Daniel Muster, daniel.muster@it-rm.ch

Haftung (für grobes Drittverschulden) beim Authentisieren

Vorbemerkung

Diese Abhandlung wurde für ein breites Zielpublikum verfasst, u.a. für Juristen, welche sich für Sicherheitsfragen in der IT interessieren, wie auch für IT-Fachleute, welche sich für die rechtlichen Aspekte der IT interessieren. Wenn ein breites Publikum angesprochen werden soll, ist es aus didaktischen Gründen nur folgerichtig, dass Ungenauigkeiten aus allen Fachbereichen in dieser Abhandlung enthalten sind.

Diese Abhandlung soll primär als Diskussionsgrundlage dienen und beansprucht für sich nicht, der Weisheit letzter Schluss zu sein.

Worum es geht

U.a. soll Folgendes hier dargelegt werden:

> Dort, wo Verlässlichkeit, resp. die Haftung im *eGovernment* relevant ist, ist lediglich ein online Authentisierungsverfahren auf Basis nach ZertES geregelten Zertifikaten sinnvoll. Dabei sollte ein zu Art. 59a OR analoges Haftungskonstrukt wie beim Leisten einer elektronischen Signatur oder eines elektronischen Siegels unter einem Dokument geschaffen werden.
>
> Insbesondere, wenn aufgrund der Angaben nach dem online Authentisieren etwelche kostenträchtige Dispositionen getroffen oder sensitive Daten, wie ein Strafregisterauszug oder Patientendaten, transferiert oder erfasst werden.

Anhand des online Authentisierens mit Username und Passwort soll die Problematik der bestehenden Haftungsbestimmungen erläutert und *mögliche Lösungsansätze* skizziert werden.

Anmerkung: Das Leisten einer elektronischen Signatur, welche mit einem nach ZertES geregelten Zertifikat verifiziert werden kann, impliziert eine Haftung für grobes Drittverschulden (Art. 59a OR).

> **Begründung:** Angenommen, einem Dritten C gelingt es, in den Besitz des privaten Schlüssels von A zu gelangen und (absichtlich) elektronische Signaturen im Namen von A herzustellen und dabei B zu schädigen. Dies, weil sich B auf diese Signatur verlassen hat, welche mit einem nach ZertES geregelten Zertifikat von A verifiziert

werden kann. Dann haftet A grundsätzlich für den Schaden von B (Art. 59a Abs. 1 OR). Also haftet A für grobes Drittverschulden des C. Der Haftung kann sich A nur entziehen, wenn er glaubhaft darlegt, dass er sorgsam den privaten Schlüssel geschützt hat (Art. 59a Abs. 2 OR).

Analoges gilt für die Herausgabe geregelter Zertifikate (Art. 17 ZertES). Nur, dass der Herausgeber der geregelten Zertifikate beweisen muss, dass er die Sorgfaltspflicht im Umgang mit seinem privaten Schlüssel für die Erstellung geregelter Zertifikate erfüllt hat.

Begriffe: Online Authentisierung bedeutet die Authentisierung für den Aufbau einer interaktiven Kommunikation zwischen den Beteiligten. Beispiel hierfür ist das Anmelden bei einem Web-Server. Eine elektronische Signatur unter einem digitalen Dokument dient ebenfalls der Prüfung der Authentizität, doch ist das Dokument dann nicht Bestandteil einer interaktiven Kommunikation, sondern stellt etwas Statisches dar.

Online Authentisieren mit Username und Passwort

Folgende Randbedingungen sollen gelten:

Behörde B authentisiert Privatperson PP mittels Username und Passwort. Aufgrund der nach der Authentisierung vorgenommenen Eingaben entsteht bei B ein Schaden. B will nun den Schaden von PP beglichen haben, weil er annimmt, dass PP die zum Schaden führenden Anweisungen beim System von B eingegeben hat.

Hierbei stellen sich u.a. folgende 2 Probleme:

1. PP dementiert die entsprechenden Eingaben vorgenommen zu haben. Er stellt die These auf, dass B die Eingaben selber vorgenommen hat, weil B das Passwort von PP ebenfalls kennt.
2. PP bestreitet, sich am System angemeldet zu haben. Er stellt die These auf, ein externer Dritter C habe sich Kenntnis über Username und Passwort von PP verschafft und den Schaden bei B absichtlich herbeigeführt.

Lösungsansatz zu Punkt 1

Lösungssatz: Das online Authentisieren von PP erfolgt auf Zertifikatsbasis. Dies bedeutet, PP besitzt ein Geheimnis (privater Schlüssel) und authentisiert sich bei B. Dies, indem er B da-

von überzeugt, dass er das Geheimnis kennt, es aber dabei nicht preisgeben muss. B kann sich aber aufgrund des Zertifikats (öffentlicher Schlüssel darin) davon überzeugen, dass PP im Besitz des Geheimnisses ist. Folglich kann PP nicht die These aufstellen, dass B sich selber angemeldet und den Schaden verursacht hat.

Problematiken und Lösungsansatz zu Punkt 2

Annahme: PP authentisiert auf Basis eines (geregelten) Zertifikats bei B

Problematik: PP kann nun immer noch dahingehend argumentieren, dass ein Dritter C sich des Geheimnisses (privaten Schlüssels) für die online Authentisierung bemächtigt hat, C sich dann im Namen von PP angemeldet und den Schaden absichtlich verursacht hat. Bei dem von C absichtlich verursachten Schaden handelt es sich nun um grobes Drittverschulden in der haftpflichtrechtlichen Beziehung zwischen PP und B. Grobes Drittverschulden des C reduziert die Haftung von PP oder schliesst sie sogar aus. Siehe dazu u.a. KELLER, S. 81 ff, S. 131, LUTERBACHER, S. 122, KELLER/SCHMIED-SYZ, S. 44.

Wenn eine Haftung nach OR 41 vorliegt, dann hat B zusätzlich darzulegen, dass der Schaden aufgrund einer Sorgfaltspflichtverletzung von PP entstanden ist, nämlich die unsorgfältige Handhabung des Geheimnisses. Dies in der IT nachzuweisen, ist prinzipiell schwierig. Weil zwischen Eintritt des Schadens und der Gerichtsverhandlung beträchtlich Zeit verstreichen kann, hat PP viele Möglichkeiten, etwelche Indizien und Beweise beiseite zu schaffen. Es besteht Verdunklungsgefahr.

Lösungsansatz: Angenommen, es läge eine zu Art. 59a OR analoge Haftung vor. PP authentisiert sich nun bei B auf Basis eines geregelten Zertifikats online, und es entsteht infolgedessen dem B ein Schaden. Um keinen Schadenersatz zu leisten, muss PP glaubhaft darlegen, dass er sorgfältig mit seinem Geheimnis (privaten Schlüssel) umgegangen ist (in Analogie zu Art. 59a OR). Gelingt PP dies nicht, so hat er für den von C (absichtlich) verursachten Schaden einzustehen. Ähnliches gilt beim Ausstellen von geregelten Zertifikaten für den Zertifikatsanbieter (Art. 17 ZertES). Hierbei hat der Aussteller des Zertifikats jedoch zu beweisen, dass er die Sorgfaltspflicht erfüllt hat.

Problem: Damit B belegen kann, dass der Schaden aufgrund der Eingaben nach der Authentisierung entstanden ist, hat er die einzelnen Schritte vom Authentisieren bis zum Abmelden am System *nachvollziehbar* zu belegen.

Risikoabwälzung

Im Unterschied zum eBanking kann die Behörde nicht wie eine Bank das Risiko im eGovernment per Vertrag an Privatpersonen überwälzen. U.a. auch, weil im eGovernment meist kein Vertrag zwischen Behörde und Bürger besteht. Deshalb ist es im Interesse von B, dass die ausservertragliche Haftung greift.

Weitere Probleme zur bestehenden Haftungsregelung (nach OR 59a)

Hier werden einige Probleme dargelegt, welche aufgrund der angedachten, eingeschränkten Haftungsanwendung nach OR 59a entstehen können.

Abgrenzung: Gemäss Botschaft des Bundesrats zur Totalrevision des ZertES, S. 1032 2. Absatz von unten, „soll die Haftung“ nach OR 59a „auf elektronische Signaturen und elektronische Siegel beschränkt sein und für die Authentisierung oder weitere Anwendungen elektronischer Zertifikate nicht gelten“[1].

Hierbei stellt sich folgendes Problem der Haftungsabgrenzung:

- Mit der Prüfung einer elektronischen Signatur ist stets eine Verifikation der Authentizität (Authentisierung) und der Integrität eines Dokuments verbunden.
- Viele online Authentisierungsverfahren basieren auf elektronischen Signaturen.[2] Somit werden elektronische Signaturen nicht nur unter einem digitalen Dokument geleistet. Somit ist der folgende Satz in der Botschaft nicht zutreffend: „In der Praxis wird das Vertrauen zwischen Partnern im elektronischen Verkehr in der Mehrzahl der Fälle nicht durch eine signierte Meldung, sondern durch die Authentisierung gegenüber einem Online-Dienst hergestellt.“

Was ist ein digitales Dokument? Nun kann dahingehend argumentiert werden, dass sich die Haftung nach Art. 59a OR auf die elektronische Signatur unter einem digitalen Dokument beschränkt. Nun stellt sich aber dabei folgendes Problem:

[1] Da sich die Gesetzesvorlage ans Parlament vom Gesetz, wie es das Parlament verabschiedet hat, inhaltlich nicht unterscheidet, ist es vertretbar, die Botschaft als Interpretation für das Gesetz heranzuziehen.

[2] So z.B. die Authentisierung des Web Servers mit /TLS mit Diffie-Hellman, wie auch die Authentisierung des Benutzers gegenüber dem Webserver

Wie definiert man ein Dokument und grenzt es von einem Datensatz ab? Bei Dateien im XML-Format ist dies eine verzwackte Angelegenheit, weil die Übergänge fliessend sind. Dokumente können zudem aus verschiedenen getrennten Dateien, Datensätzen oder -objekten zusammengesetzt werden. Will man solche Dokumente signieren, sind die einzelnen Bestandteile von der Signatur zu erfassen[3].

Zudem beschränkt sich die Haftung nach OR 59a nicht auf bestimmte Dokumentformate wie auf das pdf-Format.

Online Authentisierung basierend auf dokumentähnlichen Dateien. Gewisse online Authentisierungen basieren auf dokumentähnlichen Strukturen, welche bei einer optimal gesicherten online Authentisierung ebenfalls signiert werden sollten, wie eine Attributbestätigung des zu Authentisierenden oder ein XML-Schema[4].

Attribute - Haftung

Folgender Prozess legt dar, welches Problem entstehen kann, wenn Attribute zusätzlich zu den im Zertifikat vorhandenen für die Authentisierung benötigt werden und folglich geliefert werden müssen:

PP authentisiert sich beim Server B auf Basis eines geregelten Zertifikats mittels der Sicherheitstechnologie TLS, welche auch beim eBanking verwendet wird. Die mit der Sicherheitstechnologie geschützte Anwendung jedoch benötigt für die Authentisierung/Autorisation andere Attribute, als im geregelten Zertifikat enthalten sind. Ein Attributdienst AD liefert die zu PP (vermeintlich) gehörenden, notwendigen Attribute in einer elektronisch signierten Meldung.

Beispiel: Max Meier (PP) authentisiert sich auf Basis eines geregelten Zertifikats bei der Behörde Byte (B) mittels der Sicherheitstechnologie TLS. Die Applikation bei der Behörde Byte verwaltet die Benutzer und die Zugangsberechtigung anhand der E-Mail-Adresse. Der Attributdienst liefert versehentlich die E-Mail Adresse von Max Meyer (max.meyer@bluewin.ch) anstatt max.meier@bluewin.ch.

[3] W3C Signature Syntax and Processing Version 1.1, 2013

[4] Ein XML-Schema ist eine XML-Datei, welche das Format und die Attribute einzelner Elemente einer anderen XML-Datei festlegt.

Bemerkung: Erfolgt die Prüfung der Authentizität der Attributbestätigung nicht auf Basis eines geregelten Zertifikats, so liegt keine nahtlose Authentisierung von PP auf Basis geregelter Zertifikate vor.

Nun entsteht ein Schaden bei B oder bei Max Meyer infolge, dass die gelieferten Attribute bei AD verwechselt oder falsch erfasst wurden und somit inkorrekt sind. Wenn nun, wie im E-ID-Gesetz vorgesehen, die Haftung von AD nach OR geregelt ist und die elektronisch signierte Attributbestätigung von AD nicht von OR 59a erfasst wird, gilt meines Wissens Folgendes:

- Besteht kein Vertrag zwischen AD und B oder Max Meyer, dann haftet AD gegenüber den Geschädigten nach OR 41 (Verschuldenshaftung).
- B oder Max Meyer hat die Sorgfaltspflichtverletzung von AD zu beweisen. (In der IT eine schwierige Angelegenheit, insbesondere für Max Meyer.)
- Ob ein Vertrag vorliegt oder nicht, hat AD grundsätzlich nicht für grobes Drittverschulden einzustehen.

Unabhängig von der Art der Haftung ist es für eine Privatperson im eGovernment schwierig, den Verursacher des Schadens zu ermitteln. Damit dies möglich ist, müssen die IT-Prozesse mindestens nachvollziehbar ausgestaltet sein und Max Meyer die dafür notwendigen Informationen zugänglich gemacht werden.

Bemerkung zur IT-Sicherheit: Die online Authentisierung mit Attributbestätigung kann die Sicherheit der rein auf dem geregelten Zertifikat basierenden Authentisierung schmälern. Abhilfe könnte schaffen:

- Die Applikation authentisiert nur auf Basis der Attribute, welche im geregelten Zertifikat enthalten sind.
- Es dürfen mehr Attribute ins geregelte Zertifikat aufgenommen werden. Die Aufzählung, was ins geregelte Zertifikat aufgenommen werden darf, ist im ZertES jedoch abschliessend definiert (Art. 7 Abs. 2 und 3 ZertES).
- Der ganze Prozess der Attributbestätigung von der Registrierung bis zur Zustellung ist in Bundesvorschriften ähnlich festgelegt wie der Ausstellungsablauf geregelter Zertifikate.

Quellenangabe, Abkürzungsliste, Normen

Abs.	Absatz
Art.	Artikel
Botschaft ZertES	Botschaft des Bundesrats zur Totalrevision des ZertES, BBl 2014 1001
Bst.	Buchstabe
E-ID-Gesetz	Bundesgesetz über anerkannte elektronische Identifizierungseinheiten, Gesetzesvorlage 2018
KELLER	Alfred Keller, Haftpflicht im Privatrecht, Band I, Stämpfli Verlag AG, Bern 1993
KELLER/ SCHMIED-SYZ	Max Keller, Carole Schmied-Syz, Haftpflichtrecht -Ein Grundriss in Schemen und Tafeln-, Schulthess Verlag, 1997
LUTERBACHER	Thierry Luterbacher, Fischer Willi (Hrsg.), Haftpflichtkommentar, Dike Verlag, 2016
OR	Schweizerisches Obligationenrecht vom 30. März 1911, SR 220
Rz	Randziffer
TLS	Request for Comments: 5246, The Transport Layer Security (TLS) Protocol Version 1.3
u.a.	unter anderem
VZertES	Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate vom 23. November 2016, SR 943.032
W3C-Signature	W3C Signature Syntax and Processing Version 1.1, 2013, https://www.w3.org/
z.B.	zum Beispiel
ZertES	Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate vom 18. März 2016, SR 943.03