Thomas Zefferer, Peter Teufl, Herbert Leitold

Mobile qualifizierte Signaturen in Europa

Konzepte zur Vereinfachung elektronischer Signaturen durch die Verwendung mobiler Endgeräte

Die EU Signaturrichtlinie stellt die rechtliche Äquivalenz zwischen handschriftlichen Unterschriften und qualifizierten elektronischen Signaturen sicher. Die Komplexität aktueller chipkartenbasierter Signaturlösungen und damit einhergehende Mängel in der Benutzerfreundlichkeit verhinderten bisher oft einen breiten Einsatz elektronischer Signaturen. Die Verwendung mobiler Technologien zur sicheren Erstellung qualifizierter elektronischer Signaturen verspricht hier Abhilfe zu schaffen. Dieser Artikel stellt verschiedene Ansätze der mobilen Signaturerstellung vor und analysiert diese bezüglich diverser rechtlicher und sicherheitstechnischer Aspekte.

Herbert Leitold

ist Standortleiter am A-SIT, Zentrum für sichere Informationstechnologie - Austria und Leiter des E-Government Innovationszentrums EGIZ.
E-Mail: Herbert.Leitold@a-sit.at

Peter Teufl

ist Universitätsassistent am Institut für Angewandte Informationsverarbeitung und Kommunikationstechnologie (IAIK) der Technischen Universität Graz.
E-Mail: Peter.Teufl@iaik.tugraz.at

Thomas Zefferer

ist wissenschaftlicher Mitarbeiter des österreichischen E-Government Innovationszentrums EGIZ am IAIK der Technischen Universität Graz.
E-Mail: Thomas.Zefferer@iaik.tugraz.at

Einleitung

Die elektronische Signatur konnte sich in den letzten Jahren in vielen europäischen Ländern als weitgehend ausgereifte und häufig verwendete Technologie etablieren. Legitimiert durch nationale Gesetze und Verordnungen entsprechend den Vorgaben der EU Signaturrichtlinie [1] finden heutzutage qualifizierte elektronische Signaturen vor allem im öffentlichen Sektor breite Anwendung. Durch deren rechtliche Äquivalenz zu herkömmlichen handschriftlichen Unterschriften werden qualifizierte elektronische Signaturen beispielsweise im Rahmen verschiedenster E-Government Lösungen verwendet, um ursprünglich papierbasierte Verfahren in IT basierte Prozesse überzuführen. In Österreich wurde auch das Konzept der elektronischen Amtssignatur [2] eingeführt, welches die Ansprüche an Signaturen von Behörden auf elektronische Dokumente abbildet. In einzelnen Ländern ist die Verbreitung und Verwendung der elektronischen Signatur bereits so weit fortgeschritten, dass diese als kritische Infrastrukturkomponente betrachtet werden muss. Auch hier kann als Beispiel Österreich dienen, wo sämtliche Gesetze vor Inkrafttreten elektronisch signiert werden müssen.

Obwohl die elektronische Signatur auf Seiten der Behörden in vielen Ländern bereits intensiv genutzt wird, bleibt deren Verwendung im privaten Sektor derzeit noch hinter den Erwartungen zurück. Auch wenn einzelne Berufsgruppen wie Anwälte oder Notare die elektronische Signatur bereits regelmäßig verwenden, konnten weite Teile der Bevölkerung von den Vorzügen elektronischer Signaturen noch nicht überzeugt werden.

Die fehlende Akzeptanz scheint vor allem an zusätzlich notwendigen Komponenten wie Chipkartenlesern und in der mangelnden Benutzerfreundlichkeit aktueller technischer Umsetzungen begründet. Die korrekte Implementierung qualifizierter elektronischer Signaturen ist in der Tat ein nicht triviales Unterfangen. Die EU Signaturrichtlinie fordert zur Erstellung qualifizierter elektronischer Signaturen eine sogenannte Sichere Signaturerstellungseinheit (SSEE). Nationale Umsetzungen wie das deutsche Signaturgesetz [3] detaillieren die Anforderungen weiter und sehen beispielsweise vor, dass der Signaturschlüssel durch Besitz und Wissen, oder durch Besitz und biometrische Merkmale vor unberechtigter Anwendung geschützt werden muss. Vergleichbare Forderungen nach Mehr-

Faktor-Authentifizierung im Rahmen der Erstellung qualifizierter elektronischer Signaturen sind auch in einschlägigen Gesetzen anderer Länder zu finden.

In den meisten Fällen wird der Forderung nach Mehr-Faktor-Authentifizierung durch die Verwendung der Chipkartentechnologie nachgekommen. In Österreich können Bürgerinnen und Bürger beispielsweise ihre Sozialversicherungskarte, ihre Bankkarte, oder diverse Berufs- oder Studentenausweise als Bürgerkarte aktivieren lassen. Dabei handelt es sich bei allen Varianten um bescheinigte SSEE. Die Signaturfunktionalität bzw. der auf dem Chip der Karte sicher gespeicherte Signaturschlüssel sind durch eine geheime und nur dem Karteninhaber bekannte PIN geschützt. Für die Erstellung einer Signatur bedarf es daher sowohl der Karte (Faktor Besitz) als auch der geheimen PIN (Faktor Wissen), wodurch der Forderung nach Mehr-Faktor-Authentifizierung nachgekommen wird.

Vergleichbare Ansätze finden sich auch in zahlreichen anderen Ländern wie Deutschland, Estland oder Belgien. Obwohl sich die Verwendung der Chipkartentechnologie bisher als verlässlich und sicher erwiesen hat, zeigen sich in Bezug auf deren Benutzerfreundlichkeit einige Mängel. Vor allem die Notwendigkeit eines geeigneten Kartenlesegeräts stellt für Bürgerinnen und Bürger einen Zusatzaufwand dar, den diese oft nicht zu bestreiten bereit sind. Zu gering erscheint in den Augen vieler der sich durch elektronische Signaturen ergebende Zusatznutzen, der den durch Chipkarten verursachten Mehraufwand rechtfertigen würde. Verschärft wird die Situation zudem durch die steigende Popularität alternativer Endgeräte wie Smartphones oder Tablet-Computer, welche oftmals keine technische Möglichkeit für die Verwendung von Chipkarten bieten.

Da der Benutzerfreundlichkeit chipkartenbasierter Lösungen technologiebedingt Grenzen gesetzt sind, müssen zur Steigerung der breiten Akzeptanz elektronischer Signaturen alternative Strategien verfolgt werden. In Bezug auf Akzeptanz und Popularität sind aktuell mobile Technologien außerordentlich erfolgreich. Es erscheint daher naheliegend, deren Popularität zu nutzen, um auch die Akzeptanz und Verbreitung elektronischer Signaturen zu erhöhen. Tatsächlich wurde das Potential mobiler Technologien von vielen Ländern bereits früh erkannt und entsprechend umgesetzt. Aktuell ist die Erstellung qualifizierter elektronischer Signaturen unter Verwendung mobiler Technologien bereits in mehreren Ländern erfolgreich implementiert[1].

Durch die Abkehr von der bewährten Chipkarten-Technologien und der Miteinbeziehung mobiler Technologien und Komponenten in den Signaturerstellungsprozess ergeben sich zwangsläufig auch neue sicherheitstechnische Herausforderungen. Im Speziellen muss unter Verwendung mobiler Technologien eine geeignete Möglichkeit für die Durchführung der gesetzlich geforderten Mehr-Faktor-Authentifizierung von Unterzeichnern gefunden werden.

1 Mobile Signaturen

Die steigende Popularität mobiler Informations- und Kommunikationstechnologien führt zu einem stetig wachsenden Angebot an mobilen Diensten und Anwendungen. Diese Entwicklung führte unter anderem in mehreren Ländern zur Entwicklung mobiler Signaturlösungen. Als mobile Signatur bezeichnen wir im Folgenden eine elektronische Signatur, die unter Zuhilfenahme mobiler Technologien erstellt wird.

Obwohl prinzipiell verschiedene mobile Geräte wie PDAs, Smartphones oder auch spezielle Hardwaretoken für die Erstellung mobiler Signaturen geeignet sind, basieren die meisten aktuellen Lösungen auf Mobiltelefonen. Gründe dafür sind unter anderem deren weite Verbreitung und die unabhängig von Alter, Beruf und sozialem Umfeld bestehende Vertrautheit mit dieser Technologie. Diese Eigenschaften sollen dabei die Akzeptanz elektronischer Signaturlösungen erhöhen.

Die Flexibilität moderner Mobiltelefone lässt trotz der speziellen sicherheitstechnischen Anforderungen, die im Zuge der Erstellung qualifizierter elektronischer Signaturen eingehalten werden müssen, verschiedene Arten der Implementierung mobiler Signaturen zu. Zur Veranschaulichung der zugrundeliegenden Konzepte werden in weitere Folge zwei konkrete Ansätze zur Erstellung mobiler Signaturen vorgestellt und anhand entsprechender Implementierungen verglichen.

1 Mobile Signaturlösungen sind derzeit unter anderem in Estland, Norwegen, Finnland, Schweden und Österreich im Einsatz.

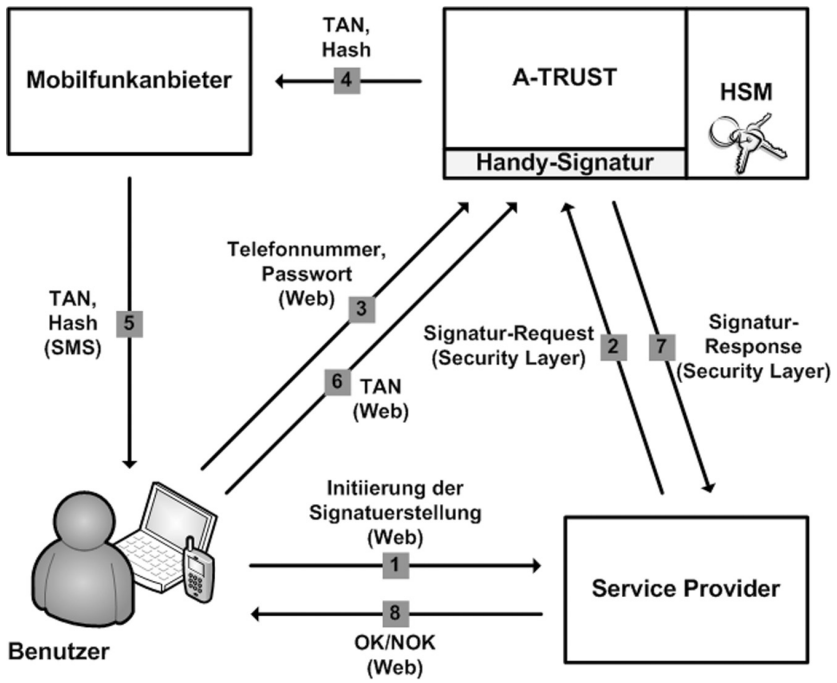
1.1 Varianten

Da qualifizierte elektronische Signaturen gemäß der EU Signaturrichtlinie der handschriftlichen Unterschrift gleichgesetzt sind, ist deren Sicherheit von zentraler Bedeutung. Zur Gewährleistung eines größtmöglichen Sicherheitsniveaus werden die Verwendung einer SSEE und eine Mehr-Faktor-Authentifizierung des Unterzeichners als Anforderungen definiert.

Aktuell verwendete mobile Signaturlösungen verfolgen eine von zwei gängigen Varianten, um diese Anforderungen zu erfüllen.

- Die Signatur wird direkt am Mobiltelefon berechnet. Dazu wird ein mit einem SSEE ausgestattetes Mobiltelefon mit dem privaten Signaturschlüssel des Benutzers personalisiert. Der Signaturschlüssel wird im SSEE sicher gespeichert und durch eine geheime PIN geschützt. Eine ebenfalls am Mobiltelefon betriebene Signaturapplikation dient als Schnittstelle zum Benutzer. Über diese Applikation kann der Benutzer die zu signierenden Daten kontrollieren, die geheime PIN eingeben und damit die Signaturerstellung auslösen. Aufgrund der steigenden technischen Möglichkeiten gibt es bereits eine Reihe verschiedener Möglichkeiten SSEEs auf Mobiltelefonen zu implementieren. Eine Studie der ENISA [4] nennt als mögliche Umsetzungen beispielsweise die in jedem Mobiltelefon vorhandene SIM Karte, zusätzliche SD oder microSD Karten mit integrierten Secure Elements, aber auch entsprechend abgesicherte Softwarelösungen. Die Zwei-Faktor-Authentifizierung von Benutzern wird bei dieser Variante der mobilen Signatur über die Faktoren Besitz (Mobiltelefon bzw. SSEE) und Wissen (PIN) sichergestellt.
- Alternativ können mobile Signaturen auch durch eine zentrale Serverkomponente erstellt werden. Die SSEE wird in diesem Fall durch ein Hardware Security Module (HSM) implementiert, das an die zentrale Serverkomponente angebunden ist. Der Signaturschlüssel ist zentral im HSM hinterlegt und über entsprechende kryptographische Methoden und ein Passwort abgesichert. Die Auslösung der Signatur erfolgt über eine TAN, die dem Benutzer über SMS an sein Mobiltelefon zugestellt wird und die dieser dann an die Zentralkompo-

Abb 1 | A-Trust Handy-Signatur (Österreich)



nente zurücksenden muss. Über die Faktoren Wissen (z.B. Passwort für Zugriff auf den Signaturschlüssel) und Besitz (Mobiltelefon, dessen Besitz durch Verwendung der SMS TAN verifiziert wird) wird auch bei dieser Variante der mobilen Signatur die Forderung nach einer Zwei-Faktor-Authentifizierung von Benutzern erfüllt.

Sämtliche bekannten im Einsatz befindlichen Systeme zur Erstellung mobiler Signaturen entsprechen grundsätzlich einer dieser beiden Varianten. Abhängig von der jeweiligen Implementierung und von geltenden nationalen gesetzlichen Vorgaben unterscheiden sich die einzelnen Systeme jedoch in bestimmten Details. Im Folgenden werden die beiden in Österreich und Estland verwendeten Systeme näher erläutert, um die Unterschiede der beiden Ansätze anhand konkreter Implementierungen zu verdeutlichen.

1.2 Fallstudie: Österreich

Österreich versuchte bereits sehr früh mobile Technologien für die Erstellung elektronischer Signaturen zu nutzen. Die erste derartige Initiative war die A1-Signatur der österreichischen Mobilfunkanbieters Mobilkom Austria [5]. Die A1-Signatur folgte dem Konzept der durch TANs autorisierten serverseitigen Signaturerstellung und erlaubte die Erstellung so genannter Verwaltungssignaturen. Diese waren in Österreich dank einer gesetzlich festgelegten Übergangsregelung bis 2007 qualifizierten Signaturen gleichgestellt. Dieser Dienst wurde mit dem Auslaufen dieser Übergangsregelung, die eine Migration auf qualifizierte Signaturen nötig gemacht hätte, eingestellt.

Die durch die Einstellung der A1-Signatur entstandene Lücke wurde im Jahr 2009 durch die im EU Large Scale Pilot STORK entwickelte und vom österreichischen Zertifizierungsdiensteanbieter A-Trust betriebene Handy-Signatur geschlossen [6]. Vom Aufbau prinzipiell mit der A1-Signatur vergleichbar, folgt auch die Handy-Signatur dem Konzept einer serverseitigen Signaturerstellung. Neu ist, dass die Handy-Signatur nun als qualifizierte Signatur ausgeführt ist.

Der generelle Aufbau der Handy-Signatur, sowie ein typischer Signaturerstellungsprozess sind in Abbildung 1 skizziert[2]. Benutzer greifen über eine webbasierte Schnittstelle auf einen Dienst des Service Providers zu (1). Dabei kann es sich beispielsweise um eine Web-Applikation o.ä. handeln. Ist im Zuge der Verwendung des beanspruchten Dienstes die Erstellung einer elektronischen Signatur notwendig, sendet der Service-Provider einen entsprechenden Request an die Handy-Signatur Komponente der A-Trust (2). Der gesendete Request entspricht dabei der für das österreichische E-Government definierten Security Layer Spezifikation [7] und enthält unter anderem die zu signierenden Daten. Nach Erhalt des Requests zeigt die Handy-Signatur Komponente im Web-Browser des Benutzers ein Web-Formular an, über welches Telefonnummer und Signaturpasswort bekanntgeben werden können[3] (3).

Der für die Erstellung der elektronischen Signatur benötigte Signaturschlüssel ist in einem an die Zentralkomponente der Handy-Signatur angebundenen HSM verschlüsselt hinterlegt. In die Ableitung des für die Verschlüsselung verwendeten Schlüssels gehen die Telefonnummer des Benutzers, dessen Signaturpasswort und ein nur im HSM verfügbarer geheimer HSM-Schlüssel ein. Der Signaturschlüssel des Benutzers ist daher sowohl an den Benutzer als auch an das HSM gebunden und kann nur durch eine Kooperation dieser beiden Komponenten verwendet werden.

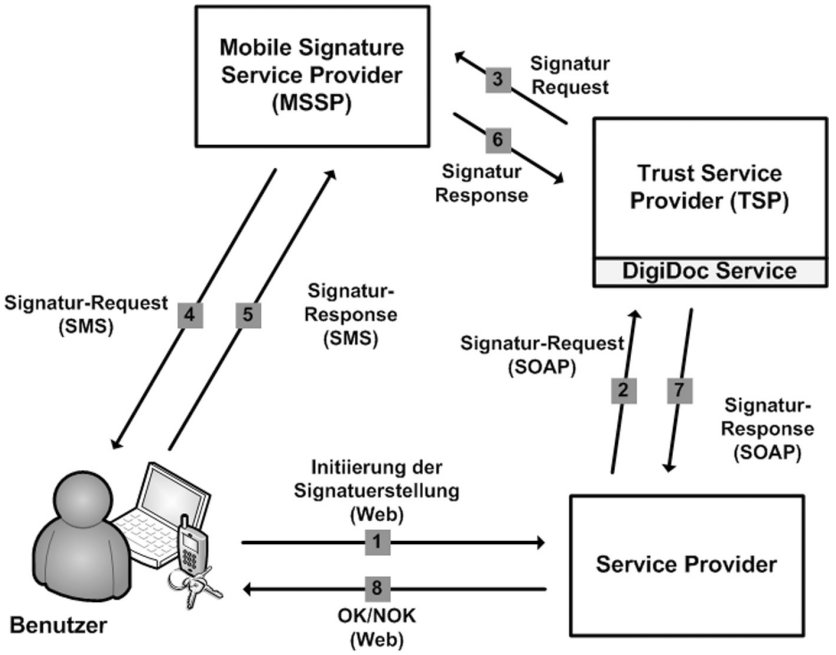
Durch die in Schritt (3) erfolgte Übermittlung der Telefonnummer und des Signaturpassworts des Benutzers kann das HSM dessen Signaturschlüssel entschlüsseln und die Signatur der in Schritt (2) übermittelten Signaturdaten vorbereiten. Vor der endgültigen Auslösung der Signaturerstellung im HSM sendet die Zentralkomponente der Handy-Signatur ein zeitlich begrenzt gültiges Einmalpasswort (TAN) und einen Hash-Wert der zu signierenden Daten an den Mobilfunkbetreiber des Benutzers (4). Dieser leitet die Daten über den SMS Kanal an das Mobiltelefon des Benutzers weiter (5). Ähnlich der Bekanntgabe von Telefonnummer und Signaturpasswort kann der Benutzer die erhaltene TAN wiederum über ein von der Handy-Signatur Komponente bereitgestelltes Web-Formular bekanntgeben (6). Über dieses Web-Formular wird ebenfalls der Hash-Wert der zu signierenden Daten dargestellt, welchen der Benutzer vor Eingabe der TAN mit dem über SMS erhaltenen Hash-Wert vergleichen kann[4].

2 Aus Übersichtlichkeitsgründen wird die Registrierung neuer Benutzer und die Erstellung entsprechender Signaturerstellungsdaten (Signaturschlüssel und Signaturzertifikat) nicht näher betrachtet.

3 Aus Gründen der Benutzerfreundlichkeit wird das von der Handy-Signatur bereitgestellte Web-Formular in der Regel über ein HTML IFRAME Tag in die Applikation des Service Providers eingebunden, sodass dieser die gewohnte Umgebung nicht verlassen muss.

4 Über eine durch das HSM erstellte Signatur ist der Hash-Wert der zu signierenden Daten zudem mit dem Einmalpasswort eindeutig verknüpft.

Abb 2 | Mobiil-ID (Estland)



Durch Erhalt der TAN kann der Benutzer gemäß den Anforderungen einer Zwei-Faktor-Authentifizierung sicher authentifiziert und der Signaturvorgang abgeschlossen werden. Die serverseitig erstellte Signatur wird der Security Layer Spezifikation entsprechend an den Service Provider retourniert (7). Über die bestehende webbasierte Schnittstelle zum Benutzer kann dieser schließlich über den Erfolg des Signaturerstellungsvorgangs informiert werden (8).

Für die spätere Sicherheitsbetrachtung bemerkenswert ist in diesem Modell, dass die zu signierenden Daten, und die signierten Daten direkt zwischen Server-Komponenten ausgetauscht werden (Schritte 2 und 7 des Schaubilds). Diese Daten sind somit von etwaiger Schadsoftware, die am PC oder Mobiltelefon des Benutzers laufen kann, nicht änderbar.

Die A-Trust Handy-Signatur ist ein typisches Beispiel einer serverseitigen mobilen Signaturlösung. Obwohl das Mobiltelefon des Benutzers lediglich als Empfangseinheit für Einmalpasswörter fungiert, erhöht dieser zweite Kommunikationskanal die Sicherheit des Gesamtsystems entscheidend und ermöglicht erst die Implementierung serverseitiger Bürgersignaturen.

1.3 Fallstudie: Estland

So wie in Österreich wurde auch in Estland bereits früh in die Entwicklung mobiler Signaturlösungen investiert. Als Resultat dieser Bestrebungen wurde im Frühjahr 2007 das Service Mobiil-ID [8] vorgestellt, welches estnischen Bürgerinnen und Bürgern eine auf Mobiltelefonen basierende sichere Authentifizierung und Erstellung elektronischer Signaturen erlaubt.

Der generelle Aufbau des Mobiil-ID Services und der typische Ablauf eines Signaturerstellungsprozesses sind in Abbildung 2 skizziert[5]. Wurde durch den Benutzer am involvierten Service Provider ein Signaturerstellungsvorgang initiiert (1), wird durch den Service Provider ein entsprechender Signatur-Request an den Trust Service Provider (TSP), der zentral als Schnittstelle zwischen Service Providern und Mobilfunkanbietern fungiert, gesendet (2). Der TSP betreibt das DigiDoc Service [9], welches unter anderem eine SOAP Schnittstelle zur Verfügung stellt, über die Signatur- und Authentifizierungs-Requests übermittelt werden können. Anhand der im Signatur-Request enthaltenen Mobiltelefonnummer wird der entsprechende Mobilfunkanbieter (Mobile Signature Service Provider - MSSP) des Benutzers ermittelt und der Request an diesen übertragen (3). Der Mobilfunkanbieter leitet den Request über sein mobiles Netzwerk an das Mobiltelefon des Benutzers bzw. an eine am Gerät installierte SIM-Applikation weiter (4). Zur Übertragung der Daten kommt in diesem Schritt ein auf SMS Nachrichten basierendes OTA[6]-Protokoll zur Anwendung.

Die Signaturerstellung selbst erfolgt am Mobiltelefon des Benutzers. Dazu ist dieses mit einer speziellen SIM-Karte des Mobilfunkbetreibers ausgestattet. Diese ist in der Lage, den über OTA empfangenen Signatur-Request abzuarbeiten und die über den Request übermittelten Daten mit Hilfe des auf der SIM-Karte sicher gespeicherten und zusätzlich durch eine geheime PIN geschützten Schlüssels zu signieren. Die nötige Interaktion mit dem Benutzer wird über eine auf dem Mobiltelefon betriebene SIM-Applikation abgewickelt. Über diese Applikation kann der Benutzer die zu signierenden Daten bzw. einen entsprechenden Referenzwert einsehen und die Signaturerstellung durch Eingabe der PIN auslösen. Nach erfolgreicher Signaturerstellung wird der berechnete Signaturwert in eine Signatur-Response Nachricht verpackt und über die OTA Schnittstelle an den MSSP retourniert (5). Dieser leitet die erhaltene Antwort an den TSP weiter (6). Der TSP übermittelt die erhaltene Signatur-Response schließlich über die SOAP Schnittstelle an den Service Provider (7), welcher den Benutzer über den Erfolg des Signaturerstellungsprozesses informiert (8).

Die estnische Mobiil-ID ist ein typischer Vertreter mobiler Signaturlösungen, welche Mobiltelefone selbst als SSEE verwenden. Die Sicherheit dieses Verfahrens beruht hauptsächlich auf einer Zwei-Faktor-Authentifizierung des Benutzers, die einerseits durch den Besitz des Mobiltelefons bzw. der darin befindlichen SIM-Karte und andererseits durch Kenntnis der geheimen PIN gewährleistet wird.

2 Analyse

Eine genauere Betrachtung der in Estland und Österreich verwendeten mobilen Signaturlösungen verdeutlicht die Unterschiede der beiden grundsätzlichen Varianten zur Erstellung mobiler Signaturen. Sowohl für serverbasierte Ansätze als auch für Verfahren, die auf SSEEs in Mobiltelefonen beruhen, ergeben sich diverse rechtliche und sicherheitstechnische Her-

5 Der Einfachheit halber wurde der Registrierungs- und Aktivierungsprozess nicht berücksichtigt.

6 OTA steht für Over-The-Air und bezeichnet eine Möglichkeit Daten von einer zentralen Serverinstanz an eine SIM-Applikation zu übermitteln.

ausforderungen, die im Folgenden diskutiert werden sollen.

2.1 Sicherheitsüberlegungen

Bei beiden Varianten der mobilen Signaturerstellung ist die sichere Authentifizierung des Benutzers von zentraler Bedeutung. Beide Ansätze verfolgen eine auf den Faktoren Besitz und Wissen basierende Mehr-Faktor-Authentifizierung. In Bezug auf die für die Durchführung der Authentifizierung verwendeten Kommunikationskanäle gibt es jedoch einen signifikanten Unterschied. Bei der in Österreich verwendeten A-Trust Handy-Signatur erfolgt die Übermittlung der Authentifizierungsdaten über zwei unterschiedliche Kanäle. Während das Signaturpasswort zur Initialisierung des Signaturvorgangs ausschließlich über den Web-Browser übertragen wird, wird die für die endgültige Signaturauslösung benötigte TAN per SMS an den Benutzer übermittelt. Die TANs werden im HSM, das die Komponenten des Autorisierungscodes kryptographisch aneinander koppelt, generiert.

Für einen erfolgreichen Angriff auf die Benutzerauthentifizierung ist daher das Kompromittieren zweier unabhängiger Kommunikationskanäle erforderlich, was die Komplexität eines Angriffs entscheidend erhöht. Bei dem u.a. in Estland verfolgten Ansatz erfolgt die Kommunikation zwar ebenfalls über die beiden Komponenten Web-Browser und Mobiltelefon, jedoch wird über den Web-Browser ausschließlich der nicht geheime Benutzername bzw. die Telefonnummer des Benutzers übertragen. Die Authentisierung selbst erfolgt ausschließlich durch die Eingabe der geheimen PIN am Mobiltelefon. Ein zusätzlicher verlässlicher Schutz durch die Verwendung eines zweiten Kommunikationskanals ist dadurch nicht gegeben.

Neben der Anzahl der für die Benutzerauthentifizierung verwendeten Kommunikationskanäle unterscheiden sich die beiden betrachteten Ansätze auch in der Art der über den mobilen Kommunikationskanal übermittelten Daten. Während im estnischen Ansatz vollständige Signatur-Requests und Responses über ein SMS basierte OTA Interface direkt an eine SIM-Applikation am Endgerät übertragen werden, beschränkt sich die mobile Kommunikation bei der österreichischen Lösung auf den Versand gewöhnlicher SMS-Nachrichten. Dadurch ist die österreichische Lösung weitgehend unabhängig vom Mobilfunkanbieter des Benutzers, während estnische Mobilfunkanbieter den Versand spezieller Signatur-Requests und Responses explizit unterstützen müssen.

Ähnliche Überlegungen gelten auch für die verwendeten mobilen Endgeräte selbst. In der in Österreich verwendeten Signaturlösung fungieren Handys ausschließlich als Empfangseinheiten für die über SMS übermittelten TANs. Zur Verwendung der mobilen Signatur in Österreich kann daher prinzipiell jedes Mobiltelefon mit integrierter SMS-Funktionalität verwendet werden. Der estnische Ansatz stellt zwar ebenfalls lediglich geringe Anforderungen an die Funktionalität des Mobiltelefons, jedoch ist für die Verwendung des Mobiil ID Dienstes der Einsatz einer speziellen SIM-Karte mit entsprechender SIM-Applikation nötig. Dies macht einen Tausch der SIM-Karte im Zuge der Aktivierung der mobilen Signaturfunktionalität notwendig und kann zu einer Einschränkung der Benutzerfreundlichkeit führen.

Der gravierendste und zugleich auch offensichtlichste Unterschied zwischen den betrachteten Ansätzen ist der Ort der Signaturerstellung. Während beim estnischen Ansatz jeder Benutzer über eine eigene SSEE in Form einer speziellen SIM-Karte verfügt, kommt bei der österreichischen Lösung eine gemeinsame zentrale SSEE für alle Benutzer zum Einsatz. Dieser zentrale Ansatz bietet diverse Vorteile. So kann eine zentrale Signaturerstellungseinheit in einer kontrollierten Umgebung betrieben und dementsprechend auch einfacher und effizienter abgesichert werden. Ein unerlaubter physischer Zugriff auf die SSEE durch potentielle Angreifer kann damit so gut wie ausgeschlossen werden[7].

Durch die Verwendung einer zentralen SSEE wird zudem gewährleistet, dass Signaturdaten ausschließlich zwischen serverseitigen Komponenten (im österreichischen Fall zwischen Service Provider und A-Trust Handy-Signatur) ausgetauscht werden. Bei der Verwendung von Mobiltelefonen als SSEEs müssen die zu signierenden Daten hingegen direkt an das mobile Endgerät des Benutzers übermittelt werden. Dies stellt ein zusätzliches Sicherheitsrisiko dar, da das Risiko einer Kompromittierung für clientseitige Komponenten naturgemäß ungleich größer ist.

Zusätzlich zu den bisher angestellten Überlegungen stellen Smartphones mobile Signaturlösungen vor neue Herausforderungen. Smartphones sind in Bezug auf Funktionalität und Leistung zunehmend mit PCs oder Laptops vergleichbar. Dadurch sind jedoch vor allem offene Smartphone-Plattformen wie Android auch anfällig für Schadsoftware jeglicher Art, welche wiederum die Sicherheit einer mobilen Signaturerstellung gefährden kann[8]. Vor diesem Hintergrund müssen bestehende mobile Signaturlösungen neu evaluiert und gegebenenfalls für eine Verwendung mit Smartphones adaptiert werden.

2.2 Rechtliche Analyse

In der rechtlichen Analyse beschränken wir uns auf die Situation einer serverseitigen SSEE, also der österreichischen Lösung. Der Grund dafür ist dass sich im Fall einer Chipkarten-SIM als SSEE, abgesehen von allenfalls für akkreditierte Zertifizierungsdiensteanbieter gegebene Anforderungen an die Lesegeräte und PIN-Eingabe, keine substantiellen Änderungen zu herkömmlichen Chipkartenlösungen ergeben. Der verbleibende Abschnitt gibt einen Überblick über die rechtliche Situation. Für weitere Details wird dabei auf [13] verwiesen.

Die EU Signaturrichtlinie stellt als drei Anforderungen an eine qualifizierte Signatur, dass diese (1) eine fortgeschrittene elektronische Signatur ist, die (2) auf einem qualifizierten Zertifikat beruht und (3) von einer SSEE erstellt wurde.

Außer Diskussion ist hier wohl der zweite Punkt, da die Anforderungen an das qualifizierte Zertifikat und dessen

7 Für mobile Signaturlösungen, die das Mobiltelefon als SSEE verwenden gelten hingegen ähnliche Überlegungen wie für chipkartenbasierte Ansätze. Die Integrität des Clientsystems ist unabdingbar für die Sicherheit des Gesamtsystems. Während die Sicherheit gewöhnlicher Mobiltelefone relativ einfach gewährleistet werden kann, ist der Schutz von Smartphones vor einer Kompromittierung durch Schadsoftware ungleich schwieriger, da der Benutzer aktive Komponenten als Apps installieren kann.

8 Wird beispielsweise bei der österreichische Handy-Signatur ein Smartphone sowohl als Web-Browser als auch für den Empfang der mobilen TAN verwendet, geht die zusätzliche Sicherheit, die durch die Verwendung zweier unabhängiger Kommunikationskanäle gewonnen wurde, wieder verloren. Da in diesem Fall beide Kommunikationskanäle über ein und dasselbe Gerät (das Smartphone) laufen, reduziert sich der Aufwand für einen erfolgreichen Angriff auf die Kompromittierung des mobilen Geräts. Die Sicherheit der Handy-Signatur ist in diesem Fall in etwa vergleichbar mit der Signaturerstellung über PC und Chipkarte bei Verwendung eines Kartenlesegeräts ohne PIN-Pad.

Eigenschaften unabhängig von der technischen Ausprägung der SSEE sind.

Für den dritten Punkt, der die SSEE behandelt, bestehen Schutzprofile als Referenznummern zur EU Signaturrichtlinie oder es können notifizierte Bestätigungsstellen die Erfüllung der technischen Anforderungen bescheinigen. Im Fall der Handy-Signatur hat die österreichische Bestätigungsstelle A-SIT eine Bescheinigung erstellt [10], die nach Art. 3 Abs. 4 der Signaturrichtlinie auch EU-weit anzuerkennen ist.

Als letzte Anforderung an qualifizierte Signaturen verbleibt also, dass es sich um eine fortgeschrittene Signatur handeln muss. Die Signaturrichtlinie zählt vier Anforderungen auf, von denen drei (Art. 2.2 lit. a, b und d) sich auf Signaturformate und kryptographische Eigenschaften beziehen, wobei sich im Fall der Handy-Signatur keine Unterschiede zur Chipkarte ergeben. Diskussionswert ist jedoch Art. 2.2. lit d, der fordert, dass eine fortgeschrittene Signatur „… mit Mitteln erstellt [wird], die der Unterzeichner unter seiner alleinigen Kontrolle halten kann". Der Gesetzgeber hat dies in den Materialien zum österreichischen Signaturgesetz [11] klargestellt. Es wird darin diskutiert, dass „alleinige Kontrolle bei entsprechenden Maßnahmen insbesondere technischer oder organisatorischer Natur auch bei softwarebasierten Zertifikaten erfüllt sein kann." Es müssen allerdings „... Sicherheitsmaßnahmen eingesetzt werden, damit der Signator die Kontrolle über den Schlüssel halten kann". Das Argument lässt sich analog auf Server-Signaturen übertragen. Die Forderung zu alleiniger Kontrolle ist eine an technische Maßnahmen, die dem Signator die Ausübung der Kontrolle ermöglichen, und nicht an die physikalische Ausgestaltung oder die Örtlichkeit der Signaturerstellungseinheit.

Zum selben Schluss kommt 2005 die Vereinigung der europäischen Aufsichtsstellen zur elektronischen Signatur (Forum of European Supervisory Authorities for Electronic Signatures, FESA). In einer Stellungnahme zu serverbasierenden Signaturen [12] ist folgende Schlussfolgerung enthalten: „FESA members cannot rule out that server based signature services could be used for creating qualified electronic signatures.". Dieser ist für Deutschland jedoch die Einschränkung "Apart from Germany, where the services in question cannot be used in this context at all" vorangestellt. FESA hat die Möglichkeit serverseitiger qualifizierter elektronischer Signaturen 2005 noch als unwahrscheinlich bewertet, fünf Jahre danach wurden diese in Österreich Realität.

3 Fazit

In diesem Papier wurden zwei unterschiedliche Systeme zu mobilen qualifizierten elektronischen Signaturen vorgestellt, die in Europa erfolgreich ausgerollt wurden. Mit der Handy-Signatur in Österreich wurde ein System vorgestellt, für das erstmals eine Server-Signatur als sichere Signaturerstellungseinheit bescheinigt wurde. Das System zeichnet sich dadurch aus, dass es keine Änderung an der mobilen Einheit erfordert. Dies bedeutet, dass jedes handelsübliche Mobiltelefon verwendet werden kann bzw. die SIM Karte im Zuge der Aktivierung der Signaturfunktionalität nicht getauscht werden muss. Das System ist damit unabhängig vom Mobilfunkbetreiber. Dem wurde das estnische System Mobiil-ID gegenüber gestellt, das auf Signaturerstellung am mobilen Endgerät über spezielle SIMs als sichere Signaturerstellungseinheit setzt. Beiden Lösungen ist gemein, dass sie über Verwendung von Mobiltelefonen eine Signaturlösung anbieten, die keine weiteren Zusatzgeräte wie Chipkartenleser am PC des Benutzers erfordert.

Literatur

[1] Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen, Amtsblatt der Europäischen Gemeinschaften, 2000

[2] Herbert Leitold, Reinhard Posch, and Thomas Rössler: Media-break resistant eSignatures in eGovernment – an Austrian experience, In: Emerging Challenges for Security, Privacy, and Trust – 24th IFIP SEC, IFIP Advances in Information and Communication Technologies, Springer, 2009

[3] Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz - SigG), http://bundesrecht.juris.de/bundesrecht/sigg_2001/gesamt.pdf, 2001

[4] European Network and Information Security Agency (ENISA): Security Issues of Authentication Using Mobile Devices, www.enisa.europa.eu/act/it/eid/mobile-eid/at_download/fullReport

[5] Mobilkom Austria, http://www.a1.net

[6] Handy-Signatur, http://www.a-trust.at/mobile

[7] Arno Hollosi, Gregor Karlinger, Thomas Rössler, Martin Centner et al.: die Applikationsschnittstelle Security-Layer zur österreichischen Bürgerkarte, http://www.buergerkarte.at/konzept/securitylayer/spezifikation/aktuell/core/core.html#core

[8] Personal Identification and Authentication with a Mobile Telephone, http://www.id.ee/?id=10995&&langchange=1

[9] DigiDoc, https://digidoc.sk.ee/?f=chg_lang&lang=en

[10] A-SIT: Sichere Signaturerstellungseinheit der A-Trust für die mobile Signatur bestehend aus HSM und HSM Server; Bescheinigung nach § 18 Abs. 5 SigG, 2009

[11] Materialen zu Signaturgesetz Novelle 2008, RV 293 BlgNR 23. GP

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

[13] Peter Kustor, Thomas Rössler: Mobile qualifizierte elektronische Signatur: technisches Konzept und rechtliche Bewertung. In: Globale Sicherheit und proaktiver Staat - die Rolle der Rechtsinformatik. Tagungsband IRIS 2010.