Digitale Identität und Datenschutzanforderungen an IT-Lösungen im E-Government

Reinhard Riedl

Institut für Informatik, Universität Zürich
CH-8057 Zürich, Winterthurerstrasse 190e
riedl@ifi.unizh.ch

Schlagworte: E-Government, Requirements Engineering, IT-Architektur

Abstract: Das Verständnis rechtlicher Prinzipien und die Integration widersprüchlicher Anforderungen ist eine Kernaufgabe des HW/SW-Entwurfs von E-Government-Lösungen durch IT-Architekten. Wir diskutieren die dabei auftretenden Probleme und leiten daraus Forderungen für die Praxis und die zukünftige Forschung ab.

1. Problematik

In diesem Beitrag diskutieren wir die Problematik des IT-Architekturentwurfs im E-Government, wie sie sich für den IT-Architekten stellt, der behördenübergreifende E-Governmet-Lösungen entwerfen muss. Neben den technischen Schwierigkeiten der Vernetzung von heterogenen, eigentlich nicht interoperablen Systemen, die insbesondere auch auf inkompatible Ontologien und diese abbildenden Datenrepositorien basieren, müssen IT-Architekten beim Entwurf von behörden- und länderübergreifenden E-Government-Lösungen auch die unterschiedlichen, gültigen Datenschutzbestimmungen einhalten. Trotz verpflichtender EU-Richtlinien sind die Gesetze zum Schutz der Privatsphäre derzeit in Europa alles andere als deckungsgleich, und auch die Erwartungen der Bürger im Spannungsfeld zwischen Schutz der Privatsphäre des Einzelnen und Schutz der Gesellschaft vor organisiertem Verbrechen und Terrorismus unterscheiden sich von Land zu Land und von Region zu Region.

Obwohl IT-Architekten im Allgemeinen keine juristische Ausbildung besitzen, und obwohl das Denken in Informatik-„Patterns" sich wesentlich unterscheidet von juristischen Betrachtungsweisen, müssen sie trotzdem die unterschiedlichen Gesetze auf der Ebene des Architekturentwurfs implementieren und letztendlich technisch in Einklang bringen, damit die

HW/SW-Implementation eines E-Government-Dienstes die Rechte der Bürger respektiert und den Behörden es ermöglicht, ihren Verpflichtungen nachzukommen. Gleichzeitig müssen aber auch alle technischen Anforderungen an ein gutes Design und das Bedürfnis der Benutzer nach Benutzerfreundlichkeit erfüllt werden, und insbesondere Gegenmaßnahmen gegen jene Sicherheitsbedrohungen getroffen werden, die bei einer Digitalisierung von Behördendienstleistungen hinzukommen. Letztere bestehen vor allem in der potentiellen Skalierbarkeit des Gebrauchs falscher Identitäten und der Skalierbarkeit von Datenzerstörungen und -veränderungen. Schließlich und oft zuallererst, besteht das Bedürfnis, die technischen Möglichkeiten zur Identifikation von krimineller Aktivitäten zu nutzen, die die Digitalisierung zusammen mit dem Einsatz heutiger und zukünftiger Data-Mining Technologie bietet. Diese und noch andere Sichten auf den IT-Architekturentwurf lassen sich nicht einfach in Einklang bringen, auch wenn es verschiedene Engineering-Metaphern wie beispielsweise „Transparenz" gibt, die widerstreitende Anforderungen zu einer Perspektive vereinigen. Die Integration aller Aspekte, nicht zuletzt sondern eher zuerst auch des Schutzes der Privatsphäre, wie er unter anderem durch Datenschutzgesetze festgeschrieben ist, setzt ein gutes Requirements Engineering voraus, damit darauf aufbauend integrative Architekturentwürfe für die vielseitig unterschiedlichen Anforderungen entwickelt werden können.

2. Probleme beim Requirements-Engineering und beim Architekturentwurf für E-Gov-Dienste

Das große Problem beim Requirements Engineering wie beim nachfolgenden Architekturentwurf ist, neben dem oft grundsätzlich fehlenden Problembewusstsein aller Beteiligter, dass Informatiker keine Rechtsexperten sind und Rechtsexperten nicht gewohnt sind, semiformale technische Anforderungsspezifikationen für den SW-Entwurf (und eventuell auch HW-Entwurf) zu verfassen. Die Strukturen der Gedankenwelt von IT-Architekten sind – so zeigt die Erfahrung – sehr verschieden von jenen der Gedankenwelt von Rechtsexperten. Viel rechtlich Wichtiges ist für den IT-Entwurf belanglos (und also „technisch" langweilig), während umgekehrt das, was IT-Architekten als „auf den Punkt gebracht" ansehen für Rechtsexperten oft eine wenig signifikante Betrachtungsweise der Problematik darstellt.

Wie problematisch eine IT-orientierte Herangehensweise der Behörden an das E-Government aus einer juristischen Perspektive betrachtet sein kann, haben beispielsweise die Analysen von UK-Online gezeigt (vergl. z.B. *Leith* und *Morison*, 2002). Ein treffliches Beispiel für den umgekehrten Fall ist die in weiten Teilen des E-Government mit juristischem Hintergrund ignorierte Problematik des Schutzes der biometrischen Daten. Für

„Techniker" (hoffentlich) ein klares Problem, taucht es in juristischen E-Government-Diskussionen selten auf: Kaum jemals wurde Protest gehört, wenn in der Öffentlichkeit eine Biometrielösung vorgestellt wurde, die die europäischen Richtlinien verletzt. Grund dafür scheint zu sein, dass es bei der Implementierung biometrischer Authentifikation wesentlich um die Frage geht, wo biometrische Daten wie gespeichert werden dürfen, also um eine technische Frage, die nur aus dem Verständnis der technischen Implikationen der Verteilung biometrischer Daten (und der Anwendung von Authentifikationsprotokollen) heraus beantwortet werden kann.

Ein weiteres Beispiel, das zeigt wie wichtig und schwierig die Übersetzung juristischer Prinzipien in IT-Architektur-Konstrukte ist, ist das in der Literatur häufig als Ziel des E-Government für Bürger definierte „One-Stop-E-Government" (vgl. z.B. *Wimmer* 2002). In den Anfängen des E-Government wurde diese Idee aus dem Wunsch heraus geboren, von behörden-zentrierten Prozessbetrachtungen und Modellierungen der Amtsvorgänge und Abläufe in den Behörden zu bürgernzentrierten Modellen und Implementationen zu gelangen. Der auf einer technischen Brokerarchitektur basierenden „E-Government-Shop" soll es dem Bürger ermöglichen, in einem Vorgang verschiedenste Interaktionen mit den Behörden „in einem" zu vollziehen. Ähnliche Ideen für integrierte Prozess-Architekturen gab es auch E-Healthcare, wo man beispielsweise in Großbritannien (motiviert durch tragische Todesfälle) das Ziel definierte, von „Silo-Diensten" zu Broker-Dienstleistungen zu gelangen (vgl. z.B. *Booth* und *Martin*, 2002).

One-Stop-E-Government und sein Analogon im E-Healthcare streben primär nach großer Bürgerfreundlichkeit und mehr Effizienz der Behörden. Wenn sie aber technisch zu „elegant" implementiert werden, dann verletzen sie eventuell die Datenschutzrechte der Bürger. Insbesondere wenn die alten Behördenvorgänge zu „glatt" zu neuen, bruchlosen „Bürgerprozessen", z.B. basierend auf Lebenslagenkonzepten, integriert werden, sind die Bürgerrechte auf Schutz ihrer Daten in Gefahr. Das grundsätzliche Problem bei der Integration zu One-Stop-Lösungen ist nämlich, dass der Bürger die Kontrolle über den Fluss von seinen Personaldaten zwischen Behörden verlieren kann. Das EU-IST-Projekt FASME (2000 – 2001) hat zwar prototypisch demonstriert, dass es skalierende und sichere, gesamtheitliche Architekturen für E-Government-Lösungen gibt, aber es hat gleichzeitig auch viele neue Fragen aufgeworfen, deren Beantwortung Voraussetzung dafür ist, vom Prototyp zur Echtweltimplementation vorwärts zu schreiten (vgl. z.B. *Riedl* 2001). In der Praxis muss außerdem vielerorten erst noch das Bewusstsein geschaffen werden, wie kritisch One-Stop-E-Government-Lösungen aus Datenschutzperspektive sind.

Beide skizzierten Beispiele zeigen, dass die eigentlichen Probleme sich erst beim Architekturentwurf materialisieren und nicht notwendigerweise

bereits beim Requirements-Engineering bereits sichtbar sind, obwohl sie von dort herrühren. Dies ist ein zusätzliches Hindernis, dass nur durch ein Qualitätscontrolling umgangen werden kann, dass bereits an der Schnittstelle zwischen Rechtsexperten und Informatikern überprüft, ob mit genügender Konkretheit (aus Sicht der Informatiker, nicht der Rechtsexperten) die rechtlichen Anforderungen spezifiziert worden sind. Selbstverständlich muss danach durch das Qualitätscontrolling sicher gestellt werden, im Sinne von V&V, dass die IT-Architektur den Anforderungen entspricht, dass das SW-Anwendungsdesign die Architektur korrekt detailliert und dass die Implementation das Design korrekt implementiert.

3. Bedenkliche, wünschenswerte und kritische, technische Implementierungen

Besonders bedenklich sind technische Umsetzungskonzepte, die im Umlauf befindliche, digitale Dokumente als besitzerlos behandeln und zu einem unkontrollierten Fliessen von Personaldaten führen. Brokerarchitekturen verstoßen zwar nicht prinzipiell gegen den Datenschutz, und die in jüngster Zeit portierten Agentennetzwerke sind durchaus geeignet, E-Government-Dienste zu implementieren, aber die generischen Architektur- und Design-Patterns aus der Informatik müssen entsprechend selektiert und angepasst werden.

Wünschenswert wäre, wenn die juristischen Richtlinien nicht nur in manchen Vorzeigebeispielen sondern europaweit überall für IT-Architekten lesbar dokumentiert existierten. Nationale E-Government-Gesetze sind in diesem Zusammenhang zweifelsohne ein Schritt in die richtige Richtung. Wünschenswert wäre darüber hinausgehend, wenn es SW- und HW-Komponenten und Baupläne gäbe, die den Entwurf von IT-Lösungen auch ohne tieferes Verständnis der juristischen Randbedingungen ermöglichten (obwohl dieses natürliche die beste Sicherheitsgarantie ist). Derartige Komponenten auf nationaler Ebene bereitzustellen ist auch hier ein guter Schritt in die richtige Richtung (vgl. z.B. *Posch* et al. 2003).

Allerdings, nationale Lösungen, wie sie vielerorten in Europa entwickelt werden sind noch nicht notwendigerweise europaweit interoperabel, auch wenn sie europäischen Richtlinien gehorchen. Und One-Stop-E-Government, dass an den Grenzen halt macht, erfüllt den eigenen Anspruch an Benutzerfreundlichkeit nur für jene, die ihre Lebenstätigkeit auf ein Land beschränken.

Technisch nutzbare Anforderungsspezifikation sind für die Implementierung von globalen E-Government-Lösungen für alle eine notwendige, aber keine hinreichende Bedingung – zumindest so lange, wie Europa in so vielerlei Hinsicht heterogen und widersprüchlich bleibt. Die unterschied-

lichen rechtlichen und kulturellen Rahmenbedingungen stellen für das behördenübergreifende, und insbesondere für das internationale, E-Government eine große Herausforderung dar, die noch einige Jahre „Bleeding Edge" bleiben wird. Beispielsweise, und ganz banal, scheint es derzeit illusorisch, eine einzige HW-Sicherheitslösung europaweit einzusetzen, weil das Akzeptanzverhalten in den einzelnen Ländern zu unterschiedlich ist. Die Integration auf technischer Ebene zu lösen ist eines, und natürlich Vorbedingung, sie auf Prozessebene zu erreichen das Ziel, aber etwas anderes, und sie auf der praktischen Verwaltungsebene zu gewährleisten letztendlich das, was die Bürger interessiert, und noch einmal etwas ein anderes.

Ein praktisches Problem stellen beispielsweise die Benutzerschnittstellen „für alle" dar. Dieses Problem wurde in Europa mit seiner großen Vielfältigkeiten an kulturellen Formen bisher nur ansatzweise gelöst, ganz abgesehen davon, dass die meisten Dienste bisher nicht einmal behindertengerecht angeboten werden. Was in einem Land als nützlicher Dienst erscheint, ist im anderen politisch inkorrekt. Was von einer Benutzergruppe kategorisch an Transparenz eingefordert wird, erschwert für andere den Umgang mit den E-Government-Lösungen so sehr, dass sie diese nicht annehmen. Auch nach der umfänglichen technischen Integration treten bei der digitalen Benutzerführung noch immer viele jener Probleme auf, die davon herrühren, dass eine Behördenkultur von einem Fremden erst verstanden werden muss, bevor er mit der Behörde effizient interagieren kann. Auch dann, wenn die Technik im Hintergrund den voll-digitalisierten, automatisch gesteuerten Dokumententransfer ermöglicht, muss die Benutzerschnittstelle beispielsweise einem Nichtbriten die Bedeutung einer englischen Stromrechnung für den Bezug von sozialer Unterstützung vermitteln. (Sie kann als Wohnortnachweis verwendet werden.) Das Verstehen kann der E-Government-Dienst dem Benutzer unter anderem auch deshalb nicht abnehmen, weil jeder Transfer von Personaldaten den Prinzipien des Datenschutzes unterliegt, und es etwas sehr verschiedenes ist, ob man einen Menschen bevollmächtigt, für einen Behördentransaktionen zu erledigen, was bisher teilweise möglich ist, oder ob man der SW einer Behörde die entsprechenden Rechte überantwortet.

4. Digitale Identität

Obiges zusammenfassend gibt es erstens das Bedürfnis nach Spezifikationen der rechtlichen Anforderungen, die für Informatiker lesbar und umsetzbar sind, i.e. die genügend einfach und trotzdem ausreichend detailliert sind, und zweitens die Notwendigkeit, Dienstleistungen datenschutzkonform so zu integrieren, dass die Bürger verstehen, was mit ihren Personaldaten passiert. Wenn dies erreicht würde, könnte man zufrieden sein,

doch scheint uns eine derartige klassische SW-Engineering-Perspektive trotzdem zu kurz gedacht.

Alle Arten von Transaktionsdiensten im E-Government setzen die Implementierung von digitaler Identität voraus. SW-Clients sprechen in effigie von Bürgern mit Servern, die für die Clients tun, was letztlich für die Bürger gedacht ist, für die die Clients kommunizieren. In den letzten Jahren mussten die Informatiker im E-Government lernen, dass nicht immer das höchste Maß an Sicherheit und Vertrauenswürdigkeit notwendig ist. Da das Prinzip, immer nur das Sicherste, für ein großes System seine ganz spezifischen Gefahren birgt, die beispielsweise durch übermäßiges Vertrauen und Delegation der Verantwortung an den „Computer" erzeugt werden, impliziert das Fehlen des Bedarfs nach Maximalsicherheit in vielen Fällen, dass es sinnvoller ist, eine leichtgewichtigere, besser handhabbare, nur schwach sichere Lösung zu implementieren statt einer optimal sicheren. Daraus leitet sich die Schlussfolgerung ab, dass wir flexible Formen von Identität für eine heterogenen Welt implementieren können müssen, die möglichst weitgehend interoperabel sind (wo immer dies die rechtliche und administrative Logik zulässt).

Neben der Notwendigkeit, eine „normale, individuelle" digitale Identität für alle zu realisieren, besteht das Bedürfnis, auch anonyme Identitäten, Gruppenmitgliedschaften und Rollen digital zu implementieren (vgl. z.B. *Spinello* 1999 oder *Auerbach* 2003) – mit unterschiedlichen Implikationen für Ermächtigungsrechte. Zwischen den Diensten die die Authentifikation einer namentlich identifizierten Person verlangen, und jenen, die anonym von jedermann genutzt werden können, gibt es auch digitale Dienste, die zwar den Nachweis der Berechtigung zum Zugriff verlangen, nicht aber das Nennen des Namens. Wer Alkohol kauft, oder eine Studenten- oder Pensionistenermäßigung nutzt, muss beispielsweise sein Alter nachweisen, aber es gibt keinen Grund, dass er seinen Namen angibt oder Verkäufern die Möglichkeit eröffnet, seine Spuren als Konsument von Waren oder Diensten zu verfolgen. Oft ist es auch wünschenswert, dass die Nutzung einer Ermäßigung zwar als solche von den digitalen Systemen registriert und richtig verbucht wird, dass aber gleichzeitig der Nutzer den Ermäßigungsgrund nicht vor seiner privaten Umgebung offenbaren muss. Je nach Szenario sind also die verschiedensten Formen von Identität wünschenswert, inklusive verschiedener Formen von anonymer Identität. Eine digitale Identitätskarte allein vermag zwar viele Probleme prinzipiell zu lösen, sie ist aber aus Benutzersicht oft nicht die beste oder vielleicht sogar eine ziemlich schlechte Lösung, die den Verstoß gegen die Datenschutzrechte erleichtert.

Die Randbedingungen und Richtlinien für die digitale Identität festzuschreiben, ist eine politische Aufgabe, doch es kann nicht erwartet wer-

den, dass sie von Politikern ohne Mithilfe von Informatik kompetent erfüllt werden wird. Ganz im Gegenteil ist die digitale Identität als Spielball politischer Profilierungswünsche eine ernsthafte Bedrohung für die Zukunft, wenn die Visionen vom „ubiquituous" oder „pervasive computing" Wirklichkeit geworden sein werden. Hier ist deshalb noch einiges an transdiziplinärer Grundlagenforschung notwendig, in der die Rechtsinformatik eine zentrale Rolle spielen sollte, in der aber auch ökonomische, organisatorische, soziale, kulturelle und psychologische Sichten mitberücksichtigt werden sollten.

„Sage mir Deine Nummer und ich sage dir wer Du bist, was Du isst, und wen Du küsst." ?? Nein – so harmlos wird das, was wir an digitaler Integration in 10 Jahren von heute an erreicht haben werden vermutlich nicht sein! Deshalb ist es aus gesellschaftlicher Hinsicht notwendig, dass einerseits die Rechtsinformatik in Bezug auf die Anforderungen des IT-Architekturentwurf schnelle Fortschritte macht und dass andererseits Grundlagenforschung über digitale Identität in einer heterogenen Welt betrieben wird, in der es sehr unterschiedliche Anforderungen an Sicherheit, Vertrauenswürdigkeit und den Schutz der Privatsphäre gibt.

5. Ausblick

In letzter Zeit wurde die E-Government-Forschung grossteils anwendungsorientiert und produktnah betrieben, was dazu führte, dass viele grundsätzlichen Probleme globaler E-Government-Lösungen derzeit unterschätzt werden. Not täte mehr grundlagenorientierte, visionsfreundliche und auch risikoreichere Forschung, die auf profunden Kenntnissen der Rechtswissenschaften, der Computerwissenschaften und der Kenntnis der Informatikgeschichte mit allen ihren Fehlschlägen und Erfolgen fußt, und die interdisziplinär durchgeführt wird.

Literatur

N.Auerbach, Smart Card Support for Anonymous Citizen Services, wird erscheinen in: Proceedings of e-Society 2003, Lisbon, Portugal, 2003.

N. Booth, M. Martin, EHR – Animations and Arguments: From Discourse to Design (Power point Presentation), 2002, zuletzt besucht: 15. Mai 2003, http://www.schin.ncl.ac.uk/durhamehr, Presentations/EHR-_20Animations_20and_20Arguments_20cambridge_202000.ppt

P. Leith, J. Morison, UK Online: Forcing Citizen Involvement into a Technically-Oriented Framework?, in: *R. Traunmüller, K. Lenk*, Electronic Government, Proceedings EGOV 02, Springer Lecture Notes in Computer Science, LNCS 2456, 2002, S. 419 – 423.

R. Posch, A. Leiningen, T. Menzel, R. Schamberger, B.Wilder, Zielsetzung und Aufgaben der IKT Stabstelle, in: *M. Wimmer* (Hg.), Quo Vadis e-Government: State-of-the-art 2003, books@ocg.at, Band 165, Österreichische Computergesellschaft, Wien 2003, S. 111 – 122.

R. Riedl, Interdisciplinary Engineering of Interstate E-Governmemnt Solutions, in: *M. Beynon, C.L. Nehaniv, K.Dautenhahn* (Hg.), Cognitive Technology: Instruments of Mind, Springer Lecture Notes in Artificial Intelligence, LNAI 2117, 2001, S. 405 – 420.

R. A. Spinello, Regulating Digital Identity, in: Ethicomp 99 Conference Documentation on CD, 1999

M. Wimmer, Integrated Service Modeling for Online One-Stop Government, EM – Electronic Markets, Vol. 12, No. 3, 2002, S. 92 – 103.