REMOTE SIGNATURES UND MÖGLICHE ANGRIFFE

Dennis Kügler

Zusammenfassung

Mit der eIDAS-Verordnung soll die Regulierung von elektronischen Signaturen in Europa erneuert und weiter harmonisiert werden. Eine kleine, aber wesentliche Änderung findet sich der Definition von qualifizierten Signaturerstellungseinheiten, die es ermöglichen soll, dass diese sich nicht mehr im unmittelbaren Besitz des Signierenden befinden muss, sondern auch entfernt bzw. zentral von einem Vertrauensdiensteanbieter verwaltet werden kann. Diese Remote- oder Server-Signaturen sollen die Verbreitung der QES durch Verringerung der infrastrukturellen Anforderungen fördern.

Einleitung

Digitale Signaturen sind aus technischer Sicht ein einfaches und wirkungsvolles Verfahren, um die Authentizität (einschließlich der Integrität) von Daten sicherzustellen. Aus kryptographischer Sicht berechnet der Signierende mithilfe eines Signaturerstellungsalgorithmus, aus seinem privaten Schlüssel und einer zu signierenden Nachricht eine digitale Signatur. Mithilfe des zugehörigen Signaturprüfalgorithmus und des öffentlichen Schlüssels des Signierenden kann diese digitale Signatur dann validiert werden.

Die digitale Signatur ist ein asymmetrisches Kryptoverfahren. Das Problem der Authentizität von Daten wird also auf das Problem der Authentizität von öffentlichen Schlüsseln reduziert. Die Authentizität von öffentlichen Schlüsseln wird i.d.R. über hierarchisch organisierte Zertifikatsstrukturen und somit rekursiv über digitale Signaturen sichergestellt, so dass letztlich nur einige wenige öffentliche Schlüssel von Wurzelzertifzierungsinstanzen über vertrauenswürdige Kanäle ausgetauscht werden müssen.

Um diesem durchaus praktischen technischen Konzept der digitalen Signatur mit einer Rechtswirkung zu versehen, wurden zunächst nationale Signaturgesetze erlassen (z. B. ist das deutsche Signaturgesetz [SigG] am 1. August 1997 in Kraft getreten), kurz darauf wurde mit der Europäischen Signaturrichtlinie [SigDir] 1999 eine Vereinheitlichung der Rechtssetzung auf europäischer Ebene angestrebt. Da EU-Richtlinien grundsätzlich nur den Rahmen vorgeben, der durch nationales Recht wiederum konkret umzusetzen ist, wurde 2001 das deutsche SigG entsprechend angepasst.

Eine »qualifizierte elektronische Signatur« (QES) ist eine fortgeschrittene elektronische Signatur, die von einer qualifizierten elektronischen Signaturerstellungseinheit erstellt wurde und auf einem qualifizierten Zertifikat für elektronische Signaturen beruht.

Eine »fortgeschrittene elektronische Signatur« ist aus technischer Sicht eine digitale Signatur wie eingangs beschrieben. Für Juristen ist es eine elektronische Signatur, die folgende Anforderungen erfüllt:

a) Sie ist ausschließlich dem Unterzeichner zugeordnet;
b) sie ermöglicht die Identifizierung des Unterzeichners;
c) sie wird mit Mitteln erstellt, die der Unterzeichner unter seiner alleinigen Kontrolle halten kann;
d) sie ist so mit den Daten, auf die sie sich bezieht, verknüpft, dass eine nachträgliche Veränderung der Daten erkannt werden kann;

Die Rechtsfolgen der Verwendung einer QES sind in den Mitgliedstaaten weiterhin durchaus unterschiedlich. Im deutschen Recht sind in Bezug auf die Schriftform hier z. B. §126a BGB und §3a VwVfG einschlägig. Insbesondere wurde für die QES ein Anscheinsbeweis in §371a ZPO verankert.

Das Ziel der Signaturrichtlinie war es, die QES als Instrument zur Förderung des europäischen Binnenmarkts Europa zu etablieren. In der Praxis bleibt die Verbreitung der QES bis heute deutlich hinter den Erwartungen zurück. Als Gründe dafür werden u.a. die unterschiedlichen nationalen Umsetzungen der Signaturrichtlinie gesehen. Daher wurde eine weitere Harmonisierung der QES und ihrer Rechtsfolgen angestrebt und die Signaturrichtlinie wird durch die Europäische Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt [eIDAS] (eIDAS-Verordnung) zum 01.07.2016 abgelöst. Da eine Verordnung in den Mitgliedstaaten unmittelbar geltendes höherrangiges Recht ist, treten die nationalen Signaturgesetze dann automatisch außer Kraft.

Die Rechtswirkung elektronischer Signaturen ist nun einheitlich in Artikel 25 der eIDAS-Verordnung geregelt:

(1) Einer elektronischen Signatur darf die Rechtswirkung und die Zulässigkeit als Beweismittel in Gerichtsverfahren nicht allein deshalb abgesprochen werden, weil sie in elektronischer Form vorliegt oder weil sie die Anforderungen an qualifizierte elektronische Signaturen nicht erfüllt.
(2) Eine qualifizierte elektronische Signatur hat die gleiche Rechtswirkung wie eine handschriftliche Unterschrift.
(3) Eine qualifizierte elektronische Signatur, die auf einem in einem Mitgliedstaat ausgestellten qualifizierten Zertifikat beruht, wird in allen anderen Mitgliedstaaten als qualifizierte elektronische Signatur anerkannt.

Der folgende Beitrag beschäftigt sich mit serverbasierten Signaturen, die nach der eIDAS-Verordnung möglich werden. Weitere Details zu den Bereichen eID und Vertrauensdienste finden sich in den Beiträgen [Bend14] und [Fied14] in diesem Tagungsband.

2 Sichere Signaturerstellung

Zur Nutzung einer QES muss nicht nur eine Signaturkarte beantragt (und bezahlt) werden, es wird auch ein geeignetes Lesegerät sowie eine Signatursoftware und Anzeigekomponente benötigt.

Die wesentlichen Sicherheitsanforderungen an diese Produkte finden sich in §15 der Signaturverordnung [SigV]:

- Eine sichere Signaturerstellungseinheit (hier die Signaturkarte) darf die Verwendung des darin sicher gespeicherten Signaturschlüssels erst nach erfolgreicher Authentisierung des Inhabers mit zwei Faktoren (Besitz und Wissen oder Besitz und Biometrie) ermöglichen.
- Signaturanwendungskomponenten (hier das Lesegerät) müssen die Identifikationsdaten des Inhabers geheim[1] halten und die Erzeugung einer Signatur eindeutig anzeigen.

Weder die Signaturrichtlinie noch die eIDAS-Verordnung stellen Anforderungen an Signaturanwendungskomponenten.

1 Hier sollte man sich fragen, wieso die Identifikationsdaten i.d.R. unverschlüsselt zwischen Anwendungskomponente und Erstellungseinheit übermittelt werden.

Nach der eIDAS-Verordnung müssen qualifizierte elektronische Signaturerstellungseinheiten folgende Anforderungen erfüllen:

(1) Qualifizierte elektronische Signaturerstellungseinheiten müssen durch geeignete Technik und Verfahren zumindest gewährleisten, dass
a) die Vertraulichkeit der zum Erstellen der elektronischen Signatur verwendeten elektronischen Signaturerstellungsdaten angemessen sichergestellt ist,
b) die zum Erstellen der elektronischen Signatur verwendeten elektronischen Signaturerstellungsdaten praktisch nur einmal vorkommen können,
c) die zum Erstellen der elektronischen Signatur verwendeten elektronischen Signaturerstellungsdaten mit hinreichender Sicherheit nicht abgeleitet werden können und die elektronische Signatur bei Verwendung der jeweils verfügbaren Technik verlässlich gegen Fälschung geschützt ist,
d) die zum Erstellen der elektronischen Signatur verwendeten elektronischen Signaturerstellungsdaten vom rechtmäßigen Unterzeichner gegen eine Verwendung durch andere verlässlich geschützt werden können.
(2) Qualifizierte elektronische Signaturerstellungseinheiten dürfen die zu unterzeichnenden Daten nicht verändern und nicht verhindern, dass dem Unterzeichner diese Daten vor dem Unterzeichnen angezeigt werden.
(3) Das Erzeugen oder Verwalten von elektronischen Signaturerstellungsdaten im Namen eines Unterzeichners darf nur von einem qualifizierten Vertrauensdiensteanbieter durchgeführt werden.

...

Konkrete Anforderungen an qualifizierte elektronische Signaturerstellungseinheiten (wie beispielsweise die Forderung nach einer Zwei-Faktor-Authentisierung) können in Durchführungsrechtsakten festgelegt werden.

3 Server-Signaturen

Die Anforderungen an eine qualifizierte elektronische Signaturerstellungseinheit erlauben also explizit die Speicherung und Verwaltung der privaten Signaturschlüssel durch einen Vertrauensdiensteanbieter. Vereinfacht gesagt kann eine im unmittelbaren Besitz des Signaturschlüsselinhabers befindliche Smartcard durch einen Server mit Hardware Sicherheitsmodul (HSM) substituiert werden, wenn sichergestellt ist, dass jeder Signaturschlüsselinhaber nur auf seinen eigenen dort gespeicherten privaten Signaturschlüssel zugreifen kann.

Das Ziel der Server-Signaturen ist die Vereinfachung der notwendigen Infrastruktur für qualifizierte elektronische Signaturen. So kann insbesondere nicht nur auf die Signaturkarte selbst verzichtet werden, sondern auch auf die Lesegeräte, die zwingend für die Interaktion mit der Signaturkarte notwendig sind.

Server-Signaturen sind an sich zunächst keine schlechte Idee. In der Tat stehend die derzeit notwendigen Aufwände zur Beantragung und Nutzung einer QES in keinem Verhältnis zu der erwarteten Anzahl an ausgestellten qualifizierten elektronischen Signaturen. Zudem trägt die Verteilung der Kosten zur Verwendung der qualifizierten elektronischen Signatur nicht unbedingt zur Verbreitung bei: Während der Schlüsselinhaber für sämtliche Kosten aufkommt (qualifiziertes Zertifikat, Signaturkarte, Lesegerät) und alle Risiken trägt (Anscheinsbeweis), hat der Signaturempfänger viele Vorteile.

3.1 Identifikation des Schlüsselinhabers

Ob und wie weit das Sicherheitsniveau von Server-Sigaturen mit dem der lokalen Signatur vergleichbar ist, liegt im Wesentlichen an der Identifikation des Schlüsselinhabers. Bei der Identifikation des Schlüsselinhabers muss zunächst zwischen der initialen Iden-

tifikation bei der Erstellung des qualifizierten Zertifikats (sowie des Schlüsselpaares) und der Authentisierung zur Nutzung des Schlüssels unterschieden werden.

Die Identifikation des Schlüsselinhabers bei der Erstellung eines qualifizierten Zertifikats ist durch die eIDAS-Verordnung eindeutig geregelt. So ist nach Artikel 24 auch eine Fernidentifikation des Antragstellers ber eID möglich, wenn diese auf dem Niveau »substantiell« oder »hoch« notifiziert wurde.

Es wäre naheliegend, auch für die Authentisierung des Schlüsselinhabers zur Signaturerstellung ein ähnliches Niveau festzulegen. Dieses wird durch den Verordnungstext implizit auch bestätigt, denn eine fortgeschrittene Signatur »*wird unter Verwendung elektronischer Signaturerstellungsdaten erstellt, die der Unterzeichner mit einem hohen Maß an Vertrauen unter seiner alleinigen Kontrolle verwenden kann*«. Weiterhin muss die qualifizierte Signaturerstellungseinheit gewährleisten, dass »*die zum Erstellen der elektronischen Signatur verwendeten elektronischen Signaturerstellungsdaten vom rechtmäßigen Unterzeichner gegen eine Verwendung durch andere verlässlich geschützt werden können*«.

Eine notifizierte eID auf dem Niveau »hoch« wird diese Anforderungen sicher erfüllen. Es ist jedoch sinnvoll, auch andere Authentisierungsverfahren zuzulassen, da nicht zwingend eine notifizierte eID zur Auslösung einer Server-Signatur verwendet werden soll. Daher ist diese offene Formulierung durchaus sinnvoll, bedarf aber einer Festlegung des Vertrauensniveaus hoch. Hierzu kann die Kommission im Rahmen von Durchführungsrechtsakten (zusammen mit den Mitgliedstaaten) geeignete Normen für Signaturerstellungseinheiten referenziert werden.

Hinweis: Das Vertrauensniveau bei eIDs (Level of Assurance) ist zu unterscheiden vom Vertrauensniveau beim Zugriff auf private Signaturschlüssel (Level of Confidence).

3.2 Handy-Signatur

Die österreichische Handy-Signatur kann als Auslöser für die Server-Signaturen in der eIDAS-Verordnung angesehen werden. Bei der Handy-Signatur wird bei der Anmeldung der Signaturschlüssel in Verbindung mit der registrierten Handynummer und einem Signaturpasswort auf einem Server gespeichert.

Die Signaturerstellung besteht aus folgenden Schritten:

1. Der Signaturschlüsselinhaber gibt als Identifikationsdaten seine Handynummer und sein Signaturpasswort in ein Webformular ein.
2. Der Signaturserver prüft ob Handynummer und Signaturpasswort passen und versendet dann einen TAN-Code, der nur für wenige Minuten gültig ist, an das Mobiltelefon (mTAN).
3. Mit der Eingabe der TAN in das Webformular löst der Signaturschlüsselinhaber die Signaturerstellung auf dem Server aus.

Vor der Signaturerstellung sollte sich der Signaturschlüsselinhaber vergewissern, dass die zu signierenden Daten korrekt sind. Da die optionale Anzeige der Daten ebenfalls über das Webformular erfolgt, setzt das allerdings ein hohes Maß an Vertrauen in den Dienstanbieter und den Webbrowser voraus.

An diese Stelle sei nochmals darauf hingewiesen, dass weder die Signaturrichtlinie noch die eIDAS-Verordnung Anforderungen an die Anzeigekomponente stellen.

3.2.1 BEWERTUNG

Für eine Bewertung, ob das Niveau hoch mit dem mTAN-Verfahren erreicht werden kann, bietet es sich an, den Vorgaben aus [TR03107] zu folgen. Eine wesentliche An-

forderung ist, dass die Übertragung der mTAN auf einem separaten Kanal erfolgt. Mittlerweile hat sich eine neue Klasse von Schadsoftware darauf eingestellt, mTANs abzufangen und an den Angreifer weiterzuleiten. Ein Beispiel dafür ist Android/FakeToken.A wie in [Cast12] beschrieben.

Auch wenn das Ziel derartiger Schadsoftware in der Regel Online-Banking ist, zeigt es, dass ähnliche Angriffe auch auf z. B. Handysignaturen anwendbar wären. Daher kommt [TR-03107] zu dem Schluss, dass nach aktuellem Bewertungsstand das mTAN-Verfahren für neue Verfahren nicht mehr für das Niveau hoch eingesetzt werden sollte.

Unabhängig davon gelten Sorgfaltspflichten für den Signierenden. Er darf natürlich nicht über das gleiche Gerät die Signatur auslösen und die mTAN empfangen. Weiterhin muss er sein Mobiltelefon mit einem wirksamen Zugangscode absichern, um die Zwei-Faktor-Authentisierung zu gewährleisten.

3.2.2 KONSEQUENZEN

Auch wenn grundsätzlich eine Handy-Signatur nach der eIDAS-Verordnung möglich scheint, müssen im Hinblick auf das mTAN-Verfahren zusätzliche Maßnahmen ergriffen werden. Denkbar wäre die Separation von Anwendungen durch hardwareunterstützte Virtualisierungstechniken auf dem Mobiltelefon.

Einfacher wäre es aber, das Auslösen der Signatur statt durch eine mTAN direkt durch ein Hardware-Token anzustoßen. Neben dem Personalausweis als universelles Token kämen dabei auch andere Token, wie z. B. FIDO U2F [FIDO] in Betracht.

3.3 Ad-hoc QES

Unter der Ad-hoc Signatur soll hier die Möglichkeit des Nachladens einer (ggf.) nur kurz gültigen QES auf den Personalausweis verstanden werden. Da die Signaturerstellung durch den Personalausweis selbst erfolgt, ist die Ad-hoc Signatur eigentlich gar keine Server-Signatur im engeren Sinne.

Der Ablauf der Signaturerstellung ist nach [TR03117] vereinfacht wie folgt:

1. Der (zukünftige) Signaturschlüsselinhaber authentisiert sich gegenüber dem Vertrauensdiensteanbieter mit dem elektronischen Identitätsnachweis.
2. Der Vertrauensdiensteanbieter liest die relevanten Identitätsdaten aus dem Ausweis aus, lässt den Personalausweis das Schlüsselpaar erzeugen, liest den öffentlichen Signaturschlüssel aus, erstellt und (optional) speichert das qualifizierte Zertifikat auf dem Personalausweis.
3. Der Signaturschlüsselinhaber erstellt lokal die qualifizierte elektronische Signatur mit den lokalen Komponenten.

Zur Signaturerstellung wird die Signatur-PIN über ein zertifiziertes Lesegerät mit PIN-Pad und Anzeige verschlüsselt an den Personalausweis übertragen.

3.3.1 BEWERTUNG

Nach Notifizierung des Personalausweises auf dem Vertrauensniveau hoch ist der elektronische Identitätsnachweis alleine für die Fernidentifizierung bei der Beantragung eines qualifizierten Zertifikats geeignet. Die Authentisierung zur Signaturerstellung erfolgt lokal mit einer Zwei-Faktor-Authentisierung ebenfalls auf dem Niveau hoch.

3.3.2 KONSEQUENZEN

Die Ad-hoc Signatur löst die wesentlichen Problem der QES, insbesondere indem sie erlaubt, die Kosten für die Ausstellung von qualifizierten Zertifikaten mit kurzen Laufzeiten durch Dritte zu übernehmen. Es verbleibt jedoch das Problem, dass ein lokales, zertifiziertes Lesegerät benötigt wird. Da die Nutzung des Personalausweises ohnehin

ein Lesegerät erfordert, stellt das keine grundsätzliche Einschränkung dar. Derzeit stellt der Personalausweis jedoch für das Erstellen von qualifizierten Signaturen hohe Anforderungen an das Lesegerät, welches sich zunächst mit einem Berechtigungszertifikat gegenüber dem Personalausweis authentisieren muss.

3.4 Stellvertretersignaturen

Die Stellvertretersignatur ist eine Server-unterstützte qualifizierte Signatur, die automatisiert durch einen Dritten, eine natürliche Person als Inhaber eines qualifizierten Zertifikats (dem Serverbetreiber), im Namen des Vertretenen (des Bürgers) erstellt wird.

1. Der Vertretene identifiziert sich gegenüber dem Stellvertreter und erteilt die Vertretungsvollmacht.

2. Der Stellvertreter erstellt die Signatur mit dem eigenen Signaturschlüssel, trägt aber in die Signatur ein, in wessen Auftrag er handelt sowie eventuelle Haftungsbeschränkungen.

3.4.1 BEWERTUNG

Für die Identifizierung gilt wiederum, dass sie mit dem elektronischen Identitätsnachweis in Verbindung mit einem Formular zur Erklärung der Vertretung erfolgen kann. Nach Notifizierung des Personalausweises sind die Anforderungen an die Identifizierung erfüllt.

Grundsätzlich sind auch andere Formen der Identifizierung möglich, z. B. über ein Hardware-Token (FIDO U2F [FIDO]) in Verbindung mit einer einmaligen Registrierung vor Ort einschließlich Erklärung der Vertretungsmacht.

3.4.2 KONSEQUENZEN

Kann der Stellvertreter in strittigen Fällen seine Vertretungsmacht nicht nachweisen, so haftet er ggf. auf Erfüllung oder Schadensersatz. Daher soll die Stellvertretersignatur Haftungsbeschränkungen enthalten, das verbleibende Restrisiko soll über ein Versicherungsmodell abgesichert werden. Die Kosten für die Ausstellung der Stellvertretersignatur trägt der Signaturempfänger. Die vereinbarten Haftungsbedingungen beeinflussen die Kosten entsprechend.

Zukünftig ermöglicht die eIDAS-Verordnung auch elektronische Siegel, d. h. Signaturen für juristische Personen. Qualifizierte elektronische Siegel könnten ab 2016 eine weitere Variante für Stellvertretersignaturen darstellen.

Fazit

In wie weit sich Server-Signaturen dazu eignen, die Verbreitung von qualifizierten Signaturen in der Praxis tatsächlich zu fördern, wird sich erst in der Zukunft zeigen. Eine sichere Umsetzung dürfte grundsätzlich in irgendeiner Form weiterhin sichere Hardware beim Signaturschlüsselinhaber erfordern. Hier kommt es dann im Wesentlichen darauf an, praktikable Lösungen zu entwickeln.

Es stellt sich jedoch grundsätzlich die Frage, warum sich der Signierende auf Niveau hoch zur Signaturerstellung authentisieren muss, wenn nicht auch gleichzeitig sichergestellt ist, dass die zu signierenden Daten authentisch sind und dem Signierenden korrekt angezeigt werden.

Da die eIDAS-Verordnung keine Anforderungen an eine sichere Anzeigekomponente stellt, kann man in strittigen Fällen dem Signierenden nicht unbedingt mangelnde Sorgfalt vorwerfen. Andererseits regelt die eIDAS-Verordnung die Rechtsfolgen einer QES für alle Mitgliedstaaten einheitlich. Da die Verordnung keinen Anscheinsbeweis (s. o. ZPO §371a) festlegt, dürfte hier die freie Beweiswürdigung gelten.

Die Stellvertretersignatur mit dem integrierten Haftungs- und Versicherungsmodell dürfte hier als einziges Verfahren diese Probleme umgehen und sich auch für mehr oder weniger unsichere Signaturumgebungen (z. B. auf dem Mobiltelefon) eignen.

Literatur

[Bend14] Bender, Jens: eIDAS Resolution: eID – Opportunities and Risks, dieser Tagungsband

[Fied14] Fiedler, Arno: Ein sicherer digitaler Binnenmarkt, dieser Tagungsband

[Cast12] Castillo, Carlos: Android Malware Pairs Man-in-the-Middle With Remote-Controlled Banking Trojan. McAfee Labs Blog, 2012 http://blogs.mcafee.com/mcafee-labs/android-malware-pairs-man-in-the-middle-with-remote-controlled-banking-trojan

[eIDAS] 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

[FIDO] FIDO Alliance Universal 2nd Factor (U2F), Technical Specifications, 2014

[TR03107] BSI Technische Richtlinie TR-03107-1, Elektronische Identitäten und Vertrauensdienste im E-Government, Teil 1: Vertrauensniveaus und Mechanismen, 2014

[TR03117] BSI Technische Richtlinie TR-03117, eCards mit kontaktloser Schnittstelle als sichere Signaturerstellungseinheit, Version 1.0, 2009

[SigDir] Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen

[SigG] Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz – SigG)

[SigV] Verordnung zur elektronischen Signatur (Signaturverordnung – SigV)

CV

Dr. Dennis Kügler hat an der Technischen Universität Darmstadt Informatik studiert und dort im Bereich der Kryptographie promoviert. Seit 2002 arbeitet er im Bundesamt für Sicherheit in der Informationstechnik und leitet dort seit 2011 das Referat »eID-Technologien und Smartcards«.

Kontakt

Dennis Kügler
Bundesamt für Sicherheit in der Informationstechnik
53175 Bonn
Tel. +49 22899 9582 5183
Fax. +49 22899 109582 5183
eMail: dennis.kuegler@bsi.bund.de