Fernsignaturen mit der Online-Ausweisfunktion

Seit dem 1. Juli 2016 gilt in allen Mitgliedstaaten der EU die Verordnung (EU) Nr. 910/2014 über „elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt“, kurz eIDAS-Verordnung[1], mit welcher einheitliche Rahmenbedingungen für die grenzüberschreitende Nutzung elektronischer Identifizierungsmittel und Vertrauensdienste geschaffen werden.

Die Umsetzung der Verordnung hat unter anderem zur Folge, dass eine qualifizierte elektronische Signatur, welche von einem Bürger eines EU-Mitgliedstaats erstellt wird, in allen Mitgliedstaaten die gleiche Rechtswirkung entfaltet wie eine handschriftliche Unterschrift in dem betreffenden Staat. Hierdurch wird erstmalig eine europaweite grenzüberschreitende elektronische Kommunikation in rechtsverbindlicher Form ermöglicht.

Die bisherige technische Umsetzung der qualifizierten elektronischen Signatur basierte auf dem Einsatz einer Signaturkarte. Die Sicherheit des Verfahrens wird durch die Signaturkarte sowie eine Zwei-Faktor-Authentifizierung realisiert: Der private Schlüssel wird durch die Signaturkarte vor unbefugten Zugriffen geschützt und seine Verwendung ist nur in Verbindung mit den Authentifizierungsfaktoren Wissen (PIN) und Besitz (Signaturkarte) möglich.

Fernsignaturen

Die eIDAS-Verordnung schafft die Möglichkeit der sogenannten Fernsignatur, die bisher in Deutschland nicht möglich war. Hierbei muss eine qualifizierte elektronische Signatur nicht mehr mit einer Signaturkarte erstellt werden, sondern darf auch durch einen qualifizierten Vertrauensdiensteanbieter im Auftrag des Unterzeichners erstellt werden. Für den Nutzer hat dieses Verfahren den Vorteil, dass er keine zusätzliche technische Ausstattung (Signaturkarte, Lesegerät) zur Erstellung einer qualifizierten elektronischen Signatur benötigt.

Bei einem Fernsignaturverfahren werden andere Sicherheitsanforderungen an das Verfahren gestellt. Insbesondere muss der Vertrauensdiensteanbieter verlässlich und vertraulich mit dem Unterzeichner kommunizieren können, damit dieser vor Signaturfälschungen geschützt ist und die Verwendung seines Signaturschlüssels durch Dritte verhindert werden kann.

Durch die zusätzlichen Sicherheitsanforderungen an den Vertrauensdienste-anbieter treten die sichere Identifizierung und die starke Authentifizierung des Unterzeichners in den Mittelpunkt der Sicherheitsbetrachtung. Außerdem muss das Verfahren sicherstellen, dass das zu unterzeichnende Dokument während der Übertragung vom Unterzeichner zum Vertrauensdiensteanbieter nicht unbemerkt verändert werden kann. Details zu den Sicherheitsanforderungen finden Sie in Anhang 1, Seite 5.

[1] http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32014R0910

„On-the-Fly“ Signatur mit der Online-Ausweisfunktion

Die Online-Ausweisfunktion des deutschen Personalausweises (PA) und des elektronischen Aufenthaltstitels (eAT) bietet bereits heute die Funktionalität, Personen auf dem benötigten

Sicherheitsniveau zu identifizieren und zu authentifizieren. Bei einer Fernsignatur mit Hilfe der Online-Ausweisfunktion entfällt die Anforderung eines zusätzlichen Lesegerätes, wodurch z.B. auch die NFC-Schnittstelle in Mobiltelefonen als Kartenleser verwendet werden kann. Dies ermöglicht die rechtsgültige elektronische Unterschrift mit dem Mobiltelefon (mobile Signatur).

Als Alleinstellungsmerkmal zu anderen Verfahren, die eine Identifizierung (zum Erhalt eines qualifizierten Zertifikates) oder eine Authentisierung (zur Signaturauslösung) als getrennte Vorgänge umsetzen, erlaubt die Online-Ausweisfunktion des PA / eAT darüber hinaus, diese beiden Funktionen **in einem Schritt** zusammenzufassen.

Dadurch wird unter Verwendung des Personalausweises auch eine sogenannte „On-The-Fly“ Signatur möglich, bei welcher sich der Unterzeichner nicht zuvor bei einem Vertrauensdiensteanbieter registrieren muss, sondern unmittelbar anlassbezogen eine qualifizierte elektronische Signatur erstellen kann.

Dieses „1-Schritt-Verfahren“ ist insbesondere für Nutzer attraktiv, welche nur gelegentlich elektronische Signaturen erstellen möchten. Durch die Verwendung von Einmal-Schlüsseln muss der Nutzer keine gesonderten Authentifizierungsmittel für den Zugang zu seinem Schlüssel beim Vertrauensdiensteanbieter nutzen und verwahren. Außerdem entfällt eine aufwändige Registrierung beim Vertrauens-diensteanbieter, da der Nutzer mit seiner Zustimmung zum Unterzeichnen eines Dokuments gleichzeitig durch die Verwendung der Online-Ausweisfunktion identifiziert wird.

Das Verfahren erfüllt alle Anforderungen für qualifizierte Signaturen gemäß der eIDAS-Verordnung, sowie alle Anforderungen an den Vertrauensdiensteanbieter und übertrifft hierbei das minimal geforderte Sicherheitsniveau sogar deutlich (vgl. dazu Anhang 2, Seite 6).

Ablauf der „On-the-Fly“ Signatur mit der Online-Ausweisfunktion

Der Ablauf des vorgeschlagenen Verfahrens soll im Folgenden schematisch skizziert werden (siehe auch Abbildung 1, Seite 3):

1. Zu Beginn bestimmt der Unterzeichner das zu unterzeichnende Dokument; dies kann auf zwei Wegen geschehen: Entweder übermittelt der Unterzeichner das zu unterzeichnende Dokument (z.B. eine PDF-Datei) an den Vertrauensdienste-anbieter (Fernsignaturanbieter) oder das Dokument liegt diesem bereits vor und wird dem Unterzeichner zur Überprüfung vorgelegt. In beiden Fällen liegt im Anschluss sowohl dem Unterzeichner als auch dem Vertrauensdienste-anbieter das identische Dokument vor.

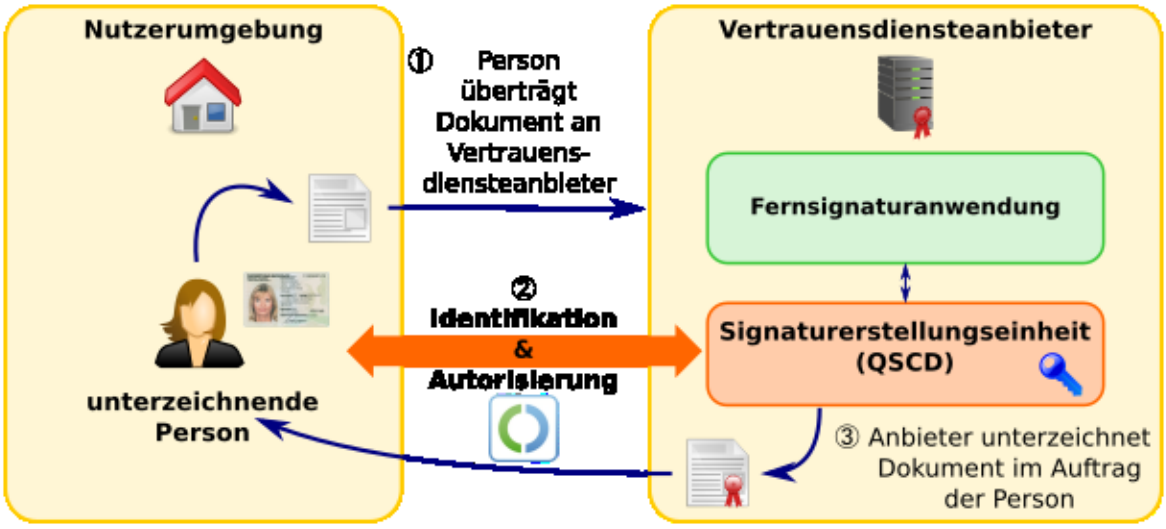

Abbildung 1: Schematischer Ablauf des Fernsignaturverfahrens

2. Im nächsten Schritt startet der Nutzer die Online-Ausweisfunktion, um sich gegenüber dem Vertrauensdiensteanbieter mit seinem Personalausweis auf einem hohen Vertrauensniveau zu identifizieren.

   In Erweiterung der klassischen Online-Ausweisfunktion werden ein erweiterter eID- Server beim Diensteanbieter und ein erweiterter eID-Client beim Nutzer eingesetzt. Diese ermöglichen es dem Diensteanbieter, einen kryptografisch sicheren Prüfwert (Hash) über das zu signierende Dokument in das Protokoll der Online-Ausweisfunktion einzubinden, welcher anschließend auf Seiten des Nutzers durch den Ausweis verifiziert wird. Auf diesem Wege kann kryptografisch nachweisbar sichergestellt werden, dass sowohl auf Seiten des Nutzers als auch des Vertrauensdiensteanbieters das identische, zu signierende Dokument vorliegt. Diese Erweiterung der Online-Ausweisfunktion ist mit allen bereits im Feld befindlichen Ausweisen kompatibel.

   Durch das beschriebene Verfahren werden die Identifizierung des Nutzers sowie die Prüfung des Dokuments miteinander verknüpft. Somit kann sichergestellt werden, dass die identifizierte Person identisch mit der Person ist, welche ihre Zustimmung zum Unterzeichnen gegeben hat.

3. Auf Grundlage der Identifizierung kann der Vertrauensdiensteanbieter für Fernsignaturen einen Signaturschlüssel für den Unterzeichner erstellen und einen Antrag für ein qualifiziertes Signaturzertifikat bei einer Zertifizierungsstelle stellen[2]. Der Antrag kann aufgrund der elektronischen Identifizierung automatisiert bearbeitet und das resultierende Zertifikat dem Vertrauens-diensteanbieter sofort zugestellt werden. Zu diesem Zeitpunkt liegen dem Vertrauensdiensteanbieter bereits das zu signierende Dokument sowie die Zustimmung des Unterzeichners zum Signieren vor, sodass sofort eine Signatur erstellt werden kann.

[2] Diese kann auch der Fernsignaturanbieter selbst sein, wenn er eine entsprechende Zertifizierungsstelle betreibt.

4. Im Anschluss bereitet der Vertrauensdiensteanbieter das signierte Dokument in ein standardkonformes Format auf und überträgt es an den Unterzeichner. Zum Abschluss werden sowohl der Signaturschlüssel als auch das Zertifikat sicher vernichtet, wodurch der Vertrauensanbieter keine weitere Beziehung zum Unterzeichner aufrechterhalten muss. Insbesondere muss der Anbieter keine Infrastruktur zum Speichern oder zum Rückruf eines Schlüssels unterhalten, da dieser jeweils nur genau einmal verwendet wird. Lediglich seitens der Zertifizierungsstelle müssen Daten zum Gültigkeitsstatus des Zertifikats bereitgestellt werden.

Anhang 1 - Sicherheitsvorgaben für Fernsignaturen

Zur Umsetzung der Sicherheitsziele für Fernsignaturen und den sich daraus ergebenden Anforderungen hat die EU (im Mandat 460) das Europäische Komitee für Normung (CEN) beauftragt, Richtlinien und Schutzprofile zu erstellen, welche ein Vertrauensdiensteanbieter für Fernsignaturen erfüllen muss. Zu diesem Zweck verfasst die WG 17 des CEN die Richtlinie EN 419 241-1 und die Schutzprofile PP EN 419 221-5 und PP EN 419 241-2.

Hierbei formuliert die Richtlinie EN 419 241-1 Kriterien für das gesamte Verfahren des Fernsignatursystems. Insbesondere wird hierbei für die Erstellung von qualifizierten Signaturen die 2-Faktor-Authentisierung des Nutzers auf einem substantiellen Vertrauensniveau gefordert, wobei die zwei Faktoren aus unterschiedlichen Kategorien (z.B. Wissen und Besitz) stammen müssen oder über unabhängige Übertragungswege bzw. Schnittstellen vom Unterzeichner zum Vertrauensdienstanbieter übertragen werden müssen. Darüber hinaus muss der Fernsignaturanbieter ein Protokoll zur Signaturauslösung (SAP) bereitstellen, welches sicherstellt, dass das Dokument welches dem Anbieter vorliegt, identisch mit dem Dokument ist, welches dem Unterzeichner vorliegt bzw. von diesem übermittelt wurde. Dieses Protokoll muss dabei das zu signierende Dokument zweifelsfrei mit der Authentifizierung des Nutzers verknüpfen, bevor der Anbieter eine Signatur im Auftrag des Unterzeichners erstellen darf.

Die beiden Schutzprofile formulieren die Zertifizierungsanforderungen an die Signaturerstellungseinheit (QSCD), welche durch einen Fernsignaturanbieter eingesetzt werden darf. Es ist Aufgabe der Signaturerstellungseinheit die privaten Signaturschlüssel der Nutzer zu verwahren und die eigentliche elektronische Signatur zu erstellen. Die Zertifizierung umfasst unter anderem die Implementierung des SAP im QSCD, sowie die Authentifizierung des Unterzeichners. Dabei muss nachgewiesen werden, dass der Unterzeichner die alleinige Kontrolle über seinen Signaturschlüssel innehat. Darüber hinaus werden alle verwendeten kryptographischen Funktionen und Algorithmen des QCDSs, sowie das Schlüsselmanagement, welches den gesamten Lebenszyklus eines Schlüssels, von der Erzeugung, über die Verwendung, bis hin zur sicheren Vernichtung im QCSD umfasst, zertifiziert.

Anhang 2 – eIDAS Kompatibilität

Im Folgenden wird die Kompatibilität der Online-Ausweisfunktion mit den Anforderungen an die Fernsignatur anhand von relevanten Passagen aus der eIDAS-VO sowie der Richtlinie für Fernsignaturanbieter dargelegt.

Anforderungen nach eIDAS-VO:

- Artikel 24 fordert für die Ausstellung von qualifizierten Zertifikaten eine Identifizierung auf Vertrauensniveau substantiell oder höher.
  - ➢ **Die Identifizierung mit dem Personalausweis erfüllt Vertrauensniveau hoch.**
- Artikel 26 fordert unter anderem, dass die Signatur sowohl eindeutig dem Unterzeichner zugeordnet ist, als auch die Identifizierung des Unterzeichners ermöglicht und außerdem unter Verwendung elektronischer Signaturerstellungsdaten erstellt wird, die der Unterzeichner mit einem *hohen Maß an Vertrauen* unter seiner *alleinigen Kontrolle* verwenden kann.
- Zusätzlich fordert Annex II, dass die zum Erstellen der elektronischen Signatur verwendeten elektronischen Signaturerstellungsdaten vom rechtmäßigen Unterzeichner gegen eine Verwendung durch Andere verlässlich geschützt werden können.
  - ➢ **Der private Schlüssel (= elektronische Signaturerstellungsdaten) wird gleichzeitig mit der Identifizierung des Nutzers erstellt, sofort einmalig im Auftrag des Nutzers verwendet und anschließend vernichtet. Hierdurch ist ein Missbrauch des Schlüssels ausgeschlossen.**

Anforderungen nach EN 419 241-1:

- The SAD SHALL be set, computed or be the result of a secured interaction between the SAM and the SIC through the SSA, to authorize the signing operation within the SCDev.
- The SAD SHALL link with a high level of confidence at least the following parameters:
  - a given DTBS/R or a set of DTBS/R,
  - items to identify the authenticated signer, and
  - default or selected signingkey.
    - ➢ **Durch die Kombination des Identifikationsprozesses mit der Autorisierung zur Unterzeichnung können die SAD unmittelbar mit einem hohen Maß an Vertrauen erstellt werden.**

- The enrolment of the signer SHALL be as specified in (EU) 2015/1502 [6] ANNEX Clause 2.1, for assurance level substantial or higher.
- The authentication mechanism SHALL be as specified in (EU) 2015/1502 [6] ANNEX Clause 2.3.1, for assurance level substantial or higher.
    - **Die Identifizierung mit dem Personalausweis erfüllt das Vertrauensniveau hoch. Die Authentifizierung ist implizit gegeben, da die Signatur sofort nach der Identifizierung erstellt wird.**