Leere Versprechen, ein vergrätzter Partner – und ein riskanter Kurs

Sollte die elektronische ID bei der Abstimmung am Sonntag durchkommen, dann dürfte Swiss Sign die Anbieterin werden. Doch die jüngere Geschichte der Firma wirft Fragen auf.

Eine Recherche von Adrienne Fichter und Patrick Seemann, 01.03.2021

Es war der typische Managersprech, den der CEO der Firma Swiss Sign – voraussichtliche Anbieterin der E-ID – vorletzte Woche in der «SRF Arena» von sich gab. Seine Firma sei ein langjähriger «Trust Service Provider», sagte Markus Naef – also ein Unternehmen, das für den geschäftlichen Austausch wichtige Dienstleistungen wie etwa rechtsgültige elektronische Signaturen anbietet. Allfällige Alternativen zur E-ID wie etwa die Suisse ID, das Vorgängerprojekt des Bunds, seien tot. Und: Als Privatunternehmen könne man anders als der Staat «agil» sein und «den Markt penetrieren».

Dabei verschweigt Naef einiges, wie Recherchen der Republik und Gespräche mit ehemaligen und aktuellen Mitarbeiterinnen zeigen.

Etwa die Tatsache, dass das Unternehmen Swiss Sign lange Zeit nur auf dem Papier ein umfassender Trust Service Provider war. Technologische Möglichkeiten wie die elektronische Signatur wurden in den letzten Jahren zwar immer wieder versprochen – aber lange nicht geliefert. Das verärgerte viele Kunden. Und auch Partner sind verstimmt.

Das wird jetzt im Abstimmungskampf zum neuen E-ID-Gesetz sichtbar, der am 7. März an der Urne entschieden wird. Die Swisscom, die eigentlich am Konsortium Swiss Sign beteiligt ist, kündigte diese Woche die Gründung eines neuen Unternehmens an: Dieses tritt unter dem Namen Trust Services fast 1:1 als Konkurrenz gegen Swiss Sign an. Für Swiss Sign ist das ein öffentlicher Schlag ins Gesicht.

Wie agil ist die Firma also? Und wie kundenorientiert ihr Angebot?

Suisse ID war beliebt

Ob sie nun «tot» ist oder doch eher ein «Flop» war, wie es Justizministerin Karin Keller-Sutter in derselben Sendung ausdrückte – die alte Suisse ID war nicht so schlecht, wie sie teilweise dargestellt wird. Das öffentlich-private Gemeinschaftsprojekt war bei Unternehmenskunden sehr beliebt, wie verschiedene Swiss-Sign-Mitarbeitende sagen.

(Damit Sie beim Lesen kein Durcheinander kriegen: Die alte Lösung hatte den französischen Namen, das jetzige Produkt der Firma Swiss Sign den englischen.)

Die Suisse ID bot einerseits ein hohes Sicherheitsniveau. Für die Ausstellung musste man persönlich am Postschalter vorbeikommen. Die Suisse ID bot etwa Mitarbeiterinnen von Unternehmen eine stark verifizierte Identität und berechtigte sie, im Namen der Firma Dokumente zu unterzeichnen – für Bankgeschäfte etwa ist das wichtig.

Die Suisse ID hatte zudem eine Funktion, auf die manche Kunden später vergeblich warteten: die elektronische Signatur. Das ermöglicht es beispielsweise einer Einkäuferin, im Namen ihrer Firma Bestellungen aufzugeben und Verträge zu unterschreiben, die eine «qualifizierte Schriftlichkeit» erfordern, also die juristisch höchste Sicherheitsstufe. Die Suisse ID war also de facto digitaler Pass und rechtsgültige Unterschrift in einem.

Diese Funktionen seien für Unternehmenskunden viel relevanter als die Integration eines simplen Benutzerkontos, wie sie die Swiss-Sign-Ersatzlösung Swiss ID bietet, sagen mehrere ehemalige Vertriebsmitarbeitende. Auch ein ehemaliger Product Manager sagt: «Die Signaturfunktion ist das, was die Unternehmen wirklich interessiert, nicht die Swiss ID.» Tatsächlich nutzten verschiedene Kundinnen wie die Zurich, das Börsenunternehmen SIX, die Finma, sämtliche Banken oder etwa der Schweizer Anwaltsverband die Suisse ID. Letzterer bedauerte gar in einem Schreiben, dass ihm mit deren Einstellung wichtige Funktionen verloren gingen.

Die Suisse ID wurde per April 2020 eingestellt. CEO Markus Naef begründete dies damit, dass die Suisse-ID-Karte nicht mehr den regulatorischen Anforderungen genügt habe und eine Weiterführung dieser Technologie massiver Investitionen bedurft hätte.

Die Unternehmenskunden wurden zwar informiert über das Ablaufdatum. Man versprach eine baldige Ersatzlösung. Nur: Diese Ersatzlösung existiert bis heute nicht.

Signaturlösungen erst jetzt spruchreif

Auf einer Unterseite der Swiss-Sign-Website – die nicht im Menü verlinkt und damit nur mit Suchmaschinen erreichbar ist – wird darauf hingewiesen, dass «man mit Hochdruck» am Nachfolgeprojekt der Suisse-ID-Signatur arbeite.

Lange Zeit fehlte den Unternehmenskunden ein wichtiges Arbeitsinstrument im täglichen digitalen Schriftenverkehr. Verschiedene Angestellte aus dem Sales-Bereich mussten sich darum nach eigener Aussage regelmässig vor den verärgerten Unternehmenskundinnen verantworten.

Im Dezember 2020 konnte Swiss Sign endlich eine Art Ersatz bieten – eine technische Lösung des Partnerunternehmens Skribble. Doch deren Umsetzung bei der Swiss ID entspricht noch nicht dem hohen Sicherheitsniveau der alten Suisse ID.

Das müsse sie auch nicht, sagt CEO Naef, der in einem ausführlichen Gespräch Stellung nimmt zu den Vorwürfen: «Nicht sämtliche Verträge verlangen aufgrund der gesetzlichen Anforderungen eine qualifizierte Signatur. Die meisten Verträge können auf Stufe ‹fortgeschritten› rechtsgültig gezeichnet werden.» Naef weist zudem darauf hin, dass man nicht untätig gewesen sei in den letzten zwei Jahren: «Wir haben mit dem Jura, St. Gallen und Fribourg Kantone, denen wir auch qualifizierte elektronische Signaturen bieten.»

Doch eine standardisierte, gleichwertige Nachfolgelösung zur Suisse ID für Bürgerinnen und Unternehmenskunden fehlt bis zum heutigen Zeitpunkt.

Google nennt Swiss Sign als schlechtes Beispiel

Nicht nur bei den elektronischen Signaturen haperte es. Bei einem umsatzträchtigen Standbein von Swiss Sign treten ebenfalls Probleme auf: im Zertifikatsgeschäft. Auch hier hinterlässt die Firma keinen guten Eindruck.

Dieses Geschäft, damals Infrastruktur der Post, erbte die Swiss Sign bei ihrer Gründung im Jahr 2017. Doch offenbar wurde es in den vergangenen Jahren vernachlässigt, wie öffentlich in verschiedenen Foreneinträgen und Dokumenten nachzulesen ist und worauf auch der IT-Security-Experte Florian Forster hinweist.

Ein Artikel des Technologiemagazins «ZDNet» vom 13. Oktober 2019 kommt zu einem vernichtenden Urteil: Gemäss einer Studie gehören Swiss Sign und Quo Vadis zu den weltweit problematischsten sogenannten Certification Authorities.

Das bedeutet: Sie stellen falsche oder fehlerhafte SSL-Zertifikate für die verschiedenen Internet-Browser aus, weil diese nicht den Standards der Browserhersteller Chrome, Mozilla und Edge entsprechen. Oft handelte es sich um Kleinigkeiten wie falsch geschriebene Kantonsnamen, teilweise wurden aber auch kritischere Elemente falsch definiert. Im Rahmen der Studie wurde primär bemängelt, dass sich die Fehler über die Zeit wiederholen.

Kurz: Das Zertifikatemanagement von Swiss Sign hat gemäss der Studie Verbesserungspotenzial.

Brisant ist, dass Google schon 2019 Swiss Sign in seinen Präsentationen als Beispiel dafür verwendete, wie man es *nicht* machen soll (Folien 11 und 35). Im Herbst 2019 wurde von Google ausserdem gedroht, Swiss Sign als Zertifikatsanbieterin nicht länger zuzulassen. Auch im Forum der Mozilla Foundation (der Stiftung, die den Browser Firefox betreibt) werden die fehlende Erreichbarkeit, die langsame Reaktion des Swiss-Sign-Teams und andere Mängel kritisiert.

Ich will es genauer wissen: Was sind digitale Zertifikate und worum geht es bei dieser Studie?

Digitale Zertifikate stehen hinter jeder sicheren Internetverbindung und stellen gleichermassen die Vertraulichkeit der Verbindung (kann niemand mithören?) wie auch die Authentisierung der Gegenseite sicher (kommuniziere ich wirklich mit dem Webserver, den ich meine?). Technisch gesehen können solche Zertifikate sehr einfach ausgestellt werden, entsprechend wichtig ist, dass diese vertrauenswürdig sind. Dafür sorgen die sogenannten Certification Authorities (CA), welche digitale Zertifikate ausstellen (und digital unterschreiben). Die Echtheit der Certification Authorities selbst wird durch besondere Root-Zertifikate bescheinigt, welche Teil jedes Betriebssystems beziehungsweise jedes Browsers sind und quasi die Basis der Authentisierung bilden.

Die Sicherheit im Internet steht und fällt also mit der Vertrauenswürdigkeit der Certification Authorities und damit, dass diese sich beim Ausstellen der Zertifikate an die geltenden Regeln halten. Die Certification Authorities haben sich im CA/Browser Forum zusammengeschlossen, einer Industrievereinigung, welche sich primär um gemeinsame Richtlinien und deren Ein-

haltung kümmert. Eine 2019 durchgeführte Studie zeigt jedoch auf, dass verschiedene Certification Authorities Geschäftsmodelle verwenden, welche die Richtlinien des Forums und andere für die Sicherheit im Internet massgebliche Standards teilweise ignorieren. Republik-Recherchen zeigen: Auch Fehler bei der Vergabe von Zertifikaten sind häufiger, als man das für eine solch hochkritische Komponente erwarten würde. Für den untersuchten Zeitraum von April 2017 bis Februar 2021 sind für Swiss Sign knapp 30 Einträge vorhanden, davon alleine 5 für 2021 – und das bei einem Marktanteil von unter 0,1 Prozent. (Im Vergleich dazu finden sich für IdenTrust mit einem Marktanteil von 52 Prozent 35 Einträge und für DigiCert mit einem Marktanteil von 20 Prozent 194 Einträge).

CEO Naef habe das Zertifikatsgeschäft nicht gross interessiert und er habe daher wenig investiert, sagen Insider zur Republik. Es handelt sich um ein aufwendiges, mühsames und komplexes Geschäftsfeld. Man bräuchte Spezialistinnen, die jeden Tag die Foren beobachten und sich mit den spezifischen Anforderungen auseinandersetzen. Doch ausgerechnet diese Einheit war von Fluktuation betroffen.

Der CEO kann die Vorwürfe nicht nachvollziehen: «Das Zertifikatsgeschäft ist enorm wichtig, wir wachsen hier in den letzten drei Jahren 18 Prozent pro Jahr», sagt er. Man habe viele Kunden, auch im Ausland, investiere viel und arbeite mit der Firma Libc an einer umfassenden Zertifikatsplattform. Die Zertifizierung der Prozesse würde monatelange Vorlaufzeit benötigen.

Ausserdem musste Naef nach eigenen Angaben die Altlasten der Vergangenheit ausräumen: «Viele der fehlerhaften Zertifikate stammten noch aus den Jahren 2015 bis 2017, vor der Gründung der SwissSign Group AG (2018) und damit auch lange vor der Ära des heutigen Managements. Seit rund zwei Jahren ist die SwissSign Group AG daran, die Fehler aus den Jahren 2015 bis 2017 zu beheben.»

Alles auf die Karte E-ID

In der Ära Naef seit 2018 gab es bei Swiss Sign einen technologischen Braindrain. Kritikerinnen verliessen das Haus oder mussten dies tun. Dass die Warnungen über technologische Versäumnisse so lange in den Wind geschlagen worden sind, erklären sich viele mit dem autoritären Führungsstil von Naef. Zudem habe der Verwaltungsrat seine Aufsichtspflicht ebenfalls nicht genügend wahrgenommen und die Produkte der Swiss Sign teilweise nicht verstanden und nicht hinterfragt.

«Auch diese Behauptungen kann ich nicht nachvollziehen», sagt Naef. «Ich pflege ein regelmässiges, gutes und transparentes Verhältnis zum Verwaltungsrat. Diverse Konsortialpartner sind zudem in diversen Projekten beteiligt. Allfällige Missstände würden ihnen sofort auffallen.»

Unbestritten jedenfalls ist – egal, ob man mit Kritikern oder Unterstützerinnen spricht: Der Fokus auf die Swiss ID und die Hoffnung auf die E-ID führten innerhalb der Swiss Sign zu einer Ressourcenverlagerung. Man bewegte sich weg vom Geschäftskundengeschäft hin zum Endkundengeschäft. Ein ehemaliger Mitarbeiter drückt es so aus: «Naef hat alle Karten auf die Vermarktung der Swiss ID und E-ID gesetzt, nicht mit dem Referendum gerechnet und die anderen Standbeine wie Signaturen und Zertifikatsgeschäft etwas vernachlässigt.»

Zumindest ein Konsortialpartner der Swiss Sign wendet sich indes ab: Swisscom. Das Verhältnis zwischen den beiden Firmen war von Anfang an

kompliziert. Auf dem Papier ist das Telecomunternehmen zwar noch Partner. Doch einige gemeinsame Projekte sind eingestellt worden. Die Ankündigung der Swisscom von letzter Woche, künftig ein eigenes Trust-Services-Geschäft zu betreiben, könnte für Swiss Sign zu keinem schlechteren Zeitpunkt kommen. CEO Markus Naef sagt auf Anfrage, dass «Swisscom damit ein bestehendes Geschäft in eine separate Gesellschaft auslagern wolle». Er wollte diesen strategischen Schritt der Swisscom jedoch nicht weiter kommentieren.

Ein ehemaliger Mitarbeiter verteidigt den CEO und schiebt die Schuld an den gescheiterten Projekten Swisscom zu. Das Telecomunternehmen verfolge eigene kommerzielle Interessen und es verhalte sich bockig.

Ob bockig oder nicht – Swiss Sign ist auch abhängig vom Telecomriesen, was den technologischen operativen Betrieb anbelangt. So arbeitet der Partner von Swiss Sign, Skribble, bei der Lieferung der Signaturzertifikate wiederum mit Swisscom zusammen. Um es mit einem Bild zu beschreiben: «Skribble ist der Hersteller des Velos, Swisscom liefert das wichtigste Stück, die Fahrradkette.»

Wie es für Swiss Sign weitergeht? Das hängt auch vom Ausgang der Abstimmung zur E-ID ab. Mindestens 50 Millionen Franken haben die Partner wie CS, ZKB, SBB und Post in Swiss Sign investiert, wie verschiedene Quellen bestätigen. Mit den Worten eines Insiders: «Es ist leider viel verbrannte Erde da.»

Vielfach ist die Rede davon, dass private Unternehmen pauschal bessere Lösungen liefern. Der Fall Swiss Sign zeigt, dass dies nicht immer der Fall ist.