Mehr Sicherheit und Benutzerfreundlichkeit für Fernsignaturen

Tobias Wich Sebastian Schuberth René Lottes
Tina Hühnlein Detlef Hühnlein

ecsec GmbH, Sudetenstraße 16, D-96247 Michelau
vorname.nachname@ecsec.de

Zusammenfassung

Der „Fernsignatur“, bei der ein Signaturvorgang durch ein per SMS versandtes Einmalpasswort ausgelöst wird, wird oft ein großes Potenzial bescheinigt. Der vorliegende Beitrag zeigt, wie die Sicherheit und Benutzerfreundlichkeit dieser Schlüsseltechnologie durch den Einsatz von elektronischen Ausweisen, sicheren abgeleiteten Identitäten und kryptographisch gesicherten Protokollen weiter gesteigert werden kann.

1 Einleitung

Bei der „Fernsignatur“[1] wird eine fortgeschrittene oder qualifizierte elektronische Signatur zwar dezentral – in der Regel in Verbindung mit einem mobilen Endgerät – ausgelöst aber letztlich in der sicheren Serverumgebung eines Vertrauensdiensteanbieters im Auftrag des Unterzeichners erstellt. Hierbei erfolgt die Authentisierung des Unterzeichners durch ein sicheres Authentisierungsverfahren[2]. Vor dem Hintergrund der äußerst positiven Erfahrungen mit diesem Ansatz in einigen EU-Mitgliedsstaaten, wie z.B. Österreich[3] und Italien[4], wird diesem nunmehr selbst für qualifizierte elektronische Signaturen EU-weit nutzbaren Verfahren ein sehr großes Potenzial bescheinigt[5]. Unglücklicherweise ist das in der Praxis häufig für Fernsignaturen eingesetzte „Mobile TAN“ (mTAN) Verfahren, bei dem das Auslösen der Signatur durch ein per SMS versandtes Einmalpasswort erfolgt, nicht nur anfällig gegen Angriffe auf die mobile Plattform[6] des Anwenders, sondern vor allem auch auf die verwendete Telekommunikationsinfrastruktur[7]. Vor diesem Hintergrund wird in diesem Beitrag aufgezeigt, wie die Sicherheit und Benutzerfreundlichkeit dieser Schlüsseltechnologie durch den

---

[1] Vgl. Erwägungsgrund (52) der eIDAS-Verordnung [2014/910/EU], [Seeg14], [KuRö10], [OCK10] und [ZTL11].

[2] Vgl. [EN419241-1] Abschnitt 6.3.2.1 (“Signer authentication for SCAL1 (SRC_SA.1)”) und Abschnitt 6.4.2.1 („Threat resistance (SRA_SAP.1)“).

[3] In [KLR+15] (Fig. 1) sind die bemerkenswerten Steigerungsraten der mobilen eID-Nutzung in Österreich mit der so genannten „Handysignatur“ in den Jahren 2013-2015 dargestellt.

[4] Gemäß der Aufsichtsbehörde für elektronische Signaturen in Italien [AGID18] waren im Dezember 2017 rund 82% aller aktiven qualifizierten Zertifikate (18.657.725 Stück) als Fernsignatur nutzbar.

[5] Siehe z.B. [Seeg14] und [Stör17].

[6] Siehe z.B. [Beni17], [DLR+14], [MBS+13] und [Koot12].

[7] Siehe [SFGA17].

Einsatz von elektronischen Ausweisen, sicheren abgeleiteten Identitäten und kryptographisch gesicherten Protokollen weiter verbessert werden kann.

Der Rest des Beitrags ist folgendermaßen gegliedert: In Abschnitt 2 werden die relevanten Grundlagen und verwandten Arbeiten zusammengetragen. Abschnitt 3 liefert einen Überblick über grundsätzliche Optionen zur Realisierung mobiler Fernsignaturen, bevor in Abschnitt 4 ein Bedrohungsmodell für Fernsignatursysteme entwickelt und in Abschnitt 5 Möglichkeiten zur Steigerung der Sicherheit und Benutzerfreundlichkeit vorgeschlagen und diskutiert werden. In Abschnitt 6 findet sich schließlich eine kompakte Zusammenfassung der wesentlichen Ergebnisse und ein Ausblick auf zukünftige Entwicklungen.

2 Grundlagen und verwandte Arbeiten

2.1 Verwandte wissenschaftliche Arbeiten

Die Fernsignatur – damals noch als „qualifizierte Serversignatur“ bezeichnet – wurde bereits in [KuRö10], [OCK10] und [ZTL11] thematisiert und beispielsweise in Österreich und Italien bereits seit geraumer Zeit erfolgreich eingesetzt [KLR+15]. Die mobile Identifizierung (eID) und Signatur ist zudem Gegenstand von [BHW+11], [HHH12], [MeSu14], [RMS12], [Ross09] und [HHW+15]. In der eIDAS-Verordnung [2014/910/EU] ist die Fernsignatur im Erwägungsgrund (52) erwähnt und kürzlich beispielsweise in [Seeg14], [Vogt16] und [Stör17] thematisiert. Authentisierungsprotokolle und Ansätze für die starke Authentisierung sind in [BoMa03], [ClJa97] und [HZH+17] erläutert. Sicherheitsaspekte mobiler Plattformen und die eher geringe Sicherheit des mTAN-Verfahrens sind beispielsweise in [Beni17], [DLR+14], [MBS+13], [Koot12] und [HaMü16] behandelt. [SFGA17] zeigt eindrucksvoll, wie unsicher Telekommunikationsnetze tatsächlich sind.

2.2 Relevante Standards und Richtlinien

Für die in der eIDAS-Verordnung regulierten Vertrauensdienste existieren zahlreiche von ETSI ESI und CEN TC 224 entwickelte Standards[8], die wiederum im Regelfall auf internationalen Basisstandards von ISO, ITU, IETF und OASIS aufsetzen. Neben den generellen Regularien der eIDAS-Verordnung (vgl. Abschnitt 2.3) sind beim Einsatz des Personalausweises mit Online-Ausweisfunktion oder bei der Videoidentifizierung verschiedene Technische Richtlinien des BSI[9] zu berücksichtigen. Für die Fernsignatur sind insbesondere [EN419241-1] und die verschiedenen Standardentwürfe [prEN419241-2], [prTS119431], [prTS119432], [OASIS-DSS2] und [OASIS-AdES2] relevant.

2.3 Die Rahmenbedingungen der eIDAS-Verordnung

2.3.1 Elektronische Identifizierung

Die eIDAS-Verordnung [2014/910/EU] sieht in Art. 9 vor, dass Mitgliedsstaaten ihre elektronischen Identifizierungssysteme bei der Europäischen Kommission notifizieren, damit diese, sofern die Voraussetzungen der Artikel 6 und 7 erfüllt sind, nach entsprechenden Begutach-

[8] Siehe https://portal.etsi.org/tbsitemap/esi/esiactivities.aspx.

[9] Siehe https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/technischerichtlinien_node.html .

tungsverfahren für Zwecke der grenzüberschreitenden Authentifizierung gegenseitig anerkannt werden können.

Gemäß Art. 8 werden bei den elektronischen Identifizierungssystemen und den darin genutzten elektronischen Identifizierungsmitteln die Sicherheitsniveaus „*niedrig*“, „*substanziell*“ und „*hoch*“ unterschieden, die ein unterschiedliches „*Maß an Vertrauen in die beanspruchte oder behauptete Identität einer Person*“ aufweisen und durch „*die Bezugnahme auf die diesbezüglichen technischen Spezifikationen, Normen und Verfahren einschließlich (entsprechender) Überprüfungen*“ „*der Gefahr des Identitätsmissbrauchs oder der Identitätsveränderung*“ unterschiedlich stark entgegenwirken.

Tab. 1: Maß an Vertrauen und Missbrauchsgefahr bei den eIDAS-Sicherheitsniveaus

Sicherheitsniveau	Maß an Vertrauen	Missbrauchsgefahr
niedrig	begrenztes Maß	Minderung der Gefahr
substanziell	substanzielles Maß	substanzielle Minderung der Gefahr
hoch	höheres Maß	Verhinderung

Durch die am 26.09.2017 erfolgte Veröffentlichung im Amtsblatt der Europäischen Kommission wurde das Notifizierungsverfahren für die Online-Ausweisfunktion des deutschen Personalausweises erfolgreich abgeschlossen. Vorausgegangen war eine Begutachtung durch technische Experten nahezu aller EU-Mitgliedstaaten, wodurch die Erfüllung des Sicherheitsniveaus „hoch“ bestätigt wurde.

Die detaillierten Anforderungen für die jeweiligen Sicherheitsniveaus sind in [2015/1502/EU] spezifiziert. Eine Übersicht über die Notifizierungsverfahren findet sich auf der Webseite der Europäischen Kommission[10].

2.3.2 Elektronische Signaturen und Siegel

Für die elektronische Abwicklung von Geschäftsprozessen in Wirtschaft und Verwaltung werden häufig elektronische Signaturen eingesetzt, um beispielsweise eine Willenserklärung beweiskräftig zu dokumentieren oder um eine gesetzlich notwendige Form zu erfüllen. Hierbei unterscheidet die [eIDAS-VO] zwischen der einfachen „elektronischen Signatur“ (Art. 3 (10)), der „fortgeschrittenen elektronischen Signatur“ (Art. 3 (11)) und schließlich der „qualifizierten elektronischen Signatur“ (Art. 3 (12)).

An die „***elektronische Signatur***“ gemäß Art. 3 (10)[11] werden praktisch keine Anforderungen gestellt.

Anders sieht dies bei der „***fortgeschrittenen elektronische Signatur***“ aus. Sie muss gemäß Art. 3 (11) und Art. 26 folgende Anforderungen erfüllen:

„*a) Sie ist eindeutig dem Unterzeichner zugeordnet.*

b) Sie ermöglicht die Identifizierung des Unterzeichners.

[10] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Country+Overview+-+eID .

[11] Die elektronische Signatur ist definiert als „*Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verbunden werden und die der Unterzeichner zum Unterzeichnen verwendet.*“

c) Sie wird unter Verwendung elektronischer Signaturerstellungsdaten erstellt, die der Unterzeichner mit einem hohen Maß an Vertrauen unter seiner alleinigen Kontrolle verwenden kann.

d) Sie ist so mit den auf diese Weise unterzeichneten Daten verbunden, dass eine nachträgliche Veränderung der Daten erkannt werden kann."

Bemerkenswert erscheint, dass in b) nicht etwa die Verwendung eines dem Unterzeichner zugeordneten Zertifikates gefordert ist, sondern lediglich eine Möglichkeit, den Unterzeichner zu identifizieren, was attraktive alternative Realisierungsoptionen (vgl. Abschnitt 3.2.2) ermöglicht.

Interessant ist auch die Formulierung in c), wonach der Unterzeichner die Signaturerstellungsdaten „mit einem hohen Maß an Vertrauen" unter seiner alleinigen Kontrolle halten muss, was bei einer wörtlichen Interpretation zwingend den Einsatz von elektronischen Identifizierungsmitteln mit Sicherheitsniveau „hoch" gemäß Art. 8 nahelegen würde. Betrachtet man weitere Regularien der eIDAS-Verordnung, wie z.B. Art. 24 (1) b)[12], und der kürzlich verabschiedeten Europäischen Norm [EN419241-1][13], so wird jedoch klar, dass hier eigentlich das Sicherheitsniveau „substanziell" ausreichend ist.

Bei der „***qualifizierten elektronischen Signatur***" gemäß Art. 3 (12) wird zusätzlich gefordert, dass sie „*von einer qualifizierten elektronischen Signaturerstellungseinheit erstellt wurde und auf einem qualifizierten Zertifikat für elektronische Signaturen beruht.*"

Analog zu den verschiedenen Stufen der elektronischen Signatur definiert die eIDAS-Verordnung entsprechende Stufen für „***elektronische Siegel***" (Art. 3 (25)), „***fortgeschrittene elektronische Siegel***" (Art. 3 (26)) und „***qualifizierte elektronische Siegel***" (Art. 3 (30)), wobei der Unterschied zur Signatur darin besteht, dass der Siegelersteller eine juristische Person ist und bei der Definition des fortgeschrittenen elektronischen Siegels im Buchstaben c) des Art. 36 nur die „Kontrolle" und nicht etwa wie bei der Signatur die „alleinige Kontrolle" gefordert wird.

2.4 Regelungen zur Schriftform und Beweiswirkung

Während die verschiedenen Formen der elektronischen Signatur gemäß Art. 25 (1) und Siegel gemäß Art. 35 (1) als Beweismittel vor Gericht genutzt werden können, ersetzt die qualifizierte elektronische Signatur gemäß Art. 25 (2) die handschriftliche Unterschrift, was in schriftformgebundenen Geschäftsprozessen, wie z.B. dem Abschluss eines Verbraucherdarlehensvertrags gemäß § 492 BGB, essentiell ist. Fragen der Beweisführung unter Verwendung von elektronischen Signaturen, Siegeln und Zeitstempeln sind in [BSI TR03138-R] ausführlich erläutert.

---

[12] Gemäß Art. 24 (1) b) der eIDAS-Verordnung [2014/910/EU] ist für die Ausstellung eines qualifizierten Zertifikates schon eine elektronische Identifizierung mit dem Sicherheitsniveau „substanziell" ausreichend, sofern „eine persönliche Anwesenheit der natürlichen Person oder eines bevollmächtigten Vertreters der juristischen Person gewährleistet war".

[13] [EN419241-1] (SRA_SAP.1.1) fordert, dass der Registrierungsprozess, die Eigenschaften der Identifizierungsmittel und das Authentisierungsprotokoll das Sicherheitsniveau „substantiell" oder „hoch" erfüllt („… assurance level substantial or higher").

3 Generelle Realisierungsoptionen

Im Allgemeinen kann bei der Erstellung einer elektronischen Signatur danach unterschieden werden, wo und durch wen der für die Signaturerstellung genutzte private Schlüssel aufbewahrt und angewandt wird.

3.1 Klassische dezentrale Signatur

Im klassischen Fall liegt der private Schlüssel direkt beim Unterzeichner in einem sicheren Schlüsselspeicher, wie z.B. einer Chipkarte oder einem sicheren mobilen Endgerät, und kann damit direkt für die Signaturerzeugung verwendet werden. Während bislang Lösungen auf Basis von Java-Applets eingesetzt wurden, steht diese Option bei aktuellen Browsern leider nicht mehr zur Verfügung. Allerdings kann in diesem Fall das von ecsec gemeinsam mit LuxTrust entwickelte „ChipGateway“-Protokoll [OASIS-LSP] genutzt werden, so dass weiterhin eine webbasierte Signaturerzeugung mit Chipkarten erfolgen kann.

3.2 Fernsignatur

Eine andere Möglichkeit ist das in diesem Beitrag näher betrachtete Auslösen einer Signatur aus der Ferne. Der private Schlüssel liegt hierbei nicht beim Benutzer selbst, sondern wird von einem (qualifizierten) Vertrauensdiensteanbieter sicher, z.B. in einem Hardware Security Module (HSM), verwaltet.

Damit der Benutzer auf den privaten Schlüssel für die Erstellung einer Signatur zugreifen kann, muss er vorher seine Identität durch eine sichere Authentisierung gegenüber dem Vertrauensdiensteanbieter nachweisen (1). Ein in der Praxis häufig genutztes Verfahren ist die Kombination aus Benutzername und Passwort sowie die Eingabe einer „Mobile TAN“ (mTAN), die per SMS an das Mobilgerät des Benutzers geschickt wird (2). Diese für den Signaturvorgang spezifische TAN wird vom Benutzer manuell beispielsweise in ein Webformular übertragen (3) und von dort wieder an den Server geschickt (4), bevor die eigentliche Signaturerstellung erfolgt und die so erstellte Signatur (5) dem Benutzer zur Verfügung gestellt wird.

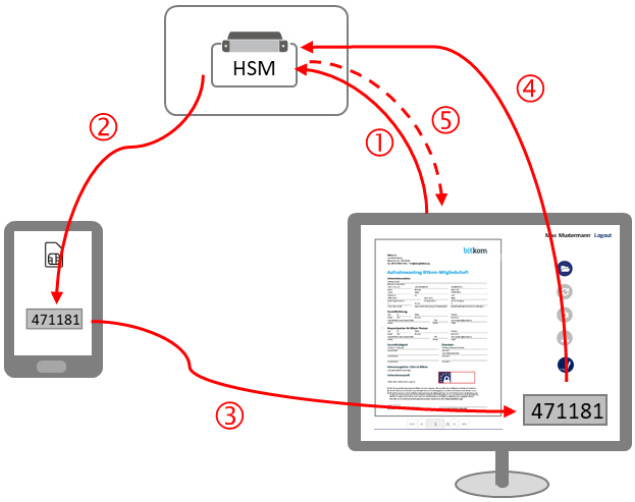

Abb. 1: Wesentliche Abläufe bei der Fernsignatur

Mit diesem Verfahren können derzeit qualifizierte elektronische Signaturen erstellt werden, die die Schriftform ersetzen können (vgl. Abschnitt 2.4). Allerdings muss vor dem Hintergrund von [SFGA17] ernsthaft bezweifelt werden, dass dieses Verfahren noch ausreichend

Sicherheit bietet und beispielsweise die in [EN419241-1] (SRA_SAP.1.2) formulierten Anforderungen[14] erfüllt.

Unabhängig vom generellen Verfahren, das in Abschnitt 4 mit den in [EN419241-1] standardisierten Begrifflichkeiten näher beschrieben wird, kann bei der Fernsignatur grob danach unterschieden werden, für wen das zur Erstellung der digitalen Signatur verwendete Zertifikat ausgestellt ist. Wie im Folgenden gezeigt, kann hierbei der Fall von „Unterzeichnerspezifischen Zertifikaten“ (Abschnitt 3.2.1) und „Siegelzertifikaten mit individueller Identitätszusicherung“ (Abschnitt 3.2.2) unterschieden werden.

3.2.1 Unterzeichnerspezifisches Zertifikat

In diesem Fall stellt der Vertrauensdiensteanbieter für jeden Unterzeichner ein eigenes Zertifikat aus. Nach der Authentisierung wird dann der mit diesem Zertifikat verbundene private Schlüssel für die Signaturerstellung genutzt.

Die Anforderung der Benutzeridentifizierung für eine fortgeschrittene oder qualifizierte elektronische Signatur ist dabei durch die eindeutige Zuordnung von Benutzer zu dessen persönlichem Zertifikat bzw. privatem Schlüssel erfüllt.

3.2.2 Siegelzertifikat mit individueller Identitätszusicherung

Alternativ kann die Signaturerstellung im Fall von fortgeschrittenen elektronischen Signaturen aber auch durch ein einziges Siegelzertifikat erfolgen, wodurch der Aufwand für die zu verwaltenden Schlüssel und Zertifikate auf ein Minimum gesenkt wird.

Um auch hier eine eindeutige Benutzeridentifizierung zu gewährleisten, wird der Beweis für die erfolgreiche Authentisierung mitsamt persönlichen Daten zur Identität wie z.B. Vor- und Nachname des Benutzers in Form einer individuellen Identitätszusicherung (SAML-Assertion) konform zu den Europäischen {C,X,P}AdES Standards [EN3191*x*2] in die Signatur eingebettet.

4 Bedrohungsmodell für Fernsignatursysteme

Um die Sicherheit der Fernsignatur genauer analysieren zu können, empfiehlt es sich, das grobe Übersichtsdiagramm aus Abb. 1 entsprechend zu verfeinern.

4.1.1 Komponenten

Bei der Beschreibung der Komponenten ist es zweckmäßig, die in [EN419241-1] definierten Begriffe zu verwenden.

Der Benutzer interagiert mit der *Signature Creation Application* (SCA), welche vor dem Signaturvorgang eine *Repräsentation der zu signierenden Daten* (DTBS/R) anzeigt. Die *Signature Activation Data* (SAD) dienen dazu, die DTBS/R und die dem Unterzeichner zugeordnete *Signer's Interaction Component* (SIC) so zu „verbinden“, dass eine Signaturerzeugung nur unter der (alleinigen) Kontrolle (vgl. Abschnitt 2.3.2) des Unterzeichners erfolgen kann. Die *Server Signing Application* (SSA) führt schließlich die eigentliche Signaturerzeugung durch.

[14] [EN419241-1] (SRA_SAP.1.2) fordert u.a. dass das Protokoll zur Signaturauslösung resistent gegen Man-in-the-Middle-Angriffe ist. Vor dem Hintergrund der praktisch durchführbaren Angriffe auf Telekommunikationsnetze [SFGA17] muss ernsthaft bezweifelt werden, dass diese Anforderung beim mTAN-Verfahren erfüllt ist.

Dazu greift sie auf das *Signature Activation Module* (SAM) zu, welches den privaten Signaturschlüssel auf dem *Signature Creation Device* (SCDev) aktiviert, um schließlich die eigentliche Signaturerzeugung anzustoßen.

Im Fall des mTAN-Verfahrens, das den Abbildungen 1 und 2 zu Grunde liegt, sind die SAD als ein transaktionsgebundenes Einmalpasswort (Transaction Authentication Number (TAN)) realisiert, das mit dem spezifischen Signaturvorgang verknüpft ist und typischer Weise per SMS an das Mobiltelefon des Unterzeichners gesandt wird. In diesem Beispiel ist die SIC als die im Mobilfunkgerät steckende SIM-Karte dargestellt, die den Benutzer letztlich gegenüber der *Server Signing Application* (SSA) repräsentieren und authentisieren soll. Im Allgemeinen kann die SIC auch als eingebettetes sicheres Element im mobilen Endgerät, als App auf dem Mobilgerät, durch eine andere kryptographische Hardware, wie z.B. ein FIDO-Token[15], und/oder biometrische Mechanismen[16] realisiert sein.

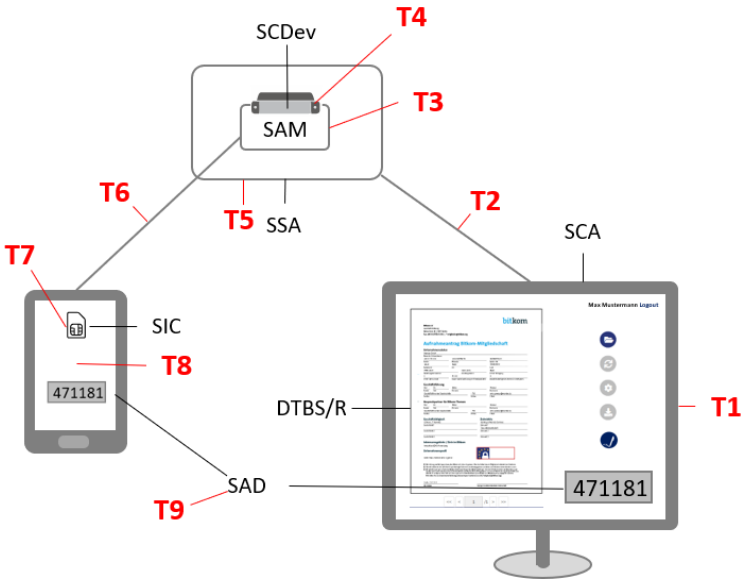

Abb. 2: Bedrohungsmodell für Fernsignatursysteme

4.1.2 Bedrohungen

Für das in Abb. 2 skizzierte Modell können insbesondere die folgenden Bedrohungen identifiziert werden:

T1: Eine bösartige SCA kann die Ansicht für die DTBS/R manipulieren und ein anderes Dokument signieren, das der Benutzer gar nicht kennt.

T2: Die Kommunikation zwischen SSA und SCA kann z.B. durch eine Man-In-The-Middle-Attacke manipuliert oder ganz unterdrückt werden. Das in **T1** gefälschte Dokument könnte hier nach dem Signaturvorgang abgegriffen werden.

T3-5: Eine Kompromittierung der SSA kann dazu führen, dass ein Angreifer direkten Zugriff auf das SAM und damit auch auf die Aktivierung von privaten Schlüsseln auf dem SCDev für Zwecke der Signaturerzeugung erhält. In einem solchen Fall wären vielfältige weitere Angrif-

[15] Siehe https://fidoalliance.org/ .

[16] Siehe z.B. [WJMM05], [BRAC09] und [ISO19002].

fe denkbar, die beispielsweise auch eine unautorisierte Erzeugung von Schlüsseln und Zertifikaten umfasst.

T6/T7: Wenn kein UMTS/EDGE/LTE vorhanden ist, findet immer noch ein Rückfall auf GSM statt, was in der Praxis durch eine bewusst herbeigeführte Signalstörung erzwungen werden kann. Bei GSM ist es möglich via "IMSI-Catcher" eine Basisstation zu simulieren [SFGA17]. Da sich Mobilfunkgeräte standardmäßig in die Funkzelle mit dem besten Empfang einwählen, kann vorgetäuscht werden, dass nur GSM vorhanden ist. Die falsche Basisstation positioniert sich so als klassischer Man-In-The-Middle zwischen den dort eingewählten Geräten und einer echten Basisstation. Mit dadurch abgegriffenen IMSIs (International Mobile Subscriber Identity) ist es möglich, die Identität einer SIM-Karte zu stehlen und sich damit in das Handy-Netz einzuwählen. Weiterhin lässt sich die bei GSM verwendete Verschlüsselung A5/1 leicht brechen und somit SMS- und Gesprächsdaten abfangen (vgl. [ck15] und [Hult08]).

T8: Trojaner oder allgemein Apps, die vom Nutzer die Berechtigung zum Lesen von SMS erhalten haben, können TANs abfangen und weiterleiten [NTV17]. Dies gilt allerdings nur für Android[17], unter iOS ist es keiner (nicht-Apple-)App gestattet, auf die SMS zuzugreifen.

T9: Ein Angreifer könnte schließlich versuchen, die SAD (TANs) zu erraten, was freilich nur bei zu kurz geratenen und/oder nicht zufälligen TANs erfolgsversprechend wäre.

Insgesamt zeigt die differenzierte Betrachtung der Bedrohungen, dass die „Achillesferse“ der mTAN-basierten Fernsignatur in den Bedrohungen T6-T8 liegt. Entsprechende Ansätze für die Steigerung der Sicherheit werden in Abschnitt 5.1 diskutiert.

5 Mehr Sicherheit und Benutzerfreundlichkeit

mTAN basierte Verfahren für die Transaktionsfreigabe gehören heute zu den meistverbreiteten Verfahren im Online Banking, sowie bei der Fernsignatur. Die große Akzeptanz dieser Verfahren bei den Nutzern liegt zu einem großen Teil an der – im Vergleich zu vielen anderen Verfahren – großen Benutzerfreundlichkeit, aber auch an der versprochenen Sicherheit, die jedoch inzwischen angezweifelt werden muss. Die Benutzerfreundlichkeit ist insbesondere darauf zurückzuführen, dass keine zusätzliche Hardware benötigt wird, die mit der Signature Creation Application (SCA) über ein technisches Verfahren gekoppelt werden müsste. Darüber hinaus ist das Verfahren für den Nutzer leicht verständlich. Die vermeintliche Sicherheit von mTAN Verfahren stützt sich Großteils auf die Sicherheit des Mobilgeräts und des Mobilfunknetzes. Aufgrund der Schwierigkeiten Malware auf modernen Smartphones auszuschließen, müssen als Gegenmaßnahme wenigstens „nutzerlose“ und somit automatisierbare Angriffe ausgeschlossen werden. Anders sieht es bei SMS Nachrichten und dem Mobilfunknetz aus. Angriffe existieren auf praktisch allen Ebenen vom Endgerät bis zur Vermittlerstelle und dem Provider selbst [SFGA17], so dass das mTAN-Verfahren prinzipiell keine in der Praxis sichere Umsetzung erlaubt.

5.1 Mehr Sicherheit

Wie oben erläutert, ist die größte sicherheitstechnische Schwachstelle der mTAN-basierten Fernsignatur das mTAN-Verfahren selbst. Deshalb sollen im Folgenden alternative Ansätze

[17] https://developer.android.com/reference/android/provider/Telephony

aufgelistet werden, mit denen nach dem heutigem Stand der Technik nicht nur das Sicherheitsniveau „substanziell“ erreicht werden kann, sondern insbesondere auch die in [EN419241-1] (SRA_SAP.1) formulierten Anforderungen nachweislich erfüllt werden können.

Aus den heute verfügbaren Möglichkeiten zur starken Authentisierung [HZH+17] können verschiedene Ansätze für sichere Fernsignatursysteme abgeleitet und zu einem sicheren Gesamtsystem integriert werden:

- Direkte oder indirekte mobile Nutzung von sicheren eID-Token, wie z.B. Personalausweis oder FIDO-Token
- Trusted Execution Environment (TEE)[18] bzw. embedded Secure Element (eSE) gestützte Signaturen
- Starke Gerätebindung der verwendeten Login-Credentials
- Kanalbindung von sekundären Token bzw. Authentication Assertions
- Absicherung von Applikationswechseln mit „sicheren URLs“ [RFC8252]
- Transaktionsbestätigung durch den Nutzer und sichere PIN Eingabe
- Attestierung der Vertrauenswürdigkeit von eingesetzten Komponenten
- vertrauenswürdige Anzeigekomponente[19] und zuverlässige Transaktionszuordnung durch sichere Kanäle zwischen den Endgeräten und Serversystemen

5.2 Zumindest gleiche oder bessere Benutzerfreundlichkeit

Elaborierte Authentisierungsprotokolle und Sicherheitsverfahren benötigen i.d.R. einen mehrstufigen Nachrichtenaustausch. Im Gegensatz zum mTAN Verfahren muss deshalb besonderes Augenmerk auf die Nutzerbeteiligung und Benutzerfreundlichkeit gelegt werden.

Im Folgenden finden sich Ansätze für den benutzerfreundlichen Einsatz von eingebetteten Sicherheitselementen in Verbindung mit abgeleitete Identitäten zur starken Authentisierung, Transaktionssicherung und sicheren Kopplung zwischen SCA und SIC.

5.2.1 Abgeleitete Identität statt Personalausweis

Fortgeschrittene und qualifizierte Signaturen erfordern sehr hohe Sicherheitsstandards und einen starken Nachweis der Identität des Unterzeichners. Zwar ist es mit modernen NFC-basierten Ausweiskarten, wie beispielsweise dem deutschen Personalausweis, möglich, diese direkt mit dem Mobilgerät zu nutzen, jedoch stellt dies einen weiteren „Bruch“ in der Benutzerführung dar. Eine abgeleitete Identität[20], die stark an das Mobilgerät gebunden ist, kann in einem einmaligen Vorgang entweder direkt auf dem Smartphone ausgestellt, oder von einem Desktop-PC übertragen werden. Entsprechende Sicherheitsmaßnahmen und vor allem die starke Bindung an das Gerät sorgen für ein nahezu äquivalentes Sicherheitsniveau.

---

[18] Hierbei ist zu beachten, dass die existierenden TEE-Implementierungen leider auch erfolgreich angegriffen werden können [Beni17].

[19] Vor dem Hintergrund von [Lang06] ist es wichtig, dass die vertrauenswürdige Anzeigekomponente („Trusted Viewer“) nicht isoliert, sondern als integraler Bestandteil eines sicheren Gesamtsystems zu sehen ist.

[20] Siehe z.B. [HHW+15], [BHJ16], [CoLe12], [CoLe14], [MiAf15], [ScMo13], [TZH17] und [TZH18].

5.2.2 Nahtlose Kopplung von Benutzergeräten

Für die Erledigung einer Aufgabe ist das Mobilgerät, auf dem die Authentisierung für die Auslösung einer Signatur durchgeführt wird, nicht zwangsläufig auch das Gerät, auf dem der Vorgang initiiert bzw. vorbereitet wird. Analog zum mTAN-Verfahren wird der Kontext für Authentisierung zwischen den Geräten gewechselt. Der Austausch über die Geräte hinweg wird durch einen von beiden Geräten bzw. dem Nutzer bestätigten Kanal vollzogen. Mittels Push-Notifications kann ein neuer Kanal durch die vormals bestätigten und persistierten kryptographischen Geheimnisse etabliert werden. Nachrichten, die die vom Mobilgerät zu erledigende Aufgabe beschreiben, können dann Ende-zu-Ende verschlüsselt zwischen den Geräten ausgetauscht werden. Es entfällt somit die manuelle Übertragung einer Transaktionsnummer, wie es beim mTAN-Verfahren nötig ist. Zudem ist eine weitergehende Integration der Benutzerführung denkbar, bei der die zu signierenden Daten in einer vertrauenswürdigen Anzeigekomponente auf dem Mobilgerät angezeigt werden können.

6 Zusammenfassung und Ausblick

Im vorliegenden Beitrag wurde ein Bedrohungsmodell für die Fernsignatur auf Basis von [EN419241-1] entwickelt, bei dem die Schwachstellen der mTAN-basierten Fernsignatur gut erkennbar werden. Auf dieser Grundlage wurden einige Ansatzpunkte für die Verbesserung der Sicherheit und Benutzerfreundlichkeit identifiziert, die aktuell im EU-Projekt FutureTrust (https://futuretrust.eu) erforscht werden und die Grundlage für die nächste Generation der Fernsignatursysteme bilden können.

Literatur

[2014/910/EU] Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG, http://data.europa.eu/eli/reg/2014/910/oj

[2015/1502/EU] Durchführungsverordnung (EU) 2015/1502 der Kommission vom 8. September 2015 zur Festlegung von Mindestanforderungen an technische Spezifikationen und Verfahren für Sicherheitsniveaus elektronischer Identifizierungsmittel …, http://data.europa.eu/eli/reg_impl/2015/1502/oj

[AGID18] AGID: *Firme elettroniche*, http://www.agid.gov.it/agenda-digitale/infrastrutture-architetture/firme-elettroniche

[Beni17] G. Beniamini: *Trust Issues: Exploiting TrustZone TEEs*, https://googleprojectzero.blogspot.de/2017/07/trust-issues-exploiting-trustzone-tees.html

[BHJ16] F. van den Broek, B. Hampiholi, B. Jacobs: *Securely Derived Identity Credentials on Smart Phones via Self-enrolment*. In: Barthe G., Markatos E., Samarati P. (eds) Security and Trust Management. STM 2016. Lecture Notes in Computer Science, vol 9871. Springer, Cham (2016)

[BHW+11] J. Braun, M. Horsch, A. Wiesmaier, D. Hühnlein: *Mobile Authentisierung und Signatur*, DACH 2011, (2011)

[BoMa03] C. Boyd & A. Mathuria: *Protocols for authentication and key establishment*, Springer, (2003)

[BRAC09] D. Bhattacharyya, R. Ranjan, F. Alisherov, M. Choi: *Biometric authentication: A review*. International Journal of u-and e-Service, Science and Technology, 2(3), 13-28, (2009)

[BSI TR03138-R] BSI: *Ersetzendes Scannen (RESISCAN), Anwendungshinweis R – Unverbindliche rechtliche Hinweise*, Technische Richtlinie des BSI TR-03138-R, Version 1.2 vom 15.06.2018

[ck15] ck: *GSM: Sniffing SMS traffic*, 29.11.2015, https://www.ckn.io/blog/2015/11/29/gsm-sniffing-sms-traffic/

[ClJa97] J. Clark, J. Jacob: *A survey of authentication protocol literature: Version 1.0*, (1997)

[CoLe12] F. Corella, K. Lewison: *Techniques for Implementing Derived Credentials*, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.477.3734&rep=rep1&type=pdf (2012)

[CoLe14] F. Corella, K. Lewison: *An Example of a Derived Credentials Architecture*, https://pomcor.com/techreports/DerivedCredentialsExample.pdf (2014)

[DLR+14] A. Dmitrienko. C. Liebchen, C. Rossow, A.-R. Sadeghi: *On the (In)Security of Mobile Two-Factor Authentication*, Financial Cryptography and Data Security, Springer, 2014

[EN3191*x*2] EN 319 12*x*: *Electronic Signatures and Infrastructures (ESI); CAdES digital signatures (x=2) / XAdES digital signatures (x=3) / PAdES digital signatures (x=4)*, 2016, https://portal.etsi.org/TBSiteMap/esi/ESIActivities.aspx

[EN419241-1] EN 419 241-1: *Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements*, 2018

[HaMü16] V. Haupert, T. Müller: *Auf dem Weg verTAN: Über die Sicherheit App-basierter TAN-Verfahren*, im Tagungsband der „Sicherheit 2016“, Lecture Notes in Informatics (LNI) 256, S. 101-112

[HHH12] G. Hornung, M. Horsch, D. Hühnlein: *Mobile Authentisierung und Signatur mit dem neuen Personalausweis*, Datenschutz und Datensicherheit – DuD, March 2012, Volume 36, Issue 3, S. 189-194, https://link.springer.com/article/10.1007/s11623-012-0063-0 (2012)

[HHW+15] D. Hühnlein, T. Hühnlein, T. Wich, B. Biallowons, M. Tuengerthal, H.-M. Haase, D. Nemmert, S. Baszanowski, C. Bergmann: *SkIDentity – Mobile eID as a Service*, DACH-Security 2015, https://ecsec.de/pub/SkIDentity_DACH2015.pdf, (2015)

[Hult08] D. Hulton: *Intercepting GSM traffic*, BlackHat Briefings (2008), http://www.blackhat.com/presentations/bh-dc-08/Steve-DHulton/Whitepaper/bh-dc-08-steve-dhulton-WP.pdf

[HZH+17] D. Hühnlein, C. Ziske, T. Hühnlein, T. Wich, D. Nemmert, S. Rohr, M. Hertlein, C. Kölbel: Starke Authentisierung – jetzt!, DACH Security 2017, https://ecsec.de/pub/DACH2017-2FA.pdf

[ISO19002] ISO 19092: *Financial services – Biometrics – Security Framework*, (2008)

[KLR+15] M. Kubach, H. Leitold, H. Roßnagel, C. H. Schunck, M. Talamo: *SSEDIC.2020 on Mobile eID*, GI LNI, Open Identity Summit 2015, https://subs.emis.de/LNI/Proceedings/Proceedings251/29.pdf

[Koot12] L. Koot: *Security of mobile TAN on smartphones*, Master's thesis, Radboud University Nijmegen, 2012, https://www.politieacademie.nl/kennisenonderzoek/kennis/mediatheek/PDF/83439.pdf

[KuRö10] P. Kustor, T. Rössler: *Mobile qualifizierte elektronische Signatur: technisches Konzept und rechtliche Bewertung*, in Globale Sicherheit und proaktiver Staat – die Rolle der Rechtsinformatik (Band 266), Österreichische Computergesellschaft, S. 279-291, (2010)

[Lang06] H. Langweg: *Malware Attacks on Electronic Signatures Revisited*, Sicherheit 2006, S. 244-255

[MBS+13] C. Mulliner, R. Borgaonkar, P. Stewin, J.-P. Seifert: *SMS-Based One-Time Passwords: Attacks and Defense*, in Detection of Intrusions and Malware, and Vulnerability Assessment, Springer, S. 150-159, 2013

[MeSu14] G. Meister, A. Summerer: *Mobile ID*, Datenschutz & Datensicherheit (2014) 38: 666. Springer Fachmedien, Wiesbaden, https://doi.org/10.1007/s11623-014-0267-6

[MiAf15] S. Mistry, Y. Aftab: *Using derived credentials for enrolment with enterprise mobile device management services*, US9668136B2, https://patents.google.com/patent/US9668136B2/en (2015)

[NTV17] NTV: *Vorsicht beim Online-Banking! Android-Trojaner greift TANs ab*, 19.07.2017 https://www.n-tv.de/technik/Android-Trojaner-greift-TANs-ab-article19944236.html

[OCK10] C. Orthacker, M. Centner, C. Kittl: *Qualified Mobile Server Signature*. In: Rannenberg K., Varadharajan V., Weber C. (eds) Security and Privacy – Silver Linings in the Cloud. SEC 2010. IFIP Advances in Information and Communication Technology, vol 330. Springer, Berlin (2010)

[OASIS-DSS2] S. Hagen. A. Kühne (ed.): *OASIS-DSS-Core-2.0, Digital Signature Service Core Protocols, Elements, and Bindings Version 2.0*, Working Draft, 2018

[OASIS-AdES2] S. Hagen, A. Kühne (ed.): *Advanced Electronic Signature Profile for OASIS Digital Signature Services Version 2.0*, Working Draft, Working Draft, 2018

[OASIS-LSP] E.J. von Nigtevecht, F. Cornelis, D. Hühnlein (eds.): *DSS Extension for Local Signature Computation Version 1.0*, OASIS DSS-X, Draft for Committee Specification Draft 04, 2018

[prTS119431] prTS 119 431: *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1-2*, Draft ETSI TS 119 431, July, 2018

[prTS119432] prTS 119 432: *Electronic Signatures and Infrastructures (ESI); Protocols for remote digital signature creation*, Draft ETSI TS 119 432, July, 2018

[prEN419241-2] prEN 419 241-2: *Trustworthy Systems Supporting Server Signing - Part 2: Protection profile for QSCD for Server Signing*, 2017

[RBD+12] T.J. Ronda, A. Boysen, A. Das, M. Varley, H. Cumming: *Methods and systems for using derived credentials to authenticate a device across multiple platforms*, US9053304B2, https://patents.google.com/patent/US9053304B2/en (2012)

[RFC8252] W. Denniss, J. Bradley: *RFC 8252: OAuth 2.0 for Native Apps*, IETF (2017)

[RMS12] A. Ruiz-Martinez, C.I.Marin-Lopez, D. Sanchez-Martinez, I. Castell Egea: *SIP-msign: a lightweight mobile signature service based on the Session Initiation Protocol*, https://doi.org/10.1002/spe.2170 (2012)

[Ross09] H. Roßnagel: *Mobile qualifizierte Signaturen*. In: Mobile qualifizierte elektronische Signaturen. Gabler (2009)

[SFGM17] M. Sahin, A. Francillon, P. Gupta, and M. Ahamad: *SoK: Fraud in Telephony Networks*, IEEE Euro S&P (2017)

[ScMo13] M. Schröder, F. Morgner: *eID mit abgeleiteten Identitäten*, Datenschutz Datensich (2013) 37: 530. Springer Fachmedien, Wiesbaden https://doi.org/10.1007/s11623-013-0213-z

[Seeg14] C. Seegebarth: *Perspektiven aus der eIDAS-Verordnung*, Datenschutz Datensich (2014) 38: 675. Springer Fachmedien, Wiesbaden, https://doi.org/10.1007/s11623-014-0269-4

[SFGA17] M. Sahin, A. Francillon, P. Gupta, M. Ahamad: *SoK: Fraud in Telephony Networks*, IEEE European Symposium on Security and Privacy (EuroSP), 2017

[Stör17] M. Störing: *Der digitale Federkiel – Potenzial der eIDAS-Verordnung wird unterschätzt*, c't 2017, Heft 10, Seite 148-151, 2017

[TZH17] D. Träder, A. Zeier, A. Heinemann: *Design- und Implementierungsaspekte mobiler abgeleiteter Identitäten*. DACH Security, 2017

[TZH18] D. Träder, A. Zeier, A. Heinemann: *Auf dem Weg zu sicheren abgeleiteten Identitäten mit Payment Service Directive 2*. In: Langweg, H., Meier, M., Witt, B. C. & Reinhardt, D. (Hrsg.), SICHERHEIT 2018. Bonn: Gesellschaft für Informatik e.V.. (S. 183-196).

[Vogt16] T. Vogt: *Die neue eIDAS-Verordnung – Chance und Herausforderung für die öffentliche Verwaltung in Deutschland*, Information-Wissenschaft & Praxis, 67.1 (2016): Seite 61-68, https://www.degruyter.com/view/j/iwp.2016.67.issue-1/iwp-2016-0011/iwp-2016-0011.xml

[WJMM05] J. Wayman, A. Jain, D. Maltoni, D. Maio: *An introduction to biometric authentication systems*, Springer London, S. 1-20, (2005)

[ZTL11] T. Zefferer, P. Teufl, H. Leitold: *Mobile qualifizierte Signaturen in Europa*, Datenschutz und Datensicherheit, DUD, November 2011, Volume 35, S. 768-773, (2011), https://doi.org/10.1007/s11623-011-0183-y