Netzguide, 9. November 2011

Ein E-Banking-Pilotprojekt auf europäischer Ebene

Was gehört alles zur Kernbanken-IT? Gehört beispielsweise IAM (Identity and Access Management) dazu? Ist IAM wirklich Teil des Banken-Kerngeschäfts? Es spricht vieles dafür, dass die Antwort «Nein» lauten sollte. Reinhard Riedl

Prof. Dr. Reinhard Riedl ist Forschungsleiter im Fachbereich Wirtschaft und Verwaltung der Berner Fachhochschule und Mitglied des Expertenrats E-Government Schweiz.
reinhard.riedl@bfh.ch

Was gehört zur Kernbanken-IT? Was ist das Maturitätsziel der Kernbanken-IT? Diese Fragen haben viel mit der Frage zu tun, wie sich das Bankgeschäft in Zukunft entwickeln wird. Denn die IT muss sich selbstverständlich am Business orientieren. Aber die IT muss sich auch die Frage gefallen lassen, was das Kerngeschäft einer Banken-IT ist, was outgesourct werden kann, weil es nicht zu diesem Kerngeschäft gehört, und wie wirtschaftlich die hausgemachten IT-Dienstleistungen sind.

Maturitätsziel «Dynamic Venturing»

Mittelfristig lautet das Maturitätsziel «Dynamic Venturing» mit der Fähigkeit, neue Geschäftsmodelle und Kollaborationen einfach aufsetzen zu können. Dynamic Venturing steht für eine IT, die ihr etabliertes Geschäft im Griff hat und als flexibler Partner für unternehmerische Innovationen auftritt. Es ist eine BoB-IT, eine Best-of-both-Worlds-IT: Dynamic Venturing verbindet die klassischen Ingenieurstugenden, die man als Techniker-Analogon zu den traditionellen Bankierstugenden ansehen kann, mit dem wilden «Der-schnellere-ist-der-geschwindere»-Hacker-Spirit, den man als Analogon zum mathematischen Erfindergeist des heutigen Investment-Bankings ansehen kann.

Im wirklichen Leben ist Dynamic Venturing ein Fernziel, auch wenn gerade in der Banken-IT einigen schon substanzielle Schritte in dieser Richtung gelungen sind. Näher lieg die Entschlackung und Beschränkung der Banken-IT-Abteilung auf die Kernbanken-IT-Aufgaben. Sie ist – cum grano salis – eine Form der Beschränkung auf die Kernkompetenzen der Banken-IT-Abteilung. Die Beschränkung aufs Kerngeschäft stellt einen wichtigen «institutionellen» Schritt Richtung Dynamic Venturing dar und wirft die Frage auf: Was gehört alles zur Kernbanken-IT? Gehört beispielsweise – und damit nähere ich mich endlich dem Kernthema dieses Beitrags an – IAM (Identity and Access Management) dazu? Ist IAM wirklich Teil des Banken-Kerngeschäfts? Es spricht vieles dafür, dass die Antwort «Nein» lauten sollte.

Kontext für ein europäischen E-Banking-Pilotprojekt

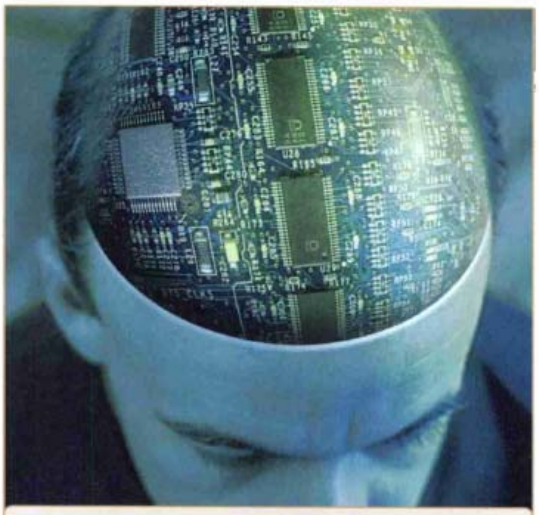
Die Perspektive, ein zukünftiges Outsourcing des IAM möglich zu machen, ist der Kontext, in dem wir ein europäisches E-Banking-Pilotprojekt mit zehn teilnehmenden europäischen Staaten vorgeschlagen, geplant und vorbereitet haben. Aber es ist nicht der einzige Kontext. Einen zweiten Kontext liefert der ungebrochene Trend zu mehr Compliance, sprich zu besserer Nachvollziehbarkeit der Geschäftstätigkeit. Mag es auch im Augenblick grössere und schwierigere Probleme

geben, unter dem Strich ändern diese nichts am Kernthema «mehr und bessere Transparenz und mehr und effektivere Regel-Compliance!». Das wird auf Jahre hinaus so bleiben. Wobei es darum gehen wird, die formalistische, regelreiche amerikanische und die inhaltlich orientierte europäische Sicht zusammenzubringen. Wie schon die Geschichte der Künstlichen Intelligenz lehrt, kann man mit einer quantitativen Maximierung von Regeln kein intelligentes Verhalten schaffen. Das gilt auch für alle Arten von Regulierungen, insbesondere solche zu Transparenz und Compliance.

Der dritte Kontext kommt aus der EU-Wirtschaftspolitik. Die EU-Kommission strebt einen einheitlichen europäischen E-Business-Raum an und dafür benötigt sie einen einheitlichen europäischen Identifikations- und Authentifikationsraum. Die nationalen eIDs (elektronische Identitäten) sollen nicht nur für nationales E-Government genutzt werden können, sondern auch für E-Business – für E-Business nicht nur im eigenen Land, sondern europaweit. Dabei soll es möglich sein, mehr Eigenschaften als nur Namen, Nationalität und Adresse dem Geschäftspartner gegenüber vertrauenswürdig auszuweisen. Auch erworbene Qualifikationen, Berufsberechtigungen und andere relevante Attribute sollen ausgewiesen werden können. Stets natürlich nach dem Prinzip der Selbstbestimmung und Minimalisierung: ich entscheide, was ich zeigen will und es wird nicht automatisch mehr ausgewiesen! (Konsequent zu Ende gedacht verlangt dies auch nach Formen vertrauenswürdiger Anonymität, die aus Compliance-Perspektive aber nur auf Basis einer klaren und korrekten Attribute-Logik zulässig ist.)

Dieser einheitliche Identifikations- und Authentifikationsraum soll weitgehen offen, aber kontrolliert sein. Offen heisst, es soll keine A-Priori-Ontologie für die auszutauschenden Attribute geben. Höchstens eine beliebig erweiterbare Basis-Ontologie, die die wichtigsten E-Business-Bedürfnisse abdeckt. Und es sollen auch kommerzielle eIDs mit hoher Authentifizierungsqualität – beispielsweise E-Banking eIDs – europaweit für alle Arten von E-Business eingesetzt werden können. Selbstverständlich auch die an Bedeutung gewinnenden «Mobile eIDs». Kontrolliert dage-

«E-Banking ist aus Sicht sehr vieler Akteure im eID-Bereich eine potenzielle Killer-Applikation für die nationalen eIDs.»



Wie schon die Geschichte der Künstlichen Intelligenz lehrt, kann man mit einer quantitativen Maximierung von Regeln kein intelligentes Verhalten schaffen.

Bildquelle: Fotolia

gen heisst, dass es eines Akkreditierungsverfahrens bedarf und dass die Technologie sicherstellt, dass Täuschungen im elektronischen Geschäftsverkehr nicht möglich sind. Es geht also darum, Geschäftsbarrieren in Europa weiter abzubauen und gleichzeitig die Sicherheit und Nachvollziehbarkeit von grenzüberschreitender Geschäftstätigkeit zu garantieren.

STORK 2.0 kurz zusammengefasst

Um das Entstehen eines einheitlichen elektronischen Identifikations- und Authentifikationsraums zu fördern, hat die EU-Kommission ein CIP-PSP-Innovationsprojekt ausgeschrieben, genauer einen sogenannten «large scale pilot (pilot A)». Ein Konsortium aus 19 Staaten – darunter erstmals und einmalig die Schweiz – hat sich um die Durchführung

des Projekts beworben und den Zuschlag bekommen. Derzeit laufen die letzten Detailverhandlungen. Doch klar ist, dass von Januar 2012 bis Dezember 2014 das Projekt STORK 2.0 durchgeführt wird und dass im Jahr 2014 vier konkrete Pilotprojekte stattfinden werden:

- ein Pilotprojekt mit Universitätsdiensten (u.a. Bereitstellung von Qualifikationszertifikaten);
- ein Pilotprojekt im Gesundheitswesen, das heisst im E-Healthcare (fokussiert auf den sicheren Zugriff auf Patientendaten im Ausland);
- ein Pilotprojekt mit elektronischen Unternehmensregistern (für Business-to-Business-Geschäftstransaktionen);
- ein Pilotprojekt im E-Banking (für Privatpersonen und vor allem für Unternehmen).

Die Schweiz wurde in der Planungsphase des Projekts im Auftrag des Seco von der Berner Fachhochschule vertreten (mit dem Autor dieses Beitrags als Verhandlungsführer). Wir haben dabei den E-Banking-Piloten geplant, ebenso wie (zusammen mit Grossbritannien) das Arbeitspaket zum Design der STORK-2.0-Infrastrukturdienstleistungen und Geschäftsmodelle und zum Entwurf einer Akkreditierungsagentur für eID-Anbieter. Und wir sind für die Leitung beider Schlüsselaktivitäten des Projekts designiert (ohne den Abschlussverhandlungen vorgreifen zu wollen). Darüber hinaus sollen wir die Schweiz im E-Health-Piloten vertreten und in weiteren Arbeitspaketen, unter anderem zur Klärung von Vertrauensaspekten und rechtlichen Fragen.

Das klassische Henne-Ei-Problem: Die Bürger kaufen keine SuisseID, weil es wenig SuisseID-taugliche Dienstleistungen gibt, und es gibt wenig SuisseID-taugliche Dienstleistungen, weil nur wenig Bürger die SuisseID besitzen. Bildquelle: Fotolia

Motivation für E-Banking in STORK 2.0

Worum geht es im STORK-2.0-E-Banking Piloten? Warum engagieren wir uns, obwohl wir als Hochschule einen Teil des Geschäftsrisikos selbst tragen müssen? Die Gründe liegen einerseits in den drei skizzierten Kontexten und anderseits in den Kosteneinsparungen und im geschäftlichen Nutzen. Es geht also um die Auslagerung des IAM aus der Kernbanken-IT, um die Erhöhung der Compliance – insbesondere die Compliance im E-Banking für Geschäftskunden – und um die Promotion eines einheitlichen europäischen eID-Raums durch eine Applikation, die grosse Breiten- und PR-Wirkung hat. E-Banking hat zweifelsohne das Potenzial, zur positiven Killer-Applikation für den einheitlichen europäischen Identifikations- und Authentifikationsraum zu werden.

Es geht aber auch darum – und vielleicht sogar an allererster Stelle –, dass Banken ihr grenzüberschreitendes Geschäft einfacher, effektiver und sicherer gestalten können. Es soll in Zukunft möglich sein, basierend auf einer ordentlich ausgegeben eID der höchsten Qualitätsstufe, Bankkonten online nicht nur zu eröffnen, sondern für eine umfängliche Nutzung freizuschalten, denn die Personenprüfung bei der Ausgabe einer eID höchster Qualitätsstufe ist vergleichbar mit der Identitätsprüfung bei der Eröffnung eines Bankkontos. Es gibt keinen Grund, warum für die Eröffnung jeder neuen Geschäftsprüfung wieder eine neue Identitätsprüfung stattfinden soll, wenn die Ausgangsprüfung im eID-Ausgabeprozess sorgfältig stattfindet. Es soll aber auch möglich sein, sicheres E-Banking anzubieten, ohne dass ein Kunde eine eigene E-Banking- eID erhalten muss, mit den entsprechenden Prozess- und Materialkosten für die Bank.

Last but not least soll es für Firmen in Zukunft einfacher und sicherer werden, ihre Banktransaktionsaufgaben auf mehrere Personen zu verteilen. Geschieht der Zugriff beim

E-Banking über persönliche eIDs auf der Basis von im Konto hinterlegten Zugriffsrechten, so können die Aufgaben flexibel umverteilt werden (durch eine Änderung der hinterlegten Zugriffsrechte) und es ist stets nachvollziehbar, wer im Namen des Unternehmens Transaktionen durchgeführt hat. Letzteres erhöht die De-facto-Nachvollziehbarkeit und damit die Compliance. Und dies alles über nationale Grenzen hinweg, ohne dass Banken im Ausland eigene Vertretungen aufbauen müssen – und selbstverständlich auch ohne dass sie für ausländische Kunden eine eigene elektronische Infrastruktur aufbauen müssen.

Den Schlüssel dazu, um all diese Ziele erreichen zu können, liefert die bereits vorhandene und in sechs früheren Pilotprojekten des Vorgängerprojekts STORK ausgetestete Interoperabilitätsinfrastruktur für nationale eIDs. Allerdings ist noch viel zu tun. Die SuisseID ist noch nicht an diese Infrastruktur angeschlossen. Und als einziges europäisches Land hat bisher Österreich zehn ausländische nationale eIDs gesetzlich der eigenen eID-«Bürgerkarte» gleichgestellt.

Strategische Perspektiven

Beim Entscheid, bei STORK 2.0 mitzumachen, standen für uns neben der Banking-IT-Perspektive die E-Economy in der Schweiz und die Schweizer Digitale Agenda 2020 im Vordergrund. Konkret geht es um das doppelte Ziel, dass einerseits die Schweizer SuisseID in ganz Europa für Geschäftstransaktionen eingesetzt werden können sollte und dass andererseits Schweizer Unternehmen ohne Sicherheitsrisiken E-Business-Dienste für ausländische Kunden mit einer nationalen eID anbieten können sollten.

Für Brüssel, aber auch für das Nachbarland Österreich, stand ein Pilot im E-Banking ganz oben auf der Prioritätenliste, wobei die Schweiz von Anfang an als «natürlicher» Pilot-Leader angesehen wurde. Denn in Europa und insbesondere bei unseren deutschsprachigen Nachbarn steht die Schweiz für hohe Seriösität und Exzellenz in der Bankwirtschaft.

E-Banking ist aus Sicht sehr vieler Akteure im eID-Bereich eine potenzielle Killer-Applikation für die nationalen eIDs. Deren Verbreitung geht in den meisten europäischen Ländern sehr schleppend vor sich. Hauptgrund dürfte sein, dass Usability und einfache Benutzbarkeit in den meisten Fällen nicht zu den Stärken der nationalen eIDs zählen. Die Österreicher, die mit ihrer Bürgerkarte einst zu den europäischen Vorreitern im eID-Bereich zählten, setzen mittlerweile stark auf die Bürgerkarte auf dem Mobiltelefon, denn diese bietet endlich echte Benutzerfreundlichkeit. Trotzdem wächst die Nutzung der Bürgerkarte noch immer nicht rasend schnell. Da ist es auch kein Wunder, dass die sehr junge SuisseID in ihrem zweiten Jahr nur recht zäh vom Fleck kommt. Die Grundproblematik besteht darin, dass wir es mit einem klassischen Henne-Ei-Problem zu tun haben: die Bürger kaufen keine SuisseID, weil es wenige SuisseID-taugliche Dienstleistungen gibt und es gibt wenige SuisseID-taugliche Dienstleistungen, weil nur wenige Bürger die SuisseID besitzen. Ähnlich schaut es in anderen Ländern aus. Doch die Möglichkeit, E-Banking mit nationalen eIDs durchzuführen, könnte dieses Henne-Ei-Problem lösen. Insbesondere dann, wenn gleichzeitig durch den einheitlichen europäischen Identifikations- und Authentifikationsraum sichergestellt wird, dass die Nützlichkeit der eIDs in Zukunft hochskaliert wird, wenn sie universell und ohne Ländergrenzen einsetzbar werden.

Aber auch umgekehrt bietet der Einsatz von nationalen eIDs im E-Banking für das Bankgeschäft signifikante Vorteile. Banken würden erheblich profitieren. Sie wären das eID-Handling weitgehend los und können die Kostenvorteile an die Kunden weitergeben. Dazu kommt, wie oben skizziert, die Erhöhung der Compliance. Und ganz nebenbei wäre es ein wichtiger Schritt zum Outsourcen des Identitäts- und Zugriffsmanagements.

Konkret für die Schweiz bietet die Leitung des E-Banking-Piloten ebenso wie die Ko-Leitung des Designs der Infrastrukturservices, der Geschäftsmodelle und der Akkreditierungsverfahren die Möglichkeit, für einmal nicht freiwillig autonom nachzuvollziehen, was die mächtige EU vorgibt, sondern im Entwurf selbst eine Schlüsselrolle zu spielen. Damit dies so passieren kann, ist vorgesehen, dass die Arbeit der Berner Fachhochschule regelmässig supervisiert wird durch das Seco und das Informatikstrategieorgan des Bundes (ISB) im Eidgenössischen Finanzdepartement (EFD). Dies stellt sicher, dass einerseits die Interessen der Bundesverwaltung Eingang in die Entwicklung zukünftiger europäischer Standards finden und andererseits die entwickelten europäischen Standards frühzeitig im Gesetzgebungsprozess mit berücksichtigt werden können. Die Schweizer Projektbeteiligung wird unterstützt durch die Schweizerische Bankiervereinigung. Ein regelmässiger Austausch mit der Finanzmarktaufsicht Finma ist ebenfalls

geplant.

Die Durchführung des E-Banking-Piloten in zehn Ländern wird eine grosse Herausforderung darstellen. Aber sie wird in verschiedensten Richtungen starke Impulse liefern für die Entwicklung der E-Economy in der Schweiz und in Europa. ■