Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Justiz- und Polizeidepartement EJPD

Bundesamt für Justiz BJ
Rechtsinformatik

Abklärung Signaturvarianten für die Eingabe ans GBA

Datum: 30. Juli 2012

Für: Teilnehmer Begleitgruppe zu Informatikthemen des Brundbuchs

Referenz/Aktenzeichen: COO.2180.109.7.78842 / 233.1/2011/01587

Abklärung Signatur

Management Summary

Ein Grundbuch (GB) -Auszug enthält vertrauliche Daten. Folglich muss der Empfänger dieser Daten persönlich identifiziert werden, damit keine vertraulichen Daten an einen unberechtigten Leser abgegeben werden.
Von einigen Kantonen wird die Zulassung von fortgeschrittenen Zertifikaten für die Identifikation der Nutzer bei der Bestellung von GB-Auszügen gewünscht. Es wurden vor der Festlegung auf eine Formulierung in der TGBV im Rahmen der Begleitgruppe zu Informatikthemen des GB weitere Abklärungen gewünscht.
Die Identifikation der Inhaber von fortgeschrittenen Zertifikaten erfolgt zum Teil anhand der E-Mail-Adresse. Das reicht nicht aus, um die Identität einer Person für die Zustellung von vertraulichen Daten hinreichend sicherzustellen, da eine E-Mail-Adresse wenig über die wahre Identität einer Person aussagen kann.
Falls die Peron anhand von Ausweispapieren geprüft werden muss, so kommt ausschliessliche ein qualifiziertes Zertifikat wie die «SuisseID» in Frage.
Weiter ist die Nutzung durch bekannte, vertraglich gebundene Nutzer im Rahmen eines anerkannten, alternativen Übermittlungsverfahrens eine zu berücksichtigende Variante.

Heute können Papier-Auszüge gemäss gängiger Praxis in einigen GB-Ämtern formlos bestellt werden, da eine gewisse Empfänger-Identifikation durch die Postzustellung an einen Briefkasten implizit erfolgt. Dieser Prozess wird in der TGBV nicht behandelt.
In der TGBV wird nur die **elektronische** Bestellung und Eingabe an ein GB-Amt sowie die elektronische Antwortmöglichkeit des GB-Amts geregelt. Aus Praktikabilitätsgründen wird im Entwurf der TGBV für alle elektronischen Bestellung und Eingabe an ein Grundbuchamt die gleiche, hohe Eintrittsschwelle angewendet. Also auch ein elektronisch bestellter Papierauszug setzt eine gleich hohe Absenderidentifikation wie die Bestellung eines elektronischen Auszugs oder eine Anmeldung voraus. Der Grund dafür ist, dass trotz fehlender Routine keine Fehler passieren dürfen. Das würde bei einer auf Natur des Geschäfts, Output, Übermitt-

Bundesamt für Justiz BJ
Rechtsinformatik, Christian Bütler
Bundesrain 20, 3003 Bern
Tel.: 031 325 17 62
E-Mail: christian.buetler@bj.admin.ch
http://www.bj.admin.ch

lungsform, etc. basierende Variantenvielfalt sehr schwierig. Sind die Prozesse einmal etabliert, können weitere Varianten hinzugefügt werden.

Frage der Kantone als Basis dieser Abklärung:

Kann für die Eingabe an ein GB-Amt eine fortgeschrittene Signatur verwendet werden? Gibt es gegebenenfalls Alternativen?

Problemstellung:

Art. 18 des Vorentwurfs der TGBV regelt, wie elektronisch Bestellungen und Eingaben an ein Grundbuchamt gemacht werden können und Art. 19 regelt wie das GB-Amt darauf antworten kann.
Da Grundbuchdaten oft vertrauliche Informationen enthalten, muss sichergestellt werden, dass sie nur von einer berechtigten Person bestellt und damit eingesehen werden können.
Bei einer Bestellung eines elektronischen Auszugs über die Distanz ist zwingend eine Absenderidentifikation nötig, da bei der Bestellung und Auslieferung des Auszugs kein Bezug zu einer aktuellen physischen Adresse mit implizitem Verifikationscharakter erfolgt. Die Vorgeschriebene Version der Zustellplattform gibt zwar eine gewisse Identifikation des Postfachinhabers vor, sie sagt aber wenig über die Aktualität der Adresse aus und schreibt keine Prüfung anhand einer Ausweisschrift vor.
Das BJ hatte als Absenderidentifikation ein PDF als Träger mit qualifizierter Signatur als Willensbekundung und Identifikator in seinem ursprünglichen Vorschlag.
Von einigen Kantonen kam der Vorschlag, auch fortgeschrittene Zertifikate zuzulassen.

Rechtsgrundlagen:

TGBV-Vorentwurf

Art. 18 Eingaben an das Grundbuchamt

Zulässige Datenformate für Eingaben an das Grundbuchamt sind:

a. für Grundbuchanmeldungen, welche nicht bereits im Rechtsgrundausweis enthalten sind: PDF/A (ISO 19005-1:2005 und 19005-2:2011) oder XML, je mit einer qualifizierten elektronischen Signatur nach Artikel 14 Absatz 2bis OR; mit der Eingabe in PDF/A kann zusätzlich eine unsignierte XML-Datei eingereicht werden;

b. für öffentlich beurkundete Rechtsgrundausweise: die Formate nach der Verordnung des EJPD vom 2. Dezember 2011[1] über die anerkannten Formate im Bereich der elektronischen öffentlichen Beurkundung;

c. für Rechtsgrundausweise in schriftlicher Form einschliesslich Beilagen: PDF/A mit einer qualifizierten elektronischen Signatur nach Artikel 14 Absatz 2bis OR;

d. für Gesuche um Ausstellung eines Grundbuchauszugs oder einer Eintragungsbescheinigung: PDF oder XML, je mit einer qualifizierten elektronischen Signatur nach Artikel 14 Absatz 2bis OR

GBV

Art. 40 Übermittlung
1 Elektronische Eingaben an die Grundbuchämter können über die Zustellplattformen nach den Artikeln 2 und 4 der Verordnung vom 18. Juni 2010[11] über die elektronische Übermittlung im Rahmen von Zivil- und Strafprozessen sowie von Schuldbetreibungs- und Konkursverfahren oder über Internetseiten des Bundes oder der Kantone erfolgen, sofern diese:

1 SR **943.033.1**

a. die Vertraulichkeit (Verschlüsselung) gewährleisten; und
b. eine mit einem Zertifikat und einem Zeitstempel einer anerkannten Anbieterin von Zertifizierungsdiensten signierte Quittung über die Eingabe ausstellen.

2 Das EJPD kann die Abwicklung und Automatisierung des elektronischen Geschäftsverkehrs regeln, namentlich in Bezug auf Formulare, Datenformate, Datenstrukturen, Geschäftsprozesse und alternative Übermittlungsverfahren.

ZertES

Art. 2 Begriffe
In diesem Gesetz bedeuten:
a. *elektronische Signatur*: Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder die logisch mit ihnen verknüpft sind und zu deren Authentifizierung dienen;
b. *fortgeschrittene elektronische Signatur*: eine elektronische Signatur, die folgende Anforderungen erfüllt:
1. Sie ist ausschliesslich der Inhaberin oder dem Inhaber zugeordnet.
2. Sie ermöglicht die Identifizierung der Inhaberin oder des Inhabers.
3. Sie wird mit Mitteln erzeugt, welche die Inhaberin oder der Inhaber unter ihrer oder seiner alleinigen Kontrolle halten kann.
4. Sie ist mit den Daten, auf die sie sich bezieht, so verknüpft, dass eine nachträgliche Veränderung der Daten erkannt werden kann;
c. *qualifizierte elektronische Signatur*: eine fortgeschrittene elektronische Signatur, die auf einer sicheren Signaturerstellungseinheit nach Artikel 6 Absätze 1 und 2 und auf einem qualifizierten und zum Zeitpunkt der Erzeugung gültigen Zertifikat beruht;

Lösungsvarianten

Als Muss-Kriterium für die Eignung einer Lösungsvariante ist die eindeutige Identifikation des Bestellers zu betrachten.
Grün: Identifikation der Person genügend (Indentifikation anhand Ausweisdokument)
Rot: Identifikation der Person ungenügend
Gelb: Eher Schwache Identifikation

Qualifizierte Signatur (z. B. SuisseID) auf PDF als Träger:

- Rechtsgültige Unterschrift als Willensbekundung
- Eindeutige Identifikation des Unterschreibenden
- Unveränderbarkeit des PDFs gewährleistet

Qualifiziert signiertes E-Mail (E-Mail als Träger der Signatur):

- Eindeutige Identifikation des Absenders
- Unveränderbarkeit des E-Mails gewährleistet

Signiertes PDF auf Basis Softzertifikat (fortgeschrittenes Zertifikat):

- Eindeutige Identifikation der E-Mail-Adresse
- Identifikation der Person kann nicht vorausgesetzt werden
- Unveränderbarkeit des Dokuments

Signiertes E-Mail auf Basis Softzertifikat (fortgeschrittenes Zertifikat):

- Eindeutige Identifikation der E-Mail-Adresse
- Identifikation der Person kann nicht vorausgesetzt werden
- Unveränderbarkeit des Dokuments gewährleistet

Zustellplattform Variante eGov bietet:

- Eindeutige Identifikation der E-Mail-Adresse
- Identifikation des Postfachinhabers über Postadresse oder SuisseID (mögliche Variante)
- Unveränderbarkeit des E-Mails gewährleistet

Authentifikation über SuisseID:

- Eindeutige Identifikation der Person
  Erklärung: Der Antragsteller ruft mittels SuisseID-Login über eine Webseite die von der Anbieterin von Zertifizierungsdiensten hinterlegten Angaben ab über den sogenannten IDP-Service (Identity Provider). Dieses Verfahren wird z. B. für Strafregister-Auskünfte verwendet.

Authentifikation über ein alternatives Übermittlungsverfahren (Terravis):

- Eindeutige Identifikation der Person
  Erklärung: Terravis hat die Anwender vertraglich gebunden, kenn sie also. Somit kann einer Bestellung ab dem Terravis-System vertraut werden.

Authentifikation über eine direkt an das Grundbuchinformatiksystem angebundene Plattform (Grudis, Grudatrans, TERINTRA):

- Eindeutige Identifikation der Person
  Erklärung: Benutzer solcher Plattformen sind vertraglich gebunden, das GB-Amt kennt sie also. Somit kann einer Bestellung ab einer solchen Plattform vertraut werden.

Bewertung der Varianten

Identifikationsstandard

Bezüglich nicht-elektronischer Bestellung von Papier-Grundbuchauszügen und Eingaben bleiben die bestehenden Prozesse und Kompetenzen unberührt, da diese nicht in der TGBV geregelt werden.

Für die elektronische Bestellung und elektronische Eingaben an ein Grundbuchamt und die Antwort von diesem werden einfache Rahmenbedingungen aufgestellt, die für alle elektronischen Geschäftsfälle zum und vom GB-Amt gelten. Basis dafür ist die TGBV. Damit haben Grundbuchämter die Sicherheit, dass sie sich korrekt verhalten und schweizweit wird ein einheitlicher Mindeststandard erreicht. Natürlich wäre es in der Ausgestaltung denkbar zu unterscheiden zwischen bestellten papierenen und elektronischen Auszügen, wobei für Papier-Auszüge weniger strenge Bestimmungen gelten würden als für elektronische Auszüge. Weiter wäre es denkbar für Bestellungen von GB-Auszügen die Variante eGov der Zustellplattformen als hinreichende Identifikation anzuerkennen und nur für GB-Anmeldungen und weiterer definierter Dokumente an das GB-Amt tatsächlich eine qualifizierte Signatur vorzuschreiben. Es wären noch unzählige weitere Nuancen mit entsprechenden Variantenfolgen möglich.

Solche Regelungen sind aber schwer zu beschreiben, zu verstehen und führen zu Unklarheiten mit Interpretationsbedarf. Sie können Prozesse bei Grundbuchämtern komplizieren, vergrössern und damit fehleranfällig machen. Zudem werden diese Geschäftsfälle in kleineren Grundbuchämtern anfänglich eher selten vorkommen, dass sich keine Routine etablieren

kann. Daher ist es in der Praxis unter Berücksichtigung einer Null-Fehler-Toleranz beim Umgang mit vertraulichen Daten am sinnvollsten, für elektronische Anfragen anfangs generell einen einheitlich hohen Standard vorzusehen, welcher zwingend eine SuisseID (oder ein anderes qualifiziertes Zertifikat) oder eine vertragliche Bindung auf einer definierten und vom Bund anerkannten oder von einem Kanton angebotenen Plattform voraussetzt.
Wenn über die Zeit Erfahrungswert vorliegen und die Prozesse etabliert sind und die Kantone eine Abstufung wünschen, können für eine neue Version der TGBV verfeinerte Regeln erlassen werden.

Qualifizierte Signatur
Eine qualifizierte Signatur braucht einen Träger auf dem sie angebracht werden kann. Bei PDF wird als Standard die Signatur in der Datei angebracht («embedded») und nicht als abgesetzte, selbständige Datei festgehalten («detached»). Damit muss in den Arbeitsprozessen nur eine Datei - die erwähnte PDF-Datei - berücksichtigt werden und nicht zwei zusammenhängende Dateien gespeichert, versandt und bearbeitet werden, wobei Wissen oder Logik vorausgesetzt wird, damit diese Dateien zueinander in Relation gesetzt werden können.
Tatsächlich ist diese Eigenschaft (Signatur «embedded») nicht nur beim Format PDF vorzufinden. Die Voraussetzungen sind somit bei einigen anderen Formaten gleich wie bei einer PDF-Datei mit Signatur. So ist z. B. «normales» E-Mail, das vor dem Versand mit einer qualifizierten Signatur versehen wird, auch als eine Datei auf dem PC ersichtlich.
Allerdings stellt sich bei E-Mail (exemplarisch für weitere gleich funktionierende Formate) die Frage, wie die Echtheit so einer Signatur in der Praxis überprüft werden kann. Die Prüfung der qualifizierten Signatur hat über eine Validation bei einer vertrauenswürdigen Stelle zu geschehen. Der Validator des BJ ist z. B. in der Lage, eine PDF-Datei zu überprüfen, ein Validator für andere Dateiformate müsste ergänzt werden.
Es kann weiter im Falle von signierten E-Mails von einem Anwender nicht erwartet werden, dass er ein E-Mail sicher vor Verwechslung aus dem Postfach zu extrahieren weiss und speichert, dass er es in der Folge im Windows Explorer auswählen und in einen Validator prüfen kann. Es kommt hinzu, dass je nach Konfiguration des Computers beim Nutzer diese Schritte gar technisch unterbunden sein können. Lokale Varianten für die Prüfung (z. B. ein Computerprogramm auf dem Computer des Nutzers installieren) sind denkbar, sind aber verhältnismässig aufwändig im Betrieb und stellen neue Probleme - das fängt z. B. schon bei den vorausgesetzten Installationsrechten bei den Nutzern an.
Es wird daher empfohlen, ausschliesslich PDF als Träger für eine qualifizierte Signatur zuzulassen.

Authentifikation über SuisseID
Die gleiche Qualität einer Identifikation wie über einer qualifizierten Signatur lässt sich auch durch Authentifizierung («Anmelden») mit einer SuisseID erzielen: Dazu werden in einem Browser (z. B. Microsoft Internet Explorer) über die SuisseID des Nutzers die bei der Ausstellerin der SuisseID hinterlegten Identifikationsdaten online und in Echtzeit abgerufen. Die Daten werden dazu nach PIN-Eingabe (der SuisseID) ab dem Identification Service Provider (IDP) der Ausstellering der SuisseID bestellt. Erst wenn die persönlichen Daten durch den Nutzer freigegeben werden, können diese an den Empfänger übermittelt werden. Der Nutzer als Eigentümer der SuisseID weiss somit jederzeit, welche Daten er freigibt. Diese Technologie ist erprobt und für den Strafregisterauszug im Einsatz und wird von privaten

Anbietern im Bereich Verkauf von alkoholischen Getränken und Erwachsenenunterhaltung vor allem zur nachweislich verlässlichen Altersbestimmung des Bestellers genutzt.
Eine solche Anwendung mit der Übermittlung aller Identifikationsangaben über alle Ausweis-Angaben ist im Bereich Grundbuch nicht im Einsatz. Sie könnte allerdings über die vorhandenen elektronischen Briefkasten (OSIS-BV), welche diese Funktion unterstützen, problemlos und innert kurzer Zeit genutzt werden.
Die Variante Authentifizierung über eine SuisseID wird als zusätzliche Option empfohlen. Eine Lösung kann durch das BJ angeboten werden.

Alternative Übermittlungsplattformen und Direktanbindung
Falls eine alternative Übermittlungsplattform eine Closed User Group für Profis ist, welche ihre Kunden vertraglich gebunden hat, ist die Identität der Anwender bekannt und die Verantwortung bestimmt.
Die Alternativen Übermittlungsplattformen werden im Rahmen des ISMS (Information Security Management System) verpflichtet, solche Prozesse sorgfältig zu betreiben, was regelmässig auditiert wird. Mittels Rollen können Anwendergruppe sehr spezifisch adressiert werden. Weiter können im Kriterienkatalog spezielle Anforderungen an die Identifikation festgehalten werden.
Analog werden heute schon Daten ausgetauscht über Plattformen, die direkt mit dem Informatiksystem des GB verbunden sind. Diese bestehende Möglichkeit wird nicht eingeschränkt.
Es wird daher empfohlen, anerkannte alternative Übermittlungsplattformen zuzulassen und bei der Direktanbindung an das Informatiksystem des GB darauf zu achten, dass diese bestehenden Prozesse unter der Hoheit der Kantone nicht behindert werden und ausgebaut werden können.

Inputs der Anbieterinnen von Zertifizierungsdiensten

Es wurden alle anerkannten Anbieterinnen von Schweizer Zertifizierungsdiensten bezüglich der Praxistauglichkeit per E-Mail angefragt:
- BIT
- Die Post
- Quo Vadis
- Swisscom

Das BIT hat keine Antwort gesandt. Die anderen Anbieter empfehlen für diese Anwendung mit Hinblick auf die Verwendbarkeit in der Praxis qualifizierte Zertifikate zu verwenden.
Die Post hat zusätzlich auf die Möglichkeiten von Zustellplattformen in der Ausprägung «eGov» hingewiesen.
Die Empfehlungen wurden in diesen Beitrag berücksichtigt und bezüglich Zertifikate komplett übernommen.

Schlussfolgerung

Basierend auf diesen Abklärungen wurden folgende Punkte in den Entwurf der TGBV aufgenommen:

- Die Entgegennahme nicht-elektronische Eingaben wird in der TGBV nicht behandelt und somit nicht verändert.
- Für elektronische Anfragen und Eingaben jeglicher Art sowie für die Antworten darauf gelten unabhängig von der Art des Outputs und des Prozesses die gleichen Anforderungen.
- Fortgeschrittene Zertifikate reichen nicht aus für die Identifizierung der Nutzer, weil die Identifikationsprüfung zum Teil nur anhand der E-Mail-Adresse geschieht.
- Eine qualifizierte Signatur eines Antragstellers hat auf einem PDF oder PDF/A als Träger zu erfolgen. Die Antwort des GB-Amts hat auf einem PDF/A zu erfolgen (siehe GBV). Andere Formate werden nicht zugelassen, da sonst die Prüfung der Gültigkeit unter Berücksichtigung der vorhandenen Infrastruktur in der Praxis nicht gewährleistet werden kann.
- Eine Authentifizierung mittels SuisseID ist erprobt und kann angeboten werden.
- Eingaben dürfen nur über anerkannte Zustellplattformen, spezielle Webseiten sowie alternative Übermittlungsverfahren und bestehende Systeme mit Direktanbindung an ein Grundbuchsystem erfolgen.