



Grundsatzpapier Mobile Signatur

Schwerpunktthema Bürgerkarte und eID

Version 1.0, 22.04.2008

DI Thomas Knall – thomas.knall@egiz.gv.at

DI Arne Tauber – arne.tauber@egiz.gv.at

Zusammenfassung: Mit dem Ende der A1-Signatur sind Bürgerkartenlösungen ohne Kartenleser nicht mehr gegeben. Dieses Grundsatzpapier stellt verschiedene Lösungen zur Erstellung Mobiler Signaturen – primär mit Mobiltelefonen – dar. Hierbei handelt es sich sowohl um Ansätze mit SIM (oder WIM) als Signaturerstellungseinheiten, als auch um Server-Lösungen (dem Muster der A1-Signatur folgend). Anhand von konkreten internationalen Projekten wird ein Überblick über bereits umgesetzte Mobile Signaturlösungen gegeben.

Inhaltsverzeichnis:

Abbildungsverzeichnis.....	2
Revision History	3
1 Einleitung	4
2 Überblick	5
2.1 Grundlagen	5
2.2 Mobiltelefon	5
2.3 Mobile Variante mit Chipkarte	15
2.4 Kapselung von Chip und Software in einem USB-Token	16
3 Internationale Projekte.....	18
3.1 BankID (Norwegen)	18
3.2 Mobii-ID (Estland)	19
3.3 "eID on SIM" (Finnland)	20
4 Zusammenfassung	23
Referenzen.....	24

Abbildungsverzeichnis

Abb. 2.1: A1.net-Login zur A1-Signatur.....	8
Abb. 2.2: A1.net-Login zur A1-Signatur.....	9
Abb. 2.3: Eingabe des übermittelten SMS-Codes sowie der Signatur-PIN	10
Abb. 2.4: Durchführung der A1-Signatur	10
Abb. 2.5: Kommunikationsmöglichkeiten für eine Signatur im Mobiltelefon	12
Abb. 3.1 Identifikation mittels VETUMA	21
Abb. 3.2 Signatur mittels VETUMA	22

Revision History

Version	Datum	Autor(en)	
0.1	13.02.2008	T. Knall	erster Entwurf, Struktur
0.2	18.02.2008	T. Knall	Motivation
0.3	19.02.2008	T. Knall	Überblick, Varianten Serverbasierter Signaturen
0.4	07.03.2008	T. Knall	Überblick
0.5	07.03.2008	A. Tauber	Internationale Projekte
0.6	10.03.2008	T. Knall	Überarbeitung
0.7	07.04.2008	T. Knall	microSD-Karte, iPhone
0.8	08.04.2008	T. Knall	Mobile Variante mit Chipkarte, Kapselung von Chip und Software
0.9	09.04.2008	T. Knall	Zusammenfassung
0.9.1	10.04.2008	T. Knall	Korrekturen, NFC, RFID
0.9.2	11.04.2008	T. Knall	Korrekturen
0.9.3	18.04.2008	T. Rössler	Anmerkungen
0.9.4	21.04.2008	T. Knall	Überarbeitung
0.9.5	22.04.2008	T. Knall	Skizzen, Ergänzungen
1.0	08.05.2008	T. Knall	Finalisierung

1 Einleitung

Bislang war es BürgerInnen in Österreich möglich, zwischen zwei Ausprägungen von Bürgerkarten zu wählen. Neben der chipbasierten Variante gab es als Alternative eine Handy-basierte Signatur, die durch eine im E-Government-Gesetz [E-GovG] festgelegte Übergangsbestimmung als sogenannte „Verwaltungssignatur“ bis Ende 2007 der qualifizierten Signatur¹ in Verwaltungsverfahren gleichgestellt war. Der Vorteil dieser Mobilien Signatur war die Unabhängigkeit der BürgerInnen von Kartenleser und einer Bürgerkarten-Software. Mittels eines Mobiltelefons konnte damit die Bürgerkartenfunktionalität auch in eingeschränkten Umgebungen, wie beispielsweise in einem Internetcafe genutzt werden.

Mit dem Auslaufen der rechtlichen Basis für Verwaltungssignaturen wurde der Betrieb der "A1-Signatur" als Mobile Signatur eingestellt. Die führt dazu, dass BürgerInnen wieder an entsprechende Umgebungen mit Kartenleser und Kartenlesersoftware gebunden sind. In Anbetracht der steigenden Mobilität der BürgerInnen stellt sich nun die Frage nach einer mobilen Variante der Bürgerkarte – gewissermaßen als Ersatz für die "A1-Signatur". Um qualifizierte Signaturen auch mit einem Mobiltelefon nutzen zu können, sind verschiedenste Lösungen denkbar, sei es mit SIM (oder WIM) als Signaturerstellungseinheit oder auch in Form einer serverbasierten Lösung mit einem HSM Modul, ähnlich der bereits bekannten A1-Lösung.

Diese Kurzstudie soll unter anderem verschiedene internationale Ansätze und Projekte im Zusammenhang mit Mobilien Signaturen aufzeigen und so eine eventuelle Entscheidungsfindung in Hinblick auf eine auf Österreich anwendbare Lösung entsprechend unterstützen.

¹ Qualifizierte Signaturen wurden vor der aktuellen Version des SigG (Novelle BGBl. I 8/2008) als "sichere elektronische Signaturen" bezeichnet. Dieses Dokument verwendet durchgängig den aktuellen Begriff "qualifizierte Signatur". Dies ist als Synonym zu sicheren elektronischen Signaturen zu sehen.

2 Überblick

Dieser Abschnitt gibt einen Überblick über mögliche technische Ausprägungen "Mobiler Signaturen". Hier wird auf grundsätzliche Verfahrensweisen eingegangen und gegebenenfalls Beispiele angeführt. Bereits umgesetzte Projekte anderer Staaten werden im nächsten Abschnitt ("Internationale Projekte") behandelt.

2.1 Grundlagen

In erster Linie wird unter einer "Mobilen Signatur" eine über ein Mobiltelefon ausgelöste Signatur assoziiert. Diese Signatur kann auf verschiedenste Art und Weise erstellt werden. Denkbare Ausführungsformen sind die Signatur mittels SIM-Karte bzw. via WIM, eine serverbasierte Signatur oder auch Signatur mittels eines SIM-Coprozessors. Die Möglichkeit, eine Mobiltelefon-basierte Signatur verwenden zu können, eröffnet dem Anwender größtmögliche Flexibilität, da sämtliche Arbeitsschritte entweder im Mobiltelefon oder serverbasiert erfolgen.

Gleichwohl kann unter einer Mobilen Signatur auch die Möglichkeit verstanden werden, Signaturvorgänge zwar mit Chipkarte durchzuführen jedoch hierzu nicht mehr auf eine lokale Software zurückgreifen zu müssen. Banken verwenden diese Variante häufig in Form von Applets für ihre Online-Banking-Lösungen, um ihren Kunden die Installation einer spezifischen Software zu ersparen. Einen entsprechenden Kartenleser vorausgesetzt nutzen die Kunden das Online-Banking gewissermaßen "mobil", da sie nicht an einen bestimmten Rechner gebunden sind.

Eine dritte Variante einer "Mobilen Signatur" geht einen Schritt weiter und sieht die Kombination von Chip, Kartenleser und Software vereint in einem (USB-)Token vor. Ein solches Token kann bequem am Schlüsselbund getragen werden und offenbart dem Anwender die Möglichkeit, weitestgehend unabhängig von bestimmter Hard- und Software, Signaturen zu erstellen.

Die folgenden drei Abschnitte behandeln diese drei Ausprägungen im Detail.

2.2 Mobiltelefon

Besonderes Augenmerk dieses Grundsatzpapiers wird auf die Variante, Mobiltelefone für Signaturen zu verwenden, gelegt. Dies erscheint vor allem in Hinblick auf die Tatsache, dass die Penetration von Mobiltelefonen in Österreich im Jahr 2007 bereits 90,3% betrug ([IKTHS2007]) sinnvoll. Mobile Signaturen auf Mobiltelefonen könnten durchaus von dieser hohen Akzeptanz profitieren und dadurch ebenfalls einen Aufschwung erfahren.

Betrachtet man die verschiedenen Mobilen Signaturansätze, die in den folgenden Abschnitten erläutert werden, stellt das Konzept "Mobile Signatur mit Mobiltelefon" am ehesten jene Variante dar, die von der BürgerIn tatsächlich mit einer "Mobilen Signatur" assoziiert wird. Aus der Sicht der BürgerInnen ersetzt das Mobiltelefon Kartenleser und Chipkarte einer herkömmlichen Bürgerkartenlösung was die theoretische Möglichkeit schafft, immer und überall Signaturen auslösen zu können. Dem gegenüber stehen jedoch zahlreiche Herausforderungen – hauptsächlich die Realisierung der Kommunikation zwischen Mobiltelefon und Signaturanwendung betreffend, die bei der Umsetzung einer entsprechenden Lösung berücksichtigt werden müssen.

Aus Usability-Sicht kann die Durchführung Mobiler Signaturen mit dem Mobiltelefon der AnwenderIn – abhängig von der konkreten Umsetzung – zahlreiche Vorteile gegenüber herkömmlichen Varianten mit Chipkarte und Kartenleser eröffnen:

- Abgesehen von einem Mobiltelefon ist auf der Signator-Seite unter Umständen keine zusätzliche Hardware für die Durchführung einer Signatur notwendig.
- Die Signaturlösung kann so umgesetzt werden, dass keine Abhängigkeiten zu spezieller Software bestehen, d.h. in diesem Fall wäre es nicht erforderlich, proprietäre Anwendungen für einzelne Dienste bzw. Aufgaben lokal zu installieren.
- Mobiltelefone genießen eine hohe Akzeptanz in der Bevölkerung. SMS/MMS-Dienste werden von allen Bevölkerungsschichten in Anspruch genommen und sogar Bezahldienste wie "Paybox²" oder "Handyparken³" (Nutzen der Wiener Kurzparkzonen via Mobiltelefon) finden durchaus Anklang. All dies hat zur Folge, dass die Hemmschwelle für die Nutzung des Mobiltelefons zum Anbringen Mobiler Signaturen niedrig sein dürfte.
- Nutzung bestehender Basistechnologie (Mobiltelefon, unter Umständen GSM-Netz...)
- Einfache Anwendung: die Bedienung eines Mobiltelefons stellt heute keine besondere Herausforderungen mehr für den durchschnittlichen Anwender dar. Darüber hinaus hat sich speziell durch die Veröffentlichung des Apple iPhones mit seinem revolutionären Bedienkonzept der Druck auf sämtliche Hersteller von Mobiltelefonen erhöht, die Usability ihrer Geräte zu überarbeiten und zu verbessern.

Bis Dezember 2007 hatten österreichische BürgerInnen die Wahl zwischen einer herkömmlichen chipbasierten Bürgerkarte und der Ausprägung als mobile A1-Signatur. Mit dem Auslaufen der rechtlichen Basis für Verwaltungssignaturen hat sich der Betreiber der A1-Signatur, die "mobikom austria", dazu entschlossen, diese nicht mehr anzubieten. Dies stellt speziell für mobile AnwenderInnen ein Erschwernis dar, da sie nun wieder gezwungen sind, ein Kartenlesegerät und die Bürgerkarte in der Ausprägung als Chipkarte zusammen mit ihrem Notebook mitzuführen. Auch das (mobile) Ausführen von E-Government-Anwendungen auf beliebigen Rechnern ohne Kartenleser, Kartenlesersoftware und Bürgerkartenumgebung ist nun nicht mehr ohne weiteres möglich.

Bei der Suche nach potentiellen Nachfolgern zur A1-Signatur bestehen grundsätzlich mehrere Optionen wobei man im Großen und Ganzen zwei Ansätze unterscheiden kann:

- Nutzung des Mobiltelefons zur Durchführung einer serverbasierten Signatur
- Durchführung der Signatur im Mobiltelefon

2.2.1 Serverbasierte Signatur

Das Prinzip der serverbasierten Signatur beruht darauf, dass keinerlei Signaturvorgänge innerhalb des Mobiltelefons erfolgen, sondern dass der komplette Prozess serverseitig abgewickelt wird. Das Mobiltelefon dient in diesem Zusammenhang in der Rolle als sicherheitsverstärkender Faktor ausschließlich als Mittel um neben des Wissens um ein Geheimnis (z.B. Wissen der Signatur-PIN zum Auslösen der Signaturfunktion) auch den Besitz des Mobiltelefons sicherzustellen. Dies entspricht einer Zwei-Faktor-Authentifizierung gegenüber dem serverseitigen Signaturlösungsgerät und ist analog zum Vorgehen bei chipkarten-basierten Signaturlösungen zu sehen (Besitz der Chipkarte und Wissen der PIN zum Auslösen der Signaturfunktion).

An ein Mobiltelefon werden bei einer serverbasierten Signatur keinerlei besondere Anforderungen gestellt, was den Vorteil hat, dass sämtliche bereits ausgelieferte Endgeräte

² <http://www.paybox.at/>

³ <https://www.handyparken.at/>

zum Auslösen einer Signatur herangezogen werden können und der AnwenderIn so keine zusätzlichen Hardware-Kosten entstehen.

Jegliche die Signatur betreffenden Daten (Zertifikat, Signaturschlüssel, ggf. Personendaten) sind auf einem Server des Dienstbieters gespeichert. Der Dienstbieter stellt sicher, dass die Signatur nur unter Mitwirkung des Signators erstellt werden kann. Dies wird durch Verwendung eines HSM⁴ bewerkstelligt. Hierbei handelt es sich um eine spezielle (üblicherweise nach gängigen Sicherheitsstandards zertifizierte) Hardware-Komponente, die die sichere Ausführung kryptographischer Operationen ermöglicht.

Grundsätzlich ist bei der serverbasierten Lösung die Kenntnis eines PIN-Codes ("Signatur-PIN") seitens des Signators erforderlich, um Signaturen auszulösen. Durch Eingabe des PIN-Codes wird üblicherweise dem Willen des Signators zur Signaturerstellung Ausdruck verliehen. Der Signator besitzt zwar mit dieser Kenntnis die alleinige Kontrolle über die Signaturerstellungseinheit, da sich das HSM jedoch auf der Serverseite befindet, muss der PIN-Code vom Signator zum Server übertragen werden. Bei der A1-Signatur fand die Übertragung durch ein Java-Applet-basiertes Web-Formular, das über eine SSL-Verbindung abgesichert war, statt.

Zur Verstärkung der Sicherheit kann ein zweiter Authentifizierungskanal eingesetzt werden, der neben dem Nachweis von "Wissen" (PIN) nun auch die Überprüfung von "Besitz" ermöglicht. Dieser Nachweis kann durch die Übermittlung eines zusätzlichen Codes, eines zeitlich begrenzten TAC⁵s, auf das mobile Endgerät (beispielsweise als SMS) realisiert werden, der nun ebenfalls zum Auslösen der Signatur benötigt wird. Durch die Zweikanal-Authentifizierung ("Wissen" und "Besitz") erhöht sich der Sicherheitswert signifikant.

Zur Verdeutlichung eines serverbasierten mobilen Signaturkonzepts kann als Beispiel die "A1-Signatur" herangezogen werden, die dem österreichischen Bürger vom 16.04.2004 bis zum 31.12.2007 zur Verfügung stand (siehe Abschnitt 2.2.1.1).

⁴ Hardware Security Module

⁵ Transaktionscode

2.2.1.1 Beispiel A1-Signatur

Ein typischer Vertreter der rein serverbasierten Signatur war die "A1-Signatur". Diese Variante einer Serversignatur, bei der am Mobiltelefon keinerlei kryptografische Operationen ausgeführt wurden, sondern sich die Beteiligung des Mobiltelefons auf den Empfang einer SMS für eine Zweikanalauthentifizierung beschränkt, stellte EU-weit eine Einzigartigkeit dar.

Zur Authentifizierung bzw. zum Anbringen einer Signatur waren folgende Schritte vorgesehen:

1. Zunächst wurde in der jeweiligen Anwendung "A1-Signatur" als Mittel zur Unterschrift gewählt. Die A1-Signatur konnte für eine Authentifizierung bei einem Login-Vorgang oder auch zur Signatur von eingegebenen Formulardaten verwendet werden. Nach der Wahl der Bürgerkartenausprägung "A1-Signatur" wurde der Benutzer zur A1-Signatur-Seite der Mobilkom weitergeleitet.

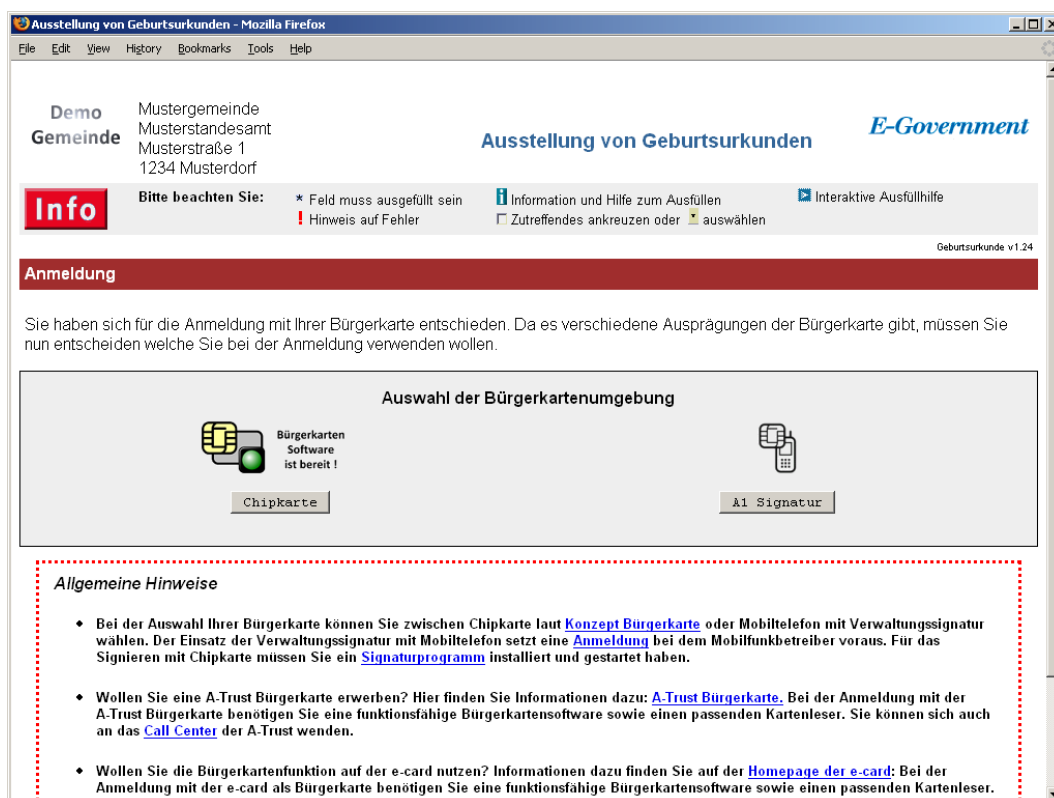


Abb. 2.1: A1.net-Login zur A1-Signatur

2. Nun musste der A1.net Benutzername sowie das Passwort eingegeben werden (siehe Abb. 2.2). Voraussetzung dafür war eine zuvor erfolgte A1.net Registrierung für die man nicht zwingenderweise A1-Kunde sein musste. Damit stand auch Nutzern anderer Provider die Möglichkeit offen, das mobile A1-Signaturservice zu verwenden. Nachdem der Signator durch Benutzername und Passwort identifiziert war, wurde an sein Mobiltelefon ein einmal verwendbarer – zeitlich begrenzter – Code ("SMS-Code") per SMS übermittelt.

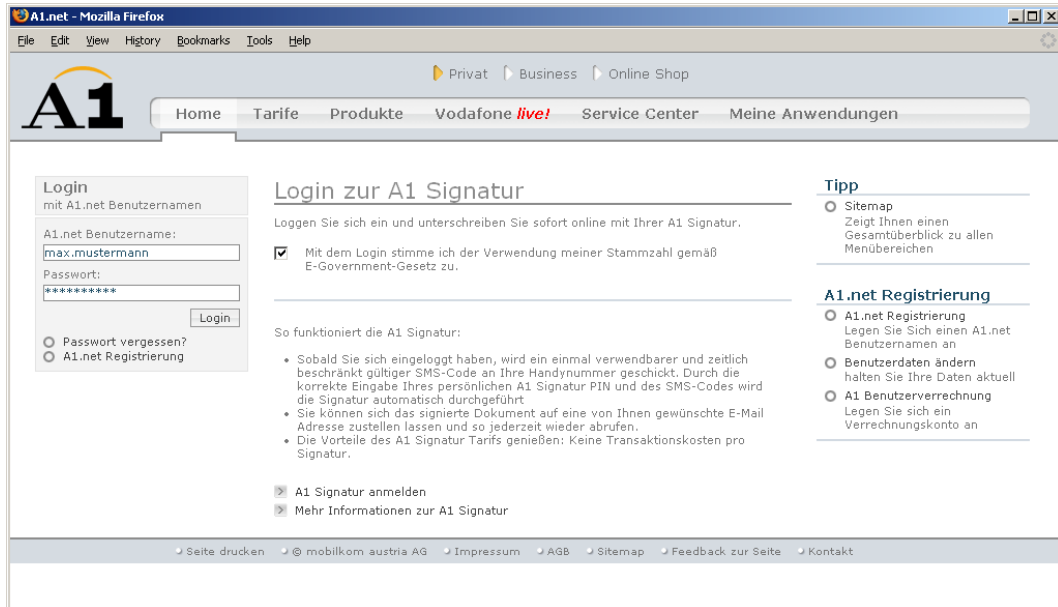


Abb. 2.2: A1.net-Login zur A1-Signatur

- Die BürgerIn hatte nun die Möglichkeit, das zu signierende Dokument einzusehen (siehe Abb. 2.3, "Dokument einsehen"). Zur Durchführung der Signatur mussten die A1-Signatur-PIN (siehe Abb. 2.3, "A1 Signatur PIN") sowie der erhaltene SMS-Code eingegeben werden (siehe Abb. 2.3, "SMS Code"). Zusätzlich bestand die Möglichkeit, das signierte Dokument an eine bestimmte E-Mail-Adresse weiterzuleiten.

The screenshot shows a web browser window with the A1.net logo and navigation menu. The main content area is titled "Signatur durchführen". Below the title, there is a message: "Bitte signieren Sie nun das bereitstehende Dokument. Zur Kontrolle können Sie das Dokument vorher ansehen." There are three main sections: 1. "Dokument ansehen" with a sub-section "SMS Code Eingabe" containing a text input field with the value "525074" and a "Hinweis" link. 2. "A1 Signatur PIN Eingabe" with a sub-section "A1 Signatur PIN" containing a masked text input field. 3. "Dokument versenden" with a checkbox for "max.mustermann@a1.net" and an empty text input field. At the bottom right, there are "Abbrechen" and "Weiter" buttons. The footer contains links for "Seite drucken", "mobilkom austria AG", "Impressum", "AGB", "Sitemap", "Feedback zur Seite", and "Kontakt".

Abb. 2.3: Eingabe des übermittelten SMS-Codes sowie der Signatur-PIN

- Im letzten Schritt wurde die Signatur serverseitig mit der übergebenen Signatur-PIN über das HSM ausgelöst (siehe Abb. 2.4). Nach Durchführung der Signatur wurde das signierte Dokument automatisch an die aufrufende Anwendung übergeben, die dann die weitere Verarbeitung übernahm.

The screenshot shows the same browser window as in Abb. 2.3, but the page title is now "Durchführung A1 Signatur". The main content area displays a message: "Ihre A1 Signatur wird jetzt durchgeführt. Bitte warten ..." followed by a progress bar. The rest of the page layout, including the navigation menu and footer, remains the same.

Abb. 2.4: Durchführung der A1-Signatur

2.2.1.2 IMEI/IMSI

Da das Mobiltelefon für eine rein serverbasierte Signatur bei der Signaturerstellung nicht direkt involviert ist, beschränken sich die Anwendungsmöglichkeiten in diesem Kontext auf den Nachweis des Besitzes.

Bei der A1-Signatur geschieht dieser Nachweis durch Übermittlung eines SMS-Codes auf das Mobiltelefon. Als mögliche Alternative zu diesem SMS-Code bietet sich die Überprüfung der IMSI⁶ oder der IMEI⁷ Nummer der SIM-Karte bzw. des Mobiltelefons des Signators an.

IMSI: Hierbei handelt es sich um die interne Teilnehmerkennung, die weltweit einmalig pro SIM-Karte vergeben wird.

IMEI: Dies ist die eindeutige Seriennummer, anhand deren jedes Mobiltelefon identifiziert werden kann.

Der Signaturprozess könnte so aussehen, dass sich der Signator zunächst – ähnlich wie bei der A1-Signatur – am Portal mit Benutzername/Passwort identifiziert. Ihm wird nun eine SMS zusammen mit dem Hash des zu signierenden Dokuments übermittelt. Diesen Hash kann der Signator mit dem Hash des zu signierenden Dokuments vergleichen. Dadurch wäre sichergestellt, dass der Signator die zu signierenden Daten Online betrachten kann während der Zusammenhang zwischen Dokument und SMS über diesen Hashwert transparent gemacht wird.

Der Besitznachweis könnte durch eine Antwort auf diese SMS erbracht werden. Über die IMSI Nummer ist die SIM-Karte bzw. über die IMEI-Nummer das Endgerät identifizierbar. Inwieweit die IMSI/IMEI-Nummer jedoch manipulationssicher verwendet werden kann, müsste in einer gesonderten Sicherheitsbetrachtung analysiert werden.

Der Vorteil der hier dargestellten Lösung offenbart sich jedoch in der Transparenz bzgl. eine eventuellen Bezahlung für die Signatur, die über eine (Mehrwert-)SMS verrechnet werden kann.

Neben dem Nachweis des Besitzes ist jedoch immer noch die Übermittlung der Signatur-PIN auf gesicherte Art und Weise erforderlich. Dies kann wie bei der A1-Signatur über das Web-Frontend via SSL-Verbindung erfolgen.

2.2.1.3 Anruf mit Code-Eingabe per Tonwahlverfahren

Um die Übermittlung der Signatur-PIN ebenfalls über das Handy durchzuführen, könnte unter Umständen auf ein Mehrfrequenzwahlverfahren (MFV) zurückgegriffen werden. Dieses kommt normalerweise bei Service-Rufnummern zum Einsatz, bei denen PINs übertragen werden müssen (z.B. beim Aufladen des Guthabens eines Mehrwertkartentelefon oder PIN-Eingabe zur Fern-Abfrage des Anrufbeantworters).

Beim Mehrfrequenzwahlverfahren werden die Tasten 0-9, A-D, sowie * und # mittels Überlagerung von 8 verschiedenen Tonfrequenzen kodiert und innerhalb des normalen Sprachfrequenzbandes übertragen. Da Sprachübertragung via GSM heutzutage (mit RC6) verschlüsselt ist, erfolgt auch die Übertragung des PIN-Codes ebenfalls verschlüsselt. Leider kann die Verschlüsselung jederzeit vom Netzbetreiber oder bei Einsatz eines IMSI-Catchers abgeschaltet werden, sodass die verschlüsselte Übertragung des PIN-Codes nicht garantiert werden kann. Ob die Verschlüsselung aktiviert ist oder nicht wird nur von einigen wenigen Handy-Modellen angezeigt.

⁶ International Mobile Subscriber Identity

⁷ International Mobile Equipment Identity

2.2.2 Signatur im Mobiltelefon

Eine sichere Variante einer Mobilten Signatur besteht darin, die Signatur direkt im Mobiltelefon durchzuführen. Der für die Signatur erforderliche private Schlüssel befindet sich dabei innerhalb eines Krypto-Moduls. Um die Signatur auszulösen, muss der Anwender ein Signatur-PIN direkt am Mobiltelefon eingeben. Diese PIN schaltet den privaten Schlüssel frei der in weiterer Folge für die Durchführung der Signatur verwendet wird. Der Signatur-Wert kann dann zur Signatur-Anwendung übertragen werden während die eingegebene PIN das Gerät nicht verlässt.

Nun stellt sich grundsätzlich die Frage, auf welche Weise die Kommunikation zwischen einer Signatur-Anwendung und dem Signatur-Gerät, d.h. dem Mobiltelefon, bewerkstelligt wird.

Hier zeigen sich zwei mögliche Lösungen:

1. Die in Abb. 2.5 "Variante 1" bezeichnete Lösung sieht die Kommunikation über einen Service-Provider vor. Hierbei startet die AnwenderIn eine Signatur-Anwendung, die über das Internet Kontakt zum Mobilfunkprovider aufnimmt. Dieser übermittelt dem mobilen Endgerät entsprechende Anweisungen zum Start eines Signaturvorgangs (beispielsweise über speziell präparierte SMS-Nachrichten oder via WAP). Nachdem die AnwenderIn die Signatur mit einer PIN ausgelöst hat, wird der Signatur-Wert an den Service-Provider übertragen. Dieser sendet die Signatur schließlich über das Internet zurück an die Signatur-Anwendung.
2. Die zweite Variante sieht eine direkte Kommunikation zwischen der Signatur-Anwendung und dem Endgerät über eine NFC-, Bluetooth⁸ oder WLAN-Schnittstelle vor. Dies setzt jedoch die Unterstützung der Funkschnittstelle durch das Terminal an dem die Signatur-Anwendung betrieben wird, voraus.

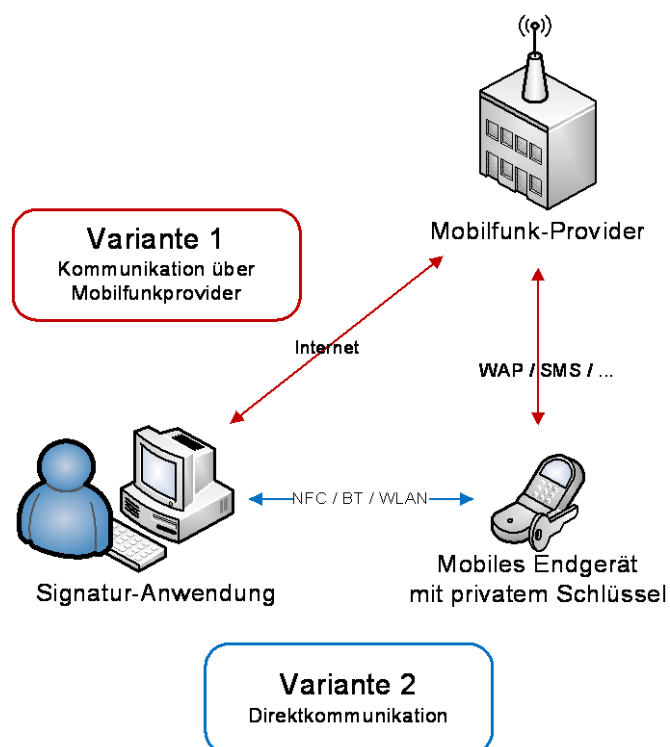


Abb. 2.5: Kommunikationsmöglichkeiten für eine Signatur im Mobiltelefon

⁸ Bluetooth ist ein Standard zur Funkvernetzung von Geräten über kurze Distanz.

Konkrete Lösungen unterscheiden sich durch die Implementierung bzw. die Ausprägung des kryptografischen Kerns. In den folgenden Abschnitten wird versucht, einige dieser Umsetzungen als Diskussionsgrundlage exemplarisch aufzuzeigen.

2.2.2.1 SIM mit kryptographischem Coprozessor

Eine mögliche Ausprägung könnte die Integration eines PKI-Moduls in einem SIM⁹ sein. Bei einem SIM handelt es sich um ein Modul mit CPU, Speicher und Schnittstellen. Das Modul ist eindeutig einem Benutzer zugeordnet, kann mit einer PIN geschützt werden und dient primär zur Authentifizierung des Benutzers am Mobilfunknetz des Providers sowie zur Speicherung von Nutzerdaten.

Der private Schlüssel der AnwenderIn muss manipulationssicher im SIM gespeichert werden. Gegebenenfalls wäre zu prüfen, ob sie SIM selbst als Signaturerstellungseinheit für qualifizierte Signaturen zugelassen ist. Kann dies nicht gewährleistet werden muss ein entsprechendes Modul bzw. ein kryptographischer Coprozessor verwendet werden.

Um eine Signatur direkt am Mobiltelefon durchzuführen, ist zunächst eine direkte Verbindung zwischen SIM-Karte und Hintergrundsystem, d.h. der Infrastruktur des Netzbetreibers aufzubauen. Dies kann über die im GSM-Standard 03.48 definierten sogenannten "Over The Air" Kommunikation erfolgen. Hierbei wird eine spezielle Kurznachricht an die jeweilige SIM-Karte versandt, die entsprechende Kommandos enthält. Das Mobiltelefon erkennt, dass es sich bei der SMS um SIM-spezifische Daten handelt und reicht diese an das SIM weiter. Die SIM-Karte interpretiert die Kommandos und führt sie aus. Für diese Kommunikationsvariante ist die Beteiligung eines Service-Providers (siehe Variante 1, Abb. 2.5) erforderlich, der für das Versenden der SMS-Nachrichten bzw. für die Rückgabe der Signatur an die Signatur-Anwendung verantwortlich ist.

Im konkreten Fall kann der Benutzer hiermit zur Signatur übermittelter Daten aufgefordert werden. Die Signatur führt der Benutzer durch Eingabe seiner Signatur-PIN am Mobilgerät durch. Die Signatur wird nun als Antwort auf die zuvor eingegangene SMS an das Hintergrundsystem übermittelt.

2.2.2.2 WIM

WAP¹⁰ wurde im Jahr 2000 als neue Internet-Technologie für mobile Endgeräte eingeführt. Über dieses Protokoll ist es mobilen Geräten möglich, über ein drahtloses Netzwerk (z.B. GSM) Informationen mit einem Server auszutauschen. WAP bezeichnet hierbei nicht nur das Protokoll sondern umfasst eine ganze Reihe von Spezifikationen. Eine dieser Spezifikationen bezeichnet ein Sicherheitsmodul namens WIM¹¹.

Die Spezifikation sieht zwei mögliche Ausprägungen vor:

- WIM als Anwendung auf einer eigenen Chipkarte. Diese Möglichkeit erfordert einen Dual-SIM-Slot, der sich bislang bei mobilen Endgeräten noch nicht durchgesetzt hat.
- WIM als zusätzliche Anwendung auf einer SIM-, USIM¹²- oder UICC¹³-Karte

Die Spezifikation von WIM basiert auf dem Cryptographic Token Information Format Standard (PKCS#15). Die Hauptaufgaben des WIM-Moduls ist zwar die kryptographische Absicherung der WAP-Datenübertragung, es kann jedoch auch für Signaturanwendungen genutzt werden. WIM befindet sich bereits standardmäßig auf vielen SIMs bzw. USIMs.

⁹ Subscriber Identity Module

¹⁰ Wireless Application Protocol

¹¹ WAP Identity Module

¹² Universal Subscriber Identity Module

¹³ Universal Integrated Circuit Card

2.2.2.3 microSD-Karte

Zwei weitere interessante Lösungen wurden unabhängig voneinander von Giesecke & Devrient¹⁴ sowie von IICS¹⁵ entwickelt. Beide Lösungen nutzen das microSD-Interface, mit dem zahlreiche mobile Endgeräte bereits ausgestattet sind, um diese mit Smartcard-Funktionen auszustatten. Applikationen des jeweiligen Endgeräts können diese Funktionen genauso verwenden, als würde es sich tatsächlich um ein Standard Smartcard System handeln.

Die Verbreitung von mobilen Geräten mit Kryptomodulen, bzw. Smartcard Funktionen, die eine (qualifizierte) Signatur ermöglichen, ist in Österreich im Vergleich zu anderen europäischen Ländern (vergleiche Abschnitt 3.1) gering. Relativ stark verbreitet sind jedoch Endgeräte mit microSD-Schnittstellen. Bei den Mobiltelefonherstellern wird die Schnittstelle vor allem von LG, Kyocera, Motorola, Samsung, Nokia, Sagem, HTC und Benq-Siemens verwendet. Mit Abmessungen von 11mm x 15mm x 0,7mm stellen sie das ideale Speichermedium für Multimedia-fähige Mobilgeräte dar. Eine Trendumkehr ist nicht in Sicht – im Jänner 2008 wurde bereits eine 12 GB-microSD-Karte vorgestellt.

Der große Mehrwert einer microSD Lösung liegt darin, Geräte ohne entsprechende Hardware jedoch mit microSD-Slot ohne großen Aufwand mit Funktionen auszustatten, die für (qualifizierte) Signaturen erforderlich sind.

Mobile Security Card (Giesecke & Devrient, [GDMSC])

G&D bezeichnen ihre auf Java Card basierende Lösung als "Mobile Security Card". Hierbei handelt es sich zunächst um eine Standard Massenspeicherkarte, die mit einem zusätzlichen "Secure Element" ausgestattet ist. Dieses sichere Element stellt Smartcard-Funktionen wie PKI Schlüssel Management oder Schlüsselgenerierung zu Verfügung. Um nun auf diese Funktionen zurückgreifen zu können kann das Mobile Commerce Extension Protokoll oder das von G&D entwickelte dateibasierte Generic Security Interface verwendet werden.

Die Mobile Security Card ist nach Common Criteria EAL 5+¹⁶ zertifiziert und unterstützt die vollständige Java Card API sowie die Open Platform.

certgate Smart Card microSD / MMC (IICS, [IICSCSC])

Eine nahezu äquivalente Lösung von certgate wird als "certgate Smart Card microSD/MMS" bezeichnet. Als Anwendungsgebiete nennt certgate die Umsetzung sicherer Umgebungen für Finanztransaktionen, Absicherung des Zugriffs auf personenbezogene bzw. unternehmenssensible Daten der Privatwirtschaft sowie der öffentlichen Verwaltung, das Gesundheitswesen, eCommerce sowie IT-Sicherheit und digitale Signaturen.

Konkret enthält das microSD Modul einen Flashspeicher von 512 MB. Das Modul ist wie auch das Modul von G&D nach EAL 5+¹⁶ zertifiziert. Es bietet Digitales Signieren, Asymmetrische Verschlüsselung (RSA), Erzeugen von Zufallszahlen, sowie das Laden von Zertifikaten und Schlüsseln auf die Smartcard.

Das Modul kann derzeit mit "Windows Mobile" Anwendungen unter Nutzung einer Crypto API (Ver-/Entschlüsseln, Signatur, Verifikation) genutzt werden (Symbian und Pocket Linux ist in Arbeit).

¹⁴ <http://www.gi-de.com>

¹⁵ <http://www.iics.de>

¹⁶ Das der Evaluierung zu Grunde gelegte Security Target (ST) bzw. Protection Profile (PP) wurde vom Hersteller nicht angegeben.

2.2.2.4 iPhone

Seit Anfang März 2008 bietet Apple Entwicklern durch Veröffentlichung eines Software Developer Kits (SDK) die Möglichkeit, Anwendungen für das iPhone zu entwickeln ([AIDEV]). Gleichzeitig arbeitet Sun an einer für das iPhone angepassten Java Virtual Machine, die jedoch frühestens im Juni 2008 verfügbar sein wird. Der Transfer von Software auf das iPhone erfolgt zukünftig ausschließlich über den sogenannten "Apple AppStore". Dabei handelt es sich um eine iPhone Anwendung, die es Benutzern erlaubt, Anwendungen von Drittherstellern direkt auf ihr iPhone herunterzuladen. Das Hosting von Anwendungen übernimmt Apple kostenlos, sofern es sich um nicht-kommerzielle Anwendungen handelt.

Mittels des SDKs bzw. unter Nutzung der Java VM von Sun könnten Signatur-Module entwickelt werden, die die Nutzung Mobiler Signaturen zusammen mit dem Internetzugang über das iPhone ermöglichen. Leider erscheint eine reine Software-Lösung ohne Modul zur sicheren Speicherung privater Schlüssel in Hinblick auf qualifizierte Signaturen nicht sinnvoll.

Derzeit unterstützt das iPhone leider lediglich WLAN bzw. EDGE und GPRS. Erst mit einer Revision, die im laufenden Jahr 2008 erfolgen soll, wird UMTS unterstützt.

2.2.2.5 NFC, Bluetooth

Near Field Communication¹⁷ bildet einen interessanten Anwendungsfall im Zusammenhang mit der Signaturerstellung in Mobiltelefonen. Jede der in diesem Abschnitt bisher genannten Möglichkeiten zur Erstellung Mobiler Signaturen kann in Kombination mit NFC oder auch mit Bluetooth als Übertragungsweg Verwendung finden.

Der Anwendungsfall sieht konkret so aus, dass der Anwender sein mobiles (NFC-/Bluetooth-fähiges) Endgerät in die Nähe eines entsprechenden Terminals der jeweiligen Anwendung (bargeldloses Zahlen, Zugangskontrolle...) bringen muss. Das Terminal überträgt den zu signierenden Text zum Endgerät, das diesen dem Anwender zur Ansicht anzeigt. Dieser signiert den Text über das mobile Endgerät, woraufhin dieses die Signatur per NFC/Bluetooth zum Terminal überträgt.

Anwendungsbeispiele hierfür lassen sich nicht nur im Bereich E-Government, sondern auch in der Wirtschaft finden: Ein Anwendungsfall wären beispielsweise Paketzustelldienste, die die jeweiligen Empfänger um eine (elektronische) Unterschrift zur Quittierung des Empfangs bitten.

2.3 Mobile Variante mit Chipkarte

Aus Sicht des Anwenders kann unter einer "Mobilen Signatur" auch die Möglichkeit verstanden werden, jederzeit und überall Signaturen an beliebigen Rechnern auslösen zu können. "Jederzeit und überall" bedingt jedoch, dass keinerlei lokale Softwareinstallationen für individuelle Anwendungen durchgeführt werden müssen. Was jedoch als Voraussetzung betrachtet werden muss ist – abgesehen von einem Internetzugang und eines Browsers – ein installiertes Kartenlesegerät. Dies muss jedoch nur ein einziges Mal eingerichtet werden und kann dann von jeder Smartcard-Software verwendet werden.

Ein Anwender, der nun eine bestimmte Applikation (Online-Banking, E-Government-Anwendung...) benutzen möchte, kann diese direkt im Browser aufrufen. Die Software, die eigentlich für die Kommunikation zwischen Kartenlesegerät und Client erforderlich wäre (z.B. Bürgerkartenumgebung für E-Government-Anwendungen), wird innerhalb des Browsers durch ein Applet¹⁸ oder durch eine ActiveX¹⁹-Komponente abgebildet.

¹⁷ Near Field Communication ist ein Übertragungsstandard zum kontaktlosen Austausch von Daten über kurze Strecken.

¹⁸ Bei einem Browser-Applet handelt es sich um ein Java-Programm, das im Browser des Anwenders ausgeführt wird. Handelt es sich um ein signiertes Applet, kann auf lokale Ressourcen, wie z.B. einen Kartenleser, zugegriffen werden.

¹⁹ ActiveX ist eine Softwarekomponente von Microsoft, die aktive Inhalte im Internet Explorer ermöglicht. ActiveX beschränkt sich auf das Betriebssystem Windows und den Internet Explorer.

Applets werden schon seit Jahren von einigen Banken verwendet (z.B. BAWAG), die ihren Kunden hiermit die Nutzung einer Signaturkarte im Rahmen von Online-Banking ermöglichen.

Eine Einschränkung in Hinblick auf die Verwendung dieser Applet-Variante ist, dass diese nur für Online-Applikationen verwendet werden kann. Lokale Anwendungen können hiervon nicht profitieren. Der Vorteil gegenüber einer lokal installierten Software ist jedoch die Möglichkeit, Updates an der Software problemlos durchführen zu können, da diese ohnehin über den Browser des Clients bei Betreten der Seite heruntergeladen wird. Umständliche Update-Mechanismen können so entfallen.

2.3.1 RFID

Einen Sonderfall einer "mobilen Variante mit Chipkarte" stellt die drahtlose Kommunikation mit der Chipkarte via RFID²⁰ dar. Hierbei wird das RFID-Tag (d.h. die Chipkarte) – ggf. ausgerüstet mit einem kryptografischen Coprozessor - in Reichweite eines Terminals gebracht (Zentimeter- bis Meterbereich). Die PIN-Eingabe zur Signatur erfolgt am Terminal. Dieses überträgt die PIN sowie den zu signierenden Hash über einen sicheren Kanal zur Chipkarte (via RFID). Diese führt die Signatur durch und retourniert den Signaturwert zum Terminal. Essentieller Punkt bei dieser Lösung einer "Mobilen Signatur" ist die sichere Übertragung der PIN. Dies kann beispielsweise durch Mechanismen und Verfahren erreicht werden, die im Chipkartenbereich als "Secure Messaging" bezeichnet werden ([HBDC]). Besondere Aufmerksamkeit muss im Falle einer Secure Messaging Lösung auf das Schlüsselmanagement gerichtet werden. Schlüssel, die zur Absicherung einer drahtlosen Verbindung verwendet werden, müssen vorab verteilt und sicher gespeichert werden (z.B. auf einer Chipkarte bzw. in einem HSM).

Ein potentieller Anwendungsfall für diese Art Mobiler Signaturen wäre der Gesundheitsbereich. Ärzte, die bei einer Visite ihre Befunde elektronisch signieren müssen, können dies nun durchführen ohne die Karte aus der Brieftasche zu nehmen und in einen Kartenleser zu stecken. Im Idealfall dient die Ausweiskarte, die am Arztkittel befestigt ist, als Transponder .

2.4 Kapselung von Chip und Software in einem USB-Token

Eine noch elegantere Variante stellt die Kapselung der Software gemeinsam mit der Chipkarte in einem USB-Token dar. Hierbei handelt es sich um Kartenlesegerät in Form eines USB-Sticks (mit Flash-Speicher). Der Chip muss aus der Chipkarte gestanzt werden und in das Token eingelegt werden. Im Flash-Speicher wird die Software gespeichert, die die Aufgabe hat, die Kommunikation zwischen Kartenleser und Client-Anwendung zu bewerkstelligen.

Die BürgerIn, die ihr USB-Token beispielsweise bequem am Schlüsselbund trägt, begibt sich im Anwendungsfall zu einem beliebigen Rechner und schließt das Token an einer USB-Schnittstelle an. Das Betriebssystem erkennt das Token und lädt die Software direkt vom Token. Die BürgerIn wird nun im Bedarfsfall nur noch zur PIN-Eingabe aufgefordert.

Im Falle einer E-Government-Anwendung handelt es sich bei der Software um die Bürgerkartenumgebung, die Browser-Anfragen über die HTTP(S)-Security-Layer-Schnittstelle entgegennimmt. Eine Herausforderung stellt jedoch die Erstellung der BKU-Software bzw. die Modifikation bestehender BKU-Software dar, die ohne Softwareinstallation und ohne Ablage von Daten am lokalen Rechner funktionieren muss. Darüber hinaus sollte versucht werden, eine Plattformunabhängigkeit zu erreichen. Dies kann beispielsweise durch Verwendung einer Java-basierten Software erzielt werden.

²⁰ Radio Frequency Identification erlaubt die Übertragung von Daten über kurze Strecken (Meterbereich) mittels eines elektromagnetischen Feldes, das gleichzeitig zur Energieversorgung des Transponders dient.

Weiters ist darauf zu achten, dass das USB-Token mit Treibern funktioniert, die bereits im Betriebssystem vorhanden sind. Dies schränkt die Nutzung jedoch auf aktuelle Betriebssysteme ein, da hier die Unterstützung durch Treiber für aktuell verfügbare Hardware gegeben ist.

3 Internationale Projekte

Dieser Abschnitt beschreibt einige internationale Projekte im Rahmen von Mobil-Signaturen. Bei sämtlichen präsentierten Lösungen werden die Signaturen direkt am Mobiltelefon mit einer integrierten PKI Funktionalität der SIM Karte erstellt. Eine bestehende Lösung in einem Mitgliedsstaat der EU, basierend auf einer serverseitig erstellten Signatur, die auf Basis des Mobiltelefons freigegeben/ausgelöst wird, ist uns derzeit nicht bekannt.

3.1 BankID (Norwegen)

Telenor Mobile²¹ entwickelte 2000/2001 eine SIM-basierte PKI Lösung, die seither für mCommerce verwendet wurde. Alle SIM Karten, die von Telenor ab diesem Zeitpunkt ausgeliefert wurden, verfügen über diese PKI Funktionalität, d.h. über 50% der norwegischen Bevölkerung (2-2,5 Mio. Einwohner) sind im Besitz einer solchen.

Die SIM Karten verfügen über einen 32 KB RAM Speicher und werden von Gemalto bzw. Giesecke & Devrient gefertigt. Sie besitzen eine karteninterne Schlüsselgenerierungs-(1024 Bit RSA Schlüssel) und PKCS#1 Signaturfunktionalität basierend auf RSA und dem Hashalgorithmus SHA-1.

Ausschließlich speziell aufbereitete SMS Nachrichten können signiert werden. Die Signatur wird nach Auslösen durch den 4-stelligen PIN Code mit der eindeutigen ICCID²² Nummer der SIM Karte zurückgesendet, sodass das verwendete Zertifikat einfach gefunden werden kann. Das jeweilige Zertifikat ist nicht auf der SIM Karte gespeichert sondern wird vom Signaturvalidator über die ICCID ausfindig gemacht. Bei dem Zertifikat dieser Lösung handelt es sich um ein qualifiziertes Zertifikat.

Bis 2005/2006 wurde die gesamte PKI Infrastruktur (CA/RA und Validator) von Telenor selbst betrieben, jedoch wurde diese aufgrund der geringen Nutzung von norwegischen Banken übernommen und als neuer Dienst unter dem Namen „BankID“ für die Identifikation/Authentifizierung im Rahmen von Online Banking gestartet. 95% der norwegischen Banken sind daran beteiligt. Der Start des vollständigen Dienstes ist für Q2/Q3 dieses Jahres geplant.

Zum aktuellen Zeitpunkt wird die Mobile Signatur lediglich von einigen tausend Nutzern in Anspruch genommen. Aufgrund des hohen Nutzungsanteils von Online Banking in Norwegen wird angenommen, dass die Verbreitung der Mobil-Signatur durch die Einführung von BankID in größerem Maße zunehmen wird.

Über einen Webbrowser gibt der Nutzer seine Mobiltelefonnummer (MSISDN²³) ein und der Dienst erzeugt eine SMS mit einer Signaturaufforderung. Die SMS wird am Mobiltelefon dargestellt und der Nutzer muss seine Signatur-PIN eingeben. Die erstellte PKCS#1 Signatur wird über das Mobilnetz rückübermittelt und validiert. Aufgrund der Verwendung von SMS ist momentan eine Limitierung von 140 Zeichen gegeben.

BankID kann aber nicht nur zur Authentifizierung/Identifikation im Rahmen von Online Banking, sondern auch für eGovernment Portale und anderweitige Transaktionen verwendet werden.

Zur Zeit wird diskutiert, ob durch die neue Generation von SIM Karten (UICC²⁴), welche größere Speicherkapazitäten besitzen, als Signaturformat der Einsatz von PKCS#7 sinnvoll wäre, da diese einen höheren Verbreitungsgrad aufweisen.

²¹ <http://www.telenor.com/>

²² <http://en.wikipedia.org/wiki/ICCID>

²³ <http://en.wikipedia.org/wiki/MSISDN>

²⁴ <http://en.wikipedia.org/wiki/UICC>

3.2 Mobiil-ID (Estland)

3.2.1 Allgemeines

Seit dem Start der Infosecurity 2009 Initiative²⁵ am 23.05.2006 in Estland hat sich die Zahl der Personen, welche die elektronischen Funktionen der eID Karte nutzen, mehr als verdoppelt. Ausgehend von ursprünglich 25.000 Personen, wird die Funktionalität bereits von über 60.000 Personen genutzt²⁶. Die Initiative hat sich zum Ziel gesetzt, die Penetration der Internetnutzung in Estland voranzutreiben und die Zahl der Nutzer der eID bzw. Mobile-ID bis 2009 auf 400.000 zu erhöhen.

Im Mai 2007 wurde in Estland der Dienst Mobile-ID (in der Landessprache "Mobiil-ID") gestartet. Dieser resultierte aus der Zusammenarbeit des Telekommunikationsproviders "EMT²⁷" und des Zertifizierungsdiensteanbieters "AS Sertifitseerimiskeskus²⁸". Eine Nutzung des Mobile-ID Dienstes wird auch vom größten Telekommunikationsprovider in Estland – "Elion²⁹" – angeboten. Mehr als 600 Personen nutzen diesen Dienst bereits.

Mobile-ID stellt die Identifikation-, Authentifizierungs- und Signaturmechanismen der estnischen eID für ein Mobiltelefon zur Verfügung. Die SIM Karte des Mobiltelefons übernimmt hier die gleichen Funktionen wie die estnische eID Chipkarte. Mit Mobile-ID kann man sich somit bei dedizierten Portalen mit der gleichen Qualität wie mit der eID Chipkarte anmelden und digitale Signaturen erstellen.

Jene digitale Signaturen, welche mit Mobile-ID erstellt werden, entsprechen den in Estland geforderten Sicherheitsbestimmungen und besitzen somit die gleiche Qualität wie eine handschriftliche Unterschrift bzw. wie eine Unterschrift mit der eID Karte.

3.2.2 Details

Die Aktivierung von Mobile-ID ist momentan ausschließlich über die eID Karte möglich. Alternative Aktivierungsmöglichkeiten sind jedoch für die Zukunft geplant. Über die Seite <http://www.sk.ee/midaktiveerimine/> kann Mobile-ID in wenigen Schritten aktiviert werden. Dazu sind die eID, die PIN-1 der eID sowie ein Kartenlesegerät notwendig. Die Qualität des Aktivierungsprozesses muss ein maximales Maß an Sicherheit bieten, da Mobile-ID zu Bankgeschäften bzw. Verwaltungsverfahren genutzt werden kann und die gleiche Rechtswirksamkeit wie die herkömmliche Unterschrift entfaltet.

Die Zertifikate der Mobile-ID besitzen eine Gültigkeit von 5 Jahren, sind jedoch nicht auf der SIM Karte gespeichert. Anschließend muss die SIM Karte getauscht werden. Die Schlüssel für Mobile-ID (Geheimhaltungs- und Signaturschlüssel) befinden sich auf der SIM Karte, sind jedoch unabhängig von der PIN des Mobiltelefons.

Um sich nun an einer Seite mit Mobile-ID anmelden zu können, muss man im Browser in einem Formular seinen Benutzernamen/Passwort bzw. seine Telefonnummer angeben. Die Identifikation/Authentifizierung wird über das zentrale DigiDocService abgewickelt, welches alle Anwendungsportale für diese Zwecke verwenden können. In einem ersten Schritt wird über OCSP der Zertifikatsstatus überprüft und an das Portal zurückübermittelt. In einem zweiten Schritt werden dem Bürger Authentifizierungsinformationen über den Telekommunikationsprovider an das Mobiltelefon gesendet und dargestellt, die er durch die Eingabe seiner PIN-1 bestätigen und somit signieren muss. Die erstellte Signatur wird über den Telekommunikationsprovider an das DigiDocService rückübermittelt und das DigiDoc Service bestätigt dem Portal die erfolgreiche Anmeldung.

Die Erstellung einer Signatur mittels Mobile-ID erfolgt ähnlich dem Prozess zur Identifikation/Authentifizierung. Der Benutzer muss vor der Erstellung die Dokumente oder

²⁵ <http://www.riso.ee/en/pub/2006it/index.php?mn=13>

²⁶ siehe <http://www.sk.ee/pages.php/02030201,1233>

²⁷ <http://www.emt.ee/>

²⁸ <http://www.sk.ee/>

²⁹ <http://www.elion.ee/>

dessen Hashwerte an das DigiDocService übermitteln. Das DigiDocService übernimmt die Erstellung der Signatur und sendet diese anschließend an den Benutzer zurück.

3.2.3 Nutzbare Dienste

Mobile-ID kann genutzt werden, um auf folgende Dienste zuzugreifen:

- [DigiDoc Portal](#)
- [EMT's self-service](#)
- [Citizen's portal](#)
- [Elion's e-service](#)
- [E-Tax Board](#)
- [ID-ticket](#)
- [Telehanza.net](#)
- [Hanza.net](#)
- [U-Net](#)
- [U-Net Business](#)
- [Krediidipank's i-pank](#)
- [Queries over X-tee](#)

3.3 "eID on SIM" (Finnland)

3.3.1 Allgemeines

2005 wurde in Finnland als Alternative zur finnischen eID Chipkarte die Signatur mit mobilen Geräten auf Basis von GSM-SIM Karten eingeführt. Das Mobiltelefon dient hierbei als sicheres Signaturerstellungsgesetz zur Erzeugung qualifizierter Signaturen.

Um einen Dienst für die elektronische Identifikation mittels Mobiltelefon zu schaffen, ist das finnische Melderegister eine Zusammenarbeit mit verschiedenen Telekommunikationsprovidern wie Elisa³⁰ und Sonera³¹ eingegangen. Ziel war es, sowohl Dienste der öffentlichen Verwaltung, als auch jene im privaten Dienstleistungssektor nutzen zu können. Das Mobiltelefon soll im Wege der Online Kommunikation als Ersatz für ein Kartenlesegerät für Chipkarten dienen.

3.3.2 Aktivierung am Beispiel Sonera

GSM-SIM Karten mit PKI Unterstützung für die finnische eID können beim Telekommunikationsprovider Sonera erworben werden. Die Registrierung selbst erfolgt bei einer beliebigen Polizeistation, welche die Identität gesichert überprüfen muss (z.B. mittels Reisepass, Führerschein, usw.). Die Polizei kontaktiert anschließend das Melderegister und veranlasst die Ausstellung eines qualifizierten Zertifikats, welches eine Gültigkeit von 5 Jahren besitzt.

Die PKI SIM Karte erzeugt am Mobiltelefon ein zusätzliches Menü, über welches die PINs für beide Schlüssel auf der Karte (Signaturschlüssel, Geheimhaltungsschlüssel) geändert werden können.

3.3.3 Details

Um das Konzept der finnischen eID-Lösung zu fördern, wurde vom finnischen Finanzministerium im Juli 2006 ein zentrales Authentifizierungs- und Bezahlservice für die finnische eID sowohl in Chipkartenform als auch in Form einer mobilen in Betrieb genommen. Der Dienst bietet eine einheitliche Schnittstelle und kann von allen Applikationen

³⁰ <http://www.elisa.fi/yksityisille/>

³¹ <http://www.sonera.fi/>

genutzt werden, die eine Identifikation oder einen Bezahlendienst für ihre Nutzer anbieten möchten. VETUMA kann weiters im Rahmen der Bezahlung beispielsweise bei Online Banking für Kreditkarten von VISA bzw. Mastercard benutzt werden.

Am ehesten vergleichbar ist das System mit der österreichischen MOA-ID³² wobei die finnische Lösung zusätzlich die Bezahlung integriert.

Die Prozesse für die Identifikation bzw. Signatuererstellung mittels VETUMA sind in folgenden Abbildungen dargestellt:

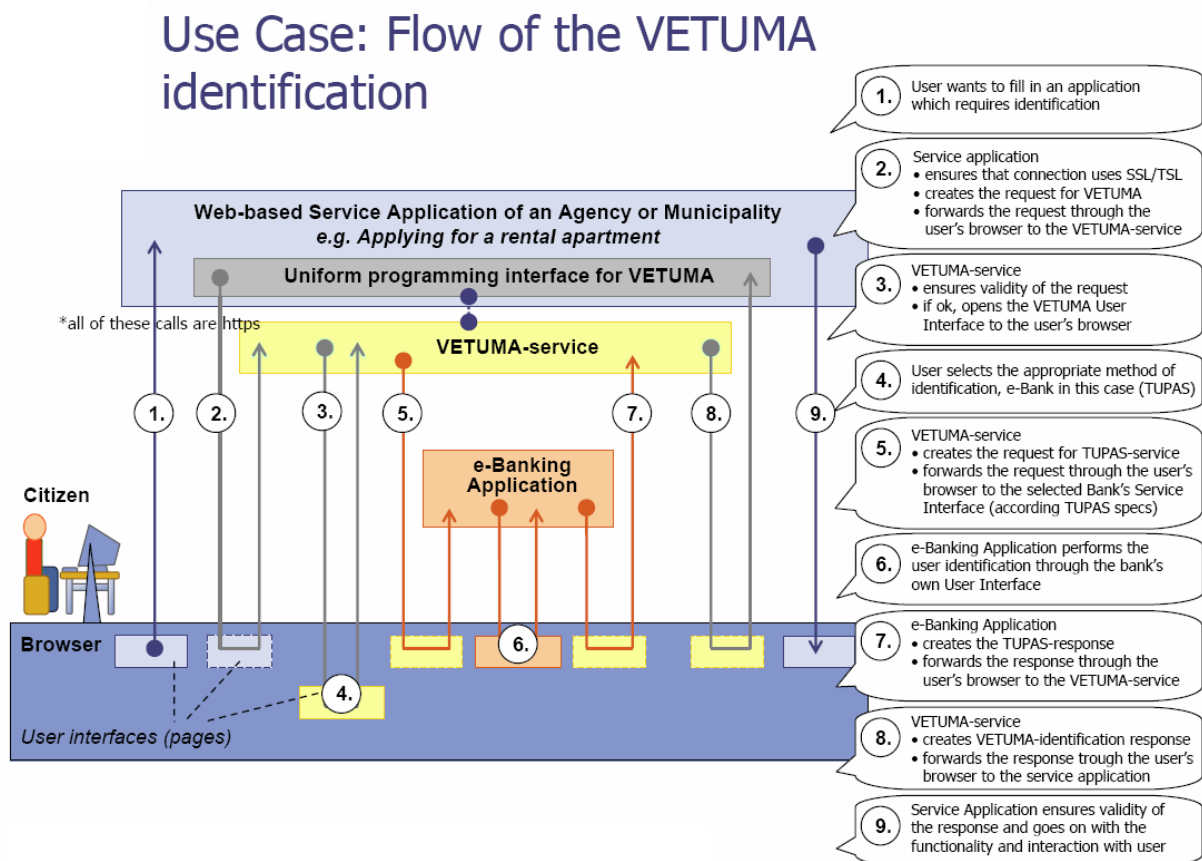


Abb. 3.1 Identifikation mittels VETUMA³³

³² <http://egovlabs.gv.at/projects/moa-idspss/>

³³ http://www.observatory.gr/files/news_events/summit_presentations/Presentation%20Timo%20Karppinen.pdf

Use Case: Flow of the VETUMA signature

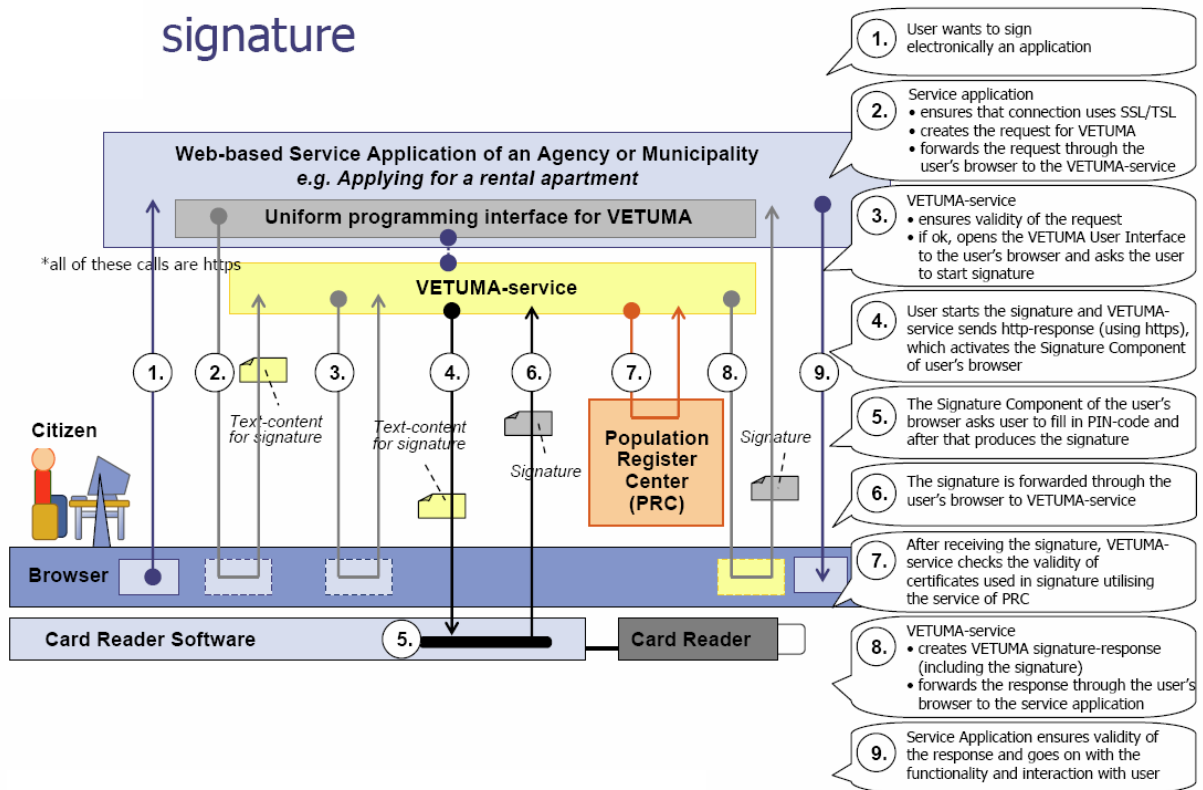


Abb. 3.2 Signatur mittels VETUMA³⁴

³⁴ http://www.observatory.gr/files/news_events/summit_presentations/Presentation%20Timo%20Karppinen.pdf

4 Zusammenfassung

Betrachtet man diverse internationale Umsetzungen, kann man feststellen, dass diese ausnahmslos auf Signaturerstellungseinheiten innerhalb der Endgeräte setzen. Lösungen, die eine Trennung der PIN-Eingabe von der Signaturerstellung vorsehen – so wie es beispielsweise bei der A1-Signatur der Fall war – sind nicht vertreten.

Österreich weist keine hohe Durchdringung von Mobiltelefonen mit PKI fähiger SIM-Karte auf, wie es vergleichsweise in Norwegen mit 50% der Fall ist. Aus diesem Grund wird sich in Österreich eine ähnliche Lösung vorerst wohl nicht etablieren können.

In Anbetracht der Tatsache, dass sich microSD-Schnittstellen als Standard bei Mobiltelefonen durchzusetzen scheinen, wäre die Nutzung einer microSD-Karte mit integriertem Chip vorstellbar. Dagegen sprechen jedoch die Kosten, die jedem Anwender durch Kauf einer solchen Karte entstehen würden. Herkömmliche Bürgerkartenlösungen werden immer wieder wegen der Kosten für den Erwerb eines Kartenlesers kritisiert. Die Propagierung der microSD-Lösung würde auch hier Ansatz für Kritikpunkte in Hinsicht entstehender Kosten schaffen..

Das Apple iPhone für die Anbringung von Mobilten Signaturen zu verwenden ist sicherlich ein netter Showcase, kann im Moment mangels sicherer Speicherung privater Schlüssel und demnach fehlender qualifizierten Signaturmöglichkeit sowie wegen der hohen Anschaffungs- bzw. Folgekosten beim Abschluss eines entsprechenden Mobilfunkvertrags nicht als optimale Lösung empfohlen werden.

In Anbetracht der Zielsetzung einer mobilen Lösung für Österreich, nämlich der Verbreitung des Konzepts Bürgerkarte in mobiler Form, bieten in Hinblick auf die bereits ausgerollten Chipkarten sowie in Hinblick auf die hohe Handypenetration vor allem zwei Varianten an: Eine serverbasierte (kartenfreie) Lösung, die mehr oder weniger auf gleiche Weise wie die bereits bekannte A1-Signatur arbeitet sowie eine clientinstallationsfreie Lösung in Form einer Browser-BKU an.

Referenzen

[KEYWORDS]	Bradner, S.: RFC 2119: <i>Key words for use in RFCs to Indicate Requirement Levels</i> . IETF Request For Comment, März 1997. Abgerufen aus dem World Wide Web am 20.09.2007 unter http://www.ietf.org/rfc/rfc2119.txt
[AIDEV]	Apple iPhone Developer Program Abgerufen aus dem World Wide Web am 08.04.2008 unter http://developer.apple.com/iphone/program/details.html
[E-GovG]	<i>Bundesgesetz über Regelungen zur Erleichterung des elektronischen Verkehrs mit öffentlichen Stellen (E-Government-Gesetz – E-GovG)</i> BGBl. I Nr. 10/2004 vom 27.02.2004, Artikel 1 Abgerufen aus dem World Wide Web am 13.02.2008 unter http://ris1.bka.gv.at/Appl/Authentic/SearchAuthResult.aspx?page=doc&docnr=20
[E-GovG-Novelle 2007]	<i>Bundesgesetz, mit dem das E-Government-Gesetz geändert wird (E-GovG-Novelle 2007)</i> BGBl. I Nr. 7/2008 vom 07.01.2008 Abgerufen aus dem World Wide Web am 13.02.2008 unter http://ris1.bka.gv.at/Appl/Authentic/SearchAuthResult.aspx?page=doc&docnr=2
[GDMSC]	Giesecke & Devrient, <i>The Mobile Security Card</i> Abgerufen aus dem World Wide Web am 14.03.2008 unter http://www.gi-de.com/portal/page?_pageid=42,95141&_dad=portal&_schema=PORTAL
[HBDC]	W. Rankl & W. Effing, <i>Handbuch der Chipkarten</i> 4. Auflage 2002, Carl Hanser Verlag München Wien
[IICSCSC]	IICS, <i>certgate Smart Card</i> Abgerufen aus dem World Wide Web am 14.03.2008 unter http://certgate.com/web_de/produkte/smartcardmmc.html
[IKTHS2007]	Statistik Austria, <i>IKT-Einsatz in Haushalten 2007</i> Abgerufen aus dem World Wide Web am 18.02.2008 unter http://www.statistik.at/web_de/statistiken/informationsgesellschaft/ikt-einsatz_in_haushalten/index.html
[RTR-SSCD]	RTR – Rundfunk & Telekom Regulierungs-GmbH, <i>Signaturestellungseinheiten mit Bescheinigungen nach § 18, Abs. 5 SigG</i> Abgerufen aus dem World Wide Web am 15.02.2008 unter http://www.signatur.rtr.at/de/providers/products.html
[SL12]	A. Hollosi, G. Karlinger: Applikationsschnittstelle Security-Layer Version 1.2.2 vom 01.03.2005 Abgerufen aus dem World Wide Web am 20.02.2008 unter http://www.buergerkarte.at/konzept/securitylayer/spezifikation/aktuell/core/Core.html

[VerwSigV]	<i>Verordnung des Bundeskanzlers, mit der die sicherheitstechnischen und organisationsrelevanten Voraussetzungen für Verwaltungssignaturen geregelt werden (VerwSigV)</i> BGBl. II Nr. 159/2004 vom 15.04.2004 Abgerufen aus dem World Wide Web am 13.02.2008 unter http://ris1.bka.gv.at/Appl/Authentic/SearchAuthResult.aspx?page=doc&docr=1
[WIM]	WAP Security, <i>Wireless Identity Module</i> Version vom 12.07.2001, WAP-260-WIM-20010712-a Abgerufen aus dem World Wide Web am 15.02.2008 unter http://www.wmlclub.com/docs/especwap2.0/WAP-260-WIM-20010712-a.pdf