grossenbacher
rechtsanwälte

SuisseID und Datenschutz

Haftung und Datenschutz im Umgang mit der SuisseID

lic. iur. Christian Leupi
Rechtsanwalt
MAS Business Information Technology

christian.leupi@gr-law.ch

Grossenbacher Rechtsanwälte AG
Zentralstrasse 44
6003 Luzern

T +41 41 500 56 56
F +41 41 500 56 57

Kurzübersicht Projekt SuisseID beim SAV

- Zusammenarbeit zwischen SAV und Quovadis.
- SuisseIDs für Anwälte und Kanzleipersonal zu günstigen Konditionen.
- Anwalts-SuisseID enthält zusätzlich das Merkmal «Rechtsanwältin/Rechtsanwalt» → kann z.B. für Zugangsberechtigungen eingesetzt werden.
- Ist mit dem Logo des jeweiligen Kantonalverbandes sowie mit einem Foto des Inhabers versehen.
- SAV informiert Mitglieder regelmässig, führt Roadshows durch und setzt sich für eine anwendergerechte Umsetzung des elektronischen Behördenverkehrs ein.

grossenbacher
rechtsanwälte

Haftungsgrundlagen

Gesetzliche Grundlagen – Art. 16 ZertES

Art. 16 Haftung der Anbieterin von Zertifizierungsdiensten
[1] Die Anbieterin von Zertifizierungsdiensten haftet der Inhaberin oder dem Inhaber des Signaturschlüssels und Drittpersonen, die sich auf ein gültiges qualifiziertes Zertifikat verlassen haben, für Schäden, die diese erleiden, weil die Anbieterin den Pflichten aus diesem Gesetz und den entsprechenden Ausführungsvorschriften nicht nachgekommen ist.
[2] Sie trägt die Beweislast dafür, den Pflichten aus diesem Gesetz und den Ausführungsvorschriften nachgekommen zu sein.
[3] Sie kann ihre Haftung aus diesem Gesetz weder für sich noch für Hilfspersonen wegbedingen. Sie haftet jedoch nicht für Schäden, die sich aus der Nichtbeachtung oder Überschreitung einer Nutzungsbeschränkung (Art. 7 Abs. 2) ergeben.

Haftungsgrundlagen

Gesetzliche Grundlagen – Art. 59a OR

Art. 59a Haftung für Signaturschlüssel
[1] Der Inhaber eines Signaturschlüssels haftet Drittpersonen für Schäden, die diese erleiden, weil sie sich auf das qualifizierte gültige Zertifikat einer anerkannten Anbieterin von Zertifizierungsdiensten im Sinne des Bundesgesetzes vom 19. Dezember 20032 über die elektronische Signatur verlassen haben.
[2] Die Haftung entfällt, wenn der Inhaber des Signaturschlüssels glaubhaft darlegen kann, dass er die nach den Umständen notwendigen und zumutbaren Sicherheitsvorkehrungen getroffen hat, um den Missbrauch des Signaturschlüssels zu verhindern.
[3] Der Bundesrat umschreibt die Sicherheitsvorkehrungen im Sinne von Absatz 2.

Haftungsgrundlagen

Zertifikatsanbieter

- Hauptrisiko beim Anbieter: mangelhafte technische Infrastruktur oder Organisationsmängel.
- Anbieter wird haftpflichtig, sofern er die gesetzlichen Vorschriften missachtet.
- Milde Kausalhaftung → Umkehr der Beweislast.
- Haftung gegenüber Zertifikatsinhaber und Dritten.
- Mögliche Anwendungsfälle: z.B. mangelhaftes Zertifikat, ungerechtfertigter Widerruf des Zertifikats, Vernachlässigung der Prüfpflichten im Rahmen der Ausstellung.

Haftungsgrundlagen

Anwender des Zertifikats

- Hauptrisiko beim Anwender: mangelhafte Sicherheitsvorkehren.
- Anwender wird haftpflichtig, wenn er seine gesetzlichen Verpflichtungen zur Verhinderung des Missbrauchs des Zertifikats verletzt.
- Ebenfalls milde Kausalhaftung → Umkehr der Beweislast, Glaubhaftmachen.
- Vermutung, dass eine elektronisch signierte Erklärung vom Inhaber des Zertifikats stammt → wenn Inhaber das Gegenteil behauptet, greift Vermutung, er habe seine Pflichten verletzt.
- Achtung: Je nach vertraglicher Vereinbarung zwischen Anbieter und Vertragspartner gelten allenfalls weitergehende Haftungsregeln!

Praktische Fragen zur Haftung

Missbrauch

- Sicherheitsvorkehren:
  - SuisseID nicht Dritten anvertrauen. Soweit zumutbar auf sich tragen oder wegschliessen.
  - Bei Verlust oder Diebstahl umgehend Ungültigerklärung beantragen.
  - PIN dürfen sich nicht auf persönliche Angaben beziehen.
  - PIN sicher und getrennt von der SuisseID aufbewahren.
  - Umgehendes ändern der PIN, sofern Verdacht oder Gewissheit besteht, dass ein Dritter davon Kenntnis hat.

- Fazit: Nicht Dritten aushändigen, bei Verlust sofort sperren lassen, keine "persönliche" PIN, sofortige PIN-Änderung bei Gefahr der Kompromittierung.

- Offene Fragen: z.B. was sind persönliche Angaben? Zugriff über Keylogger und Backdoors?

Praktische Fragen zur Haftung

Stellvertretung

- Achtung: Keine Stellvertretung über Weitergabe der SuisseID sowie der Zugangsdaten an Dritte!
- Wirkung von auf dem Zertifikat festgehaltenen Einschränkungen? Wie kann der Vertragspartner diese überprüfen?
- Gesetzgeber ist davon ausgegangen, dass die allgemeinen Regeln zur Stellvertretung gemäss Art. 32 ff. OR genügen und kein zusätzlicher Regelungsbedarf besteht.

Praktische Fragen zur Haftung

Zustellprobleme im elektronischen Behördenverkehr

- Disclaimer auf Behörden-Webseiten:
  - Achtung: Es ist Sache der Verfahrensbeteiligten, den Versand der Eingabe rechtzeitig zu veranlassen. Es kann nicht ausgeschlossen werden, dass die unten aufgeführten Kontaktformulare beispielsweise aus technischen Gründen oder wegen Revisionsarbeiten an dieser Website vorübergehend nicht zur Verfügung stehen. Für Eingaben, die aufgrund eines solchen Ausfalls verspätet eingereicht werden, wird keine Haftung übernommen.
- Ist Behörde tatsächlich nicht für "ihre" Zustellplattform verantwortlich?
- Was halten die Geschäftsbedingungen der Zustellplattformen dazu fest?

Praktische Fragen zur Haftung

Signaturzertifikat vs. Authentisierungszertifikat

- SuisseID enthält ein Signaturzertifikat ("digitale Unterschrift") sowie ein Authentisierungszertifikat ("Login-Zertifikat").
- Für das Signaturzertifikat (qualifizierte Signatur) gelten Art. 16 und 17 ZertES sowie Art. 59a OR.
- Wie sieht es mit dem Authentisierungszertifikat aus? → Dieses fällt nicht unter Art. 16 ZertES, da fortgeschrittenes Zertifikat.
- Haftung des Zertifikatanbieters? → SuisseID-Anbieter müssen Musterhaftungsklausel in ihre AGB übernehmen.
- Allerdings: Haftungsbegrenzung auf CHF 10'000.00 pro Schadensfall.

Praktische Fragen zur Haftung

Fazit

- Einhalten der Sicherheitsmassnahmen (z.B. PIN nicht an Dritte aushändigen, SuisseID sicher verwahren) stellt nicht allzu hohe Anforderungen an Benutzer, müssen zudem nur glaubhaft gemacht werden.

- Allerdings: Werden diese eher rudimentären Massnahmen der aktuellen und zukünftigen Bedrohungslage gerecht (Stichwort: Trojaner, Keylogger, Backdoors etc.)? Könnte ein Gericht zum Schluss kommen, dass auch Abwehr gegen Trojaner etc. gegeben sein muss?

- Achtung: Authentisierungszertifikat hat keine erhöhte rechtliche Bindungswirkung (≠ elektronische Unterschrift).

Tipps zur sicheren Anwendung

- Technische Massnahmen: Betriebssystem auf aktuellem Stand halten; Virenschutz installieren und aktuell halten; Schutz gegen Schadprogramme etc.

- Organisatorische Massnahmen: SuisseID nicht an Dritte aushändigen; keine «sprechende» PIN; PIN und SuisseID getrennt aufbewahren; SuisseID bei Diebstahl oder Verlust unverzüglich revozieren etc.

- Rechtliche Massnahmen: Check Nutzungsbestimmungen der Anbieter; Prüfung der AGB sofern SuisseID zur Authentisierung eingesetzt wird (Login etc.).

Datenschutz und Vertraulichkeit

Grundsätze

- Art. 14 ZertES → Nur Daten bearbeiten, welche zur Erfüllung der Aufgaben notwendig sind und keinen Handel mit diesen Daten betreiben; ansonsten Verweis auf DSG.

- «…zur Erfüllung ihrer Aufgaben…» → Grenze der zulässigen Datenbearbeitung enger gezogen als DSG. Offene Fragen:
  - Sind die Aufgaben der Anbieter gesetzlich klar definiert?
  - Kann Einwilligung in weitergehende Bearbeitung erfolgen?

- «…mit diesen Daten keinen Handel betreiben…» → Adresshandel somit selbst dann ausgeschlossen, sofern betroffene Person ihre Einwilligung geben würde?

Datenschutz und Vertraulichkeit

Personendaten auf der SuisseID

- Die SuisseID enthält minimal lediglich wenige persönliche Attribute (Name der Person) sowie eine eindeutige Seriennummer («SuisseID-Nummer»).
- Übrige Merkmale, sog. Spezifische Attribute, sind beim IDP-Service («Identity Provider») des SuisseID-Anbieters (z.B. Quovadis) gespeichert, also nicht direkt auf der SuisseID abgelegt.
- Freigabe dieser Daten geschieht immer über Authentisierung mittels SuisseID.

Datenschutz und Vertraulichkeit

Zugriff auf Daten durch Dienstleistungsanbieter – Bereitstellen Daten durch SuisseID-Anbieter

- SuisseID lässt die Abfrage sämtlicher Merkmale einer Person, wie sie auch auf amtlichen Ausweisen vorhanden sind, beim SuisseID-Anbieter zu → z.B. Name, Geburtsdatum, Heimatort, Nationalität, Geschlecht.
- Dazu noch vom Geburtsdatum abgeleitete Informationen, wie z.B. Alter in Jahren, ist Alter über 16 bzw. ist Alter über 18.
- Auskunft an Dienstleistungsanbieter geschieht über IDP-Service («Identity Provider») des SuisseID-Anbieters (z.B. Quovadis).
- Abfrage dieser Merkmale setzt das explizite Einverständnis des Benutzers voraus → Auflistung der Merkmale, Akzeptieren-Button

Datenschutz und Vertraulichkeit

Zugriff auf Daten durch Dienstleistungsanbieter – ausserhalb der SuisseID-Infrastruktur bereitgestellte Informationen

- SuisseID kann auch für die Abfrage extern bzw. auf der SuisseID zusätzlich hinterlegter Merkmale (z.B. im Falle der SAV-SuisseID das Merkmal «Rechtsanwalt») verwendet werden.
- Anwendungsbereich → berufliche Qualifikation, Mitgliedschaften etc.
- Auskünfte über berufliche Qualifikation oder Mitgliedschaften können auch durch externe «Auskunftsstellen» realisiert werden.
- Abfrage dieser Merkmale setzt ebenfalls das explizite Einverständnis des Benutzers voraus (Ausnahme: elektronische öffentliche Register).

grossenbacher
rechtsanwälte

Datenschutz und Vertraulichkeit

Fazit Datenschutzkonzept SuisseID

- Zurückhaltende Datenspeicherung auf SuisseID. Zugriff auf Daten bei IDP-Service oder externem Anbieter muss über SuisseID autorisiert werden.
- Engere rechtliche Rahmenbedingungen als DSG → enger gefasste Zweckbestimmung, Verbot Datenhandel.
- Achtung: gilt nur für Zertifikatsdiensteanbieter → Datenbearbeitung durch Empfänger der freigegebenen Daten (z.B. Online-Shop etc.) ist durch das DSG bzw. durch die vertragliche Vereinbarung mit dem Empfänger geregelt.
- Achtung: Externe «Auskunftsstellen» dürften eher nicht unter die Spezialnorm von Art. 14 ZertES fallen → auch in diesem Falle DSG und individuelle vertragliche Vereinbarung massgebend.

Datenschutz und Vertraulichkeit

Verschlüsselungszertifikat – Funktion

- QuoVadis bietet SuisseID-Inhabern ein Secure E-Mail Zertifikat an, welches zusätzlich zur Signierung von E-Mails und elektronischen Daten auch die Verschlüsselung ermöglicht.
- Dieses Angebot wird allerdings nicht sehr offensiv vermarktet.
- Sowohl Absender als auch Empfänger benötigen ein Secure E-Mail Zertifikat.
- Elektronische Nachricht als solche wird verschlüsselt, nicht nur sicherer Transportweg → E-Mail liegt nicht im Klartext vor → im Unternehmensbereich allenfalls problematisch (Stellvertretung, Ausscheiden Mitarbeitende).

Datenschutz und Vertraulichkeit

Verschlüsselungszertifikat – praktische Relevanz

- Grundsätzlich ein tauglicher Ansatz zur vertraulichen Kommunikation per E-Mail.
- Setzt allerdings voraus, dass Absender und Empfänger ein entsprechendes Zertifikat besitzen → also keine Lösung, die auf einseitige Initiative des Senders eingesetzt werden kann.
- Achtung: Muss das Zertifikat revoziert werden, sind E-Mails allenfalls nicht mehr lesbar, sofern nicht im Klartext abgespeichert.

Datenschutz und Vertraulichkeit

Zustellplattformen

- Relevant für den elektronischen Behördenverkehr → ZPO setzt die Zustellung über Zustellplattform voraus.
- Akkreditiert sind momentan Privasphere und Incamail (Lösung Kanton Bern ist im Akkreditierungsprozess).
- Nicht Nachricht an sich ist verschlüsselt, sondern Transportweg der Daten (analog E-Banking).
- Zustellplattform erlaubt, den Nachweis der Sendung zu erbringen.
- Achtung: Im elektronischen Rechtsverkehr herrscht Zugangsprinzip → Ich benötige Bestätigung der Zustellplattform, dass Sendung eingegangen ist.

Datenschutz und Vertraulichkeit

Fazit

- SuisseID ist als datenschutzfreundliches Konzept ausgearbeitet.
- Engere Schranken für Zertifikatsdiensteanbieter hinsichtlich Datenbearbeitung; Anwender hat Hoheit über den Transfer von Personendaten an Dritte.
- Allerdings ist es weiterhin am Anwender, im Einzelnen zu prüfen, wohin die Daten gehen und in welcher Form diese von Dritten bearbeitet werden → Dies wird von der gesetzlichen Regelung im ZertES nicht umfasst.

grossenbacher
rechtsanwälte

Besten Dank für Ihr Interesse!

lic. iur. Christian Leupi
Rechtsanwalt
MAS Business Information Technology

christian.leupi@gr-law.ch

Grossenbacher Rechtsanwälte AG
Zentralstrasse 44
6003 Luzern

T +41 41 500 56 56
F +41 41 500 56 57