Signaturen am mobilen Endgerät zu erzeugen. Alle ab 2001 von Telenor ausgegebenen SIM-Karten waren mit dieser Funktionalität ausgestattet und in der Lage RSA Signaturen gemäß dem PKCS#1 Standard zu erzeugen. Der öffentliche Schlüssel des Benutzers und das entsprechende Signaturzertifikat waren auf einem zentralen Server hinterlegt und über die ID der SIM-Karte mit dem entsprechenden auf der SIM-Karte hinterlegten privaten Schlüssel verlinkt. Im Jahr 2006 wurde der

[3] http://www.telenor.no

[4] http://www.gemalto.com

[5] http://www.gi-de.com

Betrieb des Dienstes aufgrund geringer Benutzerzahlen an einige norwegische Banken übergeben und unter dem Namen BankID neu gestartet.

- **Sonera SmartTrust Mobile Signature:** Bereits im Jahr 1999 wurde von den Unternehmen Sonera SmartTrust und Ericsson eine mobile Signaturlösung verlautbart[6]. Das aus Sonera SmartTrust hervorgegangene Unternehmen SmartTrust[7], das mittlerweile Teil der Giesecke & Devrient GmbH ist, ist auch heute noch im Bereich mobiler Sicherheitslösungen tätig und bietet beispielsweise entsprechende Zertifizierungen von SIM-Karten an. Der finnische Mobilfunkbetreiber Sonera war 2005 in Finnland auch eng in den Aufbau erster mobiler Signaturlösungen involviert[8].

- **M-Trust Server:** Die M-Trust Server Technologie von Brokat basierte auf den Standards des mSign Konsortiums [5]. Dementsprechend kam zwischen Netzbetreiber und Diensteanbieter ein XML basiertes Kommunikationsprotokoll zur Anwendung. Für die Erstellung elektronischer Signaturen wurde die Funktionalität der SIM-Karte herangezogen. Die Brokat Technologies AG musste im Jahr 2001 Insolvenz anmelden, wodurch auch der Fortbestand des M-Trust Servers nicht mehr gewährleistet war.

- **TruPoSign:** Im Rahmen des TruPoSign Projekts [6] wurde eine PDA basierte Lösung zur Erstellung mobiler Signaturen entwickelt. Die Idee hinter diesem Ansatz war die vollständige Auslagerung des Signaturerstellungsprozesses auf ein mobiles Gerät, von welchem Sicherheitsanforderungen einfacher erfüllt werden können als etwa von einem PC. TruPoSign sah sowohl biometrische Authentifizierungsmethoden als auch eine Integration von Smartcards als Signaturerstellungseinheiten vor.

Diese frühen Aktivitäten im Bereich der mobilen Signaturerstellung zeugen vom regen Interesse, das seit jeher an dieser Technologie besteht. Obwohl sich in den letzten zehn bis fünfzehn Jahren sowohl Mobilfunktechnologien als auch mobile Endgeräte signifikant geändert und eine rasante Weiterentwicklung erfahren haben, sind die Herausforderungen an mobile Signaturlösungen im Großen und Ganzen gleich geblieben. Die schwierigste Aufgabe ist nach wie vor die geeignete Absicherung des Signaturerstellungsprozesses, um diesen gegen Missbrauch und Angriffe von außen zu schützen. Zentrales Element ist in diesem Zusammenhang eine sichere Signaturerstellungseinheit (Secure Signature Creation Device - SSCD), wie sie beispielsweise für qualifizierte Signaturen in der Signaturrichtlinie der Europäischen Union [7] vorgeschrieben ist. Die entsprechende Implementierung eines SSCD auf mobilen Geräten ist auch heute noch von zentraler Bedeutung. Verschiedene Möglichkeiten werden im Rahmen dieser Studie näher beleuchtet, analysiert und miteinander verglichen.

1.3 Abgrenzung

Der Begriff der mobilen Signatur ist mit unterschiedlichen Technologien und Verfahren verknüpft. Häufig wird der Begriff der mobilen Signatur in Zusammenhang mit sogenannten

[6] http://findarticles.com/p/articles/mi_m0EIN/is_1999_Oct_11/ai_56187223/

[7] http://www.smarttrust.com/

[8] Siehe auch Abschnitt 4.2.3.

Signature Capturing Verfahren[9,10] genannt. Diese Verfahren erlauben Benutzern die Erbringung handschriftlicher Unterschriften auf mobilen Geräten. Meist kommt dafür ein Stylus o.ä. zur Anwendung. Manche Anbieter derartiger Systeme erlauben auch die automatisierte Überprüfung erbrachter Unterschriften mit hinterlegten Unterschriftproben. Fortgeschrittene Ansätze bedienen sich auch stochastischer Modelle (z.B. Hidden Markov Model) zur Validierung derartiger Unterschriften [8].

Im Rahmen dieser Studie werden ausschließlich mobile Signaturlösungen betrachtet, denen kryptographische Methoden der Signaturerstellung zugrunde liegen. Besonderes Augenmerk wird dabei auf jene Lösungen gelegt, die den Anforderungen einer qualifizierten Signatur entsprechen und sich damit besonders für einen Einsatz im Bereich des E-Government oder M-Government eignen.

1.4 Methodik

Grundlage dieser Studie war eine ausgedehnte Recherche über Möglichkeiten der mobilen Signaturerstellung. Hauptaugenmerk wurde dabei auf jene Ansätze gelegt, die eine Erstellung qualifizierter elektronischer Signaturen ermöglichen, da diesen speziell bei Anwendungen im Bereich E-Government eine besondere Bedeutung zukommt. Basierend auf den Resultaten dieser Recherche, welche im Rahmen dieser Studie ausführlich beschrieben und diskutiert werden, wurden schließlich jene Ansätze extrahiert, die aktuell die weiteste Verbreitung in Europa finden. Diese Ansätze wurden näher analysiert und im Speziellen im Kontext von modernen Smartphone-Plattformen auf Sicherheitsrisiken hin untersucht. Basierend auf dieser Analyse wurden schließlich diverse Vorschläge zur Erweiterung dieser Ansätze erarbeitet.

1.5 Dokumentstruktur

Der Aufbau dieser Studie folgt im Wesentlichen den in Abschnitt 1.4 beschriebenen Schritten. In Abschnitt 1 wurde die Relevanz mobiler Signaturlösungen diskutiert und ein kurzer Rückblick auf die bisherige Entwicklung mobiler Signaturlösungen gewährt. Im Folgenden widmet sich Abschnitt 2 der Klassifizierung von Verfahren der mobilen Signaturerstellung und stellt verschiedene Ansätze der Kategorisierung unterschiedlicher Methoden vor. Relevante Spezifikationen und Standards, die im Rahmen mobiler Signaturerstellungsverfahren eine Rolle spielen, werden in Abschnitt 3 näher beleuchtet. Abschnitt 4 fasst die aktuelle Situation mobiler Signaturlösungen in Europa zusammen und beschreibt verschiedene produktive Lösungen, Pilotprojekte und Initiativen einzelner Länder. Die beiden vorherrschenden Ansätze der mobilen Signaturerstellung werden in weiterer Folge in Abschnitt 5 analysiert, miteinander verglichen und im Kontext moderner Smartphone-Technologien betrachtet. Basierend auf den Resultaten dieser Analyse werden schließlich in Abschnitt 6 mögliche Forschungsfelder identifiziert. Die wichtigsten Erkenntnisse dieser Studie werden schlussendlich in Abschnitt 7 zusammengefasst.

[9] http://www.xyzmo.com/de/Pages/xyzmostart.aspx

[10] http://creativesolving.co.uk/mobile_sign.aspx

2 Klassifizierungen

Im Laufe der Jahre wurden verschiedene Ansätze erarbeitet, wie mobile Signaturen durch oder mit Hilfe von mobilen Endgeräten umgesetzt werden könnten. Einige dieser Ansätze blieben rein theoretischer Natur, die meisten wurden zumindest prototypisch umgesetzt und im Rahmen von Pilotanwendungen getestet und evaluiert. Nur wenige Vorschläge schafften es schließlich eine breite Akzeptanz und den Weg in eine produktive Anwendung zu finden.

In zahlreichen wissenschaftlichen Publikationen wird versucht, die Vielzahl von Ansätzen zur Erstellung mobiler Signaturen entsprechend zu klassifizieren, um einen Überblick über die verschiedenen Verfahren zu gewinnen. Abhängig von den Autoren bzw. vom Veröffentlichungszeitraum dieser Publikationen können die vorgenommenen Klassifizierungen durchaus unterschiedlich ausfallen. Eine qualitative Bewertung der verschiedenen Ansätze zur Klassifizierung mobiler Signaturerstellungsverfahren erscheint schwierig. Im Folgenden sollen daher Klassifizierungen, die in verschiedenen wissenschaftlichen Publikationen von verschiedenen Autoren vorgenommen wurden, kurz vorgestellt werden.

2.1 Klassifizierung nach Rossnagel (2004)

Bereits im Jahr 2004 verwendet u.a. Rossnagel eine grundlegende Klassifizierung von Methoden der mobilen Signaturerstellung [9], indem er diese in serverseitige (server based) und clientseitige (client based) Verfahren unterteilt. Die Unterscheidung erfolgt gemäß dem Ort der Signaturerstellung. Bei serverseitigen Verfahren wird die elektronische Signatur in einem zentralen Server berechnet. Bei clientseitigen Lösungen kommt dafür das mobile Gerät des Benutzers zur Anwendung. Abbildung 1 zeigt die von Rossnagel in [9] verwendete Klassifizierung mobiler Signaturerstellungsansätze.

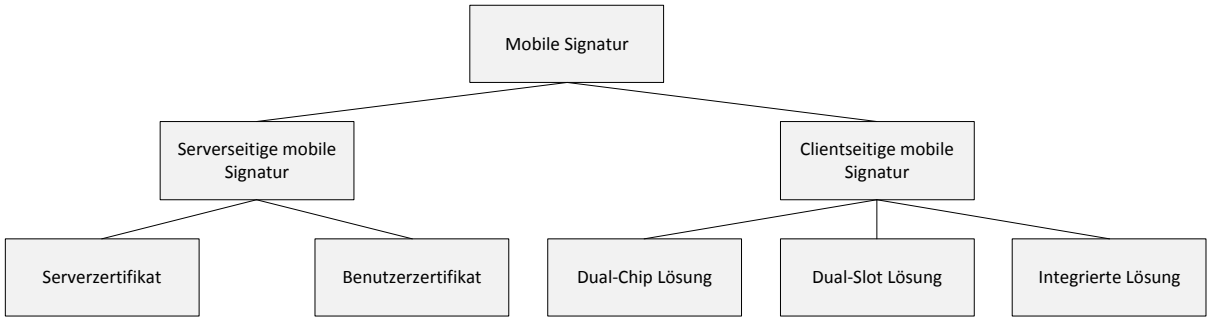

Abbildung 1. Klassifizierung mobiler Signaturen nach Rossnagel.

Bei serverseitigen mobilen Signaturlösungen unterscheidet Rossnagel in weiterer Folge zwei Varianten bezüglich des verwendeten Signaturzertifikats. Soll zur Signaturerstellung ein auf den Benutzer ausgestelltes Zertifikat verwendet werden, muss dieses und der private Signaturschlüssel des Benutzers zunächst an den Server übertragen werden. Rossnagel schließt, dass dies den Anforderungen an eine qualifizierte Signatur gemäß Signaturrichtlinie [7] widerspricht. Die Gruppe, die auch die Schutzprofile zu sicheren Signaturerstellungseinheiten (SSCD) erstellt hat, war schon in den im Jahr 2002 veröffentlichten Umsetzungsrichtlinien zu SSCDs[11] der Meinung, dass die Implementierung von Signaturservern technisch möglich sind und nicht der Richtlinie widersprechen. Einzig das Schutzprofil ist nicht an solchen Diensten orientiert. Zu einem ähnlichen Schluss kommt 2005 mit FESA die Vereinigung der Aufsichtsstellen zur Signatur [24]. Mit der Einführung der Handy-Signatur in Österreich wurde endgültig gezeigt, dass serverbasierte

[11] ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/cwa14355-00-2004-Mar.pdf

Signaturerstellungsverfahren sehr wohl in der Lage sind qualifizierte elektronische Signaturen zu erzeugen.

Laut Rossnagel können fortgeschrittene elektronische Signaturen mit qualifizierten Zertifikaten erstellt werden, die auf den Server selbst ausgestellt sind. Dies entspricht der zweiten Variante serverseitiger mobiler Signaturlösungen. In diesem Fall werden jedoch keine persönliche Signaturen von Benutzern erzeugt. Es kann daher nicht verifiziert werden, ob die Signatur tatsächlich vom Benutzer autorisiert wurde.

Clientseitige mobile Signaturlösungen verwenden ein sicheres Signaturerstellungsgerät, welches sich im mobilen Endgerät des Benutzers befindet. Rossnagel unterscheidet clientseitige mobile Signaturlösungen bezüglich der Integration dieser Signaturerstellungseinheit in das mobile Endgerät. Folgende Varianten werden dafür genannt:

- **Dual-Chip Lösung:** Die ursprüngliche SIM-Karte wird durch eine Signaturkarte, welche als sichere Signaturerstellungseinheit fungiert, ersetzt.
- **Dual-Slot Lösung:** Die Signaturkarte wird zusätzlich zur SIM Karte über ein zweites Kartenlesegerät im Gerät integriert.
- **Integrierte Lösung:** Hierbei wird eine einzige Karte verwendet, die sowohl die Funktionalität des SIM als auch jene der Signaturkarte implementiert.

2.2 Klassifizierung nach Ruiz-Martínez et al. (2007)

Im Journal of Theoretical and Applied Electronic Commerce Research[12] erschien im Jahr 2007 ein Artikel von Antonio Ruiz-Martínez et al. [10], der sich eingehend mit verschiedenen Ansätzen der mobilen Signaturerstellung beschäftigte und versuchte diese zu klassifizieren. Gemäß den Autoren dieses Artikels existieren verschiedene Kriterien, nach denen eine Klassifizierung vorgenommen werden kann (Technologien, Standards, etc.). Die Autoren entschlossen sich jedoch dazu eine Klassifizierung anhand der Ausführung der Signaturerstellungsgeräts vorzunehmen. Abbildung 2 zeigt die vier Hauptkategorien, in die Ruiz-Martínez et al. mobile Signaturlösungen unterteilen.

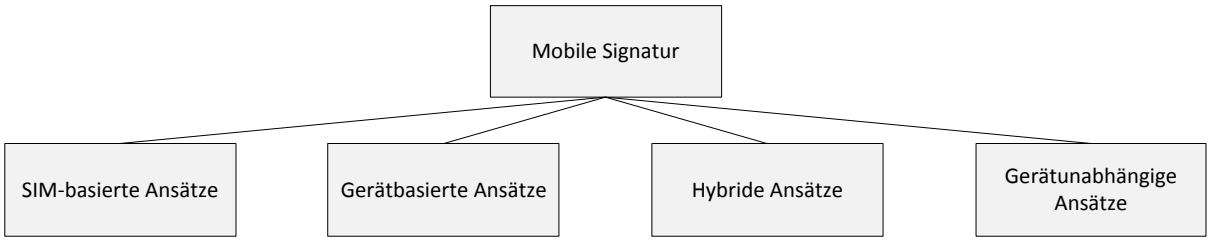

Abbildung 2. Klassifizierung nach Ruiz-Martínez et al.

Diese vier grundlegenden Ansätze werden von den Autoren in weiterer Folge in weitere Unterkategorien unterteilt. Die folgenden Unterabschnitte widmen sich diesen Unterkategorien im Detail.

2.2.1 SIM-basierte Ansätze

SIM-Karten bieten sich auf einen ersten Blick für die Erstellung mobiler elektronischer Signaturen an, da diese in jedem Mobiltelefon vorhanden sind und zudem die technischen Voraussetzungen für einen sicheren Signaturerstellungsvorgang erbringen. Ruiz-Martínez et al. unterscheiden vier Möglichkeiten elektronische Signaturen auf SIM-Karten zu erzeugen. Diese sind in Abbildung 3 dargestellt.

[12] http://www.jtaer.com/

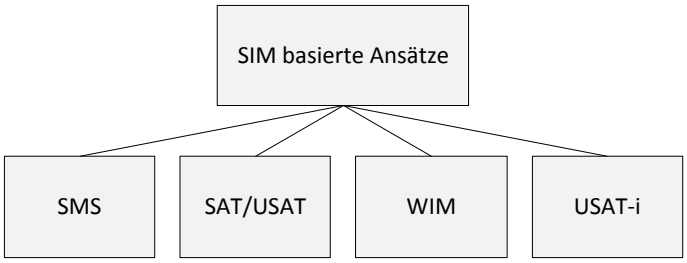

Abbildung 3. SIM-basierte Ansätze zur Erstellung elektronischer Signaturen.

Als einfachste Möglichkeit für die Erstellung elektronischer Signaturen auf SIM-Karten nennen Ruiz-Martínez et al. die Verwendung von sogenannten Security Headern zur Absicherung der SMS-Kommunikation. Da diese Technologie jedoch auf symmetrischen Schlüsseln, die vom Kartenhersteller auf die Karte aufgebracht werden, beruht und daher nicht unter der alleinigen Kontrolle des Benutzers sind, können über diesen Ansatz weder fortgeschrittene noch qualifizierte elektronische Signaturen erstellt werden.

Die SIM Application Toolkit (SAT) Technologie erweist sich diesbezüglich als bedeutend flexibler. Die SAT-Technologie erlaubt die Installation von Applikationen auf SIM-Karten. Diese Applikationen können einerseits mit dem Benutzer interagieren und andererseits mit dem GSM Netz Daten auf SMS-Basis austauschen. USAT (Universal SIM Application Toolkit) ist eine Weiterentwicklung der SAT-Technologie, speziell auf 3G Mobilfunktechnologien ausgelegt und unterstützt u.a. den Aufbau von HTTP-Verbindungen.

Der große Vorteil der SAT/USAT-Technologie liegt in der sichereren Ausführungsumgebung von Applikationen, da diese direkt auf der SIM-Karte und nicht im mobilen Gerät selbst installiert sind und auch dort ausgeführt werden. SAT/USAT-Applikationen können entweder im Zuge der Herstellung der SIM-Karte auf diese aufgebracht, oder zu einem späteren Zeitpunkt über ein OTA (Over the Air) Interface nachinstalliert werden.

Ruiz-Martínez et al. geben zu bedenken, dass über diesen Ansatz keine qualifizierten elektronischen Signaturen erzeugt werden können, da private Signaturschlüssel nicht über hardwaretechnische Sicherheitsmaßnahmen geschützt sind. Als weiterer Nachteil dieses Ansatzes wird die mäßige Performance von SAT-Applikationen bei rechenintensiven Operationen wie Schlüssel- oder Signaturerzeugung genannt.

Um SIM-Karten als sichere Signaturerstellungseinheiten betrachten zu können, müssen diese den Wireless Identity Module (WIM) Standard unterstützten. Der WIM-Standard definiert wie sicherheitskritische kryptographische Daten wie etwa private Signaturschlüssel sicher auf SIM-Karten gespeichert und wie elektronische Signaturen auf SIM-Karten sicher berechnet werden können. Das WIM selbst ist eine unabhängige Smartcard-Applikation, die im Prinzip durchaus mit SAT oder USAT Applikationen vergleichbar ist, jedoch über definierte Sicherheitsfeatures verfügt.

Als vierte Möglichkeit der Signaturerstellung in SIM-Karten nennen Ruiz-Martínez et al. die USAT-i Technologie. Wie der Name bereits suggeriert, handelt es sich auch hier um eine Weiterentwicklung der SAT/USAT Technologie. USAT-i Applikationen implementieren dabei einen Byte-Code-Interpreter, der Byte-Code über verkettete SMS-Nachrichten (oder optional auch andere Protokolle) empfängt und direkt auf der SIM-Karte ausführt. Über Plug-ins können USAT-i Applikationen auf kryptographische Funktionalität der SIM-Karte zugreifen und auf diese Weise Signaturen sicher erstellen.

2.2.2 Gerätbasierte Ansätze

Die Autoren des im Jahr 2007 erschienenen Surveys nennen Signaturen, die auf mobilen Geräten selbst erstellt werden, als weiteren möglichen Ansatz. Dabei gehen sie im Detail auf die in Abbildung 4 dargestellten Technologien Windows Mobile OS, Symbian OS und Java ME ein.

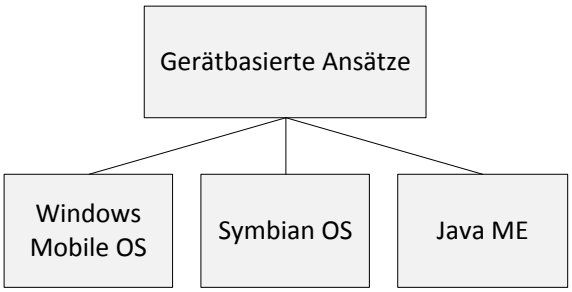

Abbildung 4. Gerätbasierte Ansätze zur Erstellung elektronischer Signaturen.

Zumindest die erste dieser drei Technologien muss zum heutigen Zeitpunkt bereits als überholt angesehen und soll daher nicht näher betrachtet werden. Java ME findet hingegen in zahlreichen Bereichen Anwendung und hat die Implementierung kryptographischer Anwendungen u.a. auf mobilen Geräten vereinfacht. Auch Symbian kann noch beachtliche Marktanteile aufweisen, dürfte aber in Zukunft eine zunehmend kleinere Rolle am globalen Markt spielen.

Auch wenn die in [10] genannten Technologien zum Teil überholt sind, so ist der generelle Ansatz elektronische Signaturen auf mobilen Geräten selbst zu erzeugen noch immer gültig. Vor allem durch den Siegeszug von Smartphones, die über beachtliche Rechenleistung und ein breites Spektrum an Features verfügen, scheint die Durchführung komplexer Berechnungen auf mobilen Endgeräten wieder zunehmend interessant. Klar ist jedoch auch, dass Mobiltelefone oder auch Smartphones ohne entsprechende Zusatzausstattung (z.B. Secure Elements) zum jetzigen Zeitpunkt keinesfalls als sichere Signaturerstellungseinheiten betrachtet werden können.

2.2.3 Hybride Ansätze

In der Praxis wird oft versucht, die Vorteile von SIM-basierten Ansätzen und jene von gerätebasierten Ansätzen zu kombinieren. Während am mobilen Gerät selbst sicherheitsunkritische Operationen ausgeführt werden, werden sicherheitskritische Operationen wie die Erstellung elektronischer Signaturen an das WIM der SIM-Karte delegiert. Derartige hybride Ansätze bedürfen einer entsprechenden Schnittstelle, über die Applikationen, die am mobilen Gerät ausgeführt werden auf die Funktionalität der SIM-Karte bzw. des WIM zugreifen können. Ruiz-Martínez et al. nennen zwei Technologien, die eine derartige Schnittstelle implementieren.

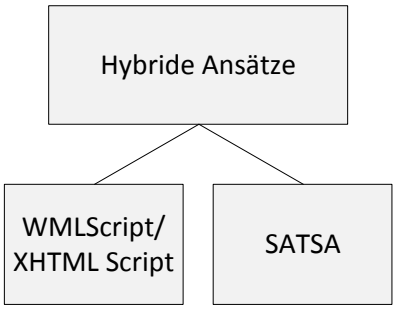

Abbildung 5. Hybride Ansätze zur Erstellung elektronischer Signaturen auf mobilen Geräten.

Die für die Erstellung mobiler Web-Applikationen geeigneten Sprachen Wireless Markup Language (WML) und XHTML verfügen über diverse Bibliotheken, die eine Ausführung diverser Prozesse auf mobilen Endgeräten erlauben. Laut [10] kann eine Crypto-Bibliothek dazu verwendet werden beliebigen Text über das im mobilen Gerät vorhandene WIM zu signieren.

Alternativ kann für mobile Applikationen, die auf Java ME basieren, die Security and Trust Services API (SATSA) verwendet werden. Auch diese API erlaubt eine Einbindung der Funktionalität einer SIM-Karte in mobile Anwendungen.

2.2.4 Geräteunabhängige Ansätze

Aus Gründen der Kosteneffizienz und um möglichst viele potentielle Benutzer bedienen zu können werden generell Signaturlösungen bevorzugt, die ohne Modifikation auf möglichst vielen mobilen Geräten anwendbar sind. Ruiz-Martínez et al. nennen zwei mögliche Varianten gerätunabhängiger Signaturlösungen.

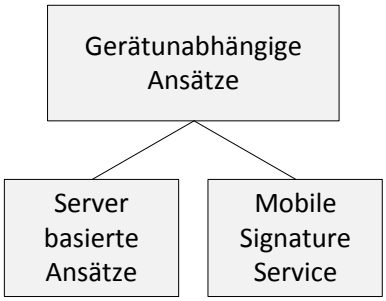

Abbildung 6. Gerätunabhängige Ansätze zur Erstellung mobiler elektronischer Signaturen.

Die Idee serverbasierter Signaturen stammt aus jener Zeit, in denen mobile Endgeräte über sehr eingeschränkte Rechen- und Speicherkapazitäten verfügten. Um rechenintensive kryptographische Operationen nicht auf mobilen Geräten ausführen zu müssen, wurden diese an einen zentralen Server delegiert. Elektronische Signaturen wurden zwar am Server erstellt, mussten jedoch vom Benutzer über das mobile Endgerät autorisiert werden. Diese Autorisierung wurde je nach Umsetzung über eine PIN, Mesage Authentication Codes (MAC) oder auch One-Time Signatures (OTS) umgesetzt.

Ruiz-Martínez et al. argumentieren in [10], dass mit diesem Ansatz keine qualifizierten Signaturen erstellt werden können, da die Signaturschlüssel zentral am Server gespeichert und daher nicht unter der alleinigen Kontrolle des Benutzers sind. Diese Behauptung wurde jedoch unter anderem durch die Einführung der österreichischen Handy-Signatur, welche im Prinzip ebenfalls diesem Ansatz folgt, widerlegt. Auch die FESA kam wie schon erwähnt bereits im Jahr 2005 zu dem Schluss, dass serverseitige qualifizierte Signaturen nicht prinzipiell ausgeschlossen werden können.

Als weiteren geräteunabhängigen Ansatz nennen Ruiz-Martínez et al. jene Lösungen, die dem Mobile Signature Service (MSS) Standard folgen. Dieser Standard und die ihm zugrundeliegenden Konzepte werden u.a. in Abschnitt 3.6 dieser Studie näher erläutert.

2.3 Klassifizierung nach Ruiz-Martínez et al. (2009)

In [11] schlagen Ruiz-Martínez et al. einen neuen Ansatz für eine mobile Signaturlösung vor. In der Einleitung ihres Artikels geben die Autoren erneut einen Überblick über bestehende Verfahren und klassifizieren Ansätze zur Erstellung mobiler Signaturen gemäß der in Abbildung 7 dargestellten Struktur.

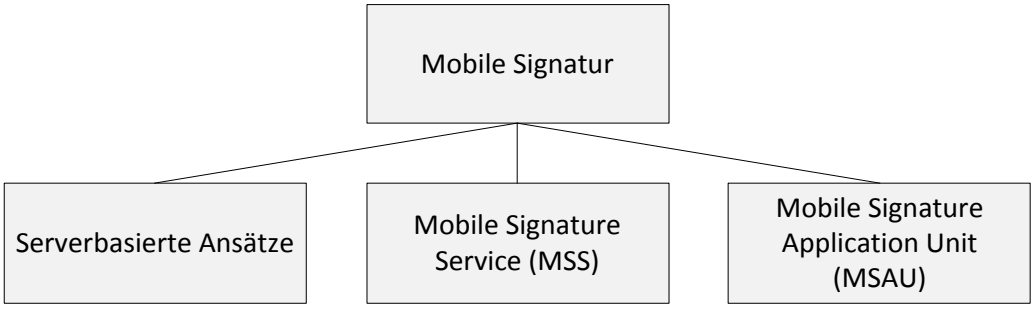

Abbildung 7. Vereinfachte Klassifizierung mobiler Signaturlösungen nach Ruiz-Martínez.

Ihre Definition von serverbasierten Ansätzen entspricht dabei weitgehend jener, die bereits in [10] vertreten und in Abschnitt 2.2.4 näher erklärt wurde.

Als zweiter Ansatz mobiler Signaturen wird erneut das von der ETSI standardisierte Mobile Signature Service (MSS) genannt. Dieses Verfahren, welches auf einer Signaturerstellung auf der SIM-Karte basiert, wird in Abschnitt 3.6 noch näher beleuchtet.

Als drittes Verfahren neben serverbasierten Ansätzen und Mobile Signature Services wird der MSAU Ansatz angegeben. MSAU steht für Mobile Signature Application Unit und wurde im Jahr 2007 von Evgenia Pisko [12] vorgestellt. Bei diesem Ansatz kommt eine mobile Applikation am mobilen Endgerät des Benutzers zur Anwendung. Services, die auf elektronischen Signaturen basieren, können mit dieser mobilen Applikation direkt kommunizieren und auf diese Weise mobile Signaturerstellungsprozesse anstoßen. Die Signatur selbst wird auf einer entsprechenden SIM-Karte berechnet. Die mobile Applikation kommuniziert mit dieser über die Java ME und SATSA Technologie. Durch die Verwendung einer sicheren Signaturerstellungseinheit können mit diesem Ansatz qualifizierte elektronische Signaturen erstellt werden.

2.4 Klassifizierung nach Samadani et al. (2010)

In [13] stellen Samadani et al. einen auf Proxy-Zertifikaten basierenden Ansatz zur Erstellung mobiler Signaturen vor. Als Einleitung zu dieser Arbeit geben die Autoren einen umfassenden Überblick über bestehende Lösungen und klassifizieren mobile Signaturlösungen generell in serverbasierte Ansätze und clientbasierte Ansätze (Abbildung 8).

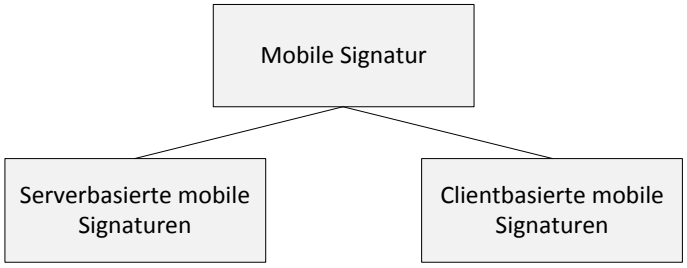

Abbildung 8. Generelle Klassifizierung von mobilen Signaturlösungen nach Samadani et al.

Ausgehend von dieser allgemeinen Klassifizierung nehmen die Autoren eine weitere Unterteilung vor, auf die in den folgenden Unterabschnitten näher eingegangen werden soll.

2.4.1 Serverbasierte mobile Signaturen

Wie Ruiz-Martínez et al. nennen auch Samadani et al. den Mangel an Rechen- und Speicherkapazität am mobilen Endgerät als Hauptgrund für den Einsatz von serverbasierten Signaturlösungen. Im Gegensatz zu anderen Autoren unterteilen Samadani et al. serverbasierte mobile Signaturlösungen in zertifikatsbasierte und zertifikatslose Ansätze.

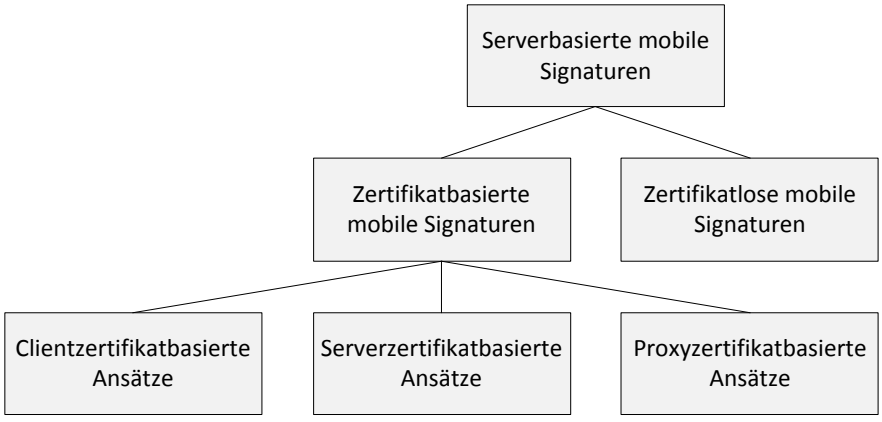

Abbildung 9. Klassifizierung serverbasierter mobiler Signaturlösungen nach Samadani et al.

Zertifikatsbasierte Signaturlösungen werden von Smadani et al. in drei Untergruppen unterteilt. Als Kriterium wird dabei der Inhaber des Zertifikats herangezogen. Demgemäß unterscheiden die Autoren clientzertifikatbasierte, serverzertifikatbasierte und proxyzertifikatbasierte Ansätze. Bei clientzertifikatbasierten Ansätzen übermitteln Benutzer ihren privaten Signaturschlüssel an einen zentralen Server, der in weiterer Folge Signaturen für diese Benutzer vornimmt. Qualifizierte elektronische Signaturen können mit diesem Ansatz nicht erzeugt werden[13]. Bei serverzertifikatbasierten Ansätzen erzeugt die Serverkomponente Signaturen in ihrem Namen. Eine persönliche Signatur des Benutzers kann daraus nicht abgeleitet werden. Proxyzertifikatsbasierte Ansätze verwenden zeitlich limitierte Proxyzertifikate um den Signaturerstellungsprozess an eine zentrale Instanz zu delegieren. Auch dieser Ansatz hat einige Schwachstellen, die die Erstellung qualifizierter Signaturen verhindern.

2.4.2 Clientbasierte mobile Signaturen

Bei clientbasierten Ansätzen wird die Signatur nicht in einem zentralen Server, sondern am mobilen Endgerät selbst erzeugt. Abhängig vom konkreten Ort der Signaturerstellung unterscheiden Samadani et al. drei Kategorien clientbasierter mobiler Signaturen (Abbildung 10).

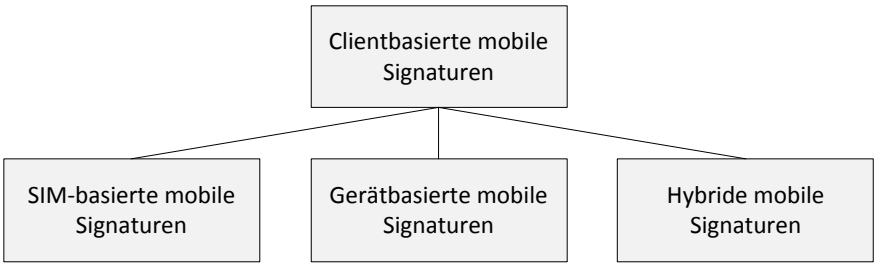

Abbildung 10. Klassifizierung clientbasierter mobiler Signaturlösungen nach Samadani et al.

SIM-basierte Ansätze verwenden die SIM-Karte eines Mobiltelefons für die Erstellung mobiler Signaturen. Die Autoren nennen SATSA- und WIM-basierte Lösungen als wichtige Vertreter dieser Kategorie. Gerätbasierte Ansätze, bei denen Signaturen ausschließlich am mobilen Gerät (ohne Miteinbeziehung einer sicheren Signaturerstellungseinheit wie etwa der SIM-Karte) erstellt werden, werden von Samadani et al. als schnell und bequem, zurecht jedoch auch als unsicher eingestuft. Als letzte Unterkategorie nennen die Autoren hybride Ansätze, bei denen die kryptographischen Schlüssel zwar sicher in der SIM-Karte gespeichert sind, die Signaturerstellung jedoch am mobilen Gerät vorgenommen wird und die Schlüssel daher aus der sicheren Umgebung ausgelesen werden müssen.

2.5 Schlussfolgerungen

Mobile Signaturen erfuhren bereits um die Jahrtausendwende einen ersten Hype, welchem aber relativ rasch eine Phase der Ernüchterung folgte. Grund dafür waren unter anderem hinter den Erwartungen zurückbleibende Benutzerzahlen. Nichtsdestotrotz wurden auch nach Abklingen der ersten Euphorie ständig neue und verbesserte Ansätze zur sicheren Erstellung mobiler Signaturen entwickelt und vorgestellt. Mit dem Hinzukommen neuer Verfahren wurde auch die Klassifizierung mobiler Signaturlösungen laufend adaptiert und verfeinert. In diesem Abschnitt wurde versucht diese Entwicklung anhand ausgewählter Publikationen und er darin vorgenommenen Unterteilungen mobiler Signaturlösungen zu veranschaulichen.

[13] Für qualifizierte elektronische Signaturen muss gewährleistet sein, dass der Signator die Mittel zur Signaturerstellung (d.h. den privaten Schlüssel) stets unter alleiniger Kontrolle halten kann. Bei einer Übermittlung des privaten Schlüssels an einen Server ist diese Anforderung nicht mehr erfüllt.

Die von Samadani et al. im Jahr 2010 vorgenommene Klassifizierung ist aus heutiger Sicht wohl eine der umfangreichsten und vollständigsten Methoden zur Kategorisierung verschiedener Ansätze der mobilen Signaturerstellung. Generell ist allen näher betrachteten Klassifizierungen gemein, dass mobile Signaturlösungen grundsätzlich in serverbasierte und clientbasierte Ansätze unterteilt werden. Beide Ansätze haben diverse Vor- und Nachteile, die im Rahmen dieses Dokuments anhand konkreter Umsetzungen analysiert werden sollen.

3 Standards

Um eine Vereinheitlichung mobiler Signaturlösungen zu erreichen wurde seit jeher versucht bewährte Ansätze zur mobilen Signaturerstellung über internationale Standards zu definieren. In diesem Abschnitt soll ein Überblick über einige relevante Spezifikationen gegeben werden. Hauptaugenmerk wird dabei auf internationale Standards gelegt. Auf nationale Spezifikationen, die ausschließlich für nationale Signaturlösungen des jeweiligen Herkunftslands Bedeutung haben, wird nicht näher eingegangen. Diese werden im Rahmen der Diskussion konkreter Implementierungen in Abschnitt 4 dieses Dokuments ergänzend erwähnt.

In einer von SURFnet[14] durchgeführten Studie wurden Sicherheitsaspekte mobiler Signaturlösungen näher beleuchtet [14]. Diese Studie enthält auch eine umfassende Auflistung von Standards, die für die Erstellung mobiler Signaturen und die Installation mobiler PKI von Relevanz sind. Relevante Standards werden von den Autoren dieser Studien in verschiedene Kategorien unterteilt. Diese und andere relevante Standards sollen in den folgenden Unterabschnitten näher diskutiert werden.

3.1 Standards zu serverbasierten Signaturen

Obwohl es bereits zahlreiche Implementierungen serverseitiger Signaturlösungen gibt, sind diesbezügliche internationale Standards und Spezifikationen eher rar. Relevant ist in jedem Fall der von OASIS publizierte Digital Signature Service Standard (OASIS-DSS)[15]. Dieser Standard spezifiziert im Wesentlichen die Verwendung eines serverbasierten Signaturservices. Im Rahmen mobiler Signaturlösungen findet dieser Standard bis dato jedoch wenig Anwendung.

3.2 Smartcard-Standards

Smartcard-Standards spielen vor allem bei clientseitigen mobilen Signaturlösungen, bei denen die elektronische Signatur direkt am Mobiltelefon (oder einem anderen mobilen Gerät) berechnet wird, eine zentrale Rolle. Sowohl bei der Kommunikation mit der SIM-Karte, als auch für die Interaktion mit zusätzlichen am mobilen Gerät vorhandenen Secure Elements kommen diese Standards zur Anwendung. Folgende Smartcard-Standards sind dabei von besonderer Relevanz:

- **ISO 7816 Reihe:** Die Standards der ISO 7816 Reihe[16] definieren Aufbau, Funktionalität und Kommunikationsschnittstellen von Smartcards. Diese Definitionen reichen von physikalischen Spezifikationen über die Spezifikation von Kommunikationsprotokollen bis hin zur möglichen Implementierung von PKI-Token.
- **Java Card:** Die Java Card Technologie[17] ermöglicht eine flexible Programmierung von Smartcards. Unterstützen Smartcards diese Technologie, können kleine Programme – sogenannte Java Card Applets – auf Smartcards installiert werden um deren Funktionalität zu erweitern. Die Programmierung dieser Applets erfolgt über die Programmiersprache Java, wobei allerdings nur ein Subset der gesamten Java-Funktionalität zur Verfügung steht. Im Rahmen mobiler Signaturlösungen spielt Java-

[14] http://www.surfnet.nl/nl/Pages/default.aspx

[15] http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=dss

[16] http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=54089

[17] http://www.oracle.com/technetwork/java/javacard/overview/index.html

Card vor allem für die Implementierung entsprechender Secure Elements eine wichtige Rolle.

- **Global Platform:** Der Global Platform Standard[18] ergänzt hauptsächlich den Java Card Standard und definiert das Management von Java Card Applikationen. Über den Global Platform Standard wird beispielsweise geregelt, wie neue Java Card Applets auf Java Card kompatiblen Smartcards installiert werden können.

3.3 SIM-Karten-Standards

Die SIM-Karte ist das zentrale Element jedes Mobiltelefons. Über die SIM-Karte kann sich das Telefon bzw. der Benutzer gegenüber dem Mobilfunknetzwerk und dessen Betreiber authentifizieren. Da SIM-Karten im Prinzip auch eine Form von Smartcards sind, können diesen im Rahmen mobiler Signaturerstellungsverfahren besondere Aufgaben zukommen. Aufbau, Funktionalität und Kommunikationsschnittstellen von Smartcards sind über Standards definiert. Dies ist unumgänglich, da eine Vielzahl an Mobiltelefonherstellern und eine entsprechend große Anzahl an Mobiltelefontypen existieren, welche alle zu den ausgegebenen SIM-Karten kompatibel sein müssen. SIM-Karten und deren Funktionalität werden im Wesentlichen über folgende Standards definiert:

- **ETSI GSM 11.11:** Der ETSI GSM 11.11 Standard[19] beschreibt, wie sich SIM-Karten gegenüber dem Mobilfunkbetreiber über dessen Mobilfunknetz authentifizieren. Die Sicherheit beruht dabei auf einem symmetrischen Schlüssel, der sicher auf der SIM-Karte hinterlegt ist und von dieser auch nicht extrahiert werden kann. Der ETSI GSM 11.11 Standard definiert darüber hinaus ein einfaches Dateisystem, welches zur Speicherung von Daten verwendet werden kann. Optional können diese Daten durch Zugriffsschutzmechanismen (z.B. PIN) geschützt werden.
- **ETSI GSM 11.14:** Der ETSI GSM 11.14 Standard[20] beschreibt die Erweiterung der Funktionalität von SIM-Karten mit Hilfe sogenannter SIM Toolkit Applikationen. Dabei handelt es sich im Prinzip um Java Card Applets, die auch remote durch den Mobilfunkbetreiber verwaltet werden können. Auf zusätzliche Funktionen, die durch diese Applets bereitgestellt werden, können Benutzer in der Regel über ein spezielles „Tools“ oder „Extras“ Menü zugreifen. Da SIM Toolkit Applikationen direkt auf der SIM-Karte installiert sind und auch dort ausgeführt werden, genießen diese einen umfangreicheren Schutz als Anwendungen, die direkt am mobilen Gerät laufen.
- **3GPP GSM 03.48:** Der 3GPP GSM 03.48 Standard[21] definiert Sicherheitsmechanismen für das SIM Application Toolkit. Unter anderem wird der sichere Datenaustausch zwischen externen Einheiten und einer SIM Toolkit Applikation spezifiziert. Ein Überblick über weitere Standards und Spezifikationen, die von 3GPP publiziert wurden (z.B. USIM Spezifikation, etc.) ist auf der 3GPP Website[22] verfügbar.

3.4 PKI Standards

Public Key Infrastructures (PKI) spielen in allen produktiven mobilen Signaturlösungen eine zentrale Rolle. Vor allem in den Bereichen E-Government und M-Government führt an PKI basierten Lösungen zur Identifizierung und Authentifizierung von Bürgerinnen und Bürgern

[18] http://www.globalplatform.org/

[19] http://www.etsi.org/deliver/etsi_gts/11/1111/05.03.00_60/gsmts_1111v050300p.pdf

[20] http://www.etsi.org/deliver/etsi_gts/11/1114/05.01.00_60/gsmts_1114v050100p.pdf

[21] http://www.3gpp.org/ftp/specs/html-info/0348.htm

[22] http://www.3gpp.org/ftp/specs/html-INFO/TSG-WG--C6.htm

kein Weg vorbei. Die verwendeten PKI folgen dabei zu meist den von ITU-T[23] und RSA Security[24] veröffentlichten Public Key Cryptography Standards (PKCS)[25].

3.5 Standards zu elektronischen Signaturen

Da sich mobile Signaturen von elektronischen Signaturen ausschließlich durch die im Zuge ihrer Erstellung verwendeten Technologien unterscheiden, gelten für mobile Signaturen generell dieselben Rahmenbedingungen wie für elektronische Signaturen im Allgemeinen. Grundsätzlich sind verschiedene Arten elektronischer Signaturen zu unterscheiden. Als gesetzliche Basis dient dabei die Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen[26].

Generell unterscheidet diese Richtlinie zwischen fortgeschrittenen elektronischen Signaturen und qualifizierten elektronischen Signaturen[27]. Für letztere gelten neben den Anforderungen für fortgeschrittene Signaturen zusätzlich noch die Forderung nach Verwendung einer sicheren Signaturerstellungseinheit und eines qualifizierten Zertifikats. Anforderungen an sichere Signaturerstellungseinheiten und qualifizierte Zertifikate sind ebenfalls durch die Richtlinie definiert.

Da vor allem im Rahmen von E-Government Anwendungen qualifizierte elektronische Signaturen eine zentrale Rolle spielen und in vielen Bereichen für die Durchführung von Prozessen unumgänglich sind, hängt auch die Bewertung verschiedener Ansätze zur mobilen Signaturerstellung davon ab, ob diese in der Lage sind die Anforderungen qualifizierter Signaturen zu erfüllen.

3.6 Mobile Signature Service (MSS)

Einer der wichtigsten Standards für die Erstellung mobiler elektronischer Signaturen ist der von ETSI veröffentlichte Mobile Signature Service (MSS) Standard. Die grundlegende Idee dieses Standards ist die Verwendung der SIM-Karte bzw. einer entsprechenden SIM Toolkit Applikation zu Berechnung der Signatur. Als Gateway zwischen Dienstanbietern und den mobilen Endgeräten der Benutzer fungiert eine zentrale Instanz, die in der Regel durch den Mobilfunkanbieter implementiert wird.

3.6.1 Spezifikationen

Der ETSI Standard ist relativ vage formuliert, einzig die SOAP basierte Kommunikation zwischen Dienstanbietern und Mobilfunkbetreibern ist einigermaßen detailliert spezifiziert. Eine der derzeit am weitest verbreiteten Lösungen zur mobilen Signaturerstellung basiert auf dem MSS Standard. Diese wird in Abschnitt 4 noch näher vorgestellt. Im Folgenden sollen die einzelnen Teile des MSS Standards sowie verwandte Dokumente kurz angeführt werden.

- **ETSI TR 102 203:** Dieses Dokument[28] trägt den Titel „Business and Functional Requirements“ und dient gewissermaßen als Einführung in die ETSI 102 Standard-

[23] http://www.itu.int/ITU-T/

[24] http://www.rsa.com/

[25] http://rsa.com/rsalabs/node.asp?id=2124

[26] http://www.signatur.rtr.at/repository/legal-directive-20000119-de.pdf

[27] Der Begriff der qualifizierten elektronischen Signatur hat sich eingebürgert, kommt so jedoch in der Richtlinie explizit nicht vor. Stattdessen ist dort von fortgeschrittenen elektronischen Signaturen, die auf einem qualifizierten Zertifikat beruhen, die Rede. Aus Gründen der Verständlichkeit wird in diesem Dokument jedoch weiterhin der Begriff der qualifizierten elektronischen Signatur verwendet.

[28] http://docbox.etsi.org/EC_Files/EC_Files/tr_102203v010101p.pdf

Reihe. Es enthält allgemeine Überlegengen zu mobilen Signaturen, vergleicht verschiedene Ansätze und zeigt diverse Anwendungsfälle auf.

- **ETSI TS 102 204:** Dieser Teil der Standard-Reihe[29] trägt den Titel „Web Service Interface“ und spezifiziert das Interface zum mobilen Signaturservice, welches Dienstanbieter verwenden können um Signaturen am Endgerät des Benutzers zu initiieren.
- **ETSI TR 102 206:** In diesem Dokument[30] mit dem Titel „Security Framework“ werden Sicherheitsanforderungen für die verschiedenen in den Signaturerstellungsprozess involvierten Komponenten festgelegt.
- **ETSI TS 102 207:** Durch die Verwendung einer zentralen Instanz, über die Dienstanbieter das Signaturservice in Anspruch nehmen können, ist die Möglichkeit einer mobilen Signaturerstellung prinzipiell an den Betreiber der zentralen Instanz gebunden. In diesem Dokument[31] mit dem Titel „Specifications for Roaming in Mobile Signature Services“ wird ein entsprechender Roaming-Mechanismus beschrieben, über den Signaturanfragen zwischen verschiedenen Betreibern von mobilen Signaturdiensten ausgetauscht werden können.
- **WPKI Spezifikationen:** Die von der WPKI Non-Profit Association[32] herausgegebenen Spezifikationen basieren in einigen Punkten auf den oben angeführten ETSI Standards. Im Vergleich zu diesen sind die WPKI Spezifikationen jedoch weniger abstrakt gehalten. Sämtliche WPKI Spezifikationen können von der Website der WPKI Non-Profit Association heruntergeladen werden.

3.6.2 Architektur und Funktionalität

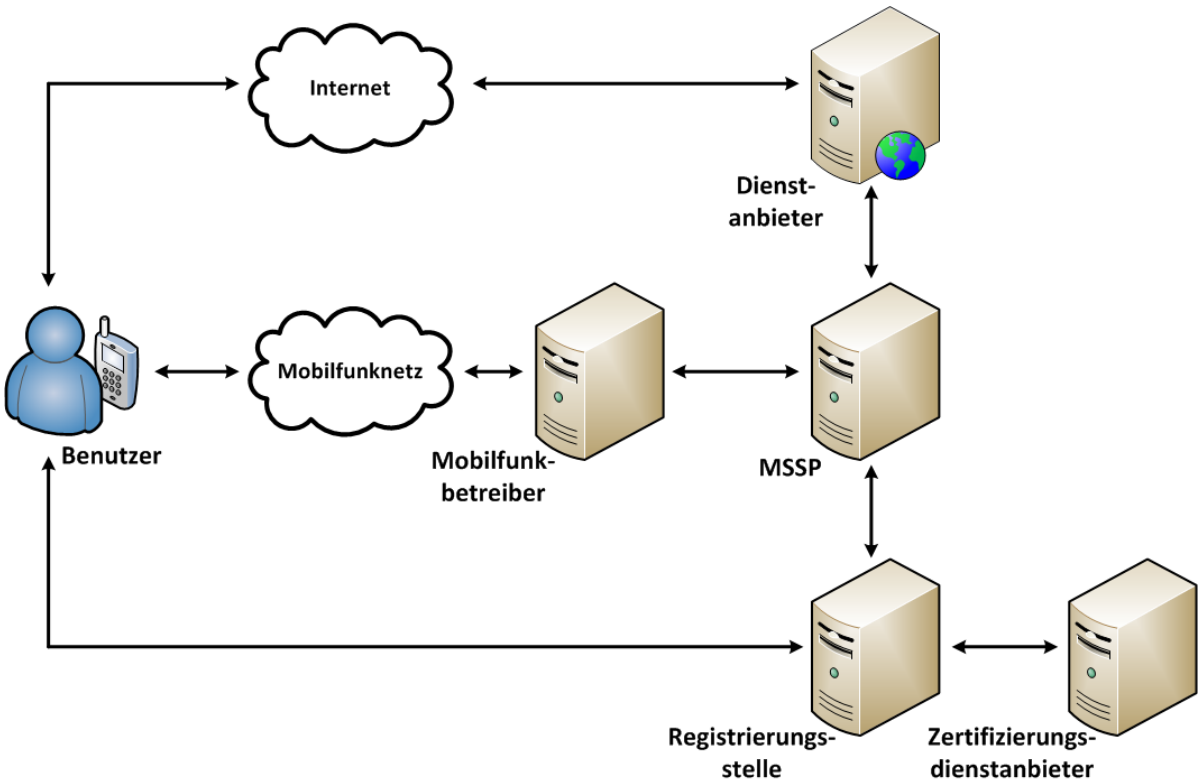

Abbildung 11. Generelle Architektur eines MSS und involvierte Komponenten.

[29] http://docbox.etsi.org/EC_Files/EC_Files/ts_102204v010104p.pdf

[30] http://docbox.etsi.org/EC_Files/EC_Files/tr_102206v010103p.pdf

[31] http://docbox.etsi.org/EC_Files/EC_Files/ts_102207v010103p.pdf

[32] http://www.wpki.net/index_eng.html

Abbildung 11 zeigt die generelle Architektur einer mobilen Signaturlösung gemäß des MSS Standards, sowie die wichtigsten Parteien und Komponenten, die in einen Signaturerstellungs- bzw. Registrierungsprozess involviert sind.

3.6.2.1 Registrierungsprozess

Um sich an einem MSS registrieren zu können, muss der Benutzer von seinem Mobilfunkbetreiber mit einer entsprechenden SIM-Karte ausgestattet worden sein. Die SIM-Karte muss in der Lage sein kryptographische Operationen wie Schlüsselgenerierung und Signaturerstellung durchzuführen. Sind diese Voraussetzungen erfüllt, kann der Benutzer den Registrierungsprozess über die vorgesehene Registrierungsstelle anstoßen.

Neben der Registrierungsstelle (Registration Authority) ist für den Registrierungsprozess vor allem der Zertifizierungsdienstanbieter (Certification Authority) relevant. Der Zertifizierungsdienstanbieter stellt die für die Erstellung und Prüfung elektronischer Signaturen benötigten Zertifikate aus. Damit wird im Prinzip die Identität des Benutzers an dessen kryptographischen Schlüssel gebunden. Die im Zuge der Zertifikatsausstellung benötigten Daten werden von der Registrierungsstelle zur Verfügung gestellt. Diese ist also unter anderem für die Verifikation der Identität des Benutzers zuständig. Die Registrierungsstelle steht mit dem Mobile Signature Service Provider (MSSP) bzw. in weiterer Folge mit dem Mobilfunkbetreiber des Benutzers in Kontakt, um relevante Daten beziehen und den Registrierungsprozess erfolgreich abschließen zu können.

3.6.2.2 Signaturerstellungsprozess

Nach erfolgter Registrierung kann das MSS vom Benutzer verwendet werden um mobile Signaturen zu erzeugen. Ein typischer Signaturerstellungsprozess unter Verwendung eines MSS wurde unter anderem in [10] beschrieben und gliedert sich in folgende Schritte:

1. Der Benutzer verwendet ein Service eines Dienstanbieters welches die Erstellung einer elektronischen Signatur voraussetzt. Um fortzufahren, stimmt der Benutzer dem Signaturerstellungsvorgang zu.
2. Der Dienstanbieter informiert den Benutzer dass die elektronische Signatur über sein Mobiltelefon durchgeführt werden soll. Alternativ wäre hier auch eine entsprechende Auswahl einer bevorzugten Signaturerstellungsgeräts (z.B. Mobiltelefon oder Smartcard) denkbar.
3. Der Dienstanbieter sendet einen entsprechenden Signaturerstellungs-Request an den MSSP. Dieser enthält den Identifier des Benutzer, sowie die zu signierenden Daten.
4. Der MSSP verarbeitet den Request und schickt die zu signierenden Daten über das Mobilfunknetz des kooperierenden Mobilfunkbetreibers an das Mobiltelefon des Benutzers.
5. Die zu signierenden Daten werden am Mobiltelefon des Benutzers angezeigt. Stimmt der Benutzer der Unterzeichnung dieser Daten zu, muss er seine persönliche PIN eingeben, um die Signaturerstellung auf der SIM-Karte auszulösen.
6. Die Signaturdaten werden über das Mobilfunknetz des Mobilfunkbetreibers an den MSSP übertragen.
7. Der MSSP verpackt diese Daten in eine geeignete Signaturerstellungs-Response und retourniert diese an den Dienstanbieter.
8. Der Dienstanbieter informiert den Benutzer über den Erhalt der Signaturdaten.
9. Der Benutzer erhält Zugriff auf das gewünschte Service.

Zentrales serverseitiges Element im Signaturerstellungsprozess sind einerseits der MSSP als auch der Mobilfunkbetreiber. Es ist daher naheliegend, dass diese beiden Komponenten eng kooperieren bzw. von ein und demselben Anbieter zur Verfügung gestellt werden. Tatsächlich ist es in der Praxis so, dass die Aufgaben des MSSP meist von einem Mobilfunkanbieter übernommen werden.

3.6.2.3 Roaming

Der oben beschriebene Ablauf zur Erstellung einer elektronischen Signatur funktioniert nur dann, wenn sowohl Dienstanbieter als auch der Mobilfunkbetreiber des Benutzers mit demselben MSSP kooperieren bzw. mit diesem entsprechende Verträge abgeschlossen haben. Um die parallele Existenz mehrerer MSSP zu gewährleisten, ist im ETSI TS 102 207 Standard die Rolle des Roaming MSSP spezifiziert. Dieser ist in Abbildung 11 aus Gründen der Übersichtlichkeit nicht explizit angeführt. Im Prinzip handelt es sich dabei um einen zusätzlichen MSSP, der die Kommunikation zwischen dem MSSP des Benutzers und jenem des Dienstanbieters gewährleistet. Damit können MSS basierte Lösungen auch in Szenarien verwendet werden, in denen sich Benutzer und Dienstanbieter keinen gemeinsamen MSSP teilen.

4 Mobile Signaturlösungen in Europa

4.1 Einleitung

Obwohl bereits zahlreiche Verfahren zur mobilen Signaturerstellung vorgeschlagen und einige davon auch bereits in Form von internationalen Standards spezifiziert wurden, existiert in Europa derzeit eine heterogene Landschaft bezüglich der Penetration der eingesetzten Lösungen. Nichtsdestotrotz unternimmt sowohl der private Sektor (meist repräsentiert durch Bankinstitute oder Mobilfunkbetreiber) als auch der öffentliche Sektor (in Form von M-Government Initiativen) wiederholt Versuche die Verbreitung mobiler Signaturlösungen durch diverse Pilotprojekte weiter zu steigern.

In diesem Abschnitt sollen einige dieser Pilotprojekte näher vorgestellt werden. Dadurch soll ein Überblick über die aktuelle Verbreitung mobiler Signaturlösungen in Europa geschaffen und jene Ansätze extrahiert werden, welche auch in der Praxis bereits Anwendung finden. In weiterer Folge sollen diese Ansätze dann analysiert und vor allem in Bezug auf eine Verwendung mit Smartphones sicherheitstechnisch evaluiert werden.

Eine zentrale Rolle bei Installation und Betrieb mobiler Signaturlösungen in Europa nimmt aktuell das finnische Unternehmen Valimo Wireless Ltd[33]. ein, das auf mobile ID- und Signaturlösungen spezialisiert und seit 2010 Teil der Gemalto-Gruppe[34] ist. Unter anderem bietet Valimo Wireless Ltd. eine auf dem Mobile Signature Service (MSS) Standard basierende Lösung zur Erstellung mobiler Signaturen an.

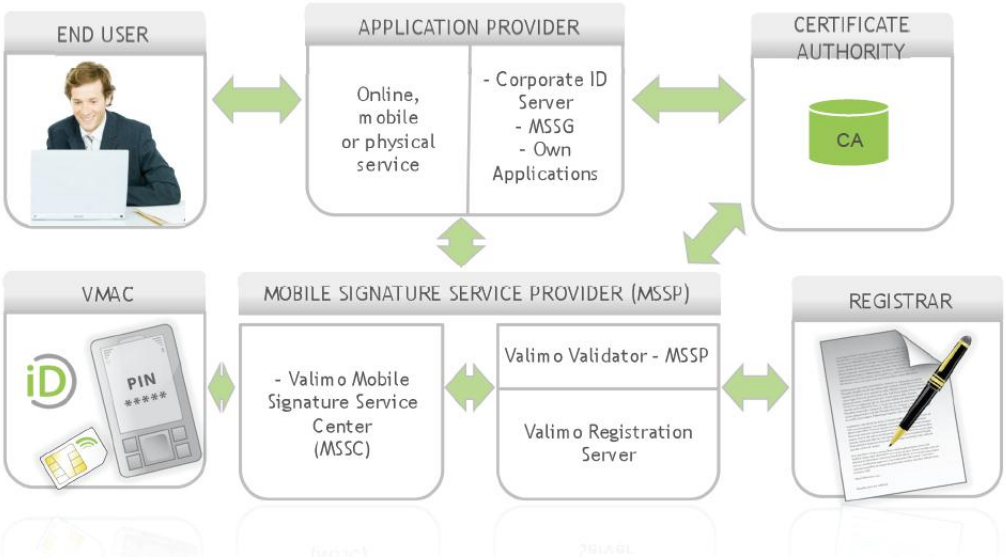

Abbildung 12. Komponenten der von Valimo Wireless Ltd. angebotenen mobilen Signaturlösung[35].

Abbildung 12 zeigt die von Valimo Wireless Ltd. entwickelten Komponenten zur mobilen Signaturerstellung. Valimo Wireless Ltd. bietet sowohl serverseitige (MSSP) als auch clientseitige Komponenten (VMAC zur Erstellung von Signaturen auf SIM-Karten) an. Eine detailliertere Beschreibung der angebotenen Produkte wird auf der Website des Herstellers[36]

[33] http://www.valimo.com

[34] http://www.gemalto.com

[35] Quelle: http://www.valimo.com/products/introduction

[36] http://www.valimo.com/products/introduction

angeboten. In den letzten Jahren wurde die von Valimo Wireless Ltd. entwickelte Lösung in verschiedenen Ländern zusammen mit kooperierenden Mobilfunkanbietern ausgerollt.

Auf diese und andere mobile Signaturlösungen wird in den folgenden Unterabschnitten genauer eingegangen. Durch die getrennte Betrachtung einzelner europäischer Länder soll ein umfassender Überblick über den aktuellen Entwicklungsstand mobiler Signaturlösungen in verschiedenen europäischen Regionen gegeben werden. Die in den folgenden Unterabschnitten präsentierten Daten beruhen größtenteils auf Daten, die in vorangegangen Studien (z.B. [15]) gesammelt und veröffentlicht, bzw. über diverse Pressemitteilungen publiziert wurden. Erwähnt werden nur jene Länder, in denen relevante mobile Signaturlösungen entwickelt bzw. betrieben werden oder wurden.

4.2 Länderüberblick

4.2.1 Deutschland

In Deutschland kommen mobile Signaturlösungen hauptsächlich im Bereich des e-Banking bzw. mobile Banking zum Einsatz. In einer Kooperation der certgate GmbH[37] und dem Informatikzentrum der Sparkassenorganisation[38] wurde bereits im Jahr 2008 eine mobile Lösung zur Durchführung von Transaktionen über mobile Geräte entwickelt[39,40]. Diese basierte auf elektronischen Signaturen, die auf einer speziellen microSD-Karte mit integriertem Secure Element berechnet wurden. Die Lösung war dementsprechend vor allem für PDAs und Smartphones konzipiert.

Das ebenfalls in Deutschland angesiedelte Unternehmen Giesecke & Devrient[41] bietet so wie das finnische Unternehmen Valimo Wireless Ltd. eine auf dem ETSI MSS Standard basierende Lösung zur mobilen Signaturerstellung an. Die SmartLicentio[42] genannte MSSP Lösung folgt den Standards ETSI TS 102 204 und ETSI TS 102 207. Dementsprechend wird die SIM-Karte des Mobiltelefons als sichere Signaturerstellungseinheit für die Berechnung der elektronischen Signatur verwendet.

4.2.2 Estland

Estland ist eines jener europäischen Länder, in denen mobile elektronische Signaturen bereits verstärkt zum Einsatz kommen. Die auch im Bereich E-Government und E-Voting eingesetzte Lösung namens Mobiil-ID wird vom estnischen Mobilfunkanbieter EMT[43] betrieben. EMT ist ein Tochterunternehmen des vor allem in Ost- und Nordeuropa operierenden Mobilfunkbetreibers TeliaSonera[44].

Die Architektur der Mobiil-ID Lösung entspricht im Prinzip jener des durch ETSI publizierten MSS Standards. Abbildung 13 zeigt Aufbau und involvierte Komponenten des Mobiil-ID Ansatzes. Die Rolle des MSSP aus dem MSS-Modell wird in der Mobiil-ID Lösung von einem

[37] http://www.certgate.com/

[38] http://www.siz.de/

[39] http://www.certgate.com/index.php?id=105&L=1

[40] https://www.info-point-security.com/security-themen/mobile-sicherheit/item/568-signatur-f%C3%BCr-ebics-mit-pda-und-smartphone.html

[41] http://www.gi-de.com/de/index.jsp

[42] http://www.gi-de.com/de/products_and_solutions/products/sim_lifecycle_management/smartlicentio/smartlicentio.jsp

[43] https://www.emt.ee/

[44] http://www.teliasonera.com/

sogenannten Trusted Service Provider übernommen. Dieser steht mit dem Mobilfunkbetreiber EMT in Kontakt, der für die Übermittlung der Signaturdaten an das Mobiltelefon bzw. die SIM-Karte des Benutzers zuständig ist. Die Signatur wird auch beim Mobiil-ID Ansatz direkt auf der SIM-Karte des Benutzers berechnet. Diese ist dazu mit einer speziellen SIM-Applikation ausgestattet. Um sich zu diesem Service erfolgreich registrieren zu können, ist also auch hier der Tausch der SIM-Karte erforderlich.

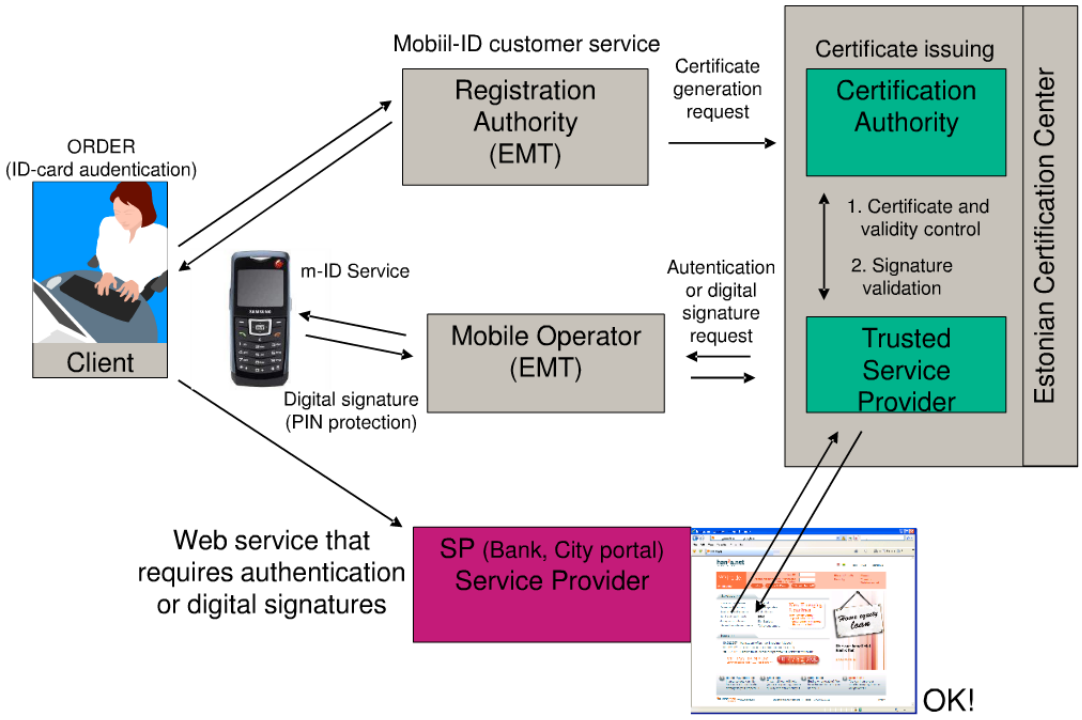

Abbildung 13. Architektur des Mobiil-ID Dienstes[45].

Die für die Registrierung benötigte Registrierungsstelle (Registration Authority) wird ebenfalls von EMT implementiert. Der Zertifizierungsdienstanbieter wird – wie auch der Trusted Service Provider – vom Estonian Certification Center bereitgestellt.

Die Mobiil-ID Lösung, die bereits im Rahmen von Parlamentswahlen beim M-Voting zum Einsatz kam[46], wird hauptsächlich durch den größten Mobilfunkbetreiber EMT zur Verfügung gestellt. Vor einigen Jahren gab es laut Medienberichten Bestrebungen eines weiteren estnischen Mobilfunkbetreibers eine Lösung zur mobilen Signaturerstellung anzubieten. Der finnische Mobilfunkbetreiber Elisa[47], welcher im Jahr 2008 auch in Estland über ca. 340.000 Kunden verfügte, unterzeichnete laut diesen Medienberichten[48] einen Vertrag mit Valimo Wireless Ltd., um seinen Kunden einen auf der von Valimo Wireless Ltd. bereitgestellten Technologie beruhenden mobilen Signaturservice bieten zu können. Auf der estnischen Website[49] von Elisa konnten jedoch keine aktuellen Informationen zu einem derartigen Dienst gefunden werden.

[45] Quelle: http://www.slideshare.net/ceed2/estonian-experience-electronicid-mobileid

[46] http://wirelessfederation.com/news/tag/digital-signature/

[47] http://www.elisa.com

[48] http://www.arcticstartup.com/2008/11/03/valimo-signs-elisa-to-offer-mobile-identification-in-finland-and-estonia

[49] http://www.elisa.ee/

4.2.3 Finnland

Wie Estland und Österreich gehört auch Finnland zu jenen europäischen Ländern, in denen früh auf mobile Signaturlösungen gesetzt wurde. Nach ersten Bestrebungen des Unternehmens SmartTrust um das Jahr 2000[50], wurde schließlich im Jahr 2005 eine entsprechende Lösung vom finnischen Melderegister in Zusammenarbeit mit verschiedenen finnischen Mobilfunkanbietern umgesetzt. Ähnlich der in Estland im Einsatz befindlichen Mobiil-ID, folgte auch die finnische Implementierung dem Ansatz einer Signaturerstellung auf der SIM-Karte des Benutzers. Details zu diesem ersten finnischen Versuch mobile Signaturlösungen auf breiter Basis zu etablieren finden sich u.a. in [1] und [23].

Im Sommer 2011 kündigten die finnischen Mobilfunkbetreiber Sonera[51] und Elisa[52] an, zusammen mit Valimo Wireless Ltd. eine landesweite Lösung für mobile Signaturen zu entwickeln[53,54]. Die Mobiilivarmenne[55] genannte Lösung basiert ebenfalls auf einer Signaturerstellung auf SIM-Karten und basiert auf den von Valimo Wireless Ltd. angebotenen Komponenten. Valimo Wireless Ltd. war auch in die Entwicklung der finnischen FiCom 2.0 Spezifikation involviert, welche die Integration persönlicher Daten wie Alter, Geschlecht, Adresse oder Sozialversicherungsnummer in elektronische Signaturen erlaubt. Aktuell wird Mobiilivarmenne von den drei finnischen Mobilfunkanbietern Sonera[56], Elisa[57] und DNA[58] unterstützt.

Neben Valimo Wireless Ltd. bietet auch das finnische Unternehmen Methics Oy[59] eine MSSP an. Die Kiuru[60] genannte Lösung implementiert ebenfalls die ETSI Mobile Signature Service Standards und folgt damit ebenfalls dem Ansatz einer mobilen Signaturerstellung auf der SIM-Karte.

4.2.4 Frankreich

Im Jahr 2008 verlautbarten die Unternehmen Valimo Wireless Ltd., Experian[61] und Keynetics[62] eine Kooperation um französischen Service Providern einen mobilen Signaturdienst anzubieten. Die Technologie zur mobilen Signaturerstellung wurde zusammen von Valimo Wireless Ltd. und Keynetics bereitgestellt. Relevante Infrastrukturkomponenten wurden von Experian zur Verfügung gestellt. Für einen ersten Pilotbetrieb war die Implementierung eines Langzeitdokumentenarchivs mit sicherem Zugang über elektronische Signatur geplant[63,64].

---

[50] Vrgleich dazu auch Abschnitt 1.2

[51] http://www.sonera.fi/

[52] http://www.elisa.com/en/

[53] http://www.ad-hoc-news.de/sonera-and-elisa-jointly-launch-valimo-mobile-signature--/de/News/22246764

[54] http://www.valimo.com/news_and_events/28-06-2011/sonera-and-elisa-jointly-launch-valimo-mobile-signature-solution-finland

[55] http://www.mobiilivarmenne.fi/en/index.html

[56] http://www.sonera.fi/puhelin+ja+liittyma/palvelut/huvi+ja+hyoty/sonera+id

[57] http://www.elisa.fi/varmenne/

[58] http://www.dna.fi/yksityisille/puhe/palvelut/Sivut/DNAMobiilivarmenne.aspx

[59] http://www.methics.fi/

[60] http://www.methics.fi/pdf/Kiuru_MSSP_Product_Brochure.pdf

[61] http://www.experian.com/

[62] http://keynetics.com/

[63] http://next-generation-communications.tmcnet.com/news/2008/02/19/3279252.htm

4.2.5 Italien

In Italien ging Capgemini Italia[65] im Jahr 2007 eine Kooperation mit Valimo Wireless Ltd. ein. Ziel war die Entwicklung einer mobilen Signaturlösung für italienische Banken und Finanzinstitutionen[66].

4.2.6 Lettland

In Lettland können Benutzer ebenfalls ihr Mobiltelefon zur Erstellung elektronischer Signaturen benutzen. Unter anderem kann damit Zugang zu Online-Diensten von Banken und öffentlichen Einrichtungen erlangt werden. Die entsprechende Infrastruktur wurde vom lettischen Mobilfunkbetreiber Lattelcom[67] in Kooperation mit Valimo Wireless Ltd. entwickelt. Damit basiert auch die lettische Lösung auf Komponenten des finnischen Anbieters mobiler Signaturlösungen. Der Dienst wurde im Jahr 2009 in Betrieb genommen und wurde zu diesem Zeitpunkt von neun Service Providern genutzt[68].

4.2.7 Litauen

In Litauen wurde ein erstes Pilotprojekt zur Einführung mobiler Signaturlösungen im Jahr 2004 gestartet[69]. Während erste Erfahrungen mit mobilen Signaturen also bereits recht früh gesammelt werden konnten, ging eine erste produktive mobile Identifizierungs- und Signaturlösung erst im Jahr 2007 in Betrieb. Der Mobilfunkbetreiber Omnitel verwendete dazu die auch in Estland von EMT angebotene Lösung[70]. Auch die litauische mobile Signaturlösung basiert daher auf einer Signaturerstellung auf SIM-Karten. Auch in Litauen müssen Benutzer, die die mobile Signaturlösung verwenden möchten, einen entsprechenden SIM-Karten-Tausch vornehmen. Einsatz finden mobile Signaturlösungen in Litauen vor allem im Bankensektor, in dem diese zur Benutzerauthentifizierung und Transaktionsautorisierung verwendet werden[71,72].

4.2.8 Niederlande

Für die Niederlande wurde im Jahr 2009 eine Kooperation des niederländischen Zertifizierungsdienstanbieters DigiNotar[73] und Valimo Wireless Ltd. verlautbart[74]. Im Jahr 2011 kam DigiNotar in ernste Turbulenzen, nachdem bekannt wurde, dass sich Angreifer unbefugt Zertifikate für mehrere Domains ausgestellt hatten. Dies führte schließlich im September 2011 zur Insolvenz des Unternehmens.

---

[64] http://www.mobilemarketer.com/cms/news/banking-payments/557.html

[65] http://www.it.capgemini.com/

[66] http://news.thomasnet.com/companystory/Valimo-Signs-Partnership-with-Capgemini-Italia-for-Offering-Mobile-Signature-Services-in-Italy-526351

[67] http://www.lattelecom.lv/

[68] http://www.computescotland.com/latvia-telecoms-offers-a-really-useful-mobile-id-service-2583.php

[69] http://ec.europa.eu/idabc/servlets/Doc2dc4.pdf?id=29088

[70] http://www.ebaltics.com/01005557?PHPSESSID=6860b32431a84abc40d853ee1306cb18

[71] http://www.ub.lt/en/news/view/155/all-three-means-of-electronic-signature-operating-in-lithuania-are-available-at-ukio-bankas

[72] http://www.swedbank.lt/en/articles/view/763

[73] http://www.diginotar.nl/

[74] http://www.valimo.com/news_and_events/03-03-2009/diginotar-and-valimo-introduce-mobile-authentication-and-signing-service-

4.2.9 Norwegen

Skandinavien gehört zu jenen europäischen Regionen, in denen mobile Identifikations- und Signaturlösungen am weitesten verbreitet sind und auch bereits sehr früh zum Einsatz kamen. In Norwegen spielen dabei vor allem der Mobilfunkanbieter Telenor[75], sowie das Unternehmen Banking and Business Solutions (BBS), das seit 2010 Teil der NETS Gruppe ist[76], eine zentrale Rolle[77]. Mobile ID und Signaturlösungen werden in Norwegen vor allem im Bankensektor verwendet. Zentrales Element für die Signaturerstellung ist auch in der in Norwegen verwendeten Lösung die SIM-Karte.

Im Jahr 2007 demonstrierten BBS aus Norwegen und Valimo Wireless Ltd. aus Finnland die erste internationale Roaming-Lösung für mobile Signaturen. Diese basierte vollständig auf dem von ETSI veröffentlichten Mobile Signature Service Standard[78].

4.2.10 Österreich

In Österreich wurden erste Erfahrungen mit mobilen Signaturlösungen bereits im Jahr 2004 gesammelt. Damals bot der österreichische Mobilfunkbetreiber Mobilkom Austria[79] ein Service namens A1-Signatur an, das Benutzern die Erstellung von elektronischen Signaturen über Mobiltelefone erlaubte und auf Verwaltungssignaturen beruhte. Diese waren gemäß einer gesetzlichen Übergangsregelung qualifizierten Signaturen im Rahmen von E-Government-Anwendungen gleichgestellt. Nach Auslaufen dieser Verordnung im Jahr 2007 wurde der Dienst von der Mobilkom Austria nicht weiter angeboten.

Im Jahr 2009 wurde in Österreich mit der Handy-Signatur[80] eine neue mobile Signaturlösung vorgestellt [17]. Vom Konzept her mit der A1-Signatur durchaus vergleichbar, beruht auch die Handy-Signatur auf einer zentralen Signaturerstellungseinheit. Im Gegensatz zu den in Skandinavien und den baltischen Staaten verbreiteten Lösungen wird bei der Handy-Signatur die Signatur nicht auf der SIM-Karte des Mobiltelefons, sondern in einem serverseitigem HSM berechnet. Die persönlichen Signaturschlüssel der Benutzer sind zentral verschlüsselt gespeichert. Ein geheimes, nur dem Benutzer bekanntes Passwort ist integraler Bestandteil des zur Verschlüsselung des Signaturschlüssels verwendeten Schlüssels. Ein weiterer Bestandteil des Verschlüsselungsschlüssels ist im HSM nicht auslesbar gespeichert. Der Signaturschlüssel des Benutzers kann also nur nach Eingabe des geheimen Passworts und nur direkt im HSM entschlüsselt werden.

Nach erfolgter Entschlüsselung des Signaturschlüssels wird ein Einmalpasswort mit begrenzter Gültigkeit an das Mobiltelefon des Benutzers per SMS übertragen. Dieses muss vom Benutzer über ein Web-Formular eingegeben werden, um auf diese Weise den Besitz des Mobiltelefons nachzuweisen. Nach erfolgreicher Eingabe des Einmalpassworts wird die Signatur schließlich im zentralen HSM berechnet.

Abbildung 14 illustriert die Architektur und den prinzipiellen Prozessablauf der österreichischen Handy-Signatur. Eine Signaturerstellung wird durch den Benutzer über eine Web-Schnittstelle zu einem Dienstanbieter (Service Provider) gestartet (1). Dieser schickt einen standardisierten Signaturerstellungs-Request an den Betreiber der Handy-Signatur (A-Trust) (2). Über ein Web-Formular, das in die Web-Site des Service Providers eingebunden ist, werden vom Benutzer Telefonnummer und geheimes Passwort gesichert über HTTPS abgefragt (3). Eine TAN zur Auslösung der Signatur wird über den Mobilfunkanbieter des

[75] http://www.telenor.com/

[76] http://www.nets.eu/Pages/default.aspx

[77] Vergleiche auch Abschnitt 1.2

[78] http://www.cellular-news.com/story/22207.php

[79] http://www.a1.net/

[80] https://www.handy-signatur.at/PortalHandySignatur/

Benutzers an diesen übermittelt (4,5). Diese wird vom Benutzer wiederum über das Web-Formular gesichert an den Betreiber der Handy-Signatur übertragen (6), woraufhin die Signatur im zentralen HSM ausgelöst wird. Das Ergebnis der Signaturerstellung wird an den Service-Provider über eine standardisierte Signaturerstellungs-Response übermittelt (7). Der Erfolg oder Misserfolg der Signaturerstellung wird dem Benutzer über das Web-Frontend des Service Providers angezeigt (8).

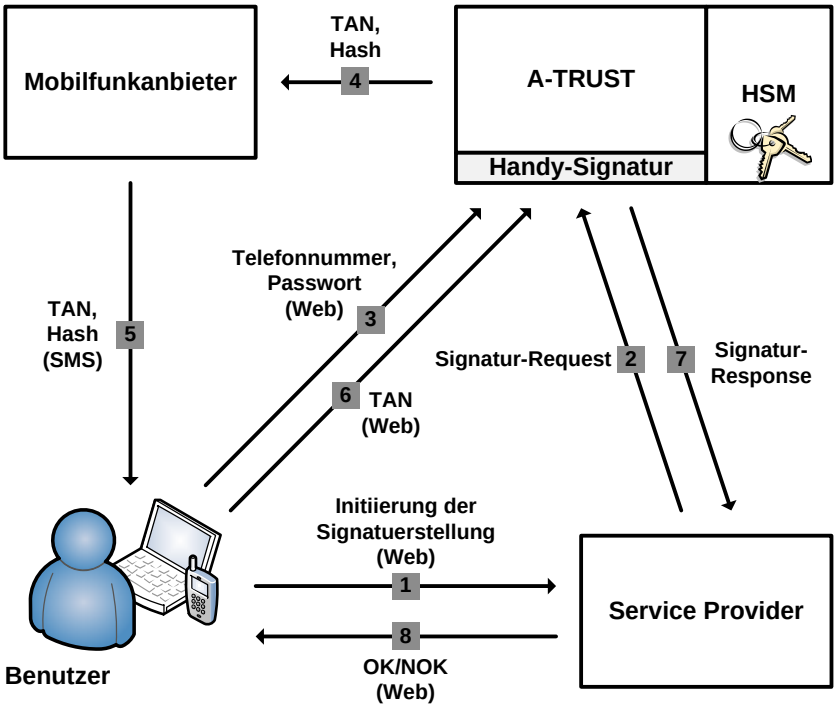

Abbildung 14. Österreichische Handy-Signatur – Architektur und Prozessablauf[81].

Im Gegensatz zur A1-Signatur können mit der Handy-Signatur qualifizierte elektronische Signaturen erstellt werden. Als sichere Signaturerstellungseinheit – eine der Voraussetzungen für qualifizierte elektronische Signaturen – dient das zentrale HSM. Durch Verwendung des geheimen Passworts, und der Zweifaktorauthentifizierung basierend auf Wissen (Passwort) und Besitz (Mobiltelefon) ist zudem gewährleistet, dass sich der Signaturschlüssel stets unter alleiniger Kontrolle des Benutzers befindet.

Das Handy-Signatur-Service wird derzeit vom österreichischen Zertifizierungsdienstanbieter A-Trust[82] betrieben, welcher auch die entsprechenden Zertifikate ausstellt. Entwickelt wurde die Lösung im Rahmen des EU Large Scale Pilots STORK[83]. Die Handy-Signatur findet in Österreich breite Anwendung und kommt vor allem im Rahmen von E-Government-Diensten zum Einsatz.

4.2.11 Polen

Für Polen wurde bereits im Jahr 2003 eine mobile Signaturlösung des damaligen Mobilfunkbetreibers Polska Telefonia Cyfrowa angekündigt[84]. Mittlerweile wurde dieser Telekomanbieter von der Deutschen Telekom übernommen und in die Marke T-Mobile umbenannt. Ein mobiles Signaturservices von diesem Betreiber ist aktuell nicht bekannt.

[81] Quelle: [16]

[82] http://www.a-trust.at/

[83] https://www.eid-stork.eu/

[84] http://www.cellular-news.com/story/9177.php

4.2.12 Schweden

Erste Pilottests zur Einführung mobiler Signaturlösungen wurden in Schweden bereits im Jahr 2000 vom schwedischen Finanzinstitut Swedbank[85] und dem schwedischen Mobilfunkanbieter Telia geplant[86]. Der schwedische Mobilfunkanbieter Telenor Sweden[87] ging einige Jahre später eine Kooperation mit Valimo Wireless Ltd. ein um eine entsprechende mobile Signaturlösung zu entwickeln[88].

4.2.13 Schweiz

Das schweizerische Unternehmen Sicap[89] bietet ein auf dem ETSI MSS Standard basierendes mobiles Signatur-Service an. Gemäß den zugrundeliegenden Standards verwendet die Mobile Ink[90] genannte Signaturlösung die SIM-Karte des Mobiltelefons zur Erstellung der elektronischen Signatur. Zur Entwicklung eines neuen Dienstes wurde kürzlich eine Kooperation mit dem finnischen Unternehmen Methics bekanntgegeben[91].

4.2.14 Slowakei

In der Slowakei wurde im Jahr 2008 ein Projekt zur Einführung einer mobilen Signaturlösung gestartet. Das Projekt wird vom privaten slowakischen Unternehmen PosAm[92] und dem finnischen Anbieter mobiler Signaturlösungen Valimo Wireless Ltd. durchgeführt[93].

4.2.15 Slowenien

In Slowenien wird eine mobile Signaturlösung vom Mobilfunkbetreiber Mobitel[94] angeboten. Diese beruht auf Komponenten des finnischen Unternehmens Valimo Wireless Ltd. und erlaubt Benutzern die Erstellung mobiler qualifizierter Signaturen[95,96].

4.2.16 Spanien

Die vom finnischen Unternehmen Valimo Wireless Ltd. angebotenen Komponenten zur mobilen Signaturerstellung kommen auch in Spanien zum Einsatz. Zusammen mit Valimo Wireless Ltd. und Ericsson verkündete der spanische Mobilfunkanbieter Telefónica Móviles España die Entwicklung einer mobilen Signaturlösung bereits im Jahr 2007[97]. Im Jahr 2008 wurde ein ähnliches Services vom Mobilfunkanbieter Vodafone Spain angekündigt[98,99].

---

[85] http://www.swedbank.com/

[86] http://www.finextra.com/news/fullstory.aspx?newsitemid=780

[87] http://www.telenor.se/privat/index.html

[88] http://www.prnewswire.co.uk/cgi/news/release?id=249140

[89] http://www.sicap.com/

[90] http://www.sicap.com/en/Mobile_Ink.335.0.html

[91] http://www.sicap.com/en/News_Single.107.0.html?&tx_ttnews[tt_news]=179&cHash=5ac9c1c1bc

[92] http://en.posam.sk/

[93] http://www.radiomuzeum.sk/wwwsite/index_en.nsf/0/747BC968D1B74D1CC125751A0028E531?OpenDocument

[94] http://www.mobitel.si/

[95] http://www.valimo.com/news_and_events/14-02-2006/mobitel-deploys-valimo-validator-mssp

[96] http://www.mobitel.si/storitve/mcertifikat.aspx

[97] http://news.soft32.com/spain-to-prepare-for-mobile-signature-solution_3461.html

[98] http://orhanyildirim.blogspot.com/2008/04/vodafone-spain-launches-electronic.html

4.2.17 Türkei

Die Türkei war eines der ersten Länder, in denen die von Valimo Wireless Ltd. entwickelte Lösung auf breiter Basis ausgerollt wurde. Bereits im Jahr 2007 konnten alle Kunden des türkischen Mobilfunkanbieters Turkcell die von Valimo Wireless Ltd. bereitgestellte SIM-basierte Technologie zur Erstellung mobiler Signaturen nutzen[100].

Neben dieser Lösung ist in der Türkei noch ein zweiter Anbieter mobiler Signaturlösungen verfügbar. Der türkische Mobilfunkanbieter Avea[101] bietet Kunden ebenfalls ein Service zur mobilen Signaturerstellung an, welches auf einer Signaturerstellung auf SIM-Karten beruht[102].

4.2.18 Ungarn

In Ungarn bietet das Unternehmen E-Group[103] eine mobile Authentifizierungs- und Signaturlösung an[104]. Diese basiert ähnlich wie die von Valimo Wireless Ltd. entwickelte Lösung auf dem öffentlichen ETSI MSS Standard.

4.3 Schlussfolgerungen

Die Untersuchung bestehender mobiler Signaturlösungen in Europa zeigte, dass diese Technologie in den einzelnen europäischen Ländern sehr unterschiedlich entwickelt ist. Vor allem in Skandinavien, Österreich und den baltischen Ländern sind mobile Signaturlösungen bereits gut entwickelt und seit Jahren im produktiven Einsatz. Andere Länder sind hingegen bisher über einzelne Pilotversuche nicht hinausgekommen bzw. haben noch keinerlei Aktivitäten in diese Richtung gezeigt.

Interessant ist auch zu beobachten, dass der öffentliche Sektor nicht immer die treibende Kraft hinter der Einführung mobiler Signaturlösungen ist. In vielen Fällen geht hier die Initiative von Bankinstituten aus, die ihren Mitarbeitern und Kunden einen über mobile Signaturen abgesicherten Zugang zu internen Systemen und Diensten anbieten möchten. Auch Mobilfunkbetreiber sehen in mobilen Signaturlösungen zunehmend einen rentablen Business Case und treiben die Entwicklung entsprechender Lösungen voran.

Aus technischer Sicht spielt der von ETSI spezifizierte Mobile Signature Service (MSS) Standard eine zentrale Rolle. Nahezu alle mobilen Signaturlösungen folgen diesem Standard und verwenden daher die SIM-Karte als sichere Signaturerstellungseinheit. Zahlreiche private Unternehmen wie Valimo Wireless Ltd., Giesecke & Devrient oder Methics Oy bieten bereits entsprechende Implementierungen des MSS an. Einige Mobilfunkbetreiber haben eigene Lösungen implementiert, die sich jedoch ebenfalls am ETSI MSS orientieren und die SIM-Karte als sichere Signaturerstellungseinheit nutzen.

Die österreichische Handy-Signatur bildet im gesamteuropäischen Kontext eine Ausnahme und setzt im Gegensatz zu MSS basierten Lösungen auf eine zentrale Signaturerstellungseinheit. Durch ein entsprechendes auf zwei Kommunikationskanälen basierendes Zweifaktorauthentifizierungskonzept entspricht auch die österreichische Handy-Signatur den Anforderungen einer qualifizierten Signatur.

---

[99] http://www.sciencedirect.com/science/article/pii/S0965259008702330

[100] http://www.cellular-news.com/story/22943.php

[101] http://www.avea.com.tr/index_en.shtml

[102] http://www.isbank.com.tr/English/content/EN/Expatriate_Banking/Security/Avea_Mobile_Signature-1089-413.aspx#1_1

[103] http://www.egroup.hu/main/

[104] http://www.egroup.hu/main/en/payment-solutions/mobile-payment-solutions

Generell können der in Österreich verfolgte Ansatz der mobilen Signaturerstellung über einen Server bzw. ein serverseitiges HSM und die Signaturerstellung gemäß dem MSS Standard als vorherrschende Lösungsansätze zur Erstellung mobiler Signaturen betrachtet werden. Im folgenden Abschnitt werden diese beiden Ansätze verglichen und deren Anwendbarkeit und Sicherheit auf Smartphone-Plattformen diskutiert.

5 Analyse

Eine Analyse bestehender mobiler Signaturlösungen zeigte, dass derzeit nahezu alle in Europa eingesetzten mobilen Signaturlösungen dem ETSI Mobile Signature Services (MSS) Standard folgen. Eine Ausnahme bildet Österreich, wo zur Erstellung mobiler Signaturen eine serverbasierte Lösung mit serverseitiger sicherer Signaturerstellungseinheit zum Einsatz kommt. Diese beiden in der Praxis relevanten Ansätze zur mobilen Signaturerstellung sollen in diesem Abschnitt näher analysiert werden. Dazu werden zunächst Vor- und Nachteile der beiden Ansätze diskutiert und in weiterer Folge deren Anwendbarkeit auf Smartphone-Plattformen untersucht.

5.1 Vergleich vorhandener Lösungen

Betrachtet man die historische Entwicklung elektronischer Signaturlösungen, so stellen MSS basierte Ansätze die logische Weiterentwicklung chipkartenbasierter Signaturlösungen dar. Statt der Chipkarte (Bankomatkarte, Sozialversicherungskarte, Signaturkarte, etc.), für deren Verwendung ein entsprechendes Kartenlesegerät nötig ist, kommt das Mobiltelefon des Benutzers bzw. die im Telefon befindliche SIM-Karte zur Anwendung. Wie auch bei chipkatenbasierten Ansätze bleibt die sichere Signaturerstellungseinheit damit stets unter der direkten physikalischen Kontrolle des Benutzers.

Sicherheitsaspekte MSS basierter Lösungen wurden unter anderem in [14] näher analysiert. Die Autoren bescheinigen MSS basierten Lösungen ein ausreichendes Maß an Sicherheit, nennen jedoch folgende Punkte, die unter Umständen aus sicherheitstechnischer Sicht problematisch sein könnten.

- Der gemäß GSM Standard für die sichere Übertragung der Signaturdaten verwendete Algorithmus A5 kann nicht mehr uneingeschränkt als sicher betrachtet werden. Zusätzliche Secure Messaging Verfahren sollten daher unbedingt implementiert werden.
- Unerfahrene Benutzer können dazu gebracht werden ihre PIN über den PC-Kanal bekanntzugeben (Phishing).
- Über installierte Schadsoftware am PC des Benutzers können Man-in-the-Browser Attacken implementiert werden. Benutzern kann beispielsweise glaubhaft gemacht werden eine bestimmte finanzielle Transaktion mit dem Betrag X zu autorisieren, während tatsächlich eine Transaktion über den Betrag Y autorisiert wird.
- Schadsoftware am mobilen Gerät kann beispielsweise verwendet werden, um den Benutzer zur Eingabe seiner PIN zu veranlassen.
- Ein Angreifer in Person eines Mitarbeiters eines Service Providers kann lokal die Daten einer autorisierten Transaktion modifizieren.
- Ein Angreifer in Person eines Mitarbeiters eines Service Providers kann eine sogenannte Mafia-in-the-Middle Attacke implementieren. Bei dieser Attacke wird dem Benutzer eine bestimmte Transaktion vorgetäuscht, während die Signaturdaten unerlaubterweise für eine gänzlich andere Transaktion verwendet werden. Diese Attacken werden u.a. in [18] beschrieben.

Eine formale Sicherheitsanalyse der in Estland verwendeten Mobiil-ID Lösung bzw. des von dieser Lösung verwendeten Protokolls wurde in [19] vorgestellt. Auch diese Analyse kommt zum Schluss, dass MSS basierte Signaturlösungen bzw. in diesem Fall die konkrete estnische Umsetzung prinzipiell als sicher einzustufen sind, es punktuell jedoch Verbesserungsmöglichkeiten gibt.

Relevante Unterschiede zwischen MSS basierten Lösungen und der österreichischen Handy-Signatur wurden bereits in [16] näher diskutiert. Gegenüber Ansätzen, die die SIM-Karte als Signaturerstellungseinheit benutzen, hat die in Österreich verfolgte zentrale Lösung

vor allem den Vorteil, dass diese auf praktisch jedem Mobiltelefon einsetzbar ist. MSS basierte Lösungen bedingen den Wechsel der SIM-Karte des Benutzers, da diese über die entsprechende SIM Toolkit Applikation zur Erstellung mobiler Signaturen verfügen muss. Da im Rahmen der österreichischen Handy-Signatur das Mobiltelefon des Benutzers ausschließlich für den Empfang der SMS, welche das Einmalpasswort enthält, herangezogen wird, ist eine spezielle Funktionalität am Client nicht erforderlich.

Die Reduktion der Anforderung an den Client auf den simplen Empfang einer SMS-Nachricht erleichtert auch das Roaming zwischen verschiedenen Anbietern. Während bei MSS basierten Ansätzen Interoperabilität zwischen einzelnen Anbietern (Service Providern und MSSP) nur mit relativ viel Aufwand und unter Verwendung eines eigenen Roaming MSSP erreichbar ist, ist die Situation bei Verwendung der Handy-Signatur ungleich einfacher. Da Roaming von SMS-Nachrichten zwischen nationalen (und größtenteils auch internationalen) Mobilfunkanbietern praktisch überall verfügbar ist, müssen zur Gewährleistung der Interoperabilität des Handy-Signatur-Ansatzes keine weiteren Vorkehrungen getroffen werden. Auf diese Weise ist die Nutzung der Handy-Signatur in der Regel sogar möglich, wenn sich der Benutzer mit seinem Endgerät in einem ausländischen Mobilfunknetz befindet.

Sowohl die österreichische Handy-Signatur als auch MSS basierte Verfahren verwenden zur Erstellung mobiler Signaturen zwei getrennte Kommunikationskanäle. Neben dem mobilen Kanal kommt zusätzlich ein webbasiertes Kommunikationsinterface zur Anwendung. Die Verwendung eines zusätzlichen Kommunikationskanals ist ein wesentliches Sicherheitsmerkmal dieser beiden Lösungsansätze. Allerdings unterscheidet sich die Art der Daten, die über die beiden Kanäle übertragen werden. Von besonderer Bedeutung ist in diesem Zusammenhang der mobile Kommunikationskanal, da dieser einerseits das mobile Endgerät des Benutzers anbindet und andererseits dessen Sicherheit durch bekannte Schwächen des GSM Protokolls zumindest fragwürdig ist. Während bei MSS basierten Lösungen die Signaturdaten über diesen mobilen Kanal übertragen werden, verwendet die Handy-Signatur diesen lediglich zur Übermittlung eines Einmalpassworts. Ein Angreifer, der Zugriff auf den mobilen Kommunikationskanal (oder das mobile Endgerät) hat, hat somit im Falle der Handy-Signatur trotzdem keinen Zugriff auf die Signaturdaten, da diese ausschließlich zwischen dem Service Provider und der zentralen Instanz der Handy-Signatur ausgetauscht werden.

Beide Ansätze – die österreichische Handy-Signatur und MSS basierte Lösungen – basieren grundsätzlich auf einer Zweifaktorauthentifizierung. Bei der Handy-Signatur werden die beiden Faktoren Besitz und Wissen durch das Mobiltelefon, dessen Besitz durch Zusenden des Einmalpassworts per SMS verifiziert wird, und durch das geheime Signaturpasswort abgedeckt. Bei MSS basierten Ansätzen wird der Faktor Besitz ebenfalls durch das Mobiltelefon bzw. die darin befindliche SIM-Karte abgedeckt. Der Faktor Wissen wird hingegen durch die geheime PIN, die zur Auslösung einer Signatur nötig ist, repräsentiert. Zweifaktorauthentifizierungsansätze sind erwiesenermaßen sicherer als die häufig verwendeten Methoden, welche auf Bekanntgabe eines Benutzernamens und Passworts basieren. Nichtsdestotrotz sind auch Zweifaktorauthentifizierungsmethoden nicht der Weisheit letzter Schluss und können – wenn auch unter beträchtlichem Mehraufwand – ausgehebelt werden. Auf mögliche Schwächen von Zweifaktorauthentifizierungsmethoden wurde bereits vor einigen Jahren unter anderem in [20] hingewiesen. Man-in-the-Middle Attacken und Trojanische Pferde werden darin als größte Gefahrenpotentiale für diese Verfahren genannt.

Vor allem die Implementierung von Attacken basierend auf Trojanischen Pferden wurde in letzter Zeit durch die rasante Verbreitung von Smartphones vereinfacht. Für viele Smartphone-Plattformen fehlen derzeit noch verlässliche Tools zum Schutz mobiler Endgeräte vor Schadsoftware. Die Verwendung von Zweifaktorauthentifizierungsmethoden auf Smartphones kann daher ein erhöhtes Risiko für die Sicherheit dieser Verfahren darstellen. Im Folgenden soll diskutiert werden, inwieweit sich eine Verwendung gängiger

Methoden zur mobilen Signaturerstellung auf Smartphones negativ auf deren Sicherheit auswirken könnte.

5.2 Anwendbarkeit auf Smartphones

Durch die seit einigen Jahren anhaltende Popularität von Smartphones und deren damit einhergehenden gesteigerten Verbreitung stellt sich die Frage inwieweit etablierte mobile Signaturerstellungslösungen für eine Verwendung auf Smartphone-Plattformen geeignet sind. Wir beschränken uns in weitere Folge auf die beiden am weitesten verbreiteten Ansätze und diskutieren im Folgenden die Verwendung der österreichischen Handy-Signatur und MSS basierter Lösungen auf Smartphones.

5.2.1 Handy-Signatur auf Smartphones

Im Rahmen der Handy-Signatur wird das mobile Endgerät ausschließlich als Empfangseinheit für das zeitlich begrenzte Einmalpasswort (TAN) verwendet. Dieses wird dem Benutzer per SMS-Nachricht zugestellt. Die Ausführung des mobilen Endgeräts ist dabei letztendlich irrelevant. Die Möglichkeit SMS-Nachrichten zu empfangen stellt die einzige Anforderung an das mobile Endgerät dar. Da diese Anforderung bereits von praktisch jedem modernen Mobiltelefon erfüllt wird, ist auch die Verwendung der Handy-Signatur auf Smartphones ohne Probleme möglich.

Neben dem Empfang von SMS-Nachrichten (und natürlich der Telefonie) bieten Smartphones noch eine Vielzahl zusätzlicher Funktionen. So ist beispielsweise auf jedem Smartphone ein mobiler Web-Browser vorhanden. In Kombination mit der Handy-Signatur erscheint dies durchaus positiv, da auf diese Weise vollständig mobil auf webbasierte E-Government Inhalte zugegriffen und etwaige Transaktionen über die mobile Signaturlösung der Handy-Signatur durchgeführt werden können. Bei näherer Betrachtung kann diese Vorgehensweise jedoch ein erhöhtes Gefahrenpotential bergen.

Die Sicherheit der Handy-Signatur beruht unter anderem auf der Tatsache, dass Benutzer mit der zentralen Signaturerstellungseinheit über zwei getrennte Kanäle kommunizieren. Telefonnummer und geheimes Signatur-Passwort werden über ein Web-Interface bekanntgegeben, das Einmalpasswort (TAN) wird hingegen über den mobilen SMS-Kanal zugestellt. Ein Angreifer muss daher Kontrolle über zwei unterschiedliche Kanäle erlangen, um das Sicherheitskonzept der Handy-Signatur erfolgreich auszuhebeln.

Smartphones ermöglichen nun die Nutzung ein und desselben Geräts als Endpunkt beider Kommunikationskanäle, da mit einem Smartphone sowohl SMS-Nachrichten empfangen, als auch Web-Seiten betrachtet werden können. Ein Angreifer muss daher lediglich ein Gerät unter seine Kontrolle bringen um einen erfolgreichen Angriff zu implementieren. Die Schwierigkeit eines erfolgreichen Angriffs hängt dabei entscheidend von der jeweiligen Smartphone-Plattform, und den verfügbaren Sicherheitsmechanismen wie Sandboxing, Domain-Separation, etc. ab.

Die Risiken, die sich durch einen Wegfall des zweiten Kommunikationskanals ergeben können sind durchaus bekannt. Entsprechende Angriffe werden beispielsweise in [21] beschrieben. In den Nutzungsrichtlinien der Handy-Signatur ist sinnvollerweise eine entsprechende Trennung der Kommunikationskanäle als Anforderung definiert.

Für die österreichische Handy-Signatur kann zusammenfassend festgehalten werden, dass deren Verwendung auf Smartphones ohne Einbußen in Bezug auf Sicherheit möglich ist. Voraussetzung ist jedoch die Trennung der beiden vorgesehenen Kommunikationskanäle. Das Smartphone darf also ausschließlich für den Empfang des Einmalpassworts verwendet werden. Der webbasierte Kommunikationskanal muss durch ein anderes Endgerät implementiert werden.

Im Sinne eines vollständig mobilen Zugangs zu E-Government-Diensten erscheint die Möglichkeit signaturbasierte Verfahren direkt am Smartphone abwickeln zu können dennoch

interessant. In Abschnitt 6 sollen daher Möglichkeiten diskutiert werden, wie das Konzept der Handy-Signatur entsprechend erweitert werden könnte um eine sichere Signaturerstellung unter Verwendung nur eines Geräts (Smartphone) zu ermöglichen.

5.2.2 MSS basierte Ansätze auf Smartphones

Im Vergleich zur österreichischen Handy-Signatur haben MSS basierte Signaturlösungen höhere Anforderungen an das mobile Endgerät des Benutzers. Dies ist vor allem darin begründet, dass bei diesen Verfahren die elektronische Signatur direkt am Mobiltelefon berechnet wird. Vor allem einfache Mobilfunkgeräte der ersten Generationen waren nicht in der Lage, derartig komplexe Operationen durchzuführen und verfügten nicht über eine für die Erstellung qualifizierter elektronischer Signaturen nötige sichere Signaturerstellungseinheit. Dementsprechend sehen alle gängigen auf dem MSS Standard beruhenden Implementierungen einen Tausch der SIM-Karte vor, was zugleich einer der gravierendsten Nachteile dieses Verfahrens ist, da dies mit zusätzlichem Aufwand für den Benutzer verbunden ist. Ein Tausch des SIM-Karte ist jedoch unumgänglich, da diese als sichere Signaturerstellungseinheit dient.

Zur Kommunikation mit dem auf der SIM-Karte befindlichen Secure Element, welches für die Erstellung der elektronischen Signatur verantwortlich ist, kommt in der Regel eine SIM Toolkit Applikation zur Anwendung. Dies ist für einfache Mobiltelefone ein geeigneter Ansatz, da diese schwer durch zusätzliche Softwarekomponenten erweitert werden konnten. Bei Smartphones ist die Situation gänzlich anders. Einerseits bieten diese auch alternative Möglichkeiten der Integration eines Secure Elements. Denkbar ist beispielsweise die Verwendung einer microSD Karte mit integrierter sicheren Signaturerstellungseinheit. Des Weiteren können Smartphones einfach um zusätzliche Softwarekomponenten erweitert werden.

Die Frage der Anwendbarkeit MSS basierter Verfahren auf Smartphones reduziert sich daher auf die Frage ob und bis zu welchem Grad SIM Toolkit Applikationen von modernen Smartphones unterstützt werden. Durchgeführte Recherchen zeigten, dass es diesbezüglich diverse Unterschiede zwischen verschiedenen Smartphone-Plattformen und den entsprechenden mobilen Betriebssystemen gibt. Auch innerhalb eines Betriebssystems kann es durchaus zu versionsbedingten Unterschieden kommen.

5.3 Sicherheitsaspekte mobiler Signaturerstellungsverfahren am Smartphone

In diesem Abschnitt sollen Sicherheitsaspekte verschiedener Signaturerstellungsverfahren gegenübergestellt werden. Dabei sollen jene Verfahren betrachtet werden, bei denen zur Signaturerstellung auf Seiten des Benutzers ausschließlich ein Smartphone benötigt wird. Diese Verfahren sind vor allem in Hinblick auf eine vollständig mobile Nutzung signaturbasierter Dienste interessant. Prinzipiell kommen dafür folgende Varianten der mobilen Signaturerstellung in Frage:

- Handy-Signatur: Das Smartphone wird sowohl als Empfangseinheit für das Einmalpasswort als auch als Endpunkt des webbasierten Kommunikationskanals verwendet. Dies wird zwar vom Betreiber der Handy-Signatur nicht empfohlen, dennoch soll dieses Szenario hier theoretisch betrachtet werden, da dieses aus Sicht der Benutzerfreundlichkeit klare Vorteile bringt. Es ermöglicht beispielsweise die Implementierung einer Signatur-App, die am Smartphone des Benutzers installiert, und zur Signierung beliebiger digitaler Inhalte verwendet werden kann. Außerdem kann eine detailliertere Betrachtung dieses Szenarios Benutzern eine solide Grundlage für eine persönliche Risikoabschätzung zur Verfügung stellen.
- SIM basierte Ansätze: Diese umfassen unter anderem MSS basierte Verfahren und sollen ebenfalls betrachtet werden.

- microSD basierte Ansätze: Diese haben bisher keine bzw. wenige produktive Anwendungen gefunden, sollen jedoch in diesem Abschnitt ebenfalls näher betrachtet werden.

5.3.1 Kriterien

Eine Reihe von Kriterien sind für die sichere Erstellung elektronischer Signaturen auf mobilen Geräten von Bedeutung. Diese sollen im Folgenden näher beschrieben werden. Anhand dieser Kriterien sollen die einzelnen mobilen Signaturerstellungsverfahren in weiterer Folge analysiert und evaluiert werden.

5.3.1.1 Aufbewahrungsort des Signaturschlüssels

Der Aufbewahrungsort des privaten Signaturschlüssels des Benutzers spielt eine entscheidende Rolle für die Sicherheit des eingesetzten Verfahrens. Die Signatur-Richtlinie definiert als Anforderung an sichere Signaturerstellungseinheiten (die für die Erstellung qualifizierter Signaturen verpflichtend sind), dass diese die Signaturerstellungsdaten des Benutzers vor einer Verwendung durch andere verlässlich schützen müssen. Prinzipiell kann zwischen den folgenden Möglichkeiten der Speicherung von Signaturerstellungsdaten (Schlüssel) unterschieden werden:

- **Software**: Diese Variante wird aufgrund ihrer inhärenten Unsicherheit von keinem der diskutierten Verfahren verwendet, und wird hier nur aus Gründen der Vollständigkeit genannt. Bei diesem Verfahren befindet sich der private Signaturschlüssel auf einem Standard-Speicher (z.B. SD Karte), der dem Gerät zur Verfügung steht. Diese Möglichkeit bietet geringen bis keinen Schutz vor einem Kopieren und einer unerlaubten Verwendung des Schlüssels durch einen Angreifer.
- **Secure Element (SE)**: Bei den genannten Mobilsignaturlösungen kommt durchwegs ein Secure Element (oder entsprechendes Hardware Security Module) für den Schutz der verwendeten Signaturschlüssel zum Einsatz. Auf abstrakter Ebene ist dessen Verwendung dabei immer gleich: Mit Hilfe einer Art von Benutzerauthentifizierung (PIN, Passwords, TANs etc.) wird der Signaturvorgang am SE autorisiert und ausgelöst. Das SE selbst kann sich dabei prinzipiell an unterschiedlichen Positionen befinden:
    - **Smartphone**: In diesem Fall befindet sich das SE direkt im Smartphone. Dabei kann wiederum zwischen den unterschiedlichen Technologien unterschieden werden, die für die Bereitstellung des SEs verwendet werden:
        - **SIM Karte**: Das SE befindet sich auf der SIM Karte. Diese wird über das Smartphone angesprochen. Diese Lösung wird von gängigen MSS basierten Lösungen verwendet.
        - **Im Gerät**: Das SE ist direkt im Gerät integriert.
        - **Andere**: SEs können auch in andere Komponenten wie microSD Karten integriert werden.
    - **Extern**: Bei der österreichischen Mobilsignaturlösung befindet sich das SE nicht am Smartphone sondern beim Betreiber des Dienstes. Die Zugangskontrolle und Signaturautorisierung erfolgt dabei über das vorher beschriebene System und basiert auf den beiden Kommunikationskanälen Internet (Web) und SMS.

5.3.1.2 PIN-Eingabe

Alle oben genannten Signaturlösungen verlangen eine Authentifizierung des Benutzers beim SE, um den Signaturvorgang durchzuführen. Dabei kann es sich um eine einzelne PIN, um ein Passwort oder ein mehrschichtiges PIN/TAN Verfahren handeln.

- **PIN Code**: Hier wird über die Smartphone-Tastatur die benötigte PIN eingegeben. Die Sicherheit basiert darauf, dass nur der Benutzer diese PIN kennt.

- **Mehrschichtiges Verfahren**: Dieses Verfahren kommt u.a. bei der österreichischen Handy-Signatur zum Einsatz. Dabei basiert die Sicherheit einerseits – gleich wie bei der PIN Code Lösung – auf einem Passwort oder einer PIN, die nur dem Benutzer bekannt ist, und andererseits auf einem dynamischen Passwort (TAN), das über einen alternativen Kommunikationskanal (SMS) dem Benutzer übermittelt wird. Bei der Verwendung eines Smartphones muss darauf geachtet werden, dass beide Kommunikationskanäle am gleichen Gerät verwendet werden.

5.3.1.3 Verfügbarkeit des Secure Elements

Der Zugriff auf das SE ist über unterschiedliche Authentifizierungsmaßnahmen gesichert. Neben dieser Authentifizierung spielt aber auch die Verfügbarkeit des SE eine entscheidende Rolle. Steht ein SE immer zur Verfügung und kann es noch dazu automatisch über ein API verwendet werden, so ergibt dies weitere Implikationen, die im Rahmen einer Sicherheitsanalyse betrachtet werden müssen.

- **API**: Verschiedene Lösungen stellen ein API zur Verfügung, das Applikationen für einen Zugriff auf das SE zur Verfügung steht.
    - **API vorhanden**: Der Zugriff auf ein SE kann über ein von der Smartphone-Plattform oder einer externen Applikation zur Verfügung gestelltes API erfolgen. Dabei können Applikationen, die auf dem Smartphone installiert sind, dieses API für die Verwendung des SEs nutzen. Typischerweise kann über dieses API die Signaturerstellung ausgelöst und auch die dazu nötige Authentifizierung durchgeführt werden. Dies impliziert, dass ein Angreifer der in den Besitz der SE-Zugangsdaten gekommen ist (z.B. durch Phishing), das SE unter Zuhilfenahme von Schadsoftware uneingeschränkt verwenden kann. Als API versteht man auch externe Komponenten, die den Zugriff auf ein externes SE erlauben. Ein Beispiel dafür ist die Webschnittstelle der österreichischen Mobilsignatur.
    - **API nicht vorhanden**: Der Zugriff auf das SE steht in diesem Fall nicht über ein Standard API zur Verfügung. Eine Möglichkeit ist, dass die Funktionalität direkt im Betriebssystem integriert ist ohne eine Schnittstelle für externe Applikationen anzubieten. Eine andere Variante ist die Trennung der SE-Applikationsumgebung vom Betriebssystem, wie sie z.B. bei Payment-Systemen (z.B. Google Wallet) zum Einsatz kommt. Letztere Variante wird aber von keiner der Mobilsignaturlösungen eingesetzt. Je nach Implementierung kann auch bei diesen Lösungen nicht ausgeschlossen werden, dass ein automatisierter Zugriff auf das SE möglich ist. Allerdings kann davon ausgegangen werden, dass dies im Allgemeinen nur durch das Ausnutzen von Sicherheitslücken im Betriebssystem möglich ist. D.h. in diesem Fall kann Schadsoftware, die über die Rechte einer normalen Applikation verfügt, keinen Zugriff auf das SE erhalten.
- **Externer Kommunikationskanal**: Je nach Lokation des SEs erfolgt dessen Verwendung und die dafür nötige Authentifizierung über unterschiedliche Kommunikationskanäle.
    - **Externer Kommunikationskanal vorhanden**: Hierbei wird für die Verwendung des SEs ein oder mehrere Kommunikationskanäle benötigt. Diese Variante kommt typischerweise bei externen SEs zum Einsatz. Beispiele für solche Kommunikationskanäle sind das Internet, der Einsatz von SMS, oder automatisierte Anrufe. Die Kombination aus Internet und SMS ist eine gängige Lösung für die Absicherung von Online-Banking. Ein gutes Beispiel für die Implementierung aller drei Methoden ist die Zweifaktorauthentifizierung, die beispielsweise Nutzern von Google Diensten

zur Verfügung steht[105]. Auch die österreichische Handy-Signatur verwendet sowohl das Internet als auch SMS Nachrichten, um eine sichere Authentifizierung zu gewährleisten.

- **Externer Kommunikationskanal nicht vorhanden**: Alle Komponenten zur Signaturerstellung befinden sich direkt am Smartphone. Es gibt daher keine externe Abhängigkeiten für die direkte Erstellung einer Signatur mit Hilfe des SEs.

5.3.1.4 Lokation der Signaturdaten

In Bezug auf die Sicherheit spielt die Lokation, an der die Signaturdaten erstellt und verarbeitet werden und damit Ziel von Manipulation werden können, eine große Rolle. Prinzipiell lassen sich folgende Anwendungsszenarien unterscheiden:

- **Signaturdaten werden am Smartphone erstellt**: Da die Daten direkt am Smartphone des Benutzers verarbeitet werden, kann Schadsoftware in diesen Prozess eingreifen und die Daten ohne Wissen des Benutzers verändern. Ein mögliches Beispiel ist ein Überweisungsvorgang, bei dem der Angreifer mit Hilfe von Schadsoftware Betrag und/oder Empfängerkonto austauscht.
- **Signaturdaten werden von einer externen (Web-)Applikation erstellt**: Hier werden die zu signierenden Daten von einer externen Applikation erstellt und entweder direkt zu einer externen Signaturerstellungseinheit oder an das Smartphone übermittelt. Im ersten Fall kann Schadsoftware keine direkte Änderung der Daten durchführen. Im zweiten Fall ist dies zwar prinzipiell möglich, manipulierte Daten können aber durch Plausibilitätsprüfungen von der (Web-)Applikation erkannt werden.

Basierend auf diesen Anwendungsszenarien können folgende Eigenschaften abgeleitet werden:

- **(Böswillige) Applikationen haben keinen lokalen Zugriff auf die Signaturdaten**: In diesem Fall werden die Signaturdaten nicht zum Smartphone übertragen, bzw. über das Smartphone an eine externe Signaturerstellungseinheit übermittelt. Das Smartphone wird nur für die Anzeige der Signaturdaten verwendet. Somit kann potentiell die Anzeige der Signaturdaten, nicht jedoch die zu signierenden Daten selbst manipuliert werden.
- **(Böswillige) Applikationen haben lokalen Zugriff auf die Signaturdaten**: Hier befinden sich die Signaturdaten direkt am mobilen Gerät und stehen der jeweiligen Applikation zur Verfügung. Dies trifft immer dann zu wenn die Signaturerstellungseinheit direkt am Gerät ist und der Zugriff darauf über ein API erfolgt, das potentiell allen Smartphone-Applikationen zur Verfügung steht. Eine weitere Möglichkeit ist, dass sich zwar die Signaturerstellungseinheit nicht am mobilen Gerät befindet, die Signaturdaten für die Signaturerstellung aber von einer lokalen Applikation erstellt werden und an die externe Signaturerstellungseinheit übermittelt werden. Ein Zugriff ist auch dann möglich, wenn die Signaturdaten von einer externen Applikation erstellt, jedoch über das Smartphone (z.B. über dessen Browser und Verwendung eines HTTP-POST Requests) an eine externe Signaturerstellungseinheit übermittelt werden.

5.3.2 Evaluierung

Im Folgenden werden die oben genannten Verfahren zur Signaturerstellung auf Smartphones verglichen und bezüglich der zuvor definierten Kriterien evaluiert. Für die

[105] http://support.google.com/accounts/bin/answer.py?hl=de&answer=181599

folgenden Analysen wird von einem Angreifer ausgegangen, der in der Lage sein möchte beliebige Signaturen ohne des Wissens des rechtmäßigen Benutzers durchzuführen.

Eine Übersicht über die Eigenschaften der drei Verfahren wird in der folgenden Tabelle gegeben. Diese basiert auf den oben genannten Kriterien.

Tabelle 1. Erfüllung der definierten Kriterien durch die verschiedenen Ansätze.

	microSD basierte Ansätze	*Handy-Signatur (Österreich)*	*SIM basierte Ansätze*
PIN Eingabe	Einfach	Mehrschichtig	Einfach
Dynamischer PIN Anteil	Nein	Ja	Nein
API	Ja	Ja	plattformspezifisch
Externer Kommunikationskanal	Nein	Ja	Nein (Nicht für PIN)
App Zugriff auf Signaturdaten	Ja	Abhängig von Verwendung	Nein
Lokation des SE	microSD Karte	Extern	SIM

5.3.2.1 microSD basierte Ansätze

Bei diesem Ansatz handelt es sich im Prinzip um ein klassisches SE, so wie es in Form eines Smartcard-Lesers ohne Secure PIN Pad und einer Smartcard am PC verwendet wird. Der wichtige Unterschied hierbei ist aber, dass im Gegensatz zu Reader und Smartcard am PC, die microSD[106] Karte und somit der Zugriff auf das SE immer zur Verfügung steht. Dies hat weitere Implikationen für Angriffe über Schadsoftware. Die einzelnen oben genannten Kriterien können von diesem Ansatz wie folgt erfüllt werden.

- **PIN-Eingabe**: Es wird eine statische PIN für die Authentifizierung beim SE verwendet.
- **Dynamischer PIN-Anteil**: Für die Authentifizierung am SE ist keine weitere dynamische PIN/TAN etc. notwendig.
- **API**: Es steht ein API zur Verfügung[107], das den Zugriff auf das SE und die PIN Eingabe erlaubt.
- **Externer Kommunikationskanal**: Wird nicht benötigt, da sich das SE im Gerät befindet und keine dynamische PIN Komponente verwendet wird.
- **Zugriff auf Signaturdaten**: Schadsoftware hat immer Zugriff auf die Signaturdaten, da die Signaturerstellungseinheit nur direkt über die APIs, die allen Applikationen zur Verfügung stehen, angesprochen werden kann.
- **Lokation des SE**: Das SE befindet sich auf der microSD Karte und somit direkt im Smartphone. Es besteht prinzipiell die Möglichkeit die Karte aus dem Smartphone zu entfernen. Es kann aber aufgrund des dazu nötigen Aufwands und der zusätzlichen Verwendung der microSD Karte zum Speichern von Daten davon ausgegangen werden, dass die Karte üblicherweise im Smartphone verbleibt.

[106] z.B.: Giesecke and Devrient, Mobile Security Card, http://www.gd-sfs.com/the-mobile-security-card/: Auf der Android Plattform kann dabei das SEEK API (http://code.google.com/p/seek-for-android/) verwendet werden um die Funktionen des SEs zu nutzen.

[107] Hier kann es plattformabhängige Unterschiede geben. Zumindest für Google Android ist ein derartiges API bekannt.

Durch diese Eigenschaften ergeben sich – trotz des SEs – für einen Angreifer unterschiedliche Möglichkeiten, um einen erfolgreichen Angriff durchzuführen. Im einfachsten Fall kann der Angreifer eine Applikation bereitstellen die mit Hilfe von Phishing die statische PIN des Benutzers ausliest und dann beliebige Signaturvorgänge durchführt. Da ein API für den Zugriff auf das SE zur Verfügung steht, kann der Angreifer eine Standardapplikation verwenden, die keine Sicherheitslücken des Betriebssystems ausnützen muss um den Angriff durchzuführen.

In Bezug auf den Zugriff auf die Signaturdaten können hier folgende Aussagen getroffen werden:

Wird eine externe Applikation verwendet, die die Signaturdaten erstellt und an das Smartphone übermittelt, so muss diese auch gewährleisten dass die signierten Daten nicht durch etwaige Malware am Smartphone verändert wurden. Dies kann z.B. durch den Vergleich der ausgesendeten nicht signierten Daten und der zurückübermittelten signierten Daten geschehen.

Wird eine Applikation verwenden, die die Signaturdaten direkt am Smartphone erstellt, so kann etwaige Malware mit Zugriff auf diese Applikation die Signaturdaten ohne das Wissen des Benutzers ändern. Hier kann prinzipiell auch keine externe Plausibilitätsprüfung durchgeführt werden, da die zu signierenden Daten am Smartphone erstellt werden.

5.3.2.2 Handy-Signatur

Die österreichische Handy-Signatur ist generell in der Lage alle Sicherheitsanforderungen, die für eine sichere Signaturerstellung notwendig sind, zu erfüllen. Soll auf eine Trennung der Kommunikationskanäle verzichtet werden und das Smartphone als alleiniges Endgerät im Zuge der Signaturerstellung verwendet werden, ergeben sich potentiell Einschränkungen der Sicherheit. In diesem Fall werden die Kriterien wie folgt erfüllt.

- **PIN-Eingabe**: Es wird ein Signatur-Passwort für die Erstauthentifizierung über das Internet benötigt.
- **Dynamischer PIN-Anteil**: Zusätzlich wird eine dynamische TAN über den zweiten SMS-Kommunikationskanal versendet. Eine Signatur kann nur dann erstellt werden wenn sowohl das statische Passwort als auch die TAN richtig eingegeben werden.
- **API**: Es steht ein API zur Verfügung, das den Zugriff auf das SE und die PIN/TAN Eingabe erlaubt. In diesem Fall erfolgt der Aufruf dieses APIs über webbasierte Schnittstellen.
- **Externe Kommunikationskanal**: Um auf das externe SE zuzugreifen wird sowohl das Internet als auch der SMS-Kommunikationskanal benötigt.
- **Zugriff auf Signaturdaten**: Je nach Anwendung können die Signaturdaten
    - von einer externen (Web-)Applikation erstellt und direkt an die externe Signaturerstellungseinheit übermittelt werden (nicht möglich bei microSD Lösung),
    - von einer externen (Web)-Applikation erstellt und an das Smartphone übermittelt werden, das diese Signaturdaten dann an die externe Signaturerstellungseinheit übermittelt (analog zu microSD),
    - oder direkt von einer Applikation am Smartphone erstellt werden, die diese dann an die externe Signaturerstellungseinheit übermittelt (analog zu microSD).
- **Lokation des SE**: Das SE befindet sich nicht auf dem Smartphone. Ein Zugriff auf das SE ist nach einer erfolgreichen Authentifizierung von überall unter Verwendung des Internets und des SMS-Kommunikationskanals möglich.

Im Gegensatz zum microSD Ansatz muss der Angreifer weitere Schritte durchführen, um eine Signatur erstellen zu können. Neben dem Auslesen der statischen PIN (z.B. über Phishing) muss auch noch bei jeder Signaturerstellung die dynamische TAN ausgelesen und

übermittelt werden. Dazu muss die dazugehörige SMS-Nachricht abgefangen werden. Um kein Misstrauen beim Benutzer zu erwecken, muss der Angreifer auch noch versuchen, diese SMS Nachricht vor dem legitimen Benutzer zu verstecken.

Die Implementierung eines erfolgreichen Angriffs gestaltet sich hier in der Praxis schon deutlich schwieriger als bei der microSD Lösung. Auch wenn das statische Passwort recht leicht durch Phishing abgefangen werden kann, so muss der Angreifer auch noch eine Möglichkeit finden unbemerkt die SMS-Nachricht abzufangen. Dazu wird eine Plattform benötigt, die die Möglichkeit bietet, die nötigen Hintergrunddienste zu implementieren. Außerdem muss die Plattform dem Angreifer erlauben, die empfangen SMS-Nachrichten abzufangen und zu verstecken.

Mit einer einfachen Standardapplikation kann hier auf Plattformen wie iOS und Windows Phone kein erfolgreicher Angriff mehr durchgeführt werden. Es müssen Sicherheitslücken im System oder andere aufwendigere Verfahren verwendet werden um die Signaturerstellung mit Hilfe von Malware durchzuführen.

In Bezug auf die Lokation der Signaturdaten können folgende Aussagen getroffen werden:

Verwendung von externen Webapplikationen: Beim eingesetzten Login-Verfahren erstellt die Webapplikation die Signaturdaten und übermittelt diese direkt an die externe Signaturerstellungseinheit. Der Smartphone-Benutzer erhält diese nur zur Anzeige, kann diese aber nicht ändern. Etwaige Malware könnte zwar die angezeigten Daten manipulieren, hat aber keine Möglichkeit die Signaturdaten zu ändern, da diese von der Webapplikation angegeben werden.

Allerdings, können externe Webapplikationen auch die Signaturdaten an das Smartphone übermitteln. Dies geschieht typischerweise im Browser, der die erhaltenen Signaturdaten dann an die externe Signaturerstellungseinheit übermittelt. In diesem Fall könnte Malware, die Zugriff auf den Browser hat, diese Daten manipulieren. Auch hier gilt, dass dies durch Plausibilitätsprüfungen bei der Webapplikation erkannt wird.

Die Handy-Signatur kann aber auch direkt aus Smartphone-Applikationen aus verwendet werden. Dabei werden die Signaturdaten von der Smartphone-Applikation erstellt und an die externe Signaturerstellungseinheit übermittelt. Hier gelten im Prinzip die gleichen Aussagen wie beim entsprechenden Fall der bei der microSD Lösung besprochen wurden.

5.3.2.3 SIM basierte Ansätze

Bei diesen Lösungen (z.B. estnische Mobiil-ID) befindet sich das SE auf der SIM Karte. Der Zugriff auf das SE für die Signaturerstellung erfolgt über SIM Toolkit Applikationen. Die Verwendung auf Smartphones ist dabei allerdings stark von der Plattform und der Art der Implementierung abhängig. So bietet z.B. Android in den neueren Versionen keine Unterstützung mehr für diese Art von Applikationen. Für die Analyse der Sicherheit dieser Verfahren spielt auch die Integration in die Plattform eine entscheidende Rolle. Steht z.B. ein API für das SE auf der SIM-Karte zur Verfügung, ist der Ansatz mit der microSD Lösung vergleichbar. Des Weiteren müssen auch die externen Prozessabläufe beim Erstellen einer Signatur betrachtet werden. Eine tiefergehende Analyse der aktuellen Smartphone-Plattformen im Zusammenhang mit den SIM Toolkit Applikationen liegt nicht im Rahmen dieser Studie. Im Folgenden werden daher nur allgemeine plattformunabhängige Punkte besprochen:

- **PIN-Eingabe**: Es wird eine statische PIN für die Authentifizierung beim SE verwendet.
- **Dynamischer PIN-Anteil**: Im Allgemeinen ist bei den analysierten Lösungen kein dynamischer PIN-Anteil vorhanden.
- **API**: Dies stellt den wichtigsten Punkt in der MSS Analyse dar. Wenn der Zugriff auf das SE einer SIM-Karte über ein API erfolgen kann, und die automatisierte Verwendung und Authentifizierung möglich ist, dann ist diese Lösung vergleichbar mit

den bereits diskutierten microSD basierten Lösungen. Die Implementierung der SIM Toolkit Funktionalität hängt jedoch stark von der verwendeten Plattform ab.

- **Externe Kommunikationskanal**: Für die Authentifizierung am SE wird kein externer Kommunikationskanal verwendet.
- **Zugriff auf Signaturdaten**: Obwohl sich die Signaturerstellungseinheit am Gerät befindet, ist im Allgemeinen der Zugriff von Schadsoftware auf diese Einheit nicht möglich. Eine detaillierte Analyse dieser Thematik wird in weiteren Studien vorgesehen.
- **Lokation des SE**: Das SE befindet sich auf der SIM-Karte des Smartphones. Da die SIM-Karte eine für die Funktion des Smartphones relevante Komponente ist, kann davon ausgegangen werden, dass sie vom Benutzer nicht entfernt wird und somit permanent zur Verfügung steht.

5.4 Schlussfolgerungen

Generell kann festgehalten werden, dass die österreichische Handy-Signatur bzw. der von ihr verfolgte zentrale Ansatz einige Vorteile gegenüber anderen etablierten Verfahren bietet. Hier können vor allem das einfache Roaming zwischen verschiedenen Mobilfunkbetreibern und der Umstand, dass Signaturdaten nur zwischen zentralen Komponenten ausgetauscht werden genannt werden. Die Handy-Signatur erweist sich auch als zukunftssicher in Bezug auf eine mögliche Verwendung auf Smartphones. Da das mobile Endgerät ausschließlich für den Empfang von SMS-Nachrichten verwendet wird, kann die Handy-Signatur auch auf Smartphones problemlos verwendet werden. Im Gegensatz dazu scheinen MSS basierte Verfahren, die auf SIM Toolkit Applikationen beruhen, problematischer. Da die Unterstützung für SIM Toolkit Applikationen auf Smartphones stark vom mobilen Betriebssystem bzw. dessen Version abhängt, kann die Funktionalität MSS basierter Verfahren auf Smartphones beeinträchtigt sein.

Für eine Verwendung im Rahmen mobiler Anwendungen sind natürlich vor allem jene Verfahren interessant und besonders geeignet, die eine vollständig mobile Signaturerstellung erlauben. Für die Handy-Signatur ist dies nur bedingt erfüllt, da ja für eine vorschriftsmäßige Verwendung zwei getrennte Kommunikationskanäle vorgesehen sind. Für eine mobile Verwendung sind also zwei mobile Endgeräte notwendig, wovon zumindest eines web-fähig sein müsste. Auch wenn Mobiltelefone eine immer größere Verbreitung finden, haben nur die wenigsten Benutzer zwei Geräte parallel im Betrieb. Wird der gesamte Signaturvorgang über ein und dasselbe Gerät abgewickelt, ergeben sich entsprechende Sicherheitsrisiken. Die durchgeführte Analyse zeigte, dass jedoch auch andere Verfahren (z.B. SIM basierte Methoden) problematisch sein können, wenn diese auf einem Smartphone ausgeführt werden.

Im folgenden Abschnitt werden mögliche Verbesserungspotentiale mobiler Signaturlösungen aufgezeigt. Ziel ist die Erweiterung bestehender bzw. die Entwicklung neuer Ansätze, die eine sichere und vollständig mobile Signaturerstellung auf Smartphones erlauben. Hauptaugenmerk wird auf die österreichische Handy-Signatur gelegt. Gründe sind derer vielversprechender Ansatz, der diverse Vorteile gegenüber anderen Verfahren aufweist sowie das gegebene Nahverhältnis zu dieser Technologie.

6 Forschungsfelder

Prinzipiell kann jede Signaturlösung mit dem entsprechenden Aufwand geeignet abgesichert werden. Dieser Aufwand ist in der Praxis jedoch oft nicht umsetzbar, oder würde zu einer immensen Verkomplizierung des gesamten Signaturprozesses führen, was wiederum die Benutzerfreundlichkeit der mobilen Signaturlösung drastisch reduzieren würde.

Im Rahmen dieser Studie möchten wir dennoch ein breites Spektrum an möglichen Adaptierungen skizzieren. Im Vordergrund soll die Erhöhung der Sicherheit und die Gewährleistung der Zukunftssicherheit bestehender Lösungen stehen. Negative Auswirkungen diskutierter Erweiterungen auf die Benutzerfreundlichkeit der Gesamtlösung und praktische Umsetzbarkeit sollen zwar erwähnt, jedoch nicht sofort als Ausschlusskriterium herangezogen werden.

Um dennoch einen entsprechenden Bezug zur Realität sicherzustellen, sollen nur jene Adaptierungen und Weiterentwicklungen vorgeschlagen werden, die auch tatsächlich mit vertretbarem Aufwand praktisch umsetzbar sind. Es wäre beispielsweise einfach als Lösung aller eventuellen Restrisiken die Integration eines Secure Pin-Pads und einer sicheren (vertrauenswürdigen) Anzeige in Smartphones zu fordern. Im Wissen zukünftige hardwaretechnische Entwicklungen am Smartphone-Sektor kaum beeinflussen zu können, werden derartige Vorschläge in dieser Studie nicht betrachtet. Stattdessen wird das Augenmerk auf zentrale Komponenten und das Konzept der Handy-Signatur selbst gelegt und Möglichkeiten diskutiert die Sicherheit der Gesamtlösung auf Smartphones weiter zu erhöhen. Das Smartphone selbst wird dabei stets als potentiell unsicheres Gerät betrachtet.

Grundsätzlich können zur weiteren Gewährleistung der Sicherheit der Handy-Signatur auf Smartphones zwei Strategien verfolgt werden. Ziel kann und muss es in jedem Fall sein den Missbrauch der Handy-Signatur durch Angreifer zu verhindern. Entsprechende Möglichkeiten werden in Abschnitt 6.1 skizziert. Im Bewusstsein, dass erfolgreiche Angriffe mit genügend großem Aufwand durchgeführt werden können, muss das zweite Ziel eine möglichst rasche Erkennung des Missbrauchs sein. Abschnitt 6.2 widmet sich verschiedenen Möglichkeiten dies umzusetzen.

6.1 Verhindern von Missbrauch

Ein erfolgreicher Angriff auf die Handy-Signatur umfasst zumindest die folgenden Schritte:

- Ermittlung des Signatur-Passworts des Opfers
- Abfangen der mobilen TAN zur eigenen Nutzung

Wird die Handy-Signatur nur auf einem Gerät – dem Smartphone – ausgeführt, werden sowohl Signatur-Passwort als auch TAN über ein und denselben Kommunikationskanal übermittelt. Einem Angreifer reicht in diesem Fall die Kontrolle über ein Gerät um die Sicherheit der Handy-Signatur zu untergraben. Gelingt es jedoch, zumindest eine dieser beiden Komponenten geeignet zu schützen, kann ein erfolgreicher Angriff verhindert werden. Im Folgenden werden mögliche Ansätze diskutiert, die Angriffe auf das Signaturpasswort oder die mobile TAN verhindern und damit Angriffe erschweren könnten.

6.1.1 Verhindern von Angriffen auf das Signatur-Passwort

Ein zentrales zu schützendes Asset der Handy-Signatur-Lösung ist das Signatur-Passwort des Benutzers. Hierbei handelt es sich um ein textbasiertes statisches Passwort, welches bei jedem Signaturvorgang – und somit auch bei jeder Authentifizierung – an den Betreiber der Handy-Signatur übertragen werden muss. Auf Smartphones kann derzeit nicht ausgeschlossen werden, dass das Passwort im Zuge der Eingabe von Schadsoftware heimlich aufgezeichnet wird. Durch die statische Natur des Signatur-Passworts haben

Angreifer bei jedem Signaturvorgang die Chance das Passwort herauszufinden und in weiterer Folge missbräuchlich zu verwenden.

Aus derzeitiger Sicht ergeben sich folgende Möglichkeiten die Sicherheit des Signatur-Passworts zu erhöhen.

- **Alternative zu Passwörtern:** Der vielleicht nächstliegende Ansatz zur Verhinderung von Angriffen auf das Signatur-Passwort ist dessen Verwendung gänzlich zu vermeiden. Diesem Ansatz folgend muss jedoch zur Gewährleistung des Zweifaktorprinzips ein neuer Faktor in die Authentifizierung eingebracht werden. Die Verwendung von Biometrie wäre eine theoretische Möglichkeit, die auf aktuellen Smartphones aber wohl noch schwer umzusetzen wäre. Derzeit beschränken sich biometrische Verfahren hauptsächlich auf Authentifizierungen gegen das Gerät. Biometrische Ansätze zur Remote-Authentifizierung von Benutzern über potentiell unsichere Netzwerke konnten sich bis dato noch nicht entscheidend durchsetzen. Als interessante Alternative zu textbasierten Passwörtern könnte sich eventuell auch die Verwendung graphischer Passwörter, wie sie u.a. in [22] diskutiert wurden, erweisen. Entsprechende Lösungen wurden bereits vorgestellt[108]. Deren Sicherheit müsste gegebenenfalls in nachfolgenden Studien analysiert werden um deren Verwendbarkeit für sicherheitskritische Anwendungen zu evaluieren. Ähnlich wie bei Captcha-basierten Anwendung stellt sich jedoch natürlich auch bei graphischen Passwörtern die Frage nach der Zugänglichkeit.
- **Verwendung eines dynamischen Passworts:** Durch die Verwendung eines dynamischen Passworts, das sich nach jedem Signaturvorgang ändert, könnte ein Angriff auf dieses entscheidend verkompliziert werden[109]. Ein vom Angreifer unerlaubt aufgezeichnetes Passwort könnte in diesem Fall nicht für zukünftige Signaturvorgänge verwendet werden. Dieser theoretische Ansatz wirft jedoch die Frage auf, wie ein dynamisches Passwort, das sich nach jedem Signaturvorgang ändert, sicher zwischen Benutzer und Handy-Signatur-Betreiber ausverhandelt werden könnte. Auf einen ersten Blick ergeben sich hierfür zwei Möglichkeiten. Das neue Passwort kann entweder über eine SMS/MMS-Nachricht zugestellt werden, oder aber über den Web-Kanal dem Benutzer angezeigt werden. In beiden Fällen ergibt sich das Problem, dass das neue Passwort über das potentiell unsichere Smartphone zugestellt wird und daher nicht sicher vor einer Kompromittierung ist. Eine automatische Extrahierung des Passworts durch Schadsoftware könnte durch Verwendung der Captcha-Technologie zumindest erschwert werden[110]. In diesem Fall müsste die Schadsoftware das in einem Captcha enthaltene Passwort an den Angreifer weiterleiten, der dieses manuell lösen müsste.
- **Zero Knowledge Password Proof:** Angriffe auf das Signatur-Passwort des Benutzers beruhen auf der Tatsache, dass dieses Passwort im Zuge eines Signaturerstellungsvorgangs auf einem potentiell unsicheren Gerät eingegeben werden muss. Erst dadurch ist es dem Angreifer möglich das Passwort aufzuzeichnen und in weiterer Folge missbräuchlich zu verwenden. Ein Ansatz zur Erhöhung der Sicherheit wäre daher, die Eingabe des Passworts selbst obsolet zu machen. Nichtsdestotrotz muss der Benutzer den Betreiber der Handy-Signatur davon überzeugen im Besitz des geheimen Passworts zu sein. Die Erbringung des Nachweises im Besitz eines Passworts zu sein ohne dieses selbst kommunizieren zu

[108] http://www.isss.ch/veranstaltungen/2010/alternativen-zum-passwort/

[109] Durch die Verwendung eines veränderlichen Passworts würde jedoch auch die Benutzerfreundlichkeit dieser Lösung drastisch reduziert werden.

[110] Captcha-basierte Lösungen haben oft schwerwiegende Nachteile bezüglich Zugänglichkeit. Dies ist vor allem im Zusammenhang mit E-Government-Lösungen zu bedenken, welche besondere Anforderungen an die Zugänglichkeit haben.

müssen kann über Zero Knowledge Password Proofs implementiert werden. Aktuell bekannte Vertreter dieses Verfahrens beruhen jedoch auf einigermaßen komplexen kryptographischen Operationen. Eine sichere Durchführung dieser Operationen auf dem potentiell unsicheren Gerät müsste daher gewährleistet werden.Verhindern von Angriffen auf die mobile TAN

6.1.2 Verhindern von Angriffen auf die TAN

Konnte das Signatur-Passwort vom Angreifer erfolgreich kompromittiert werden, ist für einen erfolgreichen Angriff außerdem noch Zugriff auf die mobile TAN, die an das Mobiltelefon des Benutzers geschickt wird, nötig. Zur Klassifizierung möglicher Gegenmaßnahmen für Angriffe auf die TAN muss zunächst zwischen zwei möglichen Angriffsszenarien unterschieden werden.

- **Angriffsszenario A:** In diesem Szenario ist das Smartphone des Benutzers mit Schadsoftware infiziert. Diese hat weitgehend uneingeschränkte Möglichkeiten auf dem mobilen Gerät und kann Signaturerstellungsprozesse vollkommen selbstständig – ohne manuelles Eingreifen des Angreifers – durchführen. Die Schadsoftware ist also in der Lage das Signatur-Passwort des Benutzers zu sniffen, dessen Telefonnummer herauszufinden, einen Signaturprozess zu starten, die empfangene TAN unbemerkt vom Benutzer abzufangen und diese wieder an den Handy-Signatur-Betreiber zu senden.
- **Angriffsszenario B:** Auch in diesem Szenario ist das Smartphone des Benutzers mit Schadsoftware infiziert. Zur Durchführung eines Signaturerstellungsprozesses ist allerdings das aktive Mitwirken eines Angreifers nötig. Die Schadsoftware ist in der Lage für den Angriff relevante Daten wie das Signatur-Passwort zu ermitteln und TANs abzufangen. Diese Daten werden jedoch nicht von der Schadsoftware selbst verwendet, sondern an den Angreifer über einen Kommunikationskanal des Smartphones weitergeleitet.

Angriffen auf die mobile TAN kann auf drei Ebenen begegnet werden. Sicherheitsmechanismen, die auf diesen drei Ebenen ansetzen, können einem oder mehreren der oben genannten Angriffsszenarien entgegenwirken. Gegenmaßnahmen können folgenden Ebenen zugordnet werden.

- **Abfangen der TAN verhindern:** Ziel ist es hier, das Abfangen der mobilen TAN durch Schadsoftware generell zu verhindern.
- **Automatische Verarbeitung der TAN verhindern:** Ziel ist es, die automatische Verarbeitung der TAN durch Schadsoftware zu verhindern.
- **Weiterleitung der TAN verhindern:** Hier soll einer potentiellen Schadsoftware die Möglichkeit genommen werden, eine abgefangene TAN an den Angreifer weiterzuleiten.

Die wirkungsvollste Strategie ist offensichtlich die unter dem ersten Punkt erwähnte Verhinderung des Abfangens einer mobilen TAN. Wird dies von Haus aus unterbunden, kann ein erfolgreicher Angriff ausgeschlossen werden. Der dadurch erreichte Schutz umfasst sowohl Angriffsszenario A als auch Angriffsszenario B.

Die Verhinderung einer automatischen Verarbeitung einer abgefangenen TAN würde zumindest Angriffsszenario A entschärfen. Ein erfolgreicher Angriff könnte jedoch weiter durchgeführt werden wenn ein Angreifer persönlich involviert ist. Kann allerdings neben der automatischen Verarbeitung der TAN auch eine Weiterleitung (an den Angreifer) ausgeschlossen werden, kann wiederum ein vollständiger Schutz gegen beide Angriffsszenarien erreicht werden.

Die Sicherheit der mobilen Signaturerstellung über die Handy-Signatur auf Smartphones kann also entweder durch Verhinderung des Abfangens der TAN, oder durch Verhinderung einer automatischen Verarbeitung der TAN bei gleichzeitiger Verhinderung einer möglichen

Weiterleitung der TAN erreicht werden. Mögliche den einzelnen Strategien zuordenbare Gegenmaßnahmen werden in den folgenden Unterabschnitten skizziert.

6.1.2.1 Verhinderung des Abfangens der TAN

Die wirkungsvollste und zugleich am schwierigsten zu implementierende Maßnahme ist die Verhinderung des Abfangens der mobilen TAN. Folgende Ansätze können dazu theoretisch verfolgt werden.

- **Sicherstellung der Sicherheit und Integrität des Smartphones:** Grundvoraussetzung für einen erfolgreichen Angriff ist die Möglichkeit das Smartphone des Benutzers mit Schadsoftware zu infizieren. Kann diese Möglichkeit durch entsprechende Sicherheitsmechanismen ausgeschlossen werden, können Angriffe verhindert werden. Eine weitere Möglichkeit besteht darin, die Infizierung eines Smartphones bzw. ein unzulässiges Verhalten wie das Abfangen von SMS-Nachrichten zuverlässig zu detektieren. Erfahrungen aus der PC-Domäne zeigen jedoch, dass Entwickler von Schadsoftware in der Regel stets einen Schritt voraus sind. Auf neue Gefahren kann zwar relativ rasch entsprechend reagiert werden, die vollkommene Sicherheit von Geräten ist jedoch schwer bis unmöglich zu gewährleisten. Signaturlösungen für Smartphones sollten daher im Idealfall einen Ansatz verfolgen, dessen Sicherheit auch von infizierten Smartphones nicht beeinträchtigt werden kann.
- **Übertragung der TAN über alternativen Kanal:** Hauptproblem bei der Verwendung der Handy-Signatur ausschließlich auf Smartphones ist der Wegfall des zweiten Kommunikationskanals. Sowohl Signaturpasswort als auch mobile TAN werden über das Smartphone, welches als gemeinsames Endgerät sowohl für den Web-Kanal als auch für den mobilen Kanal dient, übertragen. Die Sicherheit der mobilen TAN könnte daher bedeutend gesteigert werden, wenn die TAN über einen alternativen Kanal übertragen werden würde. Um den mobilen Charakter zu wahren, müsste dieser Kanal dem Benutzer wie ein Smartphone ständig zur Verfügung stehen. Da Smartphones heutzutage bereits für die meisten alltäglichen Aufgaben verwendet werden können, ist die Auswahl an zusätzlichen Geräten, die Benutzer ständig bei sich tragen und als Kommunikationsendpunkt für einen Kanal zum Betreiber der Handy-Signatur dienen könnten, begrenzt. Tatsächlich scheint es weit praxisnäher Möglichkeiten zu erwägen einen sicheren zweiten Kommunikationskanal am Smartphone selbst zu etablieren. Denkbar wäre beispielsweise die Verwendung der VM Technologie um auf einem Smartphone zwei virtuelle Maschinen zu betreiben. Diese könnten dann jeweils als Endpunkt für einen Kommunikationskanal dienen. Für einen erfolgreichen Angriff müsste Schadsoftware auf beiden virtuellen Systemen installiert werden. Auch die Verwendung von Trustzones könnte helfen auf einem potentiell unsicheren Gerät einen sicheren geschützten Bereich zu etablieren.
- **Manuelle Aktivierung der Signaturfunktion:** Eine zentrale Eigenschaft der beiden oben beschriebenen Angriffsszenarien ist der Umstand, dass die Signatur durch den Angreifer oder die Schadsoftware vollständig unbemerkt vom Benutzer durchgeführt wird. Ein Ansatz wäre daher, das Verfahren dahingehend zu ändern, dass vor der manuellen Signaturerstellung die Signaturfunktionalität am Server vom Benutzer „aktiviert“ werden muss. Dieser Ansatz impliziert jedoch, dass eine Möglichkeit gefunden werden muss einen potentiellen Angreifer daran zu hindern, die Signatur anstelle des legitimen Benutzers zu aktivieren. Dies führt unweigerlich zur zentralen Frage wie der Betreiber der Handy-Signatur zuverlässig einen Angreifer von einem legitimen Benutzer unterscheiden kann. Die Verwendung von biometrischen Ansätzen schein hier wieder naheliegend. Denkbar wäre beispielsweise ein Challenge-Response Protokoll, welches vorsieht dass der Benutzer als Challenge einen dynamischen Text zugeschickt bekommt und diesen über die Telefonleitung dem zentralen Service vorlesen muss. Das Service kann den Benutzer dann anhand

seiner Stimme als legitimen Benutzer identifizieren. Eine Benutzerauthentifizierung über Stimme wird beispielsweise seit einiger Zeit von der Deutschen Post erfolgreich für interne Dienste (automatisiertes Rücksetzen von Passwörtern) eingesetzt. Während sich dieses Verfahren für eine geschlossene Benutzergruppe in einem internen Netzwerk bewährt hat, bleibt die Tauglichkeit und Sicherheit dieses Verfahrens in einem offenen Netz wie dem Internet fraglich.

6.1.2.2 Verhinderung der automatischen Verarbeitung der TAN

Zur Verhinderung einer automatischen Verarbeitung der TAN bietet sich die Verwendung der Captcha-Technologie an. Wird die TAN in einem Captcha kodiert zugestellt, kann eine auf dem Smartphone installierte Schadsoftware diese nur schwer extrahieren und an den Betreiber der Handy-Signatur zurückschicken. Diese Vorgehensweise kann zu einer generelleren Anforderung verallgemeinert werden: Die zugestellte TAN sollte eine Challenge enthalten, die nur vom legitimen Benutzer, jedoch nicht von etwaiger Schadsoftware gelöst werden kann. Vor allem im E-Government-Kontext ergibt sich die Zugänglichkeit als zusätzliche Anforderung, die beispielsweise eine Verwendung von Captchas verkompliziert.

6.1.2.3 Verhinderung der Weiterleitung einer TAN

Kann eine Weiterleitung der TAN verhindert und gleichzeitig eine automatische Verarbeitung der TAN ausgeschlossen werden, können Angriffe auf die Handy-Signatur weitgehend verhindert werden. Um die Weiterleitung einer TAN zu verhindern, könnten folgende Ansätze verfolgt werden:

- **Aktives Abholen der TAN:** Eine unbemerkt vom Benutzer stattfindende automatische Weiterleitung der TAN könnte verhindert werden, wenn der Benutzer aktiv in den Prozess der Zustellung involviert wäre. Denkbar wäre beispielsweise, dass der Benutzer die TAN nicht automatisch zugestellt bekommt, sondern aktiv abholen muss. Dies führt jedoch wiederum zu der bereits im Abschnitt über das Verhindern des Abfangens der TAN (Abschnitt 6.1.2.1) diskutierten Frage wie gewährleistet werden kann, dass nur der legitime Benutzer, nicht jedoch ein Angreifer eine TAN abholen kann und somit ein legitimer Benutzer von einem Angreifer unterschieden werden kann.
- **Binden der TAN an das Smartphone des Benutzers:** Eine weitere Möglichkeit bestünde darin, die Weiterleitung einer TAN zwar nicht direkt zu unterbinden, diese jedoch auf anderen Endgeräten wertlos zu machen. Dazu müsste die TAN kryptographisch an das Smartphone des legitimen Benutzers gebunden werden. Denkbar wäre beispielsweise die verschlüsselte Übertragung der TAN. Eine Entschlüsselung wäre nur mit einem entsprechenden Schlüssel, der sicher in einem Secure Element des Zielgeräts gespeichert ist, möglich. Bei diesem Ansatz wäre jedoch darauf zu achten, dass der Zugriff auf das Secure Element für Schadsoftware und Angreifer nicht möglich ist. Alternativ wäre auch die Signierung der TAN durch den legitimen Benutzer denkbar. Hier könnte ebenfalls ein Secure Element oder aber ein externes NFC-Tag mit entsprechender Funktionalität zur Anwendung kommen.

6.1.2.4 Vermeidung von mobilen TANs

Um Angriffe auf die mobilen TANs der Handy-Signatur zu verhindern, bietet sich neben den in den vorigen Abschnitten erwähnten Strategien theoretisch noch eine weitere Option: Die vollständige Vermeidung von mobilen TANs. Sinn und Zweck der mobilen TAN ist die Verifikation, ob sich der Benutzer zum Zeitpunkt der Signaturerstellung im Besitz seines Smartphones befindet. Über die TAN wird dadurch der Faktor Besitz der Zweifaktorauthentifizierung abgedeckt.

Sollen mobile TANs vermieden werden, muss eine alternative Möglichkeit des Besitznachweises gefunden werden. Eventuell kann auch ein alternatives Token herangezogen werden, dessen Besitz einfacher nachgewiesen werden kann.

6.2 Erkennung von Missbrauch

Primäres Ziel sollte in jedem Fall sein einen etwaigen Missbrauch der Signaturfunktion zu vermeiden. Mögliche Ansätze zur Erreichung dieses Ziels wurden in den vorangegangen Abschnitten skizziert. Konnte ein Missbrauch trotz aller ergriffener Gegenmaßnahmen nicht verhindert werden, so sollte zumindest sichergestellt werden, dass dieser im Nachhinein erkannt werden kann.

Eine einfache Möglichkeit wäre, dem Benutzer nach jeder erfolgten Signaturerstellung eine Bestätigungsnachricht in Form einer SMS zu schicken. Bekommt der Benutzer eine derartige Nachricht ohne selbst eine Signatur erstellt zu haben, kann von einem Missbrauch durch einen Angreifer ausgegangen werden. Dieser SMS basierte Ansatz bietet jedoch den Nachteil, dass für die Zustellung der Bestätigung derselbe Kommunikationskanal wie für die Durchführung der Signatur verwendet wird. Hat ein Angreifer Zugriff auf diesen ist es naheliegend, dass dieser nicht nur für die missbräuchliche Signaturerstellung verwendet wird, sondern auch dafür Sorge getragen wird die Bestätigungsnachricht vor dem legitimen Benutzer zu verbergen. Kann ein Angreifer den Empfang einer mobilen TAN vom Benutzer verbergen, ist davon auszugehen, dass dies auch für Bestätigungsnachrichten möglich ist.

Es scheint daher ratsam, für den Empfang der Bestätigungsnachricht einen alternativen Kommunikationskanal zu wählen. E-Mail ist hierfür eine naheliegende Lösung. Wird jede Signaturerstellung über eine E-Mail bestätigt, kann der Benutzer eine missbräuchliche Verwendung seines Signaturschlüssels ebenfalls nachvollziehen. Allerdings könnte es potentiell länger dauern bis ein Missbrauch entdeckt wird, da SMS-Nachrichten Benutzer in der Regel schneller erreichen als E-Mails. Zudem besteht ein Restrisiko, wenn das Smartphone für den Zugang zum eigenen E-Mail-Konto verwendet wird und der Angreifer auf diese Weise Zugang zum E-Mail Konto erlangen kann. In diesem Fall können entsprechende Bestätigungsmails unbemerkt vom Benutzer gelöscht werden. Der Aufwand wäre in diesem Fall für den Angreifer jedoch ungleich größer als bei einer Zustellung per SMS.

Als dritte Alternative könnten durchgeführte Signaturerstellungsvorgänge auch über ein Web-Portal zugänglich gemacht werden. Durch eine sichere Authentifizierung geschützt könnten Benutzern Protokolle ihrer eigenen Signaturerstellungsvorgänge zugänglich gemacht werden. Verschafft sich ein Angreifer unerlaubt Zugriff auf diese Daten, können diese trotzdem nicht geändert oder gelöscht werden, solange das Web-Portal keine entsprechende Funktionalität zur Verfügung stellt. Stattdessen könnten Einträge automatisch nach einer bestimmten Zeitspanne gelöscht werden.

7 Schlussfolgerungen

Ziel dieser Studie war die Erhebung und Analyse bestehender mobiler Signaturlösungen in Europa. Dabei stellte sich heraus, dass derzeit prinzipiell zwei verschiedene Ansätze zum Einsatz kommen. Vor allem in Skandinavien und in den baltischen Ländern ist der auf dem ETSI Standard basierende MSS-Ansatz stark verbreitet. Dieser sieht die SIM-Karte des Mobiltelefons als Signaturerstellungseinheit vor. Eine zentrale Rolle nimmt u.a. das finnische Unternehmen Valimo Wireless Ltd. ein, welches entsprechende Komponenten für MSS basierte Signaturlösungen anbietet. Neben dem MSS basierten Ansatz kommt auch der von Österreich gewählte zentrale Mehrkanalansatz, der minimale technische Anforderungen an das verwendete Telefon stellt, zum Einsatz. Dieser basiert auf einem zentralen HSM, in welchem die Signaturschlüssel sämtlicher registrierter Benutzer verwahrt sind und welches für die Signaturerstellung verantwortlich ist. Einem Signaturerstellungsvorgang muss eine Benutzerauthentifizierung vorangehen, welche auf Bekanntgabe eines geheimen Passworts und eines dynamischen Einmalpassworts, welches per SMS zugestellt wird, beruht.

Im Zusammenhang mit Smartphones müssen diese etablierten Technologien zur Erstellung mobiler Signaturen in Bezug auf die Sicherheit neu evaluiert werden, da sich aufgrund der hochentwickelten Smartphone-Betriebssysteme neue Gefahren ergeben können. In einem ersten Schritt wurde die prinzipielle Anwendbarkeit der beiden Verfahren auf Smartphones evaluiert. Dabei stellte sich heraus, dass die Handy-Signatur problemlos auch auf Smartphones verwendbar ist, da diese nur minimale Anforderungen an das mobile Endgerät stellt. Da dieses im Prinzip ausschließlich als Empfangseinheit für die mobile TAN dient, kann diese Aufgabe auch von jedem Smartphone erledigt werden. Für MSS basierte Verfahren ist die Situation komplizierter. Es stellte sich heraus, dass die Anwendbarkeit MSS basierter Verfahren grundsätzlich davon abhängt ob das verwendete Smartphone in der Lage ist die nötige SIM Toolkit Applikation auszuführen und damit das Secure Element der SIM-Karte entsprechend anzusprechen. Diese Frage muss für jede Smartphone-Plattform (und z.T. auch für jede Version des verwendeten Betriebssystems) getrennt beantwortet werden.

Für zukünftige mobile Anwendungen erscheinen vor allem jene Lösungen interessant, die vollständig auf Smartphones durchgeführt werden können. Um einen Vergleich der verschiedenen Verfahren auf Smartphones zu ermöglichen, wurden in dieser Studie diverse Kriterien definiert, mit denen die analysierten Lösungen beschrieben werden können. Anhand dieser Eigenschaften und verschiedener Angriffsszenarien lassen sich etwaige Angriffspunkte erkennen. Eine interessante Schlussfolgerung dabei ist, dass der Einsatz eines SEs, das die automatisierte Verwendung über ein API erlaubt, leichter angegriffen werden kann als andere Verfahren, die auf mehreren Kommunikationskanälen basieren. Obwohl bei Verwendung eines Smartphones die erhöhte Sicherheit durch die Verwendung von unterschiedlichen Geräten entfällt, stellt die dynamische Komponente (TAN) einen Mehraufwand für einen Angreifer dar. Außerdem kann abhängig von der Plattform ein erfolgreicher Angriff nicht immer mit Standardapplikationen durchgeführt werden, sondern erfordert das Ausnutzen von Sicherheitslücken des Betriebssystems.

Die Handy-Signatur erscheint daher auch im Rahmen einer ausschließlichen Verwendung auf einem Smartphone (und bei bewusstem Verzicht auf einen alternativen Kommunikationskanal) vorteilhaft gegenüber anderen Ansätzen. Trotzdem ergeben sich durch die Reduktion auf ein Kommunikationsgerät Sicherheitsrisiken, die im Rahmen sicherheitskritischer Anwendungen unter Umständen nicht akzeptiert werden können. Um die Sicherheit der Handy-Signatur weiter zu erhöhen und den potentiellen Wegfalls des alternativen Kommunikationskanals kompensieren zu können wurden in dieser Studie diverse Möglichkeiten erarbeitet wie das bestehende Verfahren adaptiert und erweitert

werden könnte. Diese Vorschläge können als Basis für Weiterentwicklungen der Handy-Signatur und für ein sicheres zukünftiges mobiles E-Government dienen.

Referenzen

[1] Thoms Knall, Arne Tauber: Grundsatzpapier Mobile Signatur. https://demo.egiz.gv.at/plain/content/download/583/3362/file/Grundsatzpapier-Mobile-Signatur.pdf, 2008

[2] TÜV-iT Arbeitspapier „Mobile elektronische Signaturen“. http://mediakomm.difu.de/documents/forschung/mobile---signatur.pdf, 2002

[3] The New York Times: Tech Brief: German Mobile Standard, http://www.nytimes.com/2001/03/26/business/worldbusiness/26iht-techbrief_ed3__67.html, 2001

[4] Golem.de: mSign stelt Schnittstelle für mobilen m-Commerce vor, http://www.golem.de/0010/10335.html, 2000

[5] Finextra: Brokat introduces mobile digital signature software, http://www.finextra.com/news/fullstory.aspx?newsitemid=1673, 2001

[6] Michael Hartmann, Levona Eckstein: TruPoSign – A trustworthy and mobile platform for electronic signatures. Securing electronic business processes : Highlights of the Information Security Solutions Europe 2003 Conference, 2003

[7] RICHTLINIE 1999/93/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:013:0012:0020:DE:PDF, 2000

[8] Martinez-Diaz, M.; Fierrez, J.; Galbally, J.; Ortega-Garcia, J.: Towards mobile authentication using dynamic signature verification: Useful features and performance evaluation. 19th International Conference on Pattern Recognition, 2008

[9] Heiko Rossnagel: Mobile Qualified Electronic Signatures and Certification on Demand. In Proceedings of EuroPKI'2004. pp.274~286, 2004

[10] Antonio Ruiz-Martínez, Daniel Sánchez-Martínez, María Martínez-Montesinos and Antonio F. Gómez-Skarmeta: A Survey of Electronic Signature Solutions in Mobile Devices. Journal of Theoretical and Applied Electronic Commerce Research ISSN 0718-1876 Electronic Version VOL 2 / ISSUE 3 / DECEMBER 2007 / 94 – 109, 2007

[11] Antonio Ruiz-Martínez, Juan Sánchez-Montesinos, Daniel Sánchez-Martínez: A mobile network operator-independent mobile signature service. Journal of Network and Computer Applications (2011) Volume: 34, Issue: 1, Pages: 294-311, 2009

[12] Evgenia Pisko: Mobile Electronic Signatures: Progression from Mobile Service to Mobile Application Unit. International Conference on the Management of Mobile Business, 2007. ICMB, 2007

[13] Mohammad Hasan Samadani, Mehdi Shajari, Mohammad Mehdi Ahaniha: Self-Proxy Mobile Signature. 24th International Conference on Advanced Information Networking and Applications Workshops (WAINA), 2010

[14] Martijn Oostdijk, MaartenWegdam: Mobile PKI – A technology scouting for security

and use of mobile authentication technologies, http://www.terena.org/news/community/download.php?news_id=2528, 2009

[15] epractice.eu: An overview of the eGovernment and eInclusion status in Europe, http://www.epractice.eu/factsheets, 2011

[16] Thomas Zefferer, Peter Teufl, Herbert Leitold: Mobile qualifizierte Signaturen in Europa, In Datenschutz und Datensicherheit 11/2011, Gabler Verlag, 2011

[17] Clemens Orthacker, Martin Centner, Christian Kittl: Qualified Mobile Server Signature. In: Proceedings of the 25th TC 11 International Information Security Conference SEC 2010, 2010

[18] Ross J. Anderson: Security Engineering: A Guide to Building Dependable Distributed Systems. John Wiley and Sons, 2010

[19] Peter Laud, Meelis Roos: Formal Analysis of the Estonian Mobile-ID Protocol. In Proceedings of the 14th Nordic Conference on Secure IT Systems: Identity and Privacy in the Internet Age (NordSec '09), Springer-Verlag, 2009

[20] Bruce Schneier: Two-Factor Authentication: Too Little, Too Late. Communications of the ACM vol 48, n 4, http://www.schneier.com/essay-083.html, 2005

[21] Peter Schartner, Stefan Bürger: Attacking mTAN-Applications like e-Banking and mobile Signatures. Klagenfurt: syssec, Juni 2010 (Technical Reports, TR-syssec-11-01), 7 pp.

[22] Xiaoyuan Suo, Ying Zhu, G. Scott. Owen: Graphical Passwords: A Survey. In *Proceedings of the 21st Annual Computer Security Applications Conference* (ACSAC '05). IEEE Computer Society, Washington, DC, USA, 2005

[23] M. Ivkovic, U. Keskel, T. Knall, H. Leitold, T. Martens: STORK Work Item 3.3.6 Mobile eID, STORK-eID Consortium, https://www.eid-stork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=1385, 2009

[24] FESA: Public Statement on Server Based Signature Services, http://www.fesa.eu/public-documents/PublicStatement-ServerBasedSignatureServices-20051027.pdf, 2005