SuisseID: Fokus auf das Wesentliche

Urs Bürge, Christof Dornbierer

Für die SuisseID ist Interoperabilität eines der zentralen Erfolgskriterien. Die Anschubfinanzierung durch die konjunkturellen Stabilisierungsmassnahmen des Bundes bedeutete eine einmalige Chance, einer schweizweit standardisierten elektronischen Identität das nötige Momentum zu verleihen. Durch die zeitliche Begrenzung dieser Fördermassnahme ergab sich für die Umsetzung ein hoher Termindruck. Dieser wurde von Projektprotagonisten geschickt genutzt: Sie holten die diversen Stakeholders an einen Tisch und brachten sie dazu, ihre unterschiedlichen Interessen in einer denkwürdigen, mehrtägigen Klausur pragmatisch auf den zentralen gemeinsamen Nenner zu bringen, indem sie ihre Ansprüche auf das Notwendigste reduzierten. Mit diesem einmaligen Vorgehen konnte in kürzester Zeit der nötige Standard gefunden werden, und auch im weiteren Verlauf der Spezifikation der SuisseID beschränkte man sich auf die absolut schlankste Lösung. Diese verzichtet anfänglich auf diverse Features, erlaubt es aber im Gegenzug, diese später nach Bedarf modular hinzuzufügen, und stellt gerade damit auch eine sehr generische Lösung dar.

Urs Bürge
Vom SECO beauftragter Teilprojektleiter SuisseID, Inhaber der Urs Bürge Beratung GmbH
mail@ursbuerge.ch

Christof Dornbierer
CTO und Mitglied der Geschäftsleitung bei AdNovum Informatik AG
christof.dornbierer@adnovum.ch

Im Sommer 2009 sah man im Rahmen eines dritten Pakets von konjunkturellen Stabilisierungsmassnahmen plötzlich die Möglichkeit, auch ein Set von Massnahmen aus der Informations- und Kommunikationstechnologie (ICT) darin unterzubringen. Dank den im Eidgenössischen Volkswirtschaftsdepartement (EVD) schon einige Zeit laufenden Arbeiten für eine E-Economy-Strategie wusste die Departementsvorsteherin Doris Leuthard, dass es in diesem Bereich in mehreren Punkten einen Aufholbedarf gab. Entsprechend sollte das ICT-Teilpaket zu denjenigen Massnahmen gehören, mit denen der Bundesrat die Zeit der Krise nutzen wollte, um optimale Rahmenbedingungen für den künftigen Aufschwung der Wirtschaft vorzubereiten.

Aus den vorangegangenen Strategiearbeiten konnten verschiedene Massnahmen zur Förderung der E-Economy in der Schweiz abgeleitet werden. Die Herausforderung bestand darin, innert Tagen ein Paket zu definieren, das alle Rahmenbedingungen des Stabilisierungspakets erfüllte, genügend attraktiv und konkret war, um in einer Krisenzeit vom Parlament Geld zu erhalten, aber auch noch genügend offen, um sich den Bedürfnissen aller Stakeholders anzupassen. Und schliesslich musste es in rechtlicher, technischer und kommerzieller Hinsicht auch tatsächlich realisierbar sein. Dabei war die prägendste Einschränkung die, dass aus Sicht des Staates die ganze Übung Ende 2010, also in eineinhalb Jahren, beendet sein musste. Entsprechend dem Charakter einer kurzfristigen konjunkturellen Stimulierung würde es über diese Zeitlimite hinaus weder eine gesetzliche Grundlage geben, noch würden Finanzmittel zur Verfügung gestellt.

Signieren und Nachweisen

Man war sich rasch einig darüber, dass mit dem Paket ein schon oft erkannter und geschilderter Mangel behoben werden sollte, nämlich das Fehlen einer Infrastruktur für einen sicheren elektronischen Identitätsnachweis und den im elektronischen Geschäftsverkehr ebenso wichtigen elektronischen Nachweis einer beruflichen Funktion (Zulassung, Vertretungsbefugnis, Amt usw.).

Der elektronische Geschäftsverkehr konnte in der Schweiz nicht in dem Masse Fuss fassen, wie man sich das vorgestellt hatte. Sowohl im privaten Bereich wie auch im Behördenverkehr läuft die verbindliche Kommunikation – Bestellungen, Rechnungen, Eingaben, Verfügungen – in der Mehrzahl der Fälle noch auf dem Papierweg ab. Zwar gibt es in der Schweiz schon seit ein paar Jahren das Signaturgesetz (ZertES) und Zertifikatsprodukte für die rechtsgültige elektronische Signatur. Diese konnten sich jedoch auf dem Markt nicht im gewünschten Masse durchsetzen. Einerseits ist es generell schwierig, eine solche Basisinfrastruktur, die erst in Kombination mit mehreren Anwendungen attraktiv und rentabel ist, auf dem Markt zu etablieren. Andererseits ist im elektronischen Geschäftsverkehr in vielen Fällen nicht die elektronische Signatur gefragt – eine rechtlich verbindliche Unterschrift wird bei vielen Geschäftstransaktionen gar nicht vorausgesetzt –, sondern die sichere Authentisierung (Identitätsnachweis) gegenüber einer Anwendung im Netz, zum Beispiel im E-Banking oder E-Shopping. Vorbedingung für eine breite Anwendung des elektronischen Identitätsnachweises ist ein einheitliches Authentisierungsmerkmal; bisher hat sich jedoch noch kein solches etabliert.

Viele wirtschaftliche und behördliche Prozesse basieren darauf, dass sich eine Person ausweisen kann bezüglich ihrer Identität, oft aber auch hinsichtlich einer bestimmten Eigenschaft. Schliesslich sind im elektronischen Wirtschaftsraum die Handelnden meist nicht einfach natürliche Personen, sondern sie vertreten eine juristische Person, nehmen eine bestimmte Funktion (z.B. Registerführer) ein oder agieren mit bestimmten, von den zuständigen Stellen vergebenen Befähigungen (z.B. Notar oder Arzt). Nur wenn sich solche Funktionen oder Kompetenzen auch über das Netz oder in elektronischen Dokumenten einfach und glaubhaft beweisen lassen, kann das notwendige Vertrauen für die elektronische Abwicklung von Geschäften auch in heikleren Fällen aufge-

baut werden. Mit dem ICT-Teil des dritten Stabilisierungspakets sollten genau diese Probleme angegangen und der Lösung einen deutlichen Schritt nähergebracht werden.

Das dritte konjunkturelle Stabilisierungspaket ging schliesslich am 10. August 2009 vom Bundesrat ans Parlament, mit einem ICT-Teil von 25 Mio. Franken, wovon 17 Mio. für die Subventionierung des Kaufs der SuisseID vorgesehen waren. Mehrere Teile des Pakets waren umstritten, so auch der ICT-Teil, bei dem es zwischendurch von einzelnen Stimmen abhing, dass er nicht entfernt wurde. Schliesslich wurde das Paket am 25. September 2009 vom Parlament stark reduziert verabschiedet, der ICT-Teil aber hatte überlebt.

Hohe Anforderungen, kluge Umsetzung

Die SuisseID sollte ihrem Inhaber also die elektronische Unterschrift sowie den Identitätsnachweis ermöglichen. Zudem sollte eine Infrastruktur geschaffen werden, die es erlaubt, aus einer vertrauenswürdigen Quelle Informationen über beliebige Eigenschaften einer Person zu beziehen, wie Geburtsdatum, Adresse, Funktion/Qualifikation usw.

Die Projektleitung stand vor der anspruchsvollen Aufgabe, innert extrem kurzer Zeit ein Produkt mit allen Stakeholders zusammen zu designen, zu spezifizieren und bereitzustellen und dabei die Rahmenbedingungen, Anforderungen und Erwartungen auf allen Ebenen laufend zu berücksichtigen und einigermassen konsistent zu erfüllen.

Auf der politischen Ebene mussten die Massnahmen unter anderem einfach, verständlich, griffig, sofort umsetzbar und sofort wirksam sein. Potenziell problematische und komplexe rechtliche Themen musste man deshalb nach Möglichkeit umschiffen. So sollte beispielsweise der Persönlichkeitsschutz nicht tangiert werden, obwohl es um Identitätsnachweis ging und damit um die Speicherung und Übermittlung personenbezogener Daten. Dies löste man mit dem Prinzip der Benutzerzentrierung: Es sollten keine Informationen über den Benutzer herumgereicht werden können, ohne dass dieser dazu explizit und bei jedem Zugriff sein Einverständnis gibt.

Aus rechtlicher Sicht musste die Lösung mittel- und langfristig ohne gesetzliche Grundlage auskommen; das Stabilisierungspaket war als Notrecht befristet, eine eigene gesetzliche Grundlage liess sich in der vorgegebenen Zeit nicht schaffen. Dies hatte einen starken Einfluss auf das Design. Die ganze Lösung musste privatwirtschaftlich getragen sein, der Staat konnte nur in der ersten Phase mithelfen und subventionieren.

	Phase	Anfang	Abschluss	Dauer
1	Pol. Entscheid	01.06.2009	04.09.2009	14w
2	Design	01.06.2009	16.10.2009	20w
3	Spezifikation	03.08.2009	26.02.2010	30w
4	Produktion	17.11.2009	03.05.2010	24w
5	Marketing, PR	01.06.2009	28.05.2010	52w

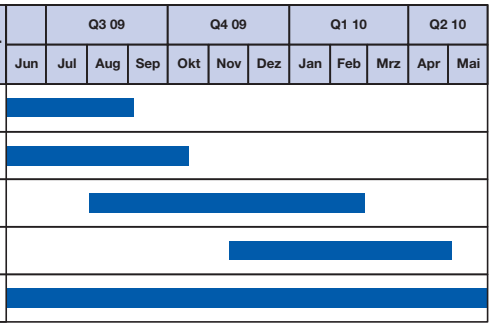

Abbildung 1: SuisseID: sich überlappende Projektphasen

Auf operativer Ebene mussten die in der Bundesverwaltung vorgegebenen Entscheidungswege und Projektabwicklungsverfahren berücksichtigt werden.

Selbstverständlich musste das Produkt in der vorgegebenen Zeit technisch machbar sein und trotzdem höchsten Sicherheitsanforderungen genügen. Die privaten Anbieter brauchten schliesslich ein kommerziell attraktives Produkt, für das die Kunden bereit waren, Geld und Zeit zu investieren.

Risiken gemeinsam meistern

Damit die SuisseID unter diesen Rahmenbedingungen rechtzeitig bereitgestellt werden konnte, waren ein paar Grundsätze und Verhaltensmuster essenziell, für die man sich teilweise explizit entschieden hat, die sich aber zu einem Teil auch einfach durchgesetzt haben:

Einfachheit: Im Zweifelsfall wird auf allen Ebenen immer die einfachere, standardisierte, etablierte Lösung für ein Problem gewählt.

Modularität: Das Produkt ist auf allen Stufen modular und mit echten Sollbruchstellen versehen. So war man beispielsweise bis kurz vor Auslieferung darauf gefasst, dass man den Teil Identity-Provider-Service (IdP) aus politischen Gründen hätte weglassen müssen, und hielt die Option aufrecht, auch ohne IdP noch ein vertretbares Produkt anzubieten.

Paralleles Vorgehen: Es wäre unmöglich gewesen, in diesem Bereich und in der vorgegebenen Zeit etwas Brauchbares rein sequenziell nach den vorgegebenen Verfahren zu realisieren. Jede Phase wurde vorzeitig in Angriff genommen, in vollem Bewusstsein, dass man sich auf unsicherem Terrain bewegte und das Risiko einging, dass die Investition teilweise oder ganz abgeschrieben werden musste. So mussten zum Beispiel die Zertifikatsanbieter schon vor der Veröffentlichung der Spezifikationen Zertifikatsträger bestellen können.

Risikobereitschaft und Vertrauen: Alle Beteiligten auf allen Stufen mussten bereit sein, ein beträchtliches Mass an Risiko zu tragen und gleichzeitig den anderen Beteiligten zu vertrauen. Innert kürzester Zeit haben sich Dutzende von Akteuren um das Vorhaben geschart und auf allen Stufen Verantwortung übernommen. Häufig wurden die formellen Erfordernisse, seien es Aufträge oder Verträge, erst verspätet erfüllt. Möglich und vertretbar war das nur, weil die Risiken nicht verneint oder verschwiegen, sondern laufend offengelegt, dokumentiert und aktiv angegangen wurden.

Standards als Ziel und Richtschnur

Mit diesen Anforderungen und der Vorgabe, die Spezifikation der SuisseID spätestens auf Ende 2009 publikationsreif bereitzuhaben, machte man sich im August desselben Jahres für die Spezifikation der Zertifikate und im Oktober für die Spezifikation des Identitäts- und Funktionsnachweises an die Arbeit. Das Vorhaben wurde anhand thematischer Kriterien in drei Teilprojekte aufgeteilt: die Spezifikation der SuisseID-Zertifikate, die Spezifikation der Bestätigungsdienste und die Vermarktung und Pilotierung der SuisseID.

In einer frühen Designphase wurde festgelegt, dass die SuisseID auf anerkannten Standards basieren sollte wie demjenigen der X.509-Zertifikate oder aber SAML 2.0 als technische Basis für den Funktionsnachweis. Dies brachte neben der Zeitersparnis technische Vorteile. Durch die Anlehnung an das ZertES-Gesetz als weiteren Standard konnte man auch viele rechtliche und organisatorische Vorgaben übernehmen. Nicht zuletzt deshalb beinhaltet die SuisseID ein qualifiziertes elektronisches Zertifikat. Damit sind zum Beispiel Haftungsansprüche, Pflichten des Benutzenden und der ausstellenden Organisation oder aber Ausstellungsprozesse klar geregelt und werden sogar periodisch geprüft und zertifiziert.

Sobald die groben Züge der Lösung umrissen waren, ging es darum, auf möglichst effizientem Weg eine hinreichende Spezifikation zu erstellen. Dazu musste die Runde um Expertinnen und Experten aus diversen Fachgebieten erweitert werden. Die Herausforderung lag nun darin, über alle involvierten Personen ein breit abgestütztes Grundverständnis der Stossrichtung und der Rahmenbedingungen zu schaffen. Dies erforderte eine enge Kommunikation unter den Beteiligten sowie eine klar geregelte Aufgabenzuweisung.

Um die Spezifikation mit überlappenden Phasen zu realisieren, wurde stets nach dem «latest to know»-Prinzip agiert. Dabei wurde festgehalten, bis wann eine Partei spätestens eine Information erhalten haben oder eine gewisse Entscheidung gefällt sein musste, um den Zieltermin noch einhalten zu können. Basierend darauf wurden gewisse Themen prioritär bearbeitet. Parallel dazu musste allerdings auch die übrige Spezifikation vorangetrieben werden.

Specification Enforcement Camp

Da ein mehrmonatiger Spezifikationsprozess mit Workshops, Protokollen, Updates und Vernehmlassungen nicht infrage kam, entschied man sich für einen unkonventionellen Ansatz: Um die gesamten Diskussions-, Entscheidungs- und Review-Prozesse zu verdichten, sperrte man eine grössere Expertenrunde für drei Tage in einem sogenannten «Specification Enforcement Camp» zusammen. Erklärtes Ziel dieses Camp war es, alle zwingend anstehenden oder besonders weit reichenden Entscheidungen breit abgestützt zu fällen. Zudem sollte am Schluss eine grössere Zahl von Personen genügend Wissen über den Auftrag und die Ziele des Vorhabens besitzen, um anschliessend auch ohne detaillierte Vorgaben selbstständig in Teilprojekten arbeiten zu können. Während des Camp wurden Themen in diversen kleineren Expertengruppen bearbeitet und die Ergebnisse anschliessend im Plenum präsentiert, diskutiert und verabschiedet. Dank den kurzen Kommunikationswegen konnte man auch komplexe Themen rasch und unkompliziert abhandeln. Am Ende des Camp waren alle weitreichenden Entscheidungen gefällt, und man hatte die diversen Beteiligten aus Industrie und Politik abgeholt. Auf dieser Basis konnte im Dezember eine Version 1.0 der SuisseID-Spezifikation erstellt, in einem kleineren Kreis geprüft und anschliessend veröffentlicht werden.

Errata und Wellen

Wo gehobelt wird, fallen Späne. So war klar, dass ein solch dicht gedrängtes Programm bei der Erstellung des Standards die eine oder andere Nebenwirkung haben würde. Dies machte sich insbesondere bemerkbar, als sich durch die Veröffentlichung der Version 1.0 die Zahl der Leser des Spezifikationsdokumentes vervielfachte. Zwar traten dabei keine gröberen Unstimmigkeiten zutage, es zeigte sich aber, dass im einen oder anderen Detailaspekt noch Lücken bestanden oder die Spezifikation noch zu ungenau war. Wie bei Standards üblich begann man deshalb, die offenen Punkte und allfällige Fehler in einem «Erratadokument» aufzuführen und fortlaufend nachzuspezifizieren.

Damit alle an der Spezifikation Beteiligten jederzeit auf dem aktuellen Stand sind, wurde eine Austausch- und Diskussionsplattform für Experten zur SuisseID geschaffen. Anregungen oder Änderungsvorschläge wurden fortan zunächst dort publiziert, diskutiert und angenommen, bevor sie den Weg in die nächste Spezifikationsversion fanden. Online-Collaboration hat sich dabei als ein mächtiges Werkzeug erwiesen. Die Plattform sollte sich auch in der Implementierungsphase bewähren.

Zukunftssicherheit und Interoperabilität

So viel zur Entstehung der SuisseID. Was aber macht einen guten Standard eigentlich aus? Neben den vorher erwähnten Anforderungen muss er vor allem auch Zukunftssicherheit und Interoperabilität bieten. Wie lassen sich diese Qualitäten gewährleisten?

Zukunftssicherheit ist stark durch die Modularität und die Erweiterbarkeit bestimmt. Systeme, die diese Eigenschaften schon von ihrem Design her mitbringen, lassen sich meist flexibel an andere Gegebenheiten anpassen. Im Falle der SuisseID wurde insbesondere im Bereich der Bestätigungsprovider stark auf diese Eigenschaften hingearbeitet. Das ganze «Claim Assertion Infrastructure»-System setzt nur wenig voraus und lässt sich im Gegenzug durch Hinzufügen weiterer Funktionsregister beliebig erweitern. Es können auch Register aus dem System ausscheiden, ohne dass das Gesamtsystem deswegen beeinträchtigt würde. Denn dieses ist absolut dezentral organisiert. Erweiterbarkeit spielte aber auch bei den eingesetzten technischen Protokollen eine grosse Rolle. So wurden etwa SAML 2.0 oder WS-Trust gewählt, die je schon von sich aus definierte Erweiterungspunkte anbieten.

Auch der Interoperabilität wurde ein wichtiger Platz eingeräumt. Die SuisseID beruht im Wesentlichen auf anerkannten Standards, sie ergänzt diese lediglich dahingehend, dass sie sich auf einige ausgewählte Anwendungsfälle beschränkt. Damit ist bereits heute Interoperabilität mit diversen existierenden und zukünftigen Komponenten gewährleistet. Ein Detail, das bei der Betrachtung der SuisseID meist unter den Tisch fällt: Dank dem Einsatz von WS-Trust ist die SuisseID schon heute für den aufkommenden «Information Card»-Standard gerüstet. Es wurde sogar lange darüber diskutiert, ob die SuisseID beim Funktionsnachweis ausschliesslich auf diesem Standard beruhen sollte.

Nützlicher Zeitdruck

Der gedrängte Zeitplan und die vielen involvierten Parteien erforderten ein spezielles, pragmatisches Vorgehen. Viele Schritte, die eigentlich zur Erstellung eines Standards üblich sind, mussten entweder weggelassen werden oder aber in komprimierter Form erfolgen. Genau dieser gedrängte Zeitplan ermöglichte, ja erforderte sogar den Einsatz neuer Methodiken und Ansätze. Nicht zuletzt deshalb war es möglich, termingerecht einen Standard zu entwickeln, der sich auch während der Entwicklungs- und Einführungsphase als sehr stabil herausstellte und damit eine gute Grundlage bietet für die Umsetzung der SuisseID-Komponenten bei diversen Parteien.