AdNovum

NOTITIA

Bemerkenswertes von und über AdNovum

Herbst 2010, Heft Nr. 19

Identity Management XXL

Inhalt

Liebe Leserin, Lieber Leser

Sich ausweisen – für viele alltägliche Handlungen und Geschäfte eine selbstverständliche Sache. Mit der Globalisierung und Vernetzung unseres Wirtschafts- und Soziallebens nimmt aber die Zahl unserer Geschäfts- und Kommunikationspartner laufend zu und damit auch die Anzahl unserer Benutzerkonten. Allein schon für unsere tägliche Arbeit benötigen wir unzählige davon. Um den Verwaltungsaufwand im Zaum zu halten, betreiben Unternehmen Identity Management, kurz IDM. Als Mitarbeiter eines Unternehmens erhalten wir damit in dessen Hoheitsbereich im Idealfall eine einzige, dafür hochwertige Identität, über die wir unsere Kompetenzen wahrnehmen können.

Eine solche Identität auf nationaler Ebene hat dieses Jahr das SECO lanciert, mit wenig Macht zur Durchsetzung, aber dafür mit geschickt konzertiertem Vorgehen und gesundem Optimismus: Die SuisseID, bis Ende Jahr noch subventioniert, soll sich verbreiten und dem elektronischen Geschäfts- und Behördenverkehr in der Schweiz Schub verleihen. Dafür haben das SECO und die beauftragten Firmen einigen Aufwand getrieben. Wie die SuisseID als Standard aufgebaut ist und welche unterstützenden Angebote von öffentlicher und privater Seite für die Nutzung bereitgestellt worden sind, erfahren Sie im Artikel von Marcel Vinzens und Christof Dornbierer, die massgeblich an der Spezifikation der SuisseID mitgewirkt haben. Die SuisseID dürfte auch als elektronische Basisidentität im Unternehmen interessant werden. Unser Gastautor Stephan Breitenmoser von der Trüb AG beleuchtet in seinem Beitrag das Potenzial der SuisseID als Erweiterung zu konventionellen Ausweiskarten aus Business- und Nutzersicht.

Generell bringt Identity Management im Unternehmen mehr Konsistenz, eine bessere Übersicht und vielfältige Audit-Möglichkeiten. Welches aber sind die Herausforderungen bei der Einführung eines IDM-Systems? Lesen Sie dazu das Interview mit Christian Hilkinger und Philipp Färber in der Heftmitte. Besonders anspruchsvoll ist das Vorhaben, wenn grosse Benutzerpopulationen migriert werden müssen. Wie solche Projekte zu einem erfolgreichen Abschluss geführt werden können, erfahren Sie im Artikel von Simon Uhde. Er berichtet über die Einführung eines neuen IAM-Systems hinter einer Webapplikation mit 1,1 Millionen Benutzern – Identity Management XXL.

Nun wünsche ich Ihnen bei der Lektüre viel Vergnügen!

Ruedi Wipf

CEO AdNovum Informatik AG

SuisseID – Standard mit Potenzial

Mit der SuisseID ist in der Schweiz erstmals ein standardisierter elektronischer Identitätsnachweis verfügbar. Der SuisseID-Standard schafft die Basis für eine Vielzahl von Anwendungen im elektronischen Geschäfts- und Behördenverkehr.

Von Marcel Vinzens und Christof Dornbierer

Viele Prozesse im elektronischen Geschäfts- und Behördenverkehr basieren darauf, dass sich eine Person ausweisen kann. Entsprechenden Online-Applikationen in der Schweiz fehlte bis jetzt aber ein Set von verbreiteten und standardisierten Identifikationsmerkmalen in hoher Qualität. Seit dem 1. Mai 2010 steht mit der SuisseID hierfür nun eine Lösung zur Verfügung, die der E-Economy und dem E-Government in der Schweiz zum Durchbruch verhelfen soll.

Hochwertige Identität dank Abstützung auf ZertES

Der SuisseID-Standard spezifiziert im ersten Teil ein Profil für ein qualifiziertes Signaturzertifikat nach ZertES, dem Bundesgesetz über die elektronische Signatur (SuisseID QC), sowie die Regeln bzgl. Ausstellung und Management des (nichtqualifizierten) SuisseID-Authentisierungszertifikats (SuisseID IAC). Eine SuisseID ist somit technisch nichts weiter als eine signaturgesetzkonforme Chipkarte oder ein USB-Stick mit diesen beiden Zertifikaten.

Die Qualität und Vertrauenswürdigkeit einer elektronischen Identität ist abhängig von der Identifikation und Registrierung der antragstellenden Person, der kryptografischen und organisatorischen Sorgfalt im Ausstellungs- und Verwaltungsprozess der Schlüssel sowie von der Verknüpfung der Personendaten mit dem öffentlichen Schlüssel im Zertifikat. Entsprechende Anforderungen für die sichere Authentisierung gegenüber Online-Applikationen sind bislang in keinem Gesetz definiert. Im Zusammenhang mit qualifizierten elektronischen Signaturen regelt jedoch ZertES die rechtlichen, technischen und organisatorischen Rahmenbedingungen und verpflichtet Anbieter von Zertifizierungsdiensten, höchste Anforderungen an die eingangs formulierten Qualitätsmerkmale zu erfüllen.

> ZertES verpflichtet die Anbieter der SuisseID auf hohe Qualität.

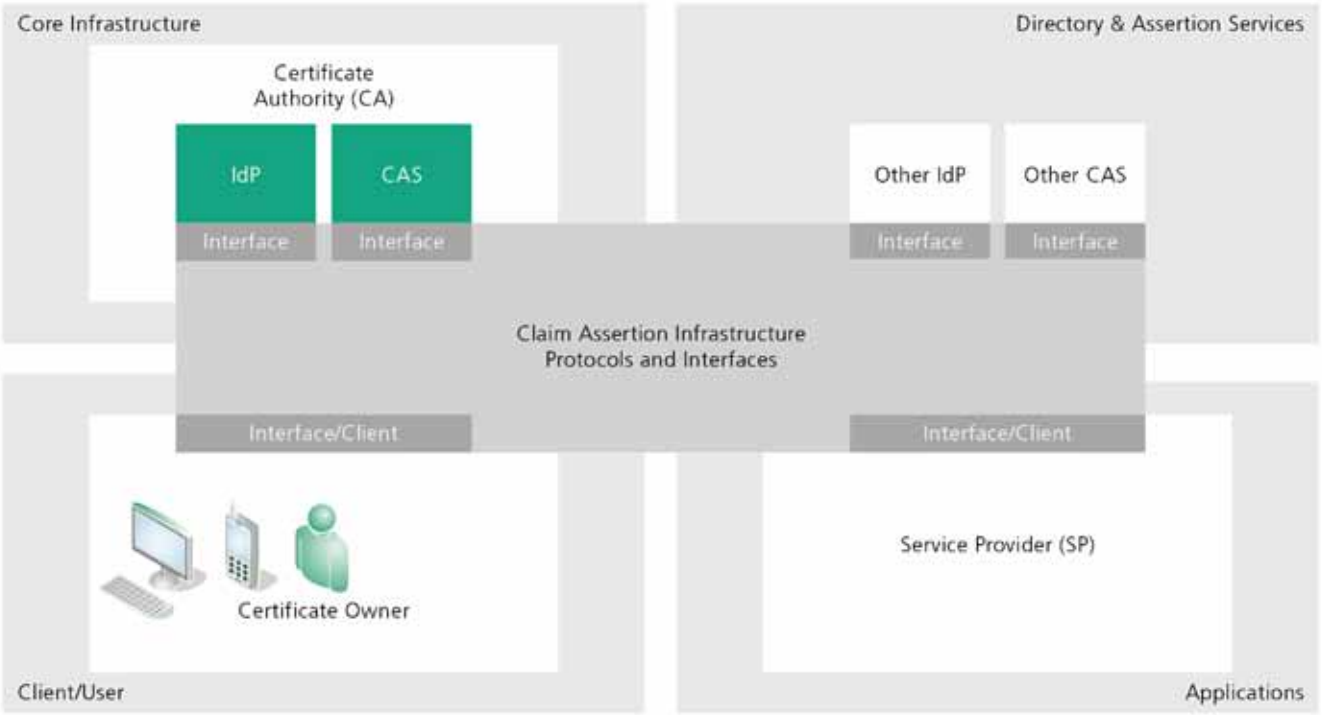
Da das Signaturzertifikat der SuisseID (SuisseID QC) ZertES-konform ist, unterliegen deren Anbieter ebenfalls diesen hohen Anforderungen. SuisseID QC und SuisseID IAC enthalten einen gemeinsamen Identifikator, die SuisseID-Nummer. Diese ist eindeutig und wird von den SuisseID-Anbietern einer Person unabhängig von weiteren Attributen exklusiv zugewiesen. Dies erlaubt es, die wesentlichen Teile der hohen Anforderungen an die Identität vom SuisseID QC auch auf das SuisseID IAC zu übertragen.

> Wegen dem Datenschutz beschränkte man die Personendaten im Zertifikat auf ein Minimum.

Mehrwert durch Funktionsnachweise

Die SuisseID bietet also als Basisnutzen starke Authentisierung auf Grund einer qualitativ hochstehenden digitalen Identität gegenüber einer Online-Applikation bzw. einem Service (Login) sowie elektronische Signaturen nach ZertES. Im elektronischen Geschäfts- und Behördenverkehr reicht es aber oft nicht aus, nur die Identität einer Person nachzuweisen. Stattdessen müssen weitere Eigenschaften überprüft werden können wie der Beruf (z. B. Arzt, Notar), die Adresse, Zeichnungsberechtigungen (z. B. gemäss Handelsregister) und Mitgliedschaften. Da es dabei oft um die Funktion einer Person geht, nennt man dies auch Funktionsnachweis.

Es wäre naheliegend gewesen, diese Attribute ins SuisseID-Zertifikat mitaufzunehmen. Damit hätte man hinsichtlich künftiger Änderungen und Erweiterungen des Attributekatalogs jedoch eine unflexible Lösung geschaffen. Deshalb und auch aus Gründen des Datenschutzes beschränkte man die Angaben zu einer Person im SuisseID-Zertifikat auf ein Minimum: Es muss nur Name und Vorname (oder ein Pseudonym) des Zertifikatsinhabers sowie



SuisseID: Claim Assertion Infrastructure (CAI).

die SuisseID-Nummer enthalten. Für Funktionsnachweise wurde dafür im SuisseID-Standard ergänzend eine offene, flexible Infrastruktur spezifiziert – die sogenannte Claim Assertion Infrastructure (CAI, s. Abbildung).

Datenfreigabe durch den Benutzer

Die CAI funktioniert wie folgt: Personenbezogene Attribute, die nicht im Zertifikat enthalten sind, können vom Zertifikatsinhaber unter Rückgriff auf SuisseID Identity Providers (IdP) und SuisseID Claim Assertion Services (CAS) an die Online-Applikation (Service Provider) übermittelt werden. Der IdP bestätigt jeweils die Identität, der CAS die Attribute. In der Implementierung werden die beiden in der Regel zu einem einzigen Service zusammengefasst, einem sogenannten Extended IdP. Es gibt ein Set von Kernattributen (Core Assertion Attributes) wie etwa Name, Vorname und Geburtsdatum, das bei der Registrierung auf Grund der Ausweisschrift des Antragstellers zwingend vom SuisseID-Aussteller erfasst wird. Diese Attribute können von einem speziellen Core-IdP/CAS des jeweiligen SuisseID-Ausstellers bezogen werden. Weitere Attribute wie Beruf etc. können in Funktionsregistern erfasst und von sogenannten «Other CAS» bezogen werden.

Die Übermittlung der Attribute erfolgt nur mit der expliziten Zustimmung des Zertifikatsinhabers.

Im Sinne der Benutzerzentrierung erfolgt die Übermittlung der Attribute unter vollständiger Kontrolle des Zertifikatsinhabers und nur mit seiner jeweiligen expliziten Zustimmung in einem entsprechenden Online-Dialog (s. Abbildung Seite 5). Eine Online-Applikation kann also ohne Einbezug des Zertifikatsinhabers keine personenbezogenen Attribute über den SuisseID Identity Provider beziehen.

Die Claim Assertion Infrastructure basiert auf offenen Standards wie SAML und WS-Trust und ist ein plattformunabhängiges Framework, d. h. unabhängig von Computersystem, Architektur, Prozessor und Betriebssystem.

Die konzeptionellen Teile des SuisseID-Standards sind bewusst möglichst generisch und technologieneutral gehalten. So wurde z. B. der neutrale Begriff Claim Assertion Service (CAS) geprägt und nicht direkt der SAML-Term «Attribute Authority» verwendet. Die Abbildung auf die entsprechenden Begriffe erfolgte dann bei der technischen Umsetzung des Konzepts.

AdNovum war im Auftrag des Staatssekretariats für Wirtschaft (SECO) massgeblich an der Spezifikation der SuisseID und insbesondere der Claim Assertion Infrastructure beteiligt und hat den zentralen SuisseID Identity Provider und Claim Assertion Service (Extended Core IdP) implementiert. Dieser Core IdP hat Referenzcharakter und wird auch bei den aktuellen Anbietern der SuisseID eingesetzt.

Integration der SuisseID

Aus der Sicht von Service Providers stellt sich nun die Frage, wie Applikationen einfach SuisseID-fähig gemacht und an die Claim Assertion Infrastructure angebunden werden können, um deren Vorteile zu nutzen.

Das SuisseID IAC ist ein standardisiertes X.509v3-Authentisierungszertifikat. Für reine Login-Abfragen sind somit neben adäquaten Sicherheitsmassnahmen auf Client-Seite meist nur konfigurative Änderungen notwendig, allenfalls geringe Anpassungen für die Auswertung der SuisseID-Nummer.

Für die Anbindung von Applikationen an die CAI steht den Service Providers ein im Rahmen des SuisseID-Projekts erstelltes Software Development Kit (SDK) für Java und .NET zur Verfügung. Damit lassen sich die SuisseID-Funktionalitäten einfach in die entsprechenden Applikationen integrieren. Das SDK hat Referenzcharakter, es diente unter anderem auch der Verifikation der Spezifikation sowie der Sicherstellung der Interoperabilität. Die Praktikabilität des SDK wiederum wurde durch seine Verwendung für die beiden Referenzapplikationen «Cashback-Portal» (.NET) und «Strafregister» (Java) sichergestellt. Alternativ gibt es inzwischen kommerzielle Applikationen und Module, die es Online-Applikationen ermöglichen, die SuisseID-Funktionalitäten transparent oder zumindest technologieneutral zu integrieren, d. h. ohne dass man sich dabei mit der Komplexität von SAML oder WS-Trust auseinandersetzen muss. AdNovum bietet mit dem Nevis SuisseID Proxy ein solches Integrationswerkzeug für Service Providers an, das diese vom gesamten SuisseID-Protokollhandling entbindet und so eine schnelle, flexible und günstige SuisseID-Unterstützung ermöglicht.

Im Weiteren wurde eine SuisseID Community initiiert, die zum Ziel hat, SuisseID-Pioniere und SuisseID-Integratoren miteinander zu vernetzen und den Erfahrungsaustausch zu fördern.

Wie kann man von den Teilnehmern der CAI Compliance zum Standard einfordern?

Verbindlicher Standard – die SuisseID als Marke

Die SuisseID-Spezifikation ist als E-Government-Standard eCH-0113 beim Verein eCH eingeordnet und soll zur weiteren Pflege einem Trägerverein übergeben werden, dem zumindest die SuisseID Certificate Service Providers angehören werden.

Wie sollte der Verbindlichkeit des SuisseID-Standards nun Nachdruck verliehen und von den verschiedenen Teilnehmern der CAI Compliance zum Standard eingefordert werden? Auf Grund der fehlenden gesetzlichen Grundlage war eine Zertifizierung dazu keine Option. Stattdessen wurde aber ein entsprechender Ansatzpunkt in Form des Markenrechts gefunden. Die SuisseID ist eine eingetragene Marke des SECO. Ein Lizenzvertrag regelt die Verwendung dieser Marke durch Applikationsanbieter. Lizenznehmer verpflichten sich, die Marke in SuisseID-enabled Online-Applikationen gemäss dem SuisseID-Styleguide darzustellen (Branding) und die SuisseID-Spezifikation einzuhalten sowie die Kompatibilität gegenüber allen SuisseID-Anbietern zu gewährleisten.

Offen, erweiterbar, wiedererkennbar

Die SuisseID kann somit einfach integriert und zeitnah für starke Authentisierung sowie qualifizierte Signaturen verwendet werden. Gemäss dem Verzeichnis der Anwendungsanbieter (s. www.suisseid.ch) wurden entsprechende Vorhaben inzwischen bei zahlreichen Unternehmen und öffentlichen Verwaltungsstellen umgesetzt und sind bereits operativ.

Die grosse Neuerung und das grösste Potenzial der SuisseID stecken aber wohl im Funktionsnachweis basierend auf der Claim Assertion Infrastructure. Dank offenen Standards und Plattformunabhängigkeit wurde ein gemeinsamer Standard für den Austausch von Beglaubigungen geschaffen. Da bei der Registrierung ein Set von Kernattributen auf dem Core IdP abgelegt wird, das im Umfang einer Kopie der Ausweisschrift entspricht, können nun alle Prozesse, die eine solche voraussetzen, mit Online-Applikationen realisiert werden. Beispiele sind die Bestellung eines

Datenfreigabe beim Bestellen eines Strafregisterauszugs: Dialog für den SuisseID-Inhaber.

Marcel Vinzens (links) und Christof Dornbierer haben im Auftrag des SECO die Spezifikation der SuisseID CAI massgeblich mitgestaltet.

Strafregisterauszugs, aber auch alle Online-Applikationen, die einen Altersnachweis (Alkohol, Spiele) oder Namensnachweis erfordern. In einer nächsten Phase dürften insbesondere auch Register («Other CAS») wie das Notariatsregister, das Ärzteregister und das Handelsregister hinzukommen. Mit dem Einsatz von WS-Trust und von Teilen des Identity Metasystem Interoperability 1.0 Profile ist die SuisseID schon heute für den aufkommenden «Information Card»-Standard gerüstet. Dank der eingetragenen Marke und dem Styleguide wird mit der zunehmenden Verbreitung der SuisseID auch ihr Wiedererkennungswert steigen.

Grosses Potenzial

Die SuisseID ermöglicht als pragmatische, auf etablierten und verbreiteten Standards aufbauende Lösung einen sicheren elektronischen Identitätsnachweis. Damit schliesst sie eine entscheidende Lücke im elektronischen Geschäfts- und Behördenverkehr in der Schweiz.

In der ersten Phase bringt die SuisseID vor allem für dedizierte geschäftliche Zwecke einen Mehrwert. Sobald sie aber ausreichend verbreitet ist und weitere Register zur CAI hinzukommen, wird der Mehrwert insbesondere für Privatpersonen noch zunehmen. Dann wird das Potenzial der SuisseID mit der Offenheit und Erweiterbarkeit der CAI so richtig zum Tragen kommen.

Marcel Vinzens

Marcel Vinzens, dipl. Informatik-Ingenieur ETH und CISSP-zertifiziert, arbeitete als Beauftragter des SECO aktiv an der Konzeption und Spezifikation der SuisseID Claim Assertion Infrastructure mit. Zudem war er als technischer Projektleiter für die Umsetzung einer zentralen Kernkomponente der SuisseID-Infrastruktur (Core Identity Provider) verantwortlich, die AdNovum für das SECO realisiert hat. Wenn er sich nicht gerade mit Informatik beschäftigt, verbringt er gerne Zeit mit seiner Familie oder bei Erlebnissport.

Christof Dornbierer

Christof Dornbierer, dipl. Informatik-Ingenieur ETH, hat seit 2004 massgeblich an der Weiterentwicklung des AdNovum-eigenen Sicherheits-Frameworks Nevis mitgewirkt. Seit August 2008 CTO und Mitglied der Geschäftsleitung, verantwortet er unter anderem die Bereiche Technologie und Security. Er hat die Konzeption und Spezifikation der SuisseID Claim Assertion Infrastructure massgeblich mitgestaltet, ebenso die Umsetzung des Core Identity Provider und die Entwicklung des Nevis SuisseID Proxy. In seiner Freizeit ist er öfter zu Fuss oder auf zwei Rädern draussen anzutreffen.

Drei Buchstaben voller Komplexität

Philipp Färber, Head of Security Engineering, und Christian Hilkinger, Business Analyst, erklären, welche Hindernisse bei der Einführung von Identity Management – kurz IDM – auftreten können, wie man sie überwindet und wo AdNovum im Konkurrenzvergleich steht.

Warum scheitern viele IDM-Projekte?

Ch.H.: Die Anforderungen an ein IDM-Projekt sind sehr unterschiedlich. Deshalb lässt sich nicht pauschal sagen, es scheitert an diesem oder jenem Punkt. Kritisch ist etwa die Masse an Systemen, die alle in einer bestimmten Form Identitäten enthalten und eingebunden sein wollen. Häufig sind Systeme in den Unternehmen gewachsen, entsprechen also nicht mehr dem Originalstandard, und es lässt sich kaum zurückverfolgen, was genau verändert wurde.

> Oft sind Systeme in den Firmen gewachsen und die Änderungen kaum nachvollziehbar.

Ph.F.: Zudem betreibt fast jede Firma schon eine Form von IDM – wenn auch weniger automatisiert und zentralisiert, als es möglich wäre – und hat damit ihre eigenen Prozesse und Directories, die es zu respektieren gilt. Da überdies jedes System seine eigene Berechtigungs- und User-Struktur hat, muss ich mich in jedes einzeln einarbeiten und die Theorie dahinter analysieren, um es in ein zentrales System zu integrieren. Beispielsweise kann ich einen Active-Directory-Konnektor nicht einfach «out of the box» benutzen, sondern muss das Active Directory verstehen. Die Komplexität von IDM wird immer unterschätzt. Man denkt, bei drei Buchstaben kann es ja nichts Kompliziertes sein. Doch es steckt mehr dahinter, als nur ein paar Werte zu kopieren.

Muss denn alles auf einen Schlag ans IDM-System angeschlossen werden?

Ch.H.: Ich erachte es als besser, modular vorzugehen und sich pro Phase auf eines bis einige wenige Systeme zu konzentrieren. Sind die Kernsysteme angeschlossen und ist die Funktionalität verifiziert, kann ich mit weiteren Systemen fortfahren. So kann ich die Komplexität und die Abhängigkeiten zwischen den Systemen auf einzelne Phasen aufteilen.

Ph.F.: Deshalb empfehlen sich sogenannte Milestones, bei denen der Kunde am Ende einer Phase einen Teil der Lösung schon mal abnimmt. Damit lassen sich auch etwaige Fehler frühzeitig erkennen.

Wozu überhaupt IDM?

Ph.F.: Ohne IDM hat man inkonsistente Daten und zu wenig Übersicht und Audit-Möglichkeiten. Eine zentrale Sicht der Benutzerrechte ermöglicht etwa nachzuvollziehen, wie etwas passieren konnte oder wer welche Rechte hat.

Ch.H.: Und auch, wer an wen welche Berechtigung vergeben hat. Ein IDM-System bietet hierfür einen zentralen Ansatzpunkt – genau das ist eine seiner grossen Stärken. Ohne IDM müsste man diese Berechtigungen in jedem System einzeln vergeben. Bei vier oder fünf Benutzern ist das kein Problem. Ab einer gewissen Anzahl wird es aber aufwendig und unübersichtlich, sodass sich mit IDM die Effizienz steigern lässt.

Ph.F.: Ein IDM-System ist natürlich kein Spontankauf. Die Entscheidungsträger in den Firmen analysieren Situation und Bedürfnisse sorgfältig.

Wie starte ich ein IDM-Projekt, wenn zahlreiche Konflikte und Inkonsistenzen schon eine schwierige Ausgangslage schaffen?

Ph.F.: Für mich bilden Interviews in der Firma und die Erarbeitung von Use Cases die Hauptpunkte. So lerne ich die Abläufe und Anforderungen sowie zugleich die Probleme und die Gründe kennen, warum eine Firma IDM einführen will. Als Nächstes würde ich die aktuellen Prozesse und Wünsche in der Spezifikation erfassen. Damit kenne ich die Vorbedingungen, meine Aufgaben und die Ziele.

Ch.H.: Technisch betrachtet bietet ein Standardsystem wie das Active Directory, das fast jedes Unternehmen hat, einen guten Einstiegspunkt.

Wann sind die Voraussetzungen geschaffen bzw. die Konflikte ausreichend bereinigt, um zu starten?

Ch.H.: Wenn die Anforderungen und der aktuelle Stand spezifiziert sind. Je genauer man hier arbeitet, desto weniger Über-

raschungen ergeben sich später bei der Umsetzung. Es wird jedoch immer noch zu Anpassungen kommen. Die Bereinigung von Daten, darunter fallen etwa unterschiedlich geschriebene Namen in verschiedenen Systemen, erfolgt beispielsweise als Teil des laufenden Projekts.

Ph.F.: Dies ist nur eine von zahlreichen Hürden, die es zu nehmen gilt. Der Start des Projekts ist meist einfach, wir können damit

Kennen die Herausforderungen rund ums Identity Management: Business Analyst Christian Hilkinger …

beginnen, sobald der Kunde uns einen Auftrag erteilt. Das Komplizierte ist das Ende, bis alle Änderungen integriert sind, die im Projektverlauf gewünscht oder notwendig werden. IDM orientiert sich grundsätzlich stark an der Praxis.

Wo verursachen IDM-Projekte generell den grössten Zeitaufwand?

Ph.F.: Bei der Integration – dauert ein Projekt länger, entwickelt der Kunde häufig zusätzliche Ideen oder Wünsche, die nachträgliche Synchronisierungen erfordern. Er will z. B. vom ursprünglich spezifizierten Mailversand an Einzelbenutzer auf Gruppenmail umstellen oder bei einer bestimmten Rolle einen zweiten oder gar dritten Approval hinzufügen, bevor sie vergeben werden darf. Bei Projektstart lassen sich solche Anforderungen leichter implementieren als nachträglich.

Ch.H.: Bei Mehraufwand entscheiden wir auf Basis der Spezifikation, was wir kulanterweise noch integrieren können und was wir als Change Request separat verrechnen müssen.

Ph.F.: Deshalb würde es sich auch anbieten, mit dem Kunden einen Fixpreis für eine Basisleistung zu vereinbaren und zusätzliche Funktionen in einer zweiten – separat verrechenbaren – Etappe zu planen.

Gibt es überhaupt eine gute Software, um IDM umzusetzen?

Ch.H.: Für ein einzelnes Programm ist die IDM-Problematik zu komplex. In verschiedenen Unternehmen müssen verschiedene Systeme angebunden werden. Deshalb muss man IDM immer als ein Projekt sehen und nicht nur als Installation einer Software.

Ph.F.: Eine «out of the box»-Lösung, die wir unverändert benutzen könnten, gibt es nicht. Es sind immer spezifische Anpassungen und Konfigurationen notwendig. Wichtig ist deshalb auch ein durchdachtes Konfigurationsmanagement.

Der Start ist einfach, kompliziert ist das Ende.

Wie ist die Qualität der heutigen IDM-Software?

Ch.H.: Jedes Produkt hat seine Vor- und Nachteile. Schreibe ich meine Software selber, kann ich sie auf das betreffende Projekt massschneidern. Benutze ich eine bewährte Standardsoftware, sind für die gängigen Systeme dafür schon Konnektoren vorhanden, die ich relativ einfach verwenden kann.

Ph.F.: Ich persönlich habe kein Lieblingsprodukt. Bei selbstgeschriebener Software zeigen sich viele Komplexitätsaspekte erst später. Dafür kann ich den Code nötigenfalls schnell anpassen. Bei einem gekauften Produkt bin ich darauf angewiesen, dass der Hersteller mit mir kooperiert. Da ist eine langjährige, etablierte Partnerschaft hilfreich.

Wo steht AdNovum im Konkurrenzvergleich?

Ph.F.: AdNovum kann bestens mit der Konkurrenz Schritt halten, da sie mit nevisIDM über ein sehr flexibles Produkt mit ausgewählten Funktionalitäten verfügt. Müssen diese auf Grund anderslautender Kundenanforderungen erweitert werden, schaffen wir das mit unserem internen Entwicklungsteam innert kurzer Zeit. Fehler können wir innerhalb eines Tages beheben.

Was macht AdNovum bei ihrer IDM-Software besonders gut?

Ph.F.: Wir besitzen intern ein erstklassiges Software-Know-how. Wir können unser IDM-Team direkt nach seinem Ansatz in der Software fragen und die Probleme sauber lösen. Für den Erfolg unserer IDM-Projekte sind wir jedoch nicht von unseren Produkten abhängig, wir bauen auch mit Produkten anderer Hersteller. Bei der Umsetzung profitiert AdNovum von ihrer Erfahrung mit vielfältigen Systemen, gerade bei der Integration. AdNovum hat immer schon integriert, nicht nur mit IDM-, sondern auch mit Access-Systemen und anderen Security-Infrastrukturen.

Wie sieht die optimale IDM-Lösung aus?

Ch.H.: Die optimale Lösung ist für jedes IDM-Problem eine andere und hängt von den spezifischen Bedürfnissen des Unternehmens ab. Die Frage ist nur schon, ob es einen grossen Namen unter seiner IDM-Lösung will. Für mich als Kunde wäre die Kernfunktionalität wichtig, die die Rollen und Berechtigungen verwaltet. Danach würde ich über einzelne Ergänzungen wie etwa einen Workflow nachdenken.

Ph.F.: Wie gut IDM solche Workflows unterstützt, ist ebenfalls entscheidend. Das gilt besonders, wenn ich Prozesse abbilden oder beim Kunden vereinfachen will. Was ich teilweise vermisse, ist die Möglichkeit eines sauberen Rollback, beispielsweise wenn ich 1000 Benutzer falsch importiert habe. Aber das ist natürlich sehr aufwendig, wenn ganz verschiedene Systeme beteiligt sind. Ebenfalls vermisse ich die Möglichkeit, den Soll-/Istzustand zu vergleichen. Damit hätte ich eine Kontrolle, sollte ich etwa die Zielsysteme mit falschen Daten überschreiben.

Wie sind die Erfahrungen mit Kunden bei der praktischen Umsetzung?

Ch.H.: Die Kunden sind sehr kooperativ, wenn Probleme auftreten. Kürzlich mussten wir bei einem Kunden auf der Datenbank ein Script ausführen. Das betreffende Team war damit aber nicht einverstanden, da es interne Richtlinien für das Ausführen von Scripts hatte und nicht genau wusste, was das Script wirklich machte. Das Produkt stammte von einem externen Hersteller. So konnten wir es ihnen zunächst auch nicht genau erklären und eine Rückfrage beim Hersteller hätte zu lange gedauert.

Ph.F.: Wir schauten das Script selber an und konnten unsere Ansprechpartner schliesslich überzeugen. Dabei half zweifellos, dass sie IT-Leute sind. Zudem profitiert man mit der Zeit von seinen Erfahrungen und kann Sackgassen meiden.

Die optimale Lösung ist für jedes IDM-Problem eine andere.

Worin unterscheidet sich IDM zwischen Branchen und Unternehmen?

Ch.H.: Ein zentraler Faktor ist die Grösse des Unternehmens. Mit ihr variiert die Vielfalt der angeschlossenen Systeme und damit die Komplexität von IDM.

Ph.F.: Zwischen den Branchen bestehen schon unterschiedliche Prozesse. In einer IT-Firma, in der jeder sein Terminal hat, sind die Prozesse automatisierter als etwa in einem Handwerksbetrieb. Danach richtet sich auch die IDM-Lösung. Wenn man seinen Mitarbeitern die nächsten Prozessschritte aufs Handy schicken muss, plant man anders, als wenn man die Information schnell auf einem Terminal einblenden kann.

Wie schafft man es, den Benutzer zu Identity Management zu bekehren?

Ph.F.: Grosse Überzeugungsarbeit müssen wir da nicht mehr leisten. Die meisten Leute sind ja schliesslich auch nicht traurig, E-Mails zu schreiben, anstatt Briefe auf der Schreibmaschine zu tippen. ■

… und Head of Security Engineering Philipp Färber.

Christian Hilkinger

Christian Hilkinger, dipl. Wirtschaftsinformatiker, ist seit 2008 bei der AdNovum Informatik AG tätig. Er beschäftigt sich vorwiegend mit Identity Management im Banken- und Versicherungsumfeld, wo er Projekte von der Spezifikation bis zur Umsetzung begleitet. In seiner Freizeit verbringt er als leidenschaftlicher Handballspieler viel Zeit in der Sporthalle.

Philipp Färber

Als Elektroingenieur mit Studienabschlüssen in München, den USA und an der ETH Zürich interessiert sich Philipp Färber seit Langem für die Tücken der Informatik. Als Verantwortlicher des Teilbereichs «Security Engineering» bringt er seit sieben Jahren seine reiche Projekterfahrung ins AdNovum-Team ein, mit Vorzug bei der Lösung kniffliger Aufgaben. Ausdauer zeigt er auch bei Marathons und Bergläufen sowie darin, seine Kollegen zur Teilnahme an derlei Events zu überreden.

Neue IAM-Lösung für E-Finance

Um für die Zukunft gerüstet zu sein, migriert PostFinance mit AdNovum die Zugangsdaten von 1,1 Millionen E-Finance-Benutzern in ein Identity-Management-System. Die Migration soll durchgeführt werden, ohne dass die Benutzer etwas davon merken. Ein Erfahrungsbericht.

Von Simon Uhde

PostFinance hat die Möglichkeiten des Internets schon früh erkannt: Seit 1998 bietet sie ihren Kunden mit E-Finance, ehemals yellownet, eine einfache und sichere Plattform, um Geldgeschäfte online zu tätigen. Heute verwenden über 1,1 Millionen Benutzer E-Finance.

Das Online-Angebot ist für PostFinance ein wichtiger Absatz- und Kommunikationskanal, der weiter ausgebaut werden soll. Dabei spielt Identity und Access Management (IAM) eine zentrale Rolle. Ohne eine automatisierte rollenbasierte Verwaltung der Benutzerdaten und eine zuverlässige Authentisierung kann die Sicherheit nicht mehr gewährleistet werden.

PostFinance entschied sich deshalb für einen Neubau der Benutzerverwaltung und der Authentisierungsinfrastruktur von E-Finance. Die Lösung sollte als Basis für den weiteren Ausbau des Online-Kanals dienen und die folgenden Voraussetzungen erfüllen:

- Die Sicherheitsinfrastruktur sollte auch von anderen Applikationen genutzt werden können.
- Die Authentisierung sollte unabhängig vom zentralen Kundensystem geschehen, um die Verfügbarkeit des Online-Angebots zu erhöhen.
- Neue Authentisierungsmittel sollten ohne grossen Aufwand integriert und der Login-Ablauf nach Bedarf angepasst werden können.

IDM löst die enge Verknüpfung von Login und E-Finance-Applikation.

Entkoppelung von Login und Applikation

Um diese Ziele zu erreichen, mussten wir die starke Verknüpfung von Login und E-Finance-Applikation lösen. Dazu migrierten wir die Zugangsdaten der E-Finance-Benutzer aus dem zentralen Kundensystem in ein dediziertes IDM-System, das eine flexible Handhabung von Authentisierungsmitteln ermöglicht.

Nevis – High-End Identity und Access Management

Nevis ist ein Security-Framework für die Entwicklung von anspruchsvollen Identity- und Access-Management-Lösungen. Nevis schützt zuverlässig gegen interne und externe Bedrohungen und wird vor allem von Unternehmen und Institutionen eingesetzt, welche hohe Anforderungen an den Schutz und die Verfügbarkeit von Daten und Dienstleistungen stellen.

Nevis-Produktkomponenten:

- *nevisProxy: Secure Reverse Proxy und Web Application Firewall*
- *nevisAuth: Authentisierungsservice*
- *nevisIDM: Identity-Management-Service*
- *nevisAdmin: Management- und Monitoring-Konsole*

Weitere Informationen finden Sie unter http://www.nevis.ch.

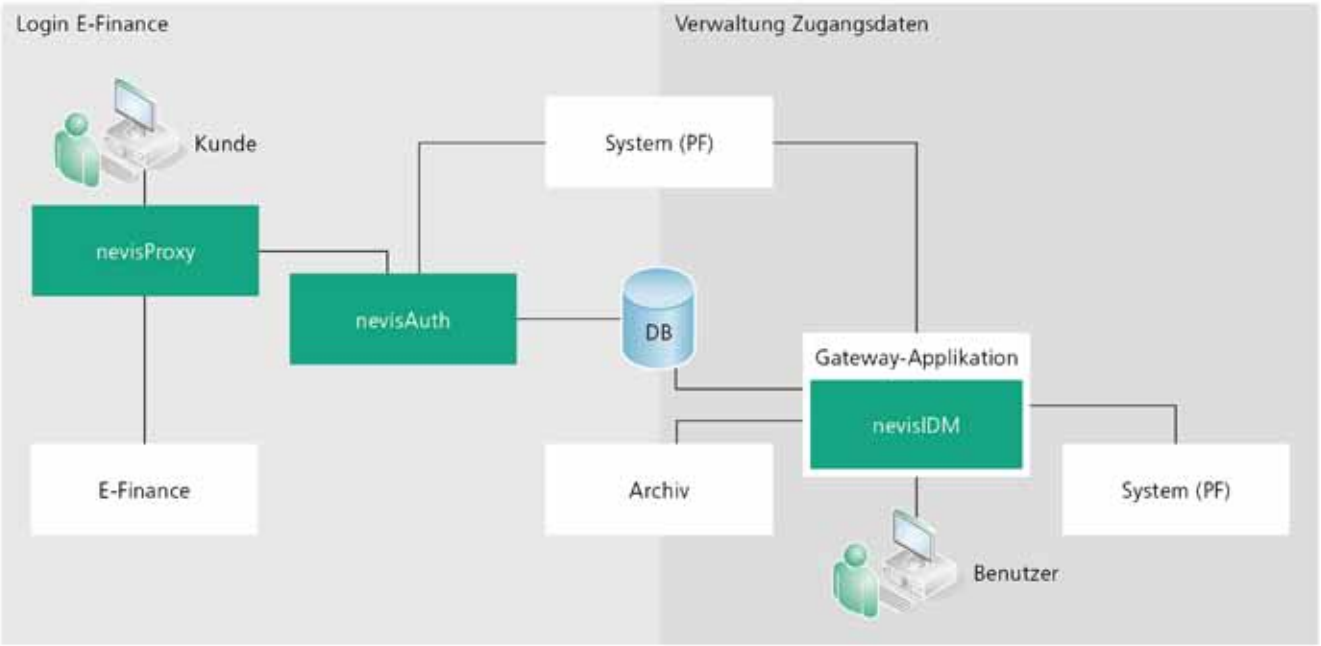
Die von AdNovum im Auftrag der PostFinance entwickelte Lösung umfasst zwei Hauptbereiche mit unterschiedlichen Anforderungen an Prozesse und Performance: das E-Finance-Login und die Verwaltung der Benutzer-Zugangsdaten.

Das E-Finance-Login wird durch den Reverse Proxy nevisProxy abgesichert. Dieser blockt sämtliche nichtautorisierten Requests auf das E-Finance-Backend ab und leitet Login-Requests an den Authentisierungsservice nevisAuth weiter. Das Login entwickelten wir mit Technologien, die nevisAuth standardmässig anbietet. Die Plugin-Architektur von nevisAuth erlaubte eine flexible Anpassung an die Bedürfnisse von PostFinance sowie eine einfache Integration in die Systemlandschaft. Für die Authentisierung wurden sowohl Komponenten aus der Nevis-Produktserie wie auch proprietäre Schnittstellen zu bestehenden Systemen eingebunden.

Nahtlose Prozess- und Systemintegration

Die Verwaltung der Benutzerdaten entwickelten wir auf der Basis der IDM-Komponente nevisIDM komplett neu. Dabei mussten

Setzt grosse IAM-Projekte um: Simon Uhde.



Identity- und Access-Management-System PostFinance.

wir die geltenden Standards einhalten und die Applikation in die bestehende Sicherheitsinfrastruktur integrieren. Die grosse Herausforderung war die Einbindung der Komponente in die PostFinance-Systemlandschaft. Deshalb bauten wir für die Verwaltung der Daten eine Gateway-Applikation auf, welche die PostFinance-spezifischen Schnittstellen anbindet und den Zugriff auf nevisIDM kapselt. Die gewählte Architektur ermöglichte es uns, eine Standardsoftware wie nevisIDM in ein komplexes Umfeld einzubinden.

EIN KLEINER FEHLER, UND HUNDERTTAUSENDE VON BENUTZERN HÄTTEN SICH VIELLEICHT NICHT MEHR EINLOGGEN KÖNNEN.

Auch beim Login-Teil gab es einige Herausforderungen. Die Anforderungen an die Entwickler waren sehr hoch, denn bei einer Finanzapplikation sind Sicherheit und Performance prioritär. Die eigentliche Logik des Login-Ablaufs und die Speicherung der Daten waren bis anhin in einem Legacy-System implementiert und mussten portiert werden. Der Ablauf an sich durfte jedoch nicht angepasst werden, um die Benutzer nicht zu verunsichern. Das Login sollte komplett neu gebaut werden, ohne dass der Kunde etwas davon merkt.

Zudem gibt es Applikationen, bei denen für Anmeldung und Zugriff zwar die E-Finance-Zugangsdaten verwendet werden, nicht aber die Nevis-Login-Infrastruktur. Die Interaktion mit der IDM-Infrastruktur erfolgt in diesen Fällen über die Gateway-Applikation. Um Wiederverwendbarkeit zu gewährleisten und in der Gateway-Applikation denselben Code verwenden zu können wie in nevisAuth, ist das Login modular aufgebaut.

Flexibilität dank asynchroner Kommunikation

Die Anforderungen an die Benutzerverwaltung hängen vom jeweiligen Prozess ab. Für Aktionen, die durch E-Finance-Benutzer initiiert werden und bei denen die Verarbeitungsgeschwindigkeit wichtig ist, setzen wir synchrone Kommunikation ein. Anders bei der automatischen Benutzerverwaltung. Um die Systeme flexibel zu halten, erfolgt der Informationsaustausch hier asynchron sowie mit Hilfe von Publish-Subscribe-Architekturen. So können die verschiedenen Systeme weitgehend entkoppelt werden.

Die Gateway-Applikation implementiert jedoch nicht nur technische Schnittstellen zu Systemen, sondern auch die notwendigen Interfaces für die Client-Applikation, die von Kundendienst und Support für die Verwaltung der E-Finance-Benutzer verwendet wird. Die Gateway-Applikation kapselt in diesem Fall nicht nur die Zugriffe auf nevisIDM, sondern liefert dem Client auch Daten von Drittsystemen, z. B. für den Zugriff auf zusätzliche Personendaten zu einem aktuellen Supportfall.

Migration ohne Probleme

Bei der produktiven Einführung mussten wir die bestehenden Benutzerdaten inklusive der Hashwerte der Passwörter migrieren. Die Hashwerte wurden hierfür beim ersten Login eines Benutzers mit dem in Java nachgebauten alten Algorithmus geprüft. An-

schliessend wurde das Passwort mit einem neuen Algorithmus gerechnet und abgespeichert. Die damit verbundenen Risiken waren hoch. Ein kleiner Fehler, und Hunderttausende von Benutzern hätten sich vielleicht nicht mehr einloggen können. Durch intensives Testen mit realen Daten konnten wir mögliche Probleme rechtzeitig identifizieren und adressieren. Die Migration der Daten war schliesslich kein Problem mehr.

Neue Rekorde bereits nach wenigen Stunden

Im Frühling 2010 wurde die neue Lösung erfolgreich in Produktion genommen. Laut Eric Müller, Architekt Online-Kanal, erfüllte sie alle Performance-Anforderungen auf Anhieb, ohne nachträgliches Tuning. Durch die Reduktion der Abhängigkeiten beim Login wurden bei gleicher Hardware bereits nach wenigen Stunden die folgenden Performance-Rekorde erzielt:

- Max. Anzahl Logins pro Minute: 575
- Max. Anzahl Logins pro Stunde: knapp 18 000
- Spitzenwert Anzahl Logins an einem Tag: 192 225

Gemäss Adrian Hertig, Leiter Entwicklung E-Finance, läuft das neue System im produktiven Betrieb stabil und zuverlässig.

Klassisches Integrationsprojekt

Bei der Einführung der neuen IAM-Lösung für PostFinance handelte es sich um ein klassisches Integrationsprojekt in einem komplexen Systemumfeld. Es galt, den Standardprozess der PostFinance samt seinen Stärken optimal zu nutzen und wo notwendig gezielt um neue Elemente zu erweitern. Die folgenden Aspekte trugen entscheidend zum Gelingen des Projekts bei.

> Der Login-Teil wurde als PoC zuerst ohne Benutzermanagement gebaut und auf Herz und Nieren geprüft.

Da das Projekt eine «Big Bang»-Migration erforderte, war es wichtig, Risiken früh zu erkennen und zu adressieren. Performanz und Stabilität des Logins gehören zu den zentralen Eigenschaften des Systems. Der Login-Teil wurde deshalb als Proof of Concept zuerst ohne Benutzermanagement gebaut und in Lasttests auf

Herz und Nieren geprüft. So konnte der zentrale Teil des Systems entwickelt werden, bevor die Schnittstellen zu den meisten Umsystemen definiert waren. Dies geschah dann parallel zur Entwicklung des Proof of Concept in einer Reihe von Workshops. Durch die Parallelisierung der beiden Aktivitäten gewannen wir viel Zeit.

In den kritischen Phasen des Projekts hielten wir täglich 15-minütige Scrum-Meetings ab.

Danach bauten wir den Proof of Concept zum vollumfänglichen System aus. Die gesamte Entwicklung erfolgte in-house bei AdNovum. Dies erlaubte es uns, von der gewohnten Umgebung und der funktionsreichen Build- und Testinfrastruktur zu profitieren.

Elemente aus agilen Prozessen

Während das Gesamtprojekt in einem traditionellen Wasserfallprozess umgesetzt wurde, verwendeten wir in der Entwicklung Elemente aus agilen Prozessen. So reicherten wir z. B. die Kommunikation und Synchronisation innerhalb des Teams mit Elementen aus dem Scrum-Prozess an. In den kritischen Phasen des Projekts hielten wir täglich 15-minütige Scrum-Meetings ab. An diesen berichteten alle Teammitglieder kurz darüber, was sie seit dem letzten Meeting gemacht hatten, womit sie sich aktuell befassten und was sie als Nächstes zu tun planten. Diese Meetings trugen viel dazu bei, Doppelspurigkeiten und Deadlocks zu vermeiden.

Die häufigen Synchronisationsmeetings förderten die regelmässige Kommunikation unter den Teammitgliedern und sorgten für einen guten Teamgeist. Um den koordinativen Aufwand im Rahmen zu halten, legten wir ausserdem Wert auf Selbstverantwortung und klare Rollenverteilungen.

Weil einige Umsystemanbindungen erst während der Entwicklung spezifiziert wurden, konnte auch die Detailspezifikation erst während der Entwicklung fertiggestellt werden. Wir mussten sie also gestaffelt schreiben. Dabei gelang es uns, aus der Not eine Tugend zu machen und den positiven Nebeneffekt dieses Vorgehens zu nutzen: Wichtige Erkenntnisse konnten während der Implementierung noch einfliessen. Der Grat zwischen Flexibilität sowie Einhaltung der Termine und Kosten ist in diesem Bereich bekanntlich schmal. Durch die enge Zusammenarbeit mit PostFinance konnten die genannten Faktoren jedoch stets ausbalanciert und optimiert werden.

Integrationstests mit Mock Services

Da es sich bei einem IAM-System um ein Middleware-System handelt, war die Integration von grosser Wichtigkeit. Wir haben die Applikation vorgängig AdNovum-intern integriert, um besser testen zu können. Dazu simulierten wir die Umsysteme mit sogenannten Mock Services, die Clients mit Standardsoftware wie SoapUI. Im Laufe des Projekts zeigte sich, dass gewisse Situationen in der AdNovum-Umgebung einfacher reproduziert werden können als im Integrationsumfeld von PostFinance. Einige unserer Mock Services und Client-Applikationen wurden deshalb auch für die Tests bei PostFinance eingesetzt.

Die Integration zu Laborbedingungen kann eine saubere Integration auf Kundenseite nicht ersetzen, sondern nur ergänzen. Denn das Verhalten von Applikationen sowie die Qualität oder die Struktur der Daten entsprechen nicht unbedingt den Erwartungen. Es ist schlicht unmöglich, im Voraus jeden einzelnen Spezialfall zu simulieren. Für den Projekterfolg war es deshalb zentral, dass wir die Integration bei PostFinance eng begleiteten. So erhielten wir jeweils auch schnell Feedback, was bei einer kurzen Integrationsphase enorm wichtig ist.

Ein voller Erfolg

Die Software wurde laut Adrian Hertig trotz sportlichem Zeitplan termingerecht eingeführt. Die Migration der 1,1 Millionen Benutzer verlief ohne Zwischenfälle, und bereits nach wenigen Stunden wurden Performance-Rekorde erzielt.

«Die neue Lösung gibt uns mehr Freiraum beim Umsetzen zukünftiger Anforderungen.»

Das neue IAM-System ebnet der PostFinance den Weg für den weiteren Ausbau des Online-Kanals. Dazu Eric Müller: «Die Lösung gibt uns mehr Freiraum beim Umsetzen zukünftiger Anforderungen. Wir können nun neue Benutzergruppen, Applikationen und Authentisierungsverfahren wesentlich einfacher und schneller integrieren.»

Aus der Sicht von E-Finance ist jedoch vor allem eines wichtig: Die Migration der über 1,1 Millionen Benutzer wurde ohne Beeinträchtigung der Kunden durchgeführt. Oder haben Sie etwas davon gemerkt? ■

Simon Uhde

Simon Uhde, Informatik-Ingenieur FH, arbeitet seit 2007 für AdNovum in Bern und betreut als technischer Projektleiter unsere Kunden vor Ort. Er beschäftigt sich vor allem mit der Entwicklung und Integration von Projekten im Nevis-Umfeld sowie mit technischen Schnittstellen. In seiner Freizeit bewegt er sich sowohl im Winter wie auch im Sommer gerne in den Bergen.

Vom physischen zum digitalen Ausweis

SuisseID: die sichere Identität jetzt mit qualifizierten Attributen auf Karte und im Identity Provider.

Von Stephan Breitenmoser, Leiter Solutions-Center, Trüb AG

Heute besitzt jeder von uns mindestens acht Plastikkarten mit Ausweischarakter, ohne die wir nicht leben wollen oder können. Mitarbeiterausweis, Identitätskarte, Fahrausweis, Kreditkarte, Versichertenkarte und Kundenbindungskarten setzen wir jeden Tag ein. Mit dem Vorweisen der Karte lösen wir Zahlungen aus, erhalten Zutritt, fordern Treuepunkte ein, beweisen unsere Fähigkeit, überschreiten nationale Grenzen und vieles mehr.

Menschen und Systeme prüfen die Gültigkeit der Karten vor Ort und vertrauen in die eindeutigen Informationen wie Foto, Geheimcode (PIN), elektronische und optische Erkennungsmerkmale und oftmals zusätzlich aufgebrachte Sicherheitsmerkmale auf der Karte.

Über Jahre haben sich Standards (z. B. VISA- und MasterCard-Richtlinien) entwickelt, welche die Ausstellung von der Berechtigungsprüfung bis zur Kartenproduktion und die Anwendung vor Ort so gestalten, dass alle involvierten Parteien Vertrauen in die Funktion haben können.

Immer mehr Geschäftsabwicklungen finden in der digitalen Welt statt. Wird aber eine eindeutige Identität benötigt, gerät die Abwicklung sehr schnell ins Stocken. Die heute übliche Identifikation kann nicht einfach in die elektronische Welt übernommen werden. Bislang ist dafür die physische Präsenz des Identitätsinhabers notwendig, z. B. bei der Überprüfung des Fahrausweises.

Die Identität in der digitalen Welt

Seit Mai ist in der Schweiz die SuisseID erhältlich, die die sichere Identifizierung und Authentisierung gegenüber Online-Applikationen (Geschäfts- und Behördenverkehr) und das rechtsverbindlichen Unterschreiben von elektronischen Dokumenten ermöglicht. Damit lassen sich Medienbrüche und Kosten vermeiden und bedeutsame Effizienzsteigerungen erzielen.

Die SuisseID wird von den zertifizierten Zertifikateherausgebern QuoVadis, SwissSign, Swisscom und BIT unter definierter hoher Sicherheit herausgegeben, sei es direkt oder mit Zusatzfunktionen unter Einbezug von Dritten (Beispiel Mitgliederausweis des Schweizerischen Anwaltsverbands). Sie wird sowohl auf Chipkarte als auch auf USB-Stick angeboten.

Die benötigten Informationen für die digitale Welt liegen als qualifizierte Attribute sicher auf der Chipkarte bzw. im Zertifikat mit den privaten Schlüsseln einerseits sowie online bei einem sogenannten Identity Provider Service (IdP) andererseits. Mittels Geheimzahl (PIN) authentisiert sich der Karteninhaber gegenüber der Karte und schaltet diese frei. Gegenüber einer Applikation ermöglichen Besitz (Karte) und Wissen (PIN-Code) eine starke Authentisierung. Diese gibt den Anwendungen die nötige Sicherheit und der Zugriff auf Daten und Systeme kann gewährt werden. Mit der SuisseID können alle Online-Applikationen unabhängig vom Kartenherausgeber davon profitieren.

Über Trüb AG

Die Trüb AG, gegründet 1859, ist heute ein in der Schweiz und international führendes Unternehmen auf dem Gebiet von Bankkarten, Mitarbeiterausweisen sowie von staatlichen Ausweisen wie Identitätskarten, Fahrausweisen und Datapages für Reisepässe. Unter streng zertifizierten Sicherheitsbedingungen finden Kartenherstellung, Kartenpersonalisierung, Chip-Applikations-Engineering sowie Datenmanagement statt. Geliefert werden u. a. PKI-Karten für z. B. Estland oder Hongkong, aber auch Mitarbeiterausweiskarten für Unternehmen wie Allianz, Fraunhofer und seit Mai dieses Jahres auch die SuisseID inkl. Identity Provider Service.
www.trueb.ch

Trüb AG und die SuisseID

Die Trüb AG erbringt umfassende Sicherheitsdienstleistungen im Umfeld von SuisseID und ist der Partner für Zertifikatanbieter und für Kartenherausgeber. Mit QuoVadis wurde eine sehr umfassende Lösung erarbeitet.
Trüb AG liefert:

- *Chipkarten und deren Ausstellung nach ZertES*
- *Kartenverwaltung mit Prüfung weiterer Merkmale (z. B. Mitgliedschaft Schweizerischer Anwaltsverband)*
- *Betrieb des QuoVadis Core Identity Provider (von AdNovum im Auftrag des SECO erstellte SuisseID-Kernkomponente)*
- *Betrieb von Identity Providers (IdP) und Claim Assertion Services (CAS) für Dritte (z. B. verschiedenste Funktionsregister)*

Mehr Infos unter www.suisseid-shop.ch.

Der digitale Funktionsnachweis

Für die Abwicklung von Geschäften gilt es oft auch die Funktion bzw. Berechtigung nachzuweisen. In der traditionellen Welt brauchte man dafür eine spezifische Karte (z. B. Angabe Fahrzeugkategorie auf Fahrausweis). Für den Inhaber einer SuisseID werden solche Attribute nun in sicheren Online-Registern geführt, den sogenannten Claim Assertion Services (CAS). Dies ermöglicht lückenlose elektronische Workflows und effiziente Autorisierungskonzepte. IdP und CAS sind in der Regel in einem Service integriert.

Nebst dem Core IdP/CAS mit einem definierten Set an Attributen (z. B. Nationalität, Alter) können unabhängige weitere IdP/CAS geschaffen werden. So werden Angaben aus Berufsregistern (Notare, Ärzte), Handelsregister, Adressdiensten und Ratingdiensten erstmals effizient und standardisiert für digitale Business-Prozesse nutzbar.

SuisseID als Funktion auf der Karte

Die SuisseID-Spezifikation erlaubt die Ausgabe von mehreren Karten pro Person. Die herkömmliche physische Karte kann so mit SuisseID-Elementen erweitert werden und wird damit multifunktional. Beispielsweise kann für ein Unternehmen, welches seine IT-Infrastruktur absichern möchte, eine «Mitarbeiter-SuisseID» produziert werden. Diese kann gleichzeitig auch kontaktlose Zutrittstechnologie (z. B. LEGIC) beinhalten und mit Foto als Sichtausweis des Unternehmens ausgestellt werden. Das Unternehmen muss so keine eigene PKI aufbauen bzw. betreiben und profitiert von deutlich tieferen Kosten je Mitarbeiter. Der Mitarbeiterausweis kann damit als Mehrwert alle Funktionen der SuisseID bieten wie die rechtsverbindliche elektronische Unterschrift, den Smartcard-Logon, die Authentisierung im Netz und die E-Mail-Signatur, mit optionalem Verschlüsselungszertifikat auch die Verschlüsselung von Mails, Daten und Festplatten.

SuisseID als Erweiterung des heutigen Mitarbeiterausweises: sichere Identität und qualifizierte Attribute für effiziente und nachvollziehbare Geschäftsprozesse.

Konzept mit Zukunft

Wir gehen auch davon aus, dass in den nächsten Jahren viele bestehende Kartenprogramme von Banken, Versicherungen und Verbänden sowie Mitarbeiterausweise die SuisseID-Funktion übernehmen. Sichere Portallösungen mit Mehrnutzen für den Karteninhaber werden so alltäglich. Der physische Ausweis für unterschiedlichste Anwendungen wird bestehen bleiben. Aber er wird mit digitalen Elementen versehen werden und damit auch unser tägliches digitales Leben absichern. Wir sind von der SuisseID überzeugt und gespannt, wann sie sich auch in einer elektronischen Schweizer Identitätskarte wiederfindet. ■

Impressum

Herausgeber:
AdNovum Informatik AG
Corporate Communication
Röntgenstrasse 22
CH-8005 Zürich
Telefon 044 272 61 11
E-Mail info@adnovum.ch
www.adnovum.ch
Verantwortung und Redaktion:
Manuel Ott
Feedback: notitia@adnovum.ch
Gestaltung und Realisation:
Rüegg Werbung, Zürich
Fotografie:
Patrick Rohner, Zürich (Titel); Gerry Nitsch, Zürich (Porträts)
Gedruckt auf Balance Pure FSC