Gesellschaft für Informatik e.V. (GI)

publishes this series in order to make available to a broad public recent findings in informatics (i.e. computer science and information systems), to document conferences that are organized in cooperation with GI and to publish the annual GI Award dissertation.

Broken down into
- seminars
- proceedings
- dissertations
- thematics

current topics are dealt with from the vantage point of research and development, teaching and further training in theory and practice. The Editorial Committee uses an intensive review process in order to ensure high quality contributions.

The volumes are published in German or English.

Information: http://www.gi.de/service/publikationen/lni/

ISSN 1617-5468
ISBN 978-88579-291-8

Die Fachtagung Verwaltungsinformatik (FTVI) und die Fachtagung Rechtsinformatik (FTRI) der Gesellschaft für Informatik haben zum Ziel, einen richtungsweisenden Dialog zwischen Wissenschaft und Verwaltungspraktikern, Rechtspraktikern und Beratern zu fördern. Die FTVI & FTRI 2012 finden in Friedrichshafen an der Zeppelin Universität unter dem Motto „Staat und Verwaltung auf dem Weg zu einer offenen, smarten und vernetzten Verwaltungskultur“ statt. Die Herausforderungen durch soziale Medien und Web 2.0-Technologien tragen derzeit erheblich zu einer Öffnung von Staat und Verwaltung und einem damit verbundenen Kulturwandel bei.

Jörn von Lucke, Christian P. Geiger, Siegfried Kaiser, Erich Schweighofer, Maria A. Wimmer (Hrsg.)
Auf dem Weg zu einer offenen, smarten und vernetzten Verwaltungskultur

197

GI-Edition

Lecture Notes in Informatics

Jörn von Lucke, Christian P. Geiger, Siegfried Kaiser, Erich Schweighofer, Maria A. Wimmer (Hrsg.)

Auf dem Weg zu einer offenen, smarten und vernetzten Verwaltungskultur

Gemeinsame Fachtagung Verwaltungsinformatik (FTVI) und Fachtagung Rechtsinformatik (FTRI) 2012

15.-16. März 2012 in Friedrichshafen

Proceedings

Jörn von Lucke, Christian P. Geiger, Siegfried Kaiser,
Erich Schweighofer, Maria A. Wimmer (Hrsg.)

Auf dem Weg zu einer offenen, smarten und vernetzten Verwaltungskultur

Gemeinsame Fachtagung Verwaltungsinformatik (FTVI) und Fachtagung Rechtsinformatik (FTRI) 2012

15.-16. März 2012

in Friedrichshafen an der Zeppelin Universität

gewidmet Univ.-Prof. Dr. Heinrich Reinermann zu seinem 75. Geburtstag

Gesellschaft für Informatik e.V. (GI)

Lecture Notes in Informatics (LNI) - Proceedings
Series of the Gesellschaft für Informatik (GI)

Volume P-197

ISBN 978-3-88579-291-8
ISSN 1617-5468

Volume Editors
Univ.-Prof. Dr. Jörn von Lucke
Zeppelin Universität - TICC
88045 Friedrichshafen, Germany
joern.vonlucke@zeppelin-university.de

Christian P. Geiger M.A.
Zeppelin Universität - TICC
88045 Friedrichshafen, Germany
christian.geiger@zeppelin-university.de

Dr. Siegfried Kaiser
ITOB GmbH
56729 Ettringen, Germany
kaiser@itob.de

Univ.-Prof. Dr. Dr. Erich Schweighofer
Universität Wien
1010 Wien, Austria
Erich.Schweighofer@univie.ac.at

Univ.-Prof. Dr. Maria A. Wimmer
Universität Koblenz-Landau
56070 Koblenz, Germany
wimmer@uni-koblenz.de

printed by Köllen Druck+Verlag GmbH, Bonn

Organisation von FTVI & FTRI 2012 in Friedrichshafen

Tagungsleitung

Prof. Dr. Jörn von Lucke, (Sprecher der FG VI), Zeppelin Universität Friedrichshafen
Prof. Dr. Maria Wimmer (Sprecherin des FB RVI der GI), Universität Koblenz-Landau
Dr. Siegfried Kaiser (ehemaliger stellvertretender Sprecher der FG VI), ITOB GmbH
Prof. Dr. Dr. Erich Schweighofer (Sprecher der FG RI), Universität Wien, Österreich
Christian Geiger, M.A., Zeppelin Universität Friedrichshafen

Programmkomitee

Prof. Dr. Walter Blocher, Universität Kassel
Dr. Uwe Brinkhoff, Bundesanstalt für Immobilienaufgaben
Dr. Michael Breidung, Stadt Dresden
Prof. Dr. Jan vom Brocke, Universität Liechtenstein
Prof. Dr. Martin Brüggemeier, HTW Berlin
Wolfgang Bruns, DLZ IT des BVBS
Prof. Dr. Ralf Daum, DHBW Mannheim
Prof. Dr. Wolfgang Eixelsberger, FH Kärnten
Prof. Dr. Andreas Engel, Stadt Köln
Prof. Dr. Nikolaus Forgó, Gottfried Wilhelm Leibniz Universität Hannover
Prof. Dr. Herbert Fiedler, Universität Bonn
Prof. Dr. Thomas Gordon, Fraunhofer FOKUS
Prof. Dr. Norbert Gronau, Universität Potsdam
Prof. Dr. Dirk Heckmann, Universität Passau und Zeppelin Universität Friedrichshafen
Hans-Peter Hess, Stadt Friedrichshafen
Prof. Dr. Dennis Hilgers, Universität Hamburg
Prof. Dr. Bernd Holznagel, Universität Münster
Prof. Dr. Gerrit Hornung, Universität Passau
Prof. Dr. Holger Hünemohr, Hochschule Rhein-Main
Dr. Siegfried Kaiser, ITOB GmbH
Prof. Dr. Sayeed Klewitz-Hommelsen, Hochschule Bonn-Rhein-Sieg
Prof. Dr. Ralf Klischewski, German University in Kairo, Ägypten
Prof. Dr. Helmut Krcmar, TU München
Tanja Krins, GfWM
Willy Landsberg, European Society for eGovernment e.V.
Prof. Dr. Klaus Lenk, Universität Oldenburg
Dr. Doris Liebwald, Universität Wuppertal
Prof. Dr. Peter Loos, Universität des Saarlandes
Prof. Dr. Jörn von Lucke, Zeppelin Universität Friedrichshafen
Prof. Dr. Dagmar Lück-Schneider, Hochschule für Wirtschaft und Recht Berlin
Prof. Dr. Andreas Meier, Universität Fribourg
Prof. Dr. Axel Metzger, Gottfried Wilhelm Leibniz Universität Hannover
Prof. Dr. Bela Mutschler, Hochschule Ravensburg-Weingarten
Prof. Dr. Philipp Müller, Universität Erfurt

Prof. Dr. Markus Nüttgens, Universität Hamburg
Prof. Dr. Günther Pernul, Universität Regensburg
Prof. Dr. Detlef Rätz, Fachhochschule der Sächsischen Verwaltung Meißen
Dr. Helmut Redeker, Rechtsanwälte Heinle, Baden, Redeker & Partner GbR, Bonn
Jürgen Renfer, Bayrischer Gemeindeunfallverband
Prof. Dr. Reinhard Riedl, FH Bern, Schweiz
Prof. Dr. Alexander Roßnagel, Universität Kassel
Georg Schäfer, Innenministerium Baden-Württemberg
Prof. Dr. Thomas Schaller, Hochschule Hof
Prof. Dr. Birgit Schenk, Hochschule Ludwigsburg
Prof. Peter Schilling, Fraunhofer FOKUS und Hochschule Ludwigsburg
Prof. Dr. Tino Schuppan, Institut für eGovernment, Potsdam
Prof. Dr. Gerd Schwabe, Universität Zürich
Prof. Dr. Dr. Erich Schweighofer, Universität Wien, Österreich
Peter Sauter, Landratsamt, Bodenseekreis
Prof. Dr. Gerald Spindler, Universität Göttingen
Ulf Steinmetz, Stadt Köln
Prof. Dr. Jürgen Stember, Hochschule Harz
Prof. Dr. Jürgen Taeger, Universität Oldenburg
Prof. Dr. Roland Traunmüller, Universität Linz, Österreich
Prof. Dr. Anne-Dore Uthe, Hochschule Harz
Prof. Dr. Andreas Wiebe, Universität Göttingen
Prof. Dr. Claus Christian Wiegandt, Universität Bonn
Prof. Dr. Maria A. Wimmer, Universität Koblenz-Landau
Dr. Petra Wolf, TU München
Dr. Marianne Wulff, Vitako
Prof. Dr. Hans-Dieter Zimmermann, Fachhochschule St. Gallen

Veranstalter

Gesellschaft für Informatik e.V. (GI)
- Fachbereich Informatik in Recht und Öffentlicher Verwaltung
  - Fachgruppe Verwaltungsinformatik
  - Fachgruppe Rechtsinformatik

Mitveranstalter

DGRI Fachausschuss Rechts- und Verwaltungsinformatik
Wissenschaftliche Gesellschaft Digital Government (WiDiGo)
Alcatel-Lucent Stiftung für Kommunikationsforschung
Bundesministerium des Innern
Innenministerium Baden-Württemberg
Bodenseekreis
Stadt Friedrichshafen
Zeppelin Universität Friedrichshafen

Grußwort

Cornelia Rogall-Grothe

Beauftragte der Bundesregierung für Informationstechnik
und Staatssekretärin im Bundesministerium des Innern

„Offen, smart und vernetzt“ – die Überschrift zur FTVI & FTRI 2012 hätte die Anforderungen an eine künftige Verwaltungskultur kaum treffender skizzieren können. Um den Erwartungen von Bürgern und Unternehmen an Qualität und Schnelligkeit von Verwaltungsleistungen auch zukünftig gerecht zu werden, müssen die Modernisierungsanstrengungen in den Bereichen E-Government und Bürokratieabbau unvermindert fortgesetzt werden.

Die Bundesregierung wird in diesem Jahr den Entwurf eines E-Government-Gesetzes verabschieden, durch das die elektronische Kommunikation mit der Verwaltung erleichtert werden soll, indem neben der qualifizierten elektronischen Signatur auch andere sichere Verfahren zur Erfüllung der Schriftform zugelassen, medienbruchfreie Prozesse ermöglicht und Anreize zur Förderung von E-Government gesetzt werden sollen. Beim Thema Bürokratiekosten geht es verstärkt darum, eine Infrastruktur mit einer einheitlichen elektronischen Schnittstelle zwischen Wirtschaft und Verwaltung zu schaffen und so die effiziente Nutzung der elektronischen Datenübermittlung weiter zu verbessern. Mit P23R | Prozess-Daten-Beschleuniger legt die Bundesregierung den Grundstein dafür, Geschäftsvorgänge zwischen Wirtschaft und Verwaltung zu analysieren und miteinander zu effizienten Prozessketten zu vernetzen. Für Unternehmen bedeutet dies eine spürbare Entlastung bei der Erfüllung ihrer Informations- und Meldepflichten.

Ich freue mich, dass auch das Thema Open Government zu den inhaltlichen Schwerpunkten der FTVI & FTRI 2012 zählt. Wir brauchen eine transparente Verwaltung, die Bürger noch mehr an ihrer Entscheidungsfindung beteiligt, um die Rückbindung des Staates an die Bedürfnisse der Bevölkerung zu stärken. Bis 2013 wird die Bundesregierung eine Strategie für ein offenes Regierungshandeln entwickeln und umsetzen. Zielstellung ist es, die vorhandenen Strukturen des Bundes, der Länder und Kommunen zu bündeln und die drei zentralen Handlungsfelder Transparenz, Partizipation und Zusammenarbeit weiter zu fördern. Ein Arbeitsschwerpunkt liegt in der Öffnung von Datenbeständen der öffentlichen Hand (Open Data). Hier werden wir uns für technische und rechtliche Standards einsetzen und die Voraussetzungen dafür schaffen, dass Wissenschaft und Wirtschaft unkompliziert von der Öffnung der Daten profitieren.

Ich wünsche den Fachtagungen einen guten Verlauf und allen Teilnehmerinnen und Teilnehmern die Gelegenheit zu einem spannenden Meinungs- und Gedankenaustausch.

Cornelia Rogall-Grothe, Beauftragte der Bundesregierung für Informationstechnik und Staatssekretärin im Bundesministerium des Innern

Grußwort

Reinhold Gall, MdL

Innenminister des Landes Baden-Württemberg

Die Landesregierung hat Bürgerbeteiligung und eine bessere Transparenz des Regierungs- und Verwaltungshandelns zu einer ihrer wichtigen politischen Aufgaben erklärt. Daher ist es begrüßenswert, dass sich die Gesellschaft für Informatik dem Thema Partizipation durch moderne Technologien des Internets widmet. Das muss weite Bereiche umfassen, von Infrastrukturprojekten und der Vorgangsbearbeitung bis zum E-Voting. Informatik und Informationstechnologie liefern hier entscheidende Innovationsimpulse und gestalten gesellschaftliches Engagement.

Ich freue mich, dass die Fachtagung Verwaltungsinformatik und die Fachtagung Rechtsinformatik ihre nächste Veranstaltung unter das Motto „Staat und Verwaltung auf dem Weg zu einer offenen, smarten und vernetzten Verwaltungskultur“ gestellt haben.

Regierung und Verwaltung dürfen gespannt sein zu erfahren, wie neuartige technologische Ansätze - etwa das semantische Web - ihre unbestrittenen Vorteile auch im täglichen Regierungs- und Verwaltungshandeln zur Geltung bringen können.

Bürgerinnen und Bürger können sich nur dann an der politischen Willensbildung beteiligen, wenn sie informiert sind. Deshalb muss die frühzeitige und für jeden über das Internet zugängliche Information Leitgedanke des staatlichen Handelns sein. Die Landesregierung hat die notwendigen Maßnahmen eingeleitet, um E-Government umzusetzen und beispielsweise Open Government nicht nur auf ein Schlagwort zu reduzieren. Dies wird in der IT-Strategie des Landes, die das Innenministerium verantwortet, seinen Niederschlag finden.

Ich wünsche den Organisatoren der Tagung viel Erfolg, den Teilnehmerinnen und Teilnehmern spannende Diskussionen und gewinnbringende Anregungen und Kontakte.

Reinhold Gall

MdL und Innenminister des Landes Baden-Württemberg

Grußwort

Lothar Wölfle

Landrat des Bodenseekreises

Sehr geehrte Damen und Herren,
liebe Mitbürgerinnen und Mitbürger,

„Staat und Verwaltung auf dem Weg zu einer offenen, smarten und vernetzten Verwaltungskultur“ – unter diesem Motto findet in diesem Jahr die gemeinsame Fachtagung Verwaltungsinformatik FTVI und die Fachtagung Rechtsinformatik FTRI in Friedrichshafen statt.

Die Bürgerinnen und Bürger von heute möchten intensiver an der Gestaltung ihrer Umwelt einbezogen werden – das Beispiel „Stuttgart 21“ haben wir alle vor Augen. Hierzu möchten sie vor allem auch die Instrumente nutzen, die ihnen der technische Fortschritt an die Hand gegeben hat: Handys, Smartphones und Tablet-PCs sind mittlerweile fester Bestandteil der Kommunikation zu den Verwaltungen geworden. Dies setzt auf kommunaler Seite zunächst den Willen aber auch die Möglichkeit voraus, auch diesen Zugangskanal stetig zu verbessern. Viel zu schnell stoßen die eng bemessenen kommunalen Haushalte dabei an ihre Grenzen. Vor allem, wenn es um größere Investitionen geht. Vor diesem Hintergrund wird der zweite Teil der Veranstaltungsüberschrift zunehmend wichtiger: Verwaltungskultur ja – aber smart und vor allem vernetzt.

Der Bodenseekreis kann bereits auf einige innovative Projekte zurückblicken – nicht zuletzt im Umfeld der T-City Friedrichshafen. Als erster Landkreis in Baden-Württemberg führte der Bodenseekreis die einheitliche Behördenrufnummer 115 ein. Auch das Ideen- und Beschwerdeportal „Sag‘s doch“ gemeinsam mit der Stadt Friedrichshafen zeigt auf, dass hier am Bodensee vernetzt gedacht sowie gemeinsam entwickelt und getestet wird. Heute und in der Zukunft.

Der Fachtagung in unserer landschaftlich schönen aber auch wirtschaftlich starken Region wünsche ich einen guten Verlauf mit interessanten und innovativen Themen.

Mit den besten Grüßen

Lothar Wölfle, Landrat des Bodenseekreises

Grußwort

Andreas Brand

Oberbürgermeister der Stadt Friedrichshafen

Herzlich Willkommen
meine sehr geehrten Damen und Herren,

zu der Fachtagung für Verwaltungsinformatik und Rechtsinformatik in der Zeppelin Universität in Friedrichshafen. Die gute Resonanz der vorangegangenen Tagungen hat die Zeppelin Universität und die Stadt Friedrichshafen, als Mitveranstalter, dazu ermutigt, in diesem Jahr die Tagungen in Friedrichshafen auszurichten und sie unter das gemeinsame Motto zu stellen: „Staat und Verwaltung auf dem Weg zu einer offenen, smarten und vernetzten Verwaltungskultur“. Ich freue mich sehr, dass dafür namhafte Referentinnen und Referenten gewonnen werden konnten, Experten, die uns ihre Sichtweisen und Einschätzungen aus ganz verschiedenen Blickwinkeln vorstellen und erläutern werden. Auch die Themenfelder bilden eine breite Palette zukunftsweisender Aspekte, wie die Verwaltungskultur der Zukunft aussehen wird.

Eines der bedeutendsten Ziele der IT ist die Sicherheit. Dies ist ein außerordentlich wichtiger Faktor für die Kommunen und Städte. Denn gerade bei mobilen Geräten wie iPhones, iPads oder Blackberries ist die Gefahr besonders hoch. Aber - ohne die neuen Techniken ist die Arbeit auch in einer Verwaltung nicht mehr denkbar.

Als Friedrichshafen vor mehr als fünf Jahren den Wettbewerb zur T-City der Deutschen Telekom gewonnen hat, war dies ein zukunftsorientierter Schritt. Das Projekt T-City war und ist für die Stadt Friedrichshafen ein großer Erfolg. Gemeinsam wurden innovative Ansätze entwickelt, um die Herausforderungen unserer Stadt, etwa transparente Verwaltung, Energiewende und vernetzte Verkehrssysteme mit moderner Informations- und Kommunikationstechnologie besser zu lösen. Durch das weltweit einzigartige Projekt T-City hat sich die Stadt Friedrichshafen nicht nur in Deutschland, sondern auch international als innovativer Wirtschaftsstandort etabliert. Dieses Image werden wir in den nächsten Jahren durch die Entwicklung weiterer zukunftsträchtiger Lösungen ausbauen.

Aber auch sonst ist Friedrichshafen für innovative Projekte offen: Zusammen mit dem Landkreis wurde die einheitliche Behördenrufnummer 115 und das Ideenportal „Sag‘s doch“ eingeführt. Hier haben die Bürgerinnen und Bürger die Möglichkeit, schnell und unkompliziert ihre Ideen und Anregungen an die Verwaltung weiterzugeben. Auch das Thema E-Government ist ein Schritt zu mehr vernetzter Arbeit innerhalb der Verwaltung. Ich wünsche den Teilnehmerinnen und Teilnehmern spannende Diskussionen und viele neue Kontakte.

Mit freundlichem Gruß

Andreas Brand, Oberbürgermeister

Grußwort

Alf Henryk Wulf

Kurator der Alcatel-Lucent Stiftung für Kommunikationsforschung und Vorstandsvorsitzender der Alcatel-Lucent Deutschland AG

Das Zusammenwirken von Wissenschaft und Praxis ist gerade auf einem Themengebiet wie Open Government doppelt wichtig. Zum einen ist die Wissenschaft als kreative partnerschaftliche Ideenlieferantin bis hin zur Implementierung bürgerfreundlicher Informationssysteme im Rahmen eines E-Government immer aufgerufen. Zum anderen aber kann und muss gerade die junge Wissenschaft zusammen mit den Verbänden und Arbeitsgruppen - sozusagen stellvertretend - auch den Part der Bürger übernehmen, um deren Sichtweise in den Gestaltungsprozess für eine „offene, smarte und vernetzte Verwaltungskultur“ aktiv einzubringen.

So ist es doppelt wichtig, dass das Hochschulkolleg E-Government der Alcatel-Lucent Stiftung im Stifterverband für die Deutsche Wissenschaft die Fachtagung Verwaltungsinformatik und die Fachtagung Rechtsinformatik 2012 in ihrem Ziel unterstützt, mithilfe systematischer wissenschaftlicher Analysen einen richtungsweisenden Dialog zwischen Wissenschaft und Verwaltungspraktikern zu fördern.

Schon im Vorfeld der FTVI & FTRI 2012 an der Zeppelin Universität in Friedrichshafen fördert die Stiftung deshalb auch das Wissenschaftliche Symposium „Gute E-Government-Forschung“ der Wissenschaftlichen Gesellschaft Digital Government und des Hochschulkollegs E-Government mit seinem Sprecher Prof. Helmut Krcmar an der Spitze. Ihm und dem ganzen Programmkomitee - stellvertretend sei an dieser Stelle nur Prof. Jörn von Lucke genannt - danke ich im Namen des Kuratoriums der Stiftung für das große Engagement bei der Vorbereitung, Durchführung und Dokumentation der Tage am Bodensee.

Man kann nur wünschen, dass das ambitionierte und dichte Arbeitsprogramm in den Tagen hinreichend Zeit lässt, die Kontakte des Gestaltungsnetzwerks aus Wissenschaft und Praxis rund um das E-Government untereinander in guten Gesprächen weiter zu vertiefen.

Alf Henryk Wulf

Vorwort

Die Fachtagung Verwaltungsinformatik (FTVI) und die Fachtagung Rechtsinformatik (FTRI) haben zum Ziel, einen richtungsweisenden Dialog zwischen Wissenschaft und Verwaltungspraktikern, Rechtspraktikern und Beratern zu fördern, indem Erfahrungen analysiert und Umsetzungsstrategien aufgezeigt werden. Die FTVI wird alle zwei Jahre von der Fachgruppe Verwaltungsinformatik der Gesellschaft für Informatik ausgerichtet. 2012 in Friedrichshafen ist es bereits zum zweiten Mal und damit gelebte Tradition, dass die FTRI der Fachgruppe Rechtsinformatik gemeinsam mit der FTVI ausgerichtet wird. Die inhaltliche Nähe und die praktische Relevanz der beiden Themenfelder und Fachgruppen legen es nahe, sich in angemessener Weise gemeinsam und interdisziplinär in die Organisation dieser Veranstaltung einzubringen.

Als verbindendes Motto der beiden Tagungen wurde 2012 „Staat und Verwaltung auf dem Weg zu einer offenen, smarten und vernetzten Verwaltungskultur“ gewählt, denn die Herausforderungen durch soziale Medien, die Web 2.0-Technologien und Cloud Computing-Angebote tragen derzeit erheblich zu einer Öffnung von Staat und Verwaltung und einem damit verbundenen Kulturwandel bei. Sie stärken zahlreiche Good-Governance-Prinzipien wie etwa Offenheit, Transparenz, Partizipation, Kollaboration, Bürgerorientierung und Verantwortungsbewusstsein. Allerdings muss das Regieren und Verwalten in offenen, dynamischen und komplexen Strukturen noch erlernt werden. Open Data und Innovationsplattformen bringen Innovations- und Öffnungsimpulse in die öffentliche Verwaltung. Interoperabilität und offene Standards helfen, bestehende Barrieren über Organisationsgrenzen hinweg zu überwinden. Daten, Informationen und Wissen lassen sich über das semantische Web, Ontologien, Simulationen, Augmented Reality, das Internet der Dinge und das Internet der Dienste vollkommen neu erschließen.

Die Konzepte prägen einen nachhaltigen gesellschaftlichen und kulturellen Wandel. In den zunehmend vernetzten Regionen und Städten Europas stößt dies auf fruchtbaren Boden und gewinnt so an weiterer Dynamik, Komplexität und Wirkung. Das Engagement der Bevölkerung und ihre Mitwirkung in vielen Bereichen sind Vorboten einer Entwicklung, die in den kommenden Jahren die Gesellschaft und den öffentlichen Sektor verändern wird. Staat und Verwaltung werden sich mit den Herausforderungen einer engagierten Öffentlichkeit konstruktiv auseinander setzen müssen und diese künftig aktiv nutzen. Dadurch kann das Vertrauen der Bürgerschaft in staatliche Institutionen gefestigt werden. Gleichzeitig ist die Verwaltung damit auf zunehmend raschere Veränderungen besser vorbereitet. Sie kann diese selbst proaktiv mitsteuern.

Zugleich sorgen die Breitbandvernetzung bei Festnetz und Mobilfunk, die zunehmende Rechenleistung der Prozessoren, mobile Endgeräte sowie die Verfügbarkeit von Hochleistungsservern über das Internet dafür, dass die Qualität, der Nutzen und die Verbreitung von vernetzten und mitdenkenden Anwendungen im E-Government zunehmen werden. Das Zusammenspiel von modernen Informations- und Kommunikationstechnologien, von Stadt- und Regionalentwicklung und von hoher Innovationsbegeisterung

eröffnen soziale und technologische Integrations- und Vernetzungspotentiale, an deren Realisierung bisher nicht zu denken war.

Die FTVI und die FTRI 2012 setzen sich vor diesem Hintergrund mit den folgenden drei Themenfeldern aus einer technischen, rechtlichen, ökonomischen, verwaltungswissenschaftlichen und politischen Sicht auseinander:

- Öffnung von Staat und Verwaltung (Open Government und Good Governance)
- Offene, smarte und vernetzte Verwaltung
- Politische und rechtliche Vorgaben für Staat und Verwaltung

Von den 20 eingereichten Vollbeiträgen aus Wissenschaft und Praxis wurden die zehn vorliegenden Beiträge vom Programmkomitee zur Veröffentlichung im Tagungsband ausgewählt. Unter Berücksichtigung der verschiedenen Ansätze wurden diese Beiträge nach den folgenden Themenschwerpunkten strukturiert:

- Electronic Government (3 Beiträge)
- Prozessmanagement (3 Beiträge)
- Rechtsinformatik (4 Beiträge)

Neben den zehn in diesem Tagungsband veröffentlichten Beiträgen wurden von den insgesamt 44 eingereichten und eingeworbenen Ausarbeitungen und Themenskizzen weitere 20 Beiträge für Vorträge im Tagungsprogramm ausgewählt. Zu diesen Vorträgen wird eine Kurzfassung von bis zu vier Seiten im Band 3 der Schriftenreihe des Deutsche Telekom Institute for Connected Cities der Zeppelin Universität in Friedrichshafen veröffentlicht. Die 20 Vorträge ergänzen die obigen Themenschwerpunkte im Programm von FTVI & FTRI 2012.

Mit zwei Keynotes von Prof. Dr. Hans Jochen Scholl von der University of Washington (Seattle) und Herrn Ministerialdirektor Dr. Herbert O. Zinell aus dem Innenministerium Baden-Württemberg wird die FTVI & FTRI 2012 eröffnet. Die Fachgruppe Verwaltungsinformatik wird die anschließende Podiumsdiskussion nutzen, ihr erstelltes Positionspapier „Open Government“ erstmalig der Öffentlichkeit vorzustellen.

Am Nachmittag des ersten Veranstaltungstages wird es im Anschluss an die ersten beiden Vortragsblöcke eine gemeinsame Podiumsdiskussion zur künftigen Zusammenarbeit und zur Förderung von Lehre und Forschung im Kontext staatlicher Modernisierung und E-Government geben. Ausgehend von den Aktivitäten der Arbeitsgruppe 3 des IT-Gipfels, des IT-Planungsrats sowie des gemeinsamen GI-Positionspapiers zur Stärkung von Lehre und Forschung soll mit Wissenschaftlern und Praktikern nach Wegen gesucht werden, wie das Ziel eines nationalen E-Government Kompetenzzentrums noch besser gemeinsam erreicht werden kann.

Am zweiten Veranstaltungstag werden zwei Panels die FTVI & FTRI 2012 bereichern, bei denen eine Rückbesinnung auf die vergangenen 50 Jahre Rechtsinformatik und die vergangenen 50 Jahre Verwaltungsinformatik im Mittelpunkt stehen. Ausgehend von dem Wunsch aller Beteiligten, die Ursprünge und die historische Entwicklung dieser beiden angewandten Wissenschaften in Deutschland für kommende Generationen schriftlich festzuhalten, soll der offizielle Startschuss für zwei weitere Publikationen

gegeben werden. Gemeinsam soll nach Wegen und Formaten gesucht werden, wie die Erinnerungen, Erfahrungen und Ergebnisse der langjährigen Protagonisten am besten für die Nachwelt aufbereitet und publiziert werden können.

Univ.-Prof. Heinrich Reinermann ist einer dieser langjährigen Mitstreiter, die alle über einen enormen Erfahrungsschatz im Umgang mit Informations- und Kommunikationstechnologien im öffentlichen Sektor verfügen. Im vergangenen Jahr wurde er für seine Verdienste um den GI Fachbereich Informatik in Recht und Verwaltung (ehemals FA 13 und FB 6) und den damaligen GI Fachausschuss Verwaltungsinformatik zum Fellow der Gesellschaft für Informatik vorgeschlagen. Das GI-Präsidium hat den Vorschlag angenommen und Heinrich Reinermann zum GI-Fellow ernannt. Zu seinem 75. Geburtstag am 11. Januar 2012 wollen wir Herrn Reinermann auch an dieser Stelle noch einmal besonders herzlich gratulieren. Dieser Tagungsband zur FTVI & FTRI 2012 ist ihm, seiner Familie, seinem langjährigen Engagement und seinen Verdiensten in ganz unterschiedlichen Rollen gewidmet.

Im Vorfeld der FTVI & FTRI 2012 findet das wissenschaftliche Symposium „Gute E-Government Forschung“ statt. Ziel dieses gemeinsam mit der Wissenschaftlichen Gesellschaft Digital Government (WiDiGo) und dem Hochschulkolleg E-Government der Alcatel-Lucent Stiftung für Kommunikationsforschung durchgeführten Symposiums ist es, sich interdisziplinär und mit viel Raum für Diskussion den grundlegenden Fragen der wissenschaftlichen Auseinandersetzung zum Einsatz von Informations- und Kommunikationstechnologien im öffentlichen Sektor zu nähern. Konkret geht es um Anforderungen an Tätigkeiten und Ergebnisse, um Ziele, Akteure, Theorien und Methoden erfolgreicher E-Government-Forschung. Die Vorträge, Diskussionsverläufe und Ergebnisse sollen in einer weiteren eigenständigen Publikation im Herbst 2012 veröffentlicht werden.

Natürlich hängt der Erfolg einer Tagung maßgeblich von den vielen helfenden Mitwirkenden ab, die sich bereits im Vorfeld um die erfolgreiche Durchführung verdient gemacht haben. Die 61 Mitglieder des Programmkomitees haben maßgeblich an der Einwerbung von Beiträgen, an der Begutachtung sowie an der Auswahl der angenommenen Beiträge mitgewirkt. An dieser Stelle gebührt ihnen ein großer Dank für ihre wertvolle und konstruktive Unterstützung!

Auch den Mitveranstaltern der FTVI & FTRI 2012

- Deutsche Gesellschaft für Recht und Informatik e.V.
  Fachausschuss Rechts- und Verwaltungsinformatik
- Wissenschaftliche Gesellschaft Digital Government (WiDiGo)
- Alcatel-Lucent Stiftung für Kommunikationsforschung
- Bundesministerium des Innern
- Innenministerium Baden-Württemberg
- Bodenseekreis
- Stadt Friedrichshafen
- Zeppelin Universität Friedrichshafen

sowie der]init[AG für Digitale Kommunikation als Unterstützer der Tagung sei an dieser Stelle ganz herzlich für ihre vielfältigen Beiträge gedankt. Unser besonderer Dank gilt zudem den beteiligten Autoren und Editoren dieses Tagungsbandes.

Die neunte FTVI und die zweite FTRI werden 2012 im Süden der Bundesrepublik Deutschland, in direkter Nachbarschaft zur Schweiz und zu Österreich, an der Zeppelin Universität in Friedrichshafen durchgeführt. Die Zeppelin Universität ist eine 2003 gegründete und staatlich anerkannte Universität mit Promotions- und Habilitationsrecht. Studenten aller Studiengänge werden von Prof. Dr. von Lucke am Deutsche Telekom Institute for Connected Cities (TICC) in Verwaltungsinformatik und in Wirtschaftsinformatik unterrichtet. Die aktuellen Forschungsschwerpunkte des Instituts sind Electronic Government, Open Government, Open Data und Open Budget. Prof. Dr. Heckmann ergänzt dieses fachliche Lehr- und Forschungsangebot mit dem Center for IT-Compliance and Trust (CIT) und seiner juristischen Expertise.

Für die Fachtagung, Vorträge, Diskussionen und Gespräche werden Räumlichkeiten direkt am Campus Seemooser Horn genutzt. Dies erlaubt es den Fachtagungsteilnehmern, am Bodensee direkt mit Blick auf die Schweizer und Vorarlberger Alpen in angenehmer Umgebung neue Kontakte zu schließen und sich gegenseitig auszutauschen, um visionär auch vollkommen neue Ideen zu generieren und diese zu diskutieren. Zudem bietet die „T-City Friedrichshafen“ auch nach Abschluss der fünfjährigen Projektphase (2007-2012) den Besuchern vielfältige Möglichkeiten, sich von den Optionen und Chancen einer flächendeckenden Breitbandvernetzung in einer vernetzten Stadt zu überzeugen. Und wenn Sie nicht weiter wissen, testen Sie doch einfach mal die 115 …

Wir wünschen allen Teilnehmenden einen angenehmen Aufenthalt in der Zeppelinstadt Friedrichshafen. Weiterhin wünschen wir allen Lesern viele anregende Erkenntnisse bei der Lektüre des vorliegenden Tagungsbandes.

Die Herausgeber:

Jörn von Lucke, Christian P. Geiger, Siegfried Kaiser, Erich Schweighofer und Maria A. Wimmer

Friedrichshafen, März 2012

Univ.-Prof. Dr. Heinrich Reinermann ist 75

Nach einer kaufmännischen Ausbildung bei den Klöckner-Werken AG und dem Studium der Betriebswirtschaftslehre in Hamburg, Münster und Mannheim promovierte Heinrich Reinermann 1966 in Münster mit einer Arbeit über die optimale Gestaltung der täglichen Arbeitszeit im Industriebetrieb. In dieser Arbeit entwickelte er Techniken der mathematischen Programmierung, um die Steuerung verschiedenster Leistungsdeterminanten zu optimieren. Für seine Dissertation erhielt er 1966 auch wegen der intensiven und damals selbst in der akademischen Welt noch ungewöhnlichen Computernutzung den Akademischen Preis der Universität Münster. Während eines anschließenden Forschungsaufenthalts am „Computer Science Department“ und in der Business School der Stanford University im Silicon Valley wechselte Reinermann zur Verwaltungswissenschaft und richtete sein wissenschaftliches Interesse auf quantitative Methoden, automatisierte Datenverarbeitung und Programmierung im Bereich der öffentlichen Verwaltung. Reinermann gehört somit zu den Pionieren der Verwaltungsinformatik in Deutschland.

1973 wurde er in Mannheim mit einer Schrift über die Grenzen und Möglichkeiten formaler Entscheidungssysteme für die Exekutive von Bund und Ländern habilitiert. Er erwarb die Venia Legendi für Betriebswirtschaftslehre. Im gleichen Jahr schlug er einen Ruf an die Universität der Bundeswehr in Hamburg aus und nahm stattdessen den Ruf an die Hochschule für Verwaltungswissenschaften in Speyer auf einen Lehrstuhl für EDV und quantitative Methoden an. Dabei bezog er sich auf Fragestellungen der öffentlichen Verwaltung und baute das Angebot zum Fach Verwaltungsinformatik aus. Der Lehrstuhl wurde konsequenterweise in „Lehrstuhl für Verwaltungswissenschaft und Verwaltungsinformatik“ umbenannt und zählt damit zu einer der ersten deutschen Institutionen in dieser Wissenschaftsdisziplin. 1978 wurde Reinermann zum Gründer und wissenschaftlichen Leiter des von ihm aufgebauten Rechenzentrums der Hochschule in Speyer. Das Ineinandergreifen von Konzipierung des Hochschulrechenzentrums und seine permanente Anpassung an neue Möglichkeiten einerseits und die Lehr- und Forschungsaufgaben andererseits haben seine Arbeit an der Verwaltungsinformatik sehr befruchtet. Heinrich Reinermann erhielt zudem Rufe von der Universität der Bundeswehr München in München, der Johannes-Kepler-Universität Linz in Österreich und der Universität Konstanz, die er alle ausschlug. Von 1990 bis 1994 war Heinrich Reinermann Rektor und Prorektor der Hochschule in Speyer. 2003 wurde er emeritiert. Bis vor kurzem war er zudem Vorsitzender des Vorstands der Johann Joachim Becher-Stiftung Speyer.

Neben seinem eigenen wissenschaftlichen Schaffen, das sich in weit über 330 Publikationen, darunter 18 Monographien, 20 Bücher als Herausgeber/Mitherausgeber und über 260 Aufsatzpublikationen widerspiegelt, übernahm Reinermann die Rolle eines Nestors der deutschen Verwaltungsinformatik.

Beispielhaft sind seine Funktionen als Sprecher der Sektion „Informatik in Recht und öffentlicher Verwaltung“ der Gesellschaft für Informatik, seine Vorstandstätigkeit bei der „Arbeitsgemeinschaft für wirtschaftliche Verwaltung e. V.“ und seine Herausgebertätigkeiten für die Zeitschrift Verwaltung und Management und die Schriftenreihe „Verwaltungsinformatik“. Bereits 1969 forderte er in der Zeitschrift für Betriebswirtschaft unter dem Titel „Die Elektronische Datenverarbeitung im Studium der Betriebswirtschaftslehre“ eine ausführliche Berücksichtigung der EDV in den Lehrplänen, also eine „Wirtschaftsinformatik“ ein. Ausgehend von der Hochschule für Verwaltungswissenschaft Speyer führte er die junge Wissenschaft „Verwaltungsinformatik“ auch in Lehrpläne der verwaltungswissenschaftlichen Hochschulausbildung ein. Seinem Verständnis nach liegt der Kern der Verwaltungsinformatik darin, die beiden Stränge der digitale Informations- und Kommunikationstechnologien mit deren Anwendungsfeldern im öffentlichen Sektor zusammenzuführen. So hat die junge Wissenschaft Verwaltungsinformatik ihren Ursprung in der Informatik und den Verwaltungswissenschaften. Dies führt zu empirischen und gestaltenden Methoden: „Wirklichkeit immer besser verstehen helfen - das Feld empirisch-theoretischer Aussagen über das Sein, und: Wirklichkeit immer besser gestalten helfen - das Feld normativ-theoretischer Aussagen über das Sollen.“ Für Heinrich Reinermann ist die Verwaltungsinformatik zudem eine „Speerspitze“, weil auf ihrem Einsatzfeld viele Voraussetzungen zu schaffen sind, bevor überhaupt an einen Computereinsatz zu denken ist. Die Verwaltungsinformatik repräsentiert mit ihrem Objektbereich Staat und Verwaltung sogar in besonderer Weise, was Fritz Krückeberg als GI-Präsident 1989 in seinem Rückblick „20 Jahre GI“ zur Verantwortung der Informatiker treffend so formulierte: Wir dürfen „nicht fragen ´Was kommt auf uns zu?´, sondern wir müssen fragen: ´Was wollen wir?´“.

Heinrich Reinermann hat von 1979 bis 2000 Fachveranstaltungen und Fachkongresse des Fachausschuss 13 und des Fachbereichs 6 mitorganisiert und geprägt. Im März 1979 wurde die erste gemeinsame Tagung von FA 13 und HfV Speyer beschlossen. Die bisher letzte Tagung fand im Jahr 2000 mit über 600 Teilnehmern in Speyer statt. Die Tagungen wurden teils im Springer-Verlag Heidelberg, teils in der damaligen „Schriftenreihe Verwaltungsinformatik“ bei Decker Heidelberg dokumentiert, wobei Herr Reinermann die Herausgabe der damit erschienenen Schriften mit übernahm. Seine Speyerer Fortbildungsveranstaltungen für die Beamten und Angestellten des höheren Dienstes waren in der Verwaltung ebenfalls sehr gefragt. Unter anderem wurde das einwöchige SpeBit (Speyerer Seminare für Büro- und Informationstechnik) mehr als 25 Mal abgehalten. Dazu gab es Sonderveranstaltungen und 14 Führungsseminare für die Ausbilder und Prüfer der Vermessungsverwaltung zu Themen der Verwaltungsmodernisierung und Verwaltungsinformatik.

Heinrich Reinermann ist Träger des Bundesverdienstkreuzes am Bande der Bundesrepublik Deutschland, Träger der Silbernen Ehrennadel des Deutschen Beamtenbundes und Träger der Verdienstmedaille der Universität Ljubljana (Slowenien) „Pro Universitate Labacensi“. Seit Oktober 2011 ist er Fellow der Gesellschaft für Informatik, da er sich in herausragender Weise um die GI und die Informatik verdient gemacht hat.

Wir wünschen ihm zu seinem 75. Geburtstag alles Gute und die beste Gesundheit für seine weiteren Lebensjahre!

Inhaltsverzeichnis

Electronic Government

Prozessmanagement

Rechtsinformatik

Electronic Government

„PuMa reloaded" – Überlegungen zu einer Erneuerung des Public Management im Lichte von Electronic Government

Martin Brüggemeier[1], Manfred Röber[2]

[1]Hochschule für Technik und Wirtschaft (HTW) Berlin
Fachbereich 3 (Wirtschaftswissenschaften I)
Treskowallee 8, 10318 Berlin
martin.brueggemeier@htw-berlin.de

[2]Universität Leipzig
Wirtschaftswissenschaftliche Fakultät
Grimmaische Straße 12, 04109 Leipzig
roeber@wifa.uni-leipzig.de

Abstract: Neue, durch moderne IKT ermöglichte prozessorientierte Organisationsformen und neue Architekturen der organisationsübergreifend vernetzten Leistungserstellung und -abgabe in Verbindung mit neuen institutionellen Arrangements im öffentlichen Sektor („Öffentliche Leistungsnetzwerke") bedeuten zugleich auch neue Herausforderungen an das bislang primär einzelbetrieblich orientierte Public Management. Der Beitrag enthält Vorschläge zu einem theoretisch-konzeptionellen Bezugsrahmen für ein im Lichte von E-Government erneuertes Public Management (PuMa), das die Gestaltung der vernetzten Produktion öffentlicher Leistungen auf der Basis leistungsfähiger Infrastrukturen ebenso in den Blick nimmt wie die kontextadäquate und effiziente Steuerung dieser Produktion im Dienste politisch legitimierter regulatorischer Interventionen.

1 Einleitung: Neue Produktionsmodelle durch E-Government

Nachdem der Fokus des Public Management (PuMa) über viele Jahre auf ein Neues Steuerungsmodell (NSM) für öffentliche Verwaltungen gerichtet und das Interesse an Fragen der Gestaltung der Leistungsprozesse nicht sonderlich ausgeprägt war [BR11a], legt die moderne Informations- und Kommunikationstechnik inzwischen neue Produktionsmodelle und -konzepte in Form „Öffentlicher Leistungsnetzwerke" nahe [zum Beispiel Br06; SR10], mit denen bestehende Grenzen zwischen Organisationen und Verwaltungsebenen überschritten werden können: Im Zuge einer vernetzten Erfüllung öffentlicher Aufgaben bilden sich neuartige Formen der Arbeitsteilung und Kooperation zwischen öffentlichen Verwaltungen untereinander, aber auch mit zivilgesellschaftlichen Nonprofit-Organisationen und privaten Unternehmen heraus. Neue, prozessorientierte Organisationsformen und neue Architekturen der Leistungserstellung in Verbin-

dung mit neuen institutionellen Arrangements bedeuten neue Herausforderungen für die Gestaltung der Produktion und deren Steuerung sowie für die politische Legitimation des Gesamtarrangements der Aufgabenerfüllung.[1]

Vor diesem Hintergrund ist davon auszugehen, dass Public Management – hier verstanden als interdisziplinär aufgeschlossene betriebswirtschaftliche Lehre von der effizienten und effektiven Erfüllung öffentlicher Aufgaben – anders zu konzeptualisieren und paradigmatisch weiterzuentwickeln ist. Es gilt vor allem, die bislang dominierende *intra*organisationale um eine *inter*organisationale Perspektive zu erweitern. Dies bedeutet aber nicht, dass die bislang primär auf die Einzelorganisation fokussierte institutionell-betriebliche Perspektive des Public Management gänzlich irrelevant wird. Ein solches einzelwirtschaftlich ausgerichtetes Management muss allerdings eingebettet sein in ein System, mit dem komplexe Organisationsgeflechte wirksam gestaltet und verantwortlich gesteuert werden können.

Ziel des vorliegenden Beitrags ist es, die theoretisch-konzeptionellen Konturen für die weitere Ausarbeitung eines Public Management der zweiten Generation zu skizzieren, das den zukünftigen Anforderungen IT-basierter vernetzter Leistungserstellung im öffentlichen Sektor umfassend Rechnung trägt.

2 Öffentliche Leistungsnetzwerke als Management-Herausforderung

2.1 Modularisierung

Ein wichtiger Schlüssel für die Nutzung der Modernisierungspotenziale durch Vernetzung ist eine Modularisierung des Leistungsprozesses. Der Prozess wird dazu in passgerechte Arbeitspakete beziehungsweise Teilprozesse aufgeteilt, die im Prinzip ganze Wertschöpfungsstufen (z.B. Vertrieb), ein Bündel von zusammenhängenden Verrichtungen (zum Beispiel Registrierung, Beratung, Bescheid-Erstellung) oder auch nur kleinste „Prozesspartikel“ (zum Beispiel Web-Services) umfassen können. Diese Module können von unterschiedlichen Produzenten erstellt und im Rahmen eines Leistungsnetzwerks über definierte Schnittstellen wieder zu einem übergeordneten (Gesamt-) Prozess verknüpft werden [BD05; Br07a; Sc09a; LSS10].

Im Kontext von E-Government können „Öffentliche Leistungsnetzwerke … als eine Form der prozessorientierten Primärorganisation (definiert werden), mit der eine politisch beschlossene Leistung unter Einbeziehung von rechtlich selbständigen öffentlichen und gegebenenfalls auch nicht-öffentlichen Partnern mit Hilfe einer sehr intensiven Nutzung von Informationstechnik in organisationsübergreifender Arbeitsteilung modular produziert und/oder an die Adressaten abgegeben wird, um Effizienz-, Effektivitäts-, Qualitäts- und Legitimationsvorteile zu erzielen“ [Br04:189].

[1] Zu einer ausführlicheren, organisationstheoretisch angeleiteten Analyse des Zusammenhanges zwischen der Produktion *in* und der Steuerung *von* Öffentlichen Leistungsnetzwerken: [BR11b].

2.2 Netzwerkmanagement

Das Management unter den Rahmenbedingungen eines solchen Netzwerkes stellt – im Vergleich zum Management einer einzelnen Organisation – andere Anforderungen, weil sich die Akteure hinsichtlich ihrer *Ziele* (erwerbswirtschaftlich oder gemeinwirtschaftlich), *Handlungslogiken* (konditional- oder zweckprogrammiert), *Kernkompetenzen* (juristisch, politisch, fachlich oder ökonomisch) und *Organisationskulturen* (bürokratisch oder unternehmerisch; technik*affin* oder technik*avers*) zum Teil sehr stark unterscheiden können [GE04:19ff.; Do06]. Diese Unterschiede wirken sich zum Beispiel in der Weise aus, dass es in den am Netzwerk beteiligten Institutionen unterschiedliche Anreiz- und Sanktionsmechanismen gibt, die nur bedingt kompatibel sind. Außerdem muss man davon ausgehen, dass die zum Netzwerk gehörenden Akteure über unterschiedliche Risikopräferenzen verfügen, die komplizierte Qualitätssicherungs- und Haftungsfragen für einzelne Teil- beziehungsweise Zwischenprodukte und das Gesamtprodukt nach sich ziehen.

Darüber hinaus ist zu berücksichtigen, dass im Falle der Modularisierung von Leistungsprozessen im öffentlichen Sektor die Leistungsprozesskette aufgespalten wird und Teilprozesse beziehungsweise Prozessstufen auf unterschiedliche Netzwerkpartner verteilt werden [Rö11]. Dadurch erhöht sich die Zahl der Schnittstellen organisationsübergreifender arbeitsteiliger Leistungsprozesse, die zu Ungewissheiten und schlechtstrukturierten Entscheidungen an den jeweiligen Übergabepunkten führen können [Sy99:284].

Schließlich werden „Produktionsprozesse“ im öffentlichen Sektor (ebenso wie Policy-Prozesse), die nie im politikfreien Raum stattfinden, häufig von Politics-Prozessen überlagert. Insofern ist – im Unterschied zu Netzwerken im privatwirtschaftlichen Bereich – zu berücksichtigen, dass das Verhalten der Akteure und die Steuerung dieser Prozesse nicht allein wirtschaftlichen, sondern auch politischen Rationalitätskriterien (wie zum Beispiel der politischen Legitimation dieser Steuerung und der Wirkung politischer Programme, aber auch der Sicherung von Mehrheiten und Macht) folgt.

2.3 „PuMa-Perspektiven“

Vor diesem Hintergrund sind – im Kontext von neuen, netzwerkartigen Produktionsmodellen – Perspektiven für die konzeptionelle Weiterentwicklung des Public Management zu erarbeiten, bei denen es darauf ankommt, die vielfach kritisierten Defizite des New Public Management (NPM) wie die Fragmentierung des Leistungsangebots durch Agencification [Rö12], die mangelnde Wirkungsorientierung sowie die „Politik- und Produktionsblindheit“ [BR11a] nach Möglichkeit zu überwinden, aber zugleich nicht hinter die mit dem NPM forcierten Standards wie etwa Ergebnisverantwortung, Kosten- und Leistungstransparenz, Effizienz- und Serviceorientierung zurückzufallen [Bu06].[2]

[2] Vgl. hierzu auch die Diskussion der Beiträge diverser „post-managerialer“ Ansätze für ein erneuertes Public Management bei [BR11b].

3 Konturen eines erneuerten Public Management

3.1 Konzeptioneller Bezugsrahmen

Ein erneuertes Public Management muss sich mit der organisationsübergreifenden Gestaltung der Produktion und einer wiederum auf die jeweiligen „Produktionsverhältnisse" abgestimmten Steuerung befassen.

In Abhängigkeit von Art und gradueller Ausprägung der Informationsbasiertheit der Kernprozesse öffentlicher Produktion liefert das E-Government unter Einbeziehung der Dienstleistungstheorie [zum Beispiel Bi07, Fl06] theoretisch-konzeptionelle Bausteine für eine adäquate IT-basierte Gestaltung der öffentlichen Leistungserstellung [LT99; Le04; Br06]. Darüber hinaus bieten die Forschung zum Netzwerkmanagement [Sy06;SD11; Br04], aber auch amerikanische Arbeiten zu einem „Collaborative Public Management" [PAR06; BO08], zu „Public Management Networks" [Ag01; Ag07] und zum „Networked Government" [GE04; GK09][3] zahlreiche Anknüpfungspunkte für den theoretisch-konzeptionellen Bezugsrahmen eines erneuerten Public Management, das freilich nicht neu erfunden werden muss, sondern auf vorhandene Wissensbestände rekurrieren kann.

Als Ausgangsbasis für die weitere Ausarbeitung eines in diesem Sinne erneuerten Public Management spannen wir im Folgenden einen theoretisch-konzeptionellen Bezugsrahmen auf (siehe Abbildung 1), der zunächst nur grob und in generischer Form die Objekte eines sowohl *politisch-regulatorisch* als auch *infrastrukturell* eingebetteten Public Management umreißt und systematisiert. In unmittelbarem Anschluss an ein Drei-Schichten-Modell von *Lenk* mit den „Schichten" (1) Gestaltung von Recht und politischen Programmen, (2) Leistungsprozesse und (3) Infrastruktur [Le11a; BL11] setzen unsere Überlegungen zu einer Neuausrichtung des Public Management bei der mittleren Schicht an, das heißt bei den Prozessen der Leistungserbringung, die es zu gestalten und zu steuern gilt. Die anlassbezogene *Gestaltung* ist dabei der laufenden *Steuerung* systematisch vorgelagert.

[3] Collaboration und Netzwerke sind in diesen Arbeiten jedoch „unplugged". Fast durchweg fehlt ein empirischer oder konzeptioneller Bezug zur IT oder zum E-Government. So stellt auch Agranoff fest: „The study of the role of ICT in networks is in its infant stages." [Ag07:233]

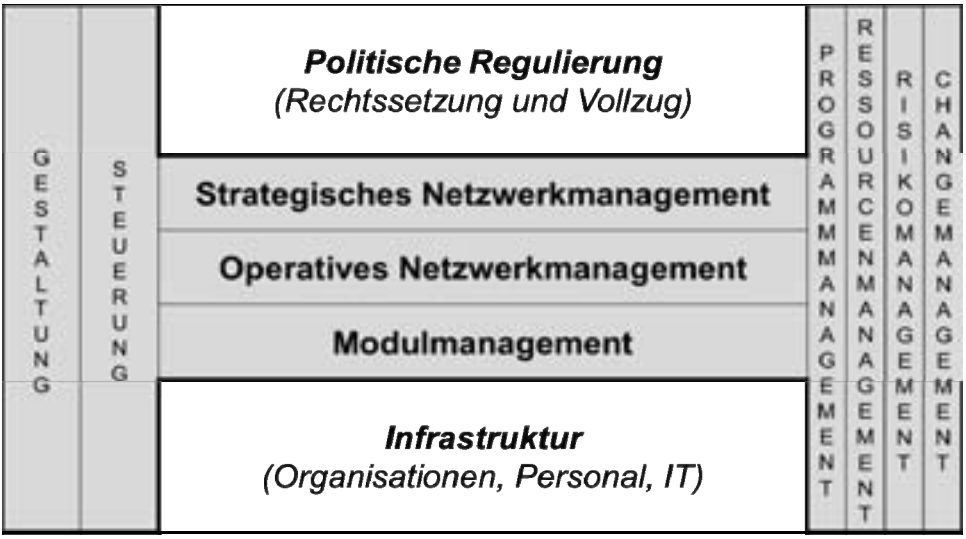

Abbildung 1: Konzeptioneller Bezugsrahmen eines erneuerten Public Management [BR11b]

Die Gestaltungs- und Steuerungsaufgaben sind auf den drei Managementebenen „Strategisches Netzwerkmanagement“, „Operatives Netzwerkmanagement“ und „Modulmanagement“ angesiedelt [Br07a:56ff.; Sc06:163ff.], die weiter unten genauer beschrieben werden. Inhaltlich geht es auf allen drei Managementebenen in unterschiedlicher Ausprägung um Fragen des Programm-, Ressourcen-, Risiko- und Change Management. Die Aktivitäten zur Gestaltung und Steuerung folgen teilweise neuen beziehungsweise veränderten paradigmatischen Grundorientierungen, bei denen es um Public Management als integralen Bestandteil einer „Bewirkensordnung“ [Hi10:18] geht, die organisationsübergreifend vernetzt und prozessorientiert angelegt ist und sich an übergeordneten Leitvorstellungen wie dem der „Coopetition“ und des „aufgeklärten Gewährleistungsstaates“ [Br07b:80ff.] orientiert. Darüber hinaus wird bei der Gestaltung und Steuerung auf ein flexibles Set von „Key Components“ [Du06:481] oder teilweise neuen Konstruktionsprinzipien mit Leitbildcharakter (wie zum Beispiel „End-to-End Service Reengineering“, „No-Stop-Government“ oder „One-Stop-Government“) zurückgegriffen, die idealerweise bereits auf der übergeordneten Ebene der politischen Regulierung mitbedacht und mitberücksichtigt werden müssen.

3.2 Public Management im Dienste von „Better Regulation“

Das erneuerte Public Management steht ganz im Dienste von „Better Regulation“ im Sinne Politischer Regulierung gesellschaftlicher Sachverhalte [Pi09; We11], soweit es dabei um den Vollzug öffentlicher Aufgaben geht. Public Management kann so strategisch und wirkungsbezogen in die Politikplanung und -implementation [Hi07; Hi10] eingebunden werden. Zugleich kann das Konzept von Better Regulation mit einem erneuerten Public Management auf der Vollzugsebene verankert werden. Erst mit dieser Rückbindung an die politisch-regulatorische Intention findet die Leistungserstellung

durch Verwaltungseinheiten und durch die Organisationsgeflechte im Gewährleistungsstaat ihren Sinn und ihre Legitimation [BL11].

3.2.1 Politische Regulierung

Gegenstand der Politischen Regulierung ist eine wirkungsorientierte und bürokratiesparende Rechtsetzung *und* Vollzugsplanung. Damit wird ein bislang kaum gesehener Weg zur Sicherung der Funktionalität von Bürokratie ermöglicht, indem der gesamte Zyklus Politischer Regulierung auch auf den Abbau von unnötigen bürokratischen Belästigungen und Belastungen ausgerichtet wird, die sowohl die Adressaten als auch die Verwaltung selbst betreffen [BL11]. Dabei sind die vollzugsrelevanten Normen und Vollzugsalternativen (Gesetzesfolgenabschätzung) sowie die Kontrolle (Evaluation) des Vollzugs im Hinblick auf die erzielten Wirkungen zu betrachten. Der Vollzug wird von den angestrebten Wirkungen her geplant, und zwar bereits unter Berücksichtigung der zur Verfügung stehenden Infrastruktur für eine vernetzte und IT-basierte Erledigung öffentlicher Aufgaben.[4] Mit Hilfe dieser technisch-organisatorischen Infrastruktur müssen ganz unterschiedliche (Produktions-) Lösungen für zunächst noch gar nicht absehbare Probleme flexibel realisierbar sein. Aus der Perspektive der Dienstleistungstheorie repräsentiert diese Infrastruktur jenen Anteil des sog. Leistungspotenzials, der auf – im weitesten Sinne – „internen" Produktionsfaktoren gründet, auf die im Gewährleistungsstaat bei der Erledigung öffentlicher Aufgaben – unabhängig von konkreten Aufgaben und Leistungsprozessen – grundsätzlich zurückgegriffen werden kann.

Aufgrund der sog. Integrativität von Dienstleistungen ist allerdings auch jenes Potenzial bei der politischen Programm- und Vollzugsplanung mit zu berücksichtigen, welches die Adressaten eines Programms als so genannter externer (Produktions-) Faktor in den Leistungsprozess einbringen können beziehungsweise sollen. Hiervon wird – wie jüngst etwa das Beispiel des „Bildungs- und Teilhabepakets" gezeigt hat – die Wirksamkeit politischer Programme maßgeblich beeinflusst.

3.2.2 Integration des externen Faktors

Art und Umfang der Integration des externen Faktors hängen von der zu erledigenden Aufgabe (einschließlich damit verbundener professioneller Standards), der Mitwirkungsfähigkeit und -bereitschaft der Adressaten (Kompetenz, Zeit, Geld, Motivation et cetera) und der politisch-regulatorischen Zielsetzung ab. So kann beispielweise entweder durch die Vermeidung überflüssiger Bürokratie oder durch Angebote zur Beteiligung am Leistungsprozess bei den Adressaten politischer Programme Akzeptanz für

[4] Es liegt in diesem Zusammenhang nahe, zu prüfen, was von dem aus dem Unternehmensbereich stammenden „IT-Business Alignment" beziehungsweise „Strategic Alignment" zu lernen ist: „ Ein Strategic Alignment ist existent, wenn die IT-Strategie vollkommen an der Geschäftsstrategie ausgerichtet ist und sie über alle Ebenen hinweg unterstützt. Im Gegenzug orientiert sich die Geschäftsstrategie an den Möglichkeiten der IT und macht sich diese gewinnbringend zunutze" [BEH10:31]. Aus verwaltungswissenschaftlicher Perspektive könnte man von *„Impact Planning"* [Ke10] sprechen. Zur Entwicklung und Bewertung neuer Vollzugsstrukturen vgl. den Ansatz eines *„Innovation Impact Assessment"* [Le11b].

diese Programme geschaffen werden. Damit wird die Gestaltung der In- beziehungsweise Exklusion von Adressaten zu einer wichtigen Qualitäts- und Steuerungsressource für die Regulierungswirkung. Deshalb muss die Planung des Leistungsprozesses gedanklich bereits auf der Ebene der Politischen Regulierung berücksichtigt und rechtzeitig überlegt werden, ob betroffene Adressaten einschlägige Regelungen verstehen oder akzeptieren oder ob bestimmte Regelungen – falls dies politisch gewollt ist – in der Lage sind, Adressaten zu aktivieren. Außerdem ist zu berücksichtigen, dass mit einer vorhandenen Infrastruktur unterschiedliche Möglichkeiten bestehen, die Integration des externen Faktors zu gestalten und die Umsetzung von politischen Programmen positiv zu beeinflussen: "E-Government is proving to be an essential support tool for the effective deployment of Better Regulation policies" (OE10:65).

Auf dieser Basis muss eine grobe Vollzugsplanung unter Einbeziehung der Managementaspekte erfolgen, um frühzeitig sicherzustellen, dass ein Performancemanagement praktiziert werden kann, das nicht nur auf die Effektivität, sondern auch auf die Effizienz der Produktion *und* der Steuerung selber (insbes. auf die Höhe der anfallenden Transaktionskosten) ausgerichtet ist.

3.3 Managementbedarf bei Öffentlichen Leistungsnetzwerken

Ausgehend von der Rechtsetzung und der Vollzugsplanung auf der Ebene der Politischen Regulierung kann der Managementbedarf bei Öffentlichen Leistungsnetzwerken (ÖLN) in die drei funktionalen Bereiche (1) strategisches Netzwerkmanagement, (2) operatives Netzwerkmanagement und (3) Modulmanagement strukturiert werden (siehe auch Abbildung 2):

3.3.1 Strategisches Netzwerkmanagement

Als strategische Aufgaben bei der Gründung oder Neuausrichtung zählen hierzu insbesondere die Gestaltung eines Grob-Designs für die Leistungsprozesse auf modularer Basis unter Berücksichtigung strategischer Aspekte der Adressatenintegration, die Auswahl und die Evaluation der im Hinblick auf die angestrebten Ergebnisse und Leistungen zu beteiligenden Netzwerkpartner („Institutional Choice“) und die (Re-) Konfiguration des konkreten, situativ angepassten Steuerungsmixes, der eine verantwortliche Gesamtsteuerung („Governance“) des Öffentlichen Leistungsnetzwerkes auf der Basis von Performance-Kennzahlen und -Indikatoren gewährleistet [BD05]. Eine besondere Herausforderung dürfte auf dieser Managementebene darin liegen, die angestrebte „Bewirkensordnung“ angesichts des Spannungsfelds unterschiedlicher Rationalitäten „autonomieschonend“ in erfolgversprechende Geschäftsmodelle zu überführen.

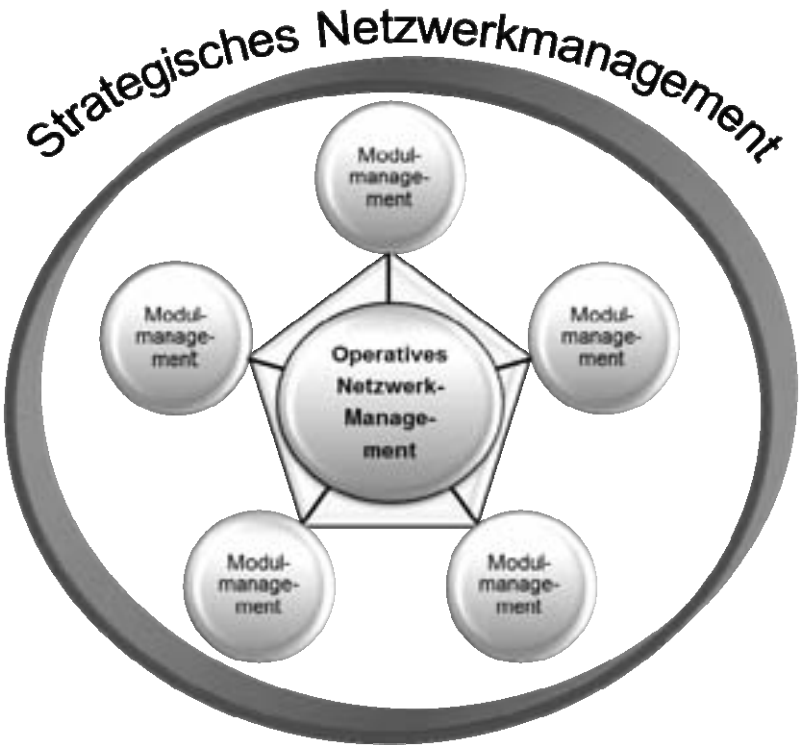

Abbildung 2: Strukturierung des Managementbedarfs bei ÖLN [BR11b]

3.3.2 Operatives Netzwerkmanagement

Beim operativen Netzwerkmanagement geht es um die Sicherstellung einer organisations- beziehungsweise partnerübergreifend konfigurierten und koordinierten, effektiven und effizienten (laufenden) Leistungserstellung in Öffentlichen Leistungsnetzwerken (operatives „Joined-up-Prozessmanagement“ auf Netzwerkebene). Hierzu zählen insbesondere die Aushandlung und das Controlling von Service-Level-Agreements und Key-Performance-Indikatoren der Netzwerkpartner, die operative bewirkensorientierte Koordination (zum Beispiel Statusmeldungen, Schnittstellenmanagement) sowie die Abrechnung von konkreten Leistungsbeiträgen, die Einrichtung und Überwachung von Budgets für netzwerkbezogene Gemeinkostenbereiche, die Pflege der Netzwerkkultur und die Klärung operativer, netzwerkübergreifender Fragen der Adressatenintegration und des Qualitätsmanagements. Auf dieser Managementebene dürfte eine besondere Herausforderung darin liegen, ein leistungsfähiges, netzwerkübergreifendes Wissensmanagement zu gewährleisten.

3.3.3 Modulmanagement

Das Modulmanagement steht in der Verantwortung der jeweiligen Netzwerkpartner und hat die betriebliche Sicherung einer ergebnisorientierten Leistungserstellung innerhalb der einzelnen Module zum Gegenstand (operatives Prozessmanagement auf der Modulebene). Hierzu zählen zunächst alle operativen Managementfunktionen, wie sie auch bei der bisher üblichen intraorganisationalen Gestaltung und Steuerung arbeitsteiliger Systeme erforderlich waren. Allerdings ergeben sich aus der Einbindung in Öffentliche Leistungsnetzwerke bestimmte Restriktionen und auch veränderte inhaltliche Anforderungen sowohl hinsichtlich der Sicherung der Netzwerkfähigkeit der Produktion (zum Beispiel Anschlussfähigkeit der Teilleistungen) als auch der Steuerung (zum Beispiel spezifische Personalführungsbedarfe) auf Modulebene. Die besondere Herausforderung liegt auf dieser Ebene darin, die arbeitsteilige modulare Leistungserstellung (zum Beispiel Anwendung von Fachkonzepten, Interaktionsstil, Adressaten-Integration „vor Ort“ et cetera) laufend auf übergeordnete Bewirkenszusammenhänge auszurichten.

Bezogen auf das strategische Management bedeutet diese Strukturierung von Managementbedarfen bei Öffentlichen Leistungsnetzwerken, dass Fragen des strategischen Managements der einzelnen, am Netzwerk (potenziell) beteiligten Netzwerkpartner (zum Beispiel Entscheidungen über die Art und den Umfang der eigenen Beteiligung an Öffentlichen Leistungsnetzwerken) hier zunächst systematisch ausgeklammert bleiben, auch wenn es diesbezüglich – beispielsweise in Abhängigkeit von der Gründungssituation – wichtige Berührungspunkte und Überschneidungen mit dem strategischen Netzwerkmanagement geben kann. Bei der weiteren theoretisch-konzeptionellen Ausarbeitung eines unter dem Einfluss von E-Government erneuerten Public Management müsste diese einzelorganisationsbezogene Management-Perspektive jedoch ebenso anschlussfähig „eingefangen“ und in ein Public Management-Gesamtsystem integriert werden, wie auch die Management-Besonderheiten der politisch-administrativen Gestaltung und Steuerung der Politischen Regulierung selbst (Management des Policy-Prozesses als eine Art „Meta-Geschäftsprozess“) sowie die Spezifika des Managements der Infrastruktur als Leistungspotenzial im oben beschriebenen Sinne. Bei alledem ist ferner nicht zu vergessen, dass nicht nur die „neue Produktion“, sondern auch die Deckung dieser Managementbedarfe unter umfassender und bedarfsgerechter IT-Nutzung zu konzipieren ist.

4 Fazit: Netzwerkfähiges Public Management als Erfolgsfaktor

Der Frage neuer Produktionsformen im Kontext von E-Government ist bislang weder von der Politik- und Verwaltungswissenschaft noch vom Public Management die ihr gebührende Aufmerksamkeit gewidmet worden [GE04:22; Du06; Ag07:233; BR11a]. Inzwischen zeichnen sich durch den Einsatz moderner IT auf der Ebene der Produktion öffentlicher Leistungen bereits an vielen Stellen mehr oder weniger weitreichende Veränderungen ab. Diese Veränderungen folgen jedoch keinem technologischen Determinismus. Außerdem ist die intelligente Nutzung der Gestaltungspotenzale durch E-Government für eine politisch legitimierte, verantwortungsbewusste, nachhaltige Sicherung und Verbesserung der Lebensqualität unter den Bedingungen von Ressour-

cenknappheit alles andere als ein Selbstläufer. Deshalb bedarf es eines handfesten, flexiblen und tatsächlich „ganzheitlichen“ Ansatzes, der statt eines neuen Einheitsmodells eine in Bezug auf die jeweilige öffentliche Aufgabe und die mit ihr verbundene politisch-regulatorische Intention konsequent kontextbezogene Synchronisation der Produktion öffentlicher Leistungen und deren Steuerung ermöglicht. Einem im Lichte der durch IT veränderten Produktionsverhältnisse erneuerten Public Management wäre dabei eine tragende Brückenrolle zuzuschreiben. Sie besteht darin, auf der Basis von leistungsfähigen Infrastrukturen einen leistungsfähigen Vollzug der jeweiligen politischen Regulierungsabsichten „auf die Beine zu stellen“. Neben der vorherrschenden primär technisch-organisatorischen Infrastruktur-Perspektive auf die Herstellung von Netzwerkfähigkeit, wie sie durch die Nationale E-Government-Strategie geprägt wird [Wen10], und der bislang kaum beachteten Frage nach der „Netzwerkfähigkeit des öffentlichen Dienstes“ [Br04:204; Sc09b] gerät somit zunehmend auch die „Netzwerkfähigkeit des Public Management“ zu einer erfolgskritischen Voraussetzung für gutes Regieren und Verwalten in einer von Informationstechnik durchdrungenen Gesellschaft.

Literaturverzeichnis

[Ag01] Agranoff, R.: Big Questions in Public Network Management Research. In: Journal of Public Administration Research and Theory, Vol. ll (2001), No.3; 295-326.

[Ag07] Agranoff, R.: Managing within Networks. Adding Value to Public Organizations, Washington D.C., 2007.

[BEH10] Bashiri, I.; Engels, C; Heinzelmann, M.: Strategic Alignment - Zur Ausrichtung von Business, IT und Business Intelligence, Berlin, Heidelberg, 2010.

[Bi07] Bieger, T.: Dienstleistungsmanagement, 4. Aufl., Bern, Stuttgart, Wien, 2007.

[Br04] Brüggemeier, M.: Gestaltung und Steuerung öffentlicher Leistungsnetzwerke im Kontext von Electronic Government. In (Reichard, C.; Scheske, M.; Schuppan, T., Hrsg.): Das Reformkonzept E-Government, Münster, 2004; S.188-209.

[Br06] Brüggemeier, M. et al.: Organisatorische Gestaltungspotenziale durch Electronic Government. Auf dem Weg zur vernetzten Verwaltung, Berlin, 2006.

[Br07a] Brüggemeier, M.: Controlling kommunaler Leistungsnetzwerke. In (Brüggemeier, M.; Schauer, R.; Schedler, K., Hrsg.): Controlling und Performance Management im Öffentlichen Sektor. Ein Handbuch. Festschrift für Dietrich Budäus, Bern u.a., 2007; S.51-60.

[Br07b] Brüggemeier, M.: Neue Perspektiven und Forschungsbedarf für einen aufgeklärten Gewährleistungsstaat auf der Basis von E-Government. In: Verwaltung & Management, 13. Jg. (2007), H.1; S.79-85.

[BD05] Brüggemeier, M.; Dovifat, A.: *„OPEN CHOICE“* – Ein strategisches Modell für das Reengineering der öffentlichen Leistungserstellung auf Basis von E-Government. In (Klischewski, R.; Wimmer, M., Hrsg.): Wissensbasiertes Prozessmanagement im E-Government, Münster, 2005; S.28-42.

[BL11] Brüggemeier, M.; Lenk, K.: Einführung: Bürokratieabbau im Verwaltungsvollzug. In (Brüggemeier, M.; Lenk, K., Hrsg.): Bürokratieabbau im Verwaltungsvollzug. Better Regulation zwischen Go-Government und No-Government, Berlin, 2011; S. 11-24.

[BO08] Blomgren Bingham, L.; O´Leary, R.: Big Ideas in Collaborative Public Management, New York, 2008.

[BR11a] Brüggemeier, M.; Röber, M.: Auf dem Weg zu einem neuen Steuerungsregime? Eine Analyse des Zusammenhangs von Steuerung und Arbeitsorganisation im öffentlichen Sektor. In (Koch, R.; Conrad, P.; Lorig, W., Hrsg.): New Public Service. Öffentlicher Dienst als Motor der Staats- und Verwaltungsmodernisierung, 2. Aufl., Wiesbaden, 2011; S.213-245.

[BR11b] Brüggemeier, M.; Röber, M.: Neue Modelle der Leistungserstellung durch E-Government – Perspektiven für das Public Management. In: dms – der moderne staat, 4. Jg. (2011), H.2; S.357-380.

[Bu06] Budäus, D.: Entwicklung und Perspektiven eines Public Management in Deutschland. In (Jann, W.; Röber, M.; Wollmann, H., Hrsg.): Public Management. Grundlagen, Wirkungen, Kritik. Festschrift für Christoph Reichard, Berlin, 2006; S.173-186.

[Do06] Dovifat, A.: „Soziale Arbeit heißt, das soziale Netz verfügbar machen…“ – Besonderheiten und Probleme bei der organisationsübergreifenden Produktion sozialer Dienstleistungen. In (Birkholz, K. et al., Hrsg.): Public Management – Eine neue Generation in Wissenschaft und Praxis. Festschrift für Christoph Reichard, Potsdam, 2006; S.315-335.

[Du06] Dunleavy, P. et al.: New Public Management is Dead – Long Live Digital-Era Governance. In: Journal of Public Administration Research and Theory, Vol. 16 (2006), H.3; S.467-494.

[Fl06] Fließ, S.: Prozessorganisation in Dienstleistungsunternehmen, Stuttgart, 2006.

[GE04] Goldsmith, S.; Eggers, W. D.: Governing by Network. The New Shape of the Public Sector, Washington D.C., 2004.

[GK09] Goldsmith, S.; Kettl, D.F.: Unlocking the Power of Networks. Keys to High-Performance Government, Washington D.C., 2009.

[Hi07] Hill, H.: Recht als Geschäftsmodell. Von Better Regulation zu New Regulation. In: Die Öffentliche Verwaltung, 60. Jg. (2007), H.19; S.809-819.

[Hi10] Hill, H.: Perspektive 2020. In (Hill, H., Hrsg.): Verwaltungsmodernisierung, Baden-Baden, 2010.

[Ke10] Keystone Accountability: Impact Planning, Assessment and Learning – an overview, London, 2010. Online: http://www.world-federation.org/NR/rdonlyres/42961DA8-CD5F-4C37-A869-163C28E62C70/0/NGO_8p1_KAImpactPlanning.pdf Zugriff: 23.09.11.

[Le04] Lenk, K.: Der Staat am Draht. Electronic Government und die Zukunft der öffentlichen Verwaltung, Berlin, 2004.

[Le11a] Lenk, K.: Perspektiven der ununterbrochenen Informatisierung der Verwaltung. In: dms – der moderne staat, 4. Jg. (2011), H.2; S.315-334.

[Le11b] Lenk, K.: Innovation Impact Assessment. Entwicklung und Bewertung neuer Vollzugsstrukturen. In (Brüggemeier, M.; Lenk, K., Hrsg.): Bürokratieabbau im Verwaltungsvollzug. Better Regulation zwischen Go-Government und No-Government, Berlin, 2011; S. 227-246.

[LSS10] Lenk, K.; Schuppan, T.; Schaffroth, M.: Vernetzte Verwaltung. Organisationskonzept für ein föderales E-Government Schweiz. eCH-White Paper, Strategieorgan Schweizerische Eidgenossenschaft, Bern, 2010 Online: http://www.ech.ch/alfresco/guestDownload/attach/workspace/SpacesStore/70206616-b39b-43ff-8231-986c1f273b3f/WP_d_DEF-2010-07-12_Lenk-Schuppan-Schaffroth_Vernetzte%20Verwaltung.pdf Zugriff: 23.09.11.

[LT99] Lenk, K.; Traunmüller, R., Hrsg.: Öffentliche Verwaltung und Informationstechnik. Perspektiven einer radikalen Neugestaltung der öffentlichen Verwaltung mit Informationstechnik, Heidelberg, 1999.

[OE10] OECD: Regulatory Policy and the Road to Sustainable Growth. Draft report, Paris, 2010.

[PAR06] Public Administration Review, Vol. 66 (2006), December, Special Issue.

[Pi09] Piesker, A.: Better regulation in Europe – Entwicklungspfade, Akteure und Instrumente in Großbritannien und Deutschland. In (Hill, H., Hrsg.): Verwaltungsmodernisierung im europäischen Vergleich, Baden-Baden, 2009; S.139-172.

[Rö11] Röber, M.: Aufgabenplanung und Aufgabenkritik. In (Blanke, B. et al., Hrsg.): Handbuch zur Verwaltungsreform, 4. Aufl., Wiesbaden 2011; S.108-117.

[Rö12] Röber, M., Hrsg.: Institutionelle Vielfalt und Neue Unübersichtlichkeit – Zukunftsperspektiven effizienter Steuerung öffentlicher Aufgaben zwischen Public Management und Public Governance, Berlin, 2012 (i.E.).

[Sc06] Schuppan, T.: Strukturwandel der Verwaltung mit E-Government, Berlin, 2006.

[Sc09a] Schuppan, T.: Reassessing Outsourcing in ICT-Enabled Public Management. Examples from the UK. In: Public Management Review, Vol. 11 (2009), H.6; S.811-831.

[Sc09b] Schuppan, T.: Neue Kompetenz-Anforderungen für (vernetztes) E-Government. In: Verwaltung & Management, 15. Jg. (2009), H.3; S.126-135.

[SD11] Sydow, J.; Duschek, S.: Management interorganisationaler Beziehungen. Netzwerke – Cluster – Allianzen, Stuttgart.

[SR10] Schuppan T.; Reichard, C.: Neubewertung staatlicher Leistungstiefe bei Informatisierung. In: Verwaltung & Management, 16. Jg. (2010), H.2, Themenschwerpunktheft E-Government, Klaus Lenk zum 70. Geburtstag gewidmet; S.84-92.

[Sy99] Sydow, J.: Führung in Netzwerkorganisationen – Fragen an die Führungsforschung. In (Schreyögg, G.; Sydow, J., Hrsg.): Führung – neu gesehen (= Managementforschung 9), Berlin, New York; S.279-292.

[Sy06] Sydow, J.: Management von Netzwerkorganisationen – Zum Stand der Forschung. In (Sydow, J., Hrsg.): Management von Netzwerkorganisationen, 4. Aufl., Wiesbaden, 2006; S.387-472.

[We11] Wegrich, K.: Das Leitbild „Better Regulation“. Ziele, Instrumente, Wirkungsweise, Berlin, 2011.

[Wen10] Wentzel, J.: Die Nationale E-Government-Strategie: Ein Schritt vor, zwei zurück? In: Verwaltung & Management, 16. Jg. (2010), H.6; S.283-292.

Regionales Servicecenter Vergaben – Weiterentwicklung einer regionalen E-Vergabeplattform zu einem Shared Service Center

Ralf Daum

Duale Hochschule Baden-Württemberg Mannheim
Coblitzallee 1-9, 68163 Mannheim
ralf.daum@dhbw-mannheim.de

Abstract: Ein Großteil der Kommunen in der Metropolregion Rhein-Neckar wickelt Ausschreibungen über eine gemeinsame E-Vergabeplattform ab. Die Bearbeitung der einzelnen Vergabevorgänge erfolgt auf Basis einheitlicher Formulare aber eigenständig durch jede Kommune. Die Komplexität des öffentlichen Vergaberechts erschwert zunehmend eine rechtssichere Abwicklung von Vergabeverfahren. E-Government bietet die Möglichkeit, die interkommunale Kooperation im Bereich Vergaben weiter auszubauen. Der Beitrag zeigt auf, wie ein regionales Servicecenter Vergaben als Shared Service Center die an der E-Vergabeplattform beteiligten Kommunen unterstützen kann. Die zentrale Dienstleistung des Servicecenters besteht in der rechtssicheren und rechtskonformen Durchführung von Vergabeverfahren. Dabei geht es vorrangig um die formale Abwicklung bezüglich Vergabe- und Vertragsrecht. Die Zuständigkeit für die Beschreibung des Bedarfes und die Bewertung der Angebote inklusive Vergabeentscheidung liegt weiterhin bei den einzelnen Kommunen, die über das jeweilige fachliche Know-how verfügen. Die E-Vergabeplattform inklusive Vergabemanagementsystem stimmt die einzelnen Arbeitsschritte im Vergabeprozess aufeinander ab und weist sie den beteiligten Sachbearbeiter/-innen in Kommunen beziehungsweise Servicecenter automatisiert zu.

1 Situation im öffentlichen Vergabewesen

1.1 Komplexität des öffentlichen Vergabewesens

In den vergangenen Jahren hat die Komplexität von Beschaffungs- und Vergabevorgängen im öffentlichen Sektor zum Leidwesen der öffentlichen Auftraggeber und der Bewerber beziehungsweise Bieter ständig zugenommen. Die Ursachen liegen in den unterschiedlichen Anforderungen, die an das öffentliche Beschaffungs- beziehungsweise Vergabewesen[5] gestellt werden. Ein zentraler Anspruch ist die Ordnungsmäßigkeit der Beschaffungs- beziehungsweise Vergabevorgänge. Es geht dabei unter anderem um

[5] Im Folgenden werden die Begriffe „Vergabe“ und „Beschaffung“ synonym verwendet.

Themen wie Korruptionsbekämpfung und -vermeidung. Die Abwicklung von Vergabeverfahren muss nach für alle Beteiligte nachvollziehbaren und rechtlich überprüfbaren Grundsätzen erfolgen. Entsprechende Anforderungen bestehen für die Dokumentation aller Schritte und Entscheidungen. Ein weiteres Ziel liegt ebenso wie bei privaten Unternehmen in der Wirtschaftlichkeit der Beschaffung. Entgegen des weit verbreiteten Vorurteils, dass öffentliche Auftraggeber immer „den niedrigsten Angebotspreis beauftragen müssen“, geht es bei einer sparsamen und wirtschaftlichen Haushaltsführung nicht um den niedrigsten Preis, sondern um das insgesamt wirtschaftlichste Angebot (Verhältnis Leistung und Preis). Durch verschiedene Vorgaben der Europäischen Union haben die Wettbewerbsförderung, die Gleichbehandlung und die Förderung des Mittelstandes stark an Bedeutung gewonnen. Im Sinne des Wettbewerbsgrundsatzes sollen eindeutige, formalisierte Verfahren bewirken, dass möglichst viele Anbieter die Gelegenheit bekommen, ihre Leistungen und Produkte anzubieten. Die Grundsätze der Gleichbehandlung und Nichtdiskriminierung sorgen dafür, dass für alle Marktteilnehmer im Wettbewerb gleiche Chancen bestehen. Persönliche, sachliche oder lokale Bevorzugungen dürfen das Vergabeverfahren beziehungsweise die Zuschlagserteilung nicht beeinflussen. Die Pflicht zur Unterteilung eines Auftrags in Teillose (Aufteilung der Menge) beziehungsweise Fachlose (Trennung nach Art oder Fachgebiet) schafft die Voraussetzungen, dass sich mittelständische Unternehmen auch an der Vergabe von Großaufträgen beteiligen können. Da sich öffentliche Einrichtungen aufgrund ihrer Vorbildfunktion und ihrer Nachfragemacht als Instrumente einer Nachhaltigkeitspolitik eignen, spielen soziale und ökologische Kriterien bei öffentlichen Beschaffungen eine zunehmende Rolle [Sa11]. Seitens der lokalen politischen Vertretungen besteht der Wunsch, das öffentliche Vergabewesen auch zur Förderung der regionalen Wirtschaft, zur Sicherung von Arbeitsplätzen, Verfolgung lokaler sozialpolitischer Zielsetzungen und so weiter zu nutzen. Schließlich geht es im öffentlichen Sektor genauso wie in der Privatwirtschaft um die Deckung der betrieblichen Bedarfe, die zur Leistungserstellung erforderlich sind.

Zwischen den verschiedenen Anforderungen bestehen zahlreiche Zielkonflikte. Der Wunsch die regionale Wirtschaft zu unterstützen steht im Widerspruch zum Gleichbehandlungsgrundsatz. Der Grundsatz der Ordnungsmäßigkeit kann gegensätzlich zur Wirtschaftlichkeit stehen oder sogar die notwendige, zeitnahe Deckung von betrieblichen Bedarfen gefährden und so weiter

Die verschiedenen Anforderungen finden ihren Niederschlag in zahlreichen Regeln und Vorschriften, die der Oberbegriff „Vergaberecht“ zusammenfasst. Zu den wesentlichen rechtlichen Vorschriften zum Vergabewesen zählen unter anderem das Gesetz gegen Wettbewerbsbeschränkungen, die Vergabeverordnung, das Haushaltsgrundsätzegesetz, die Bundeshaushaltsordnung, die Landeshaushaltsordnungen, Gemeindeordnungen, Gemeindehaushaltsverordnungen. Drei Regelwerke machen konkrete Vorgaben für die Ausgestaltung der Vergabeverfahren: die Vergabe- und Vertragsordnung für Bauleistungen (VOB), die Vergabe- und Vertragsordnung für Lieferungen und Leistungen (VOL) und die Vergabeordnung für freiberufliche Leistungen (VOF). Erschwerend kommt hinzu, dass das Vergaberecht zweigeteilt ist in einen nationalen und einen europäischen Teil, abhängig davon, ob das Auftragsvolumen europarechtlich vorgegebene Schwellenwerte erreicht. Beispielsweise liegen derzeit diese Schwellenwerte für Bau-

aufträge bei 4.845.000 Euro (netto), für Warenlieferaufträge bei 193.000 Euro (netto) und für Dienstleistungsaufträge bei 193.000 Euro (netto). Je nachdem, ob ein Beschaffungsvorgang dem nationalen oder dem EU-Bereich unterliegt, unterscheiden sich die Verfahrensgestaltung, die Transparenz- und Bekanntmachungspflichten und die Nachprüfungsmöglichkeiten für die Bieter [WS10].

Eine Komplexität anderer Art besteht bei der elektronischen Unterstützung des öffentlichen Vergabewesens. Seit Beginn des neuen Jahrtausends hat die elektronische Abwicklung von Vergabeprozessen Einzug in das deutsche Vergaberecht gehalten [He05]. Beschleunigt wurde dies durch den Aktionsplan der EU aus dem Jahr 2004 zur Einführung voll elektronischer Vergabesysteme in den Mitgliedsstaaten der EU bis Ende 2007. Das angestrebte Ziel hat Deutschland zwar verfehlt [EC10]. Dennoch steigt kontinuierlich der Einsatz der elektronischen Vergabe. Das Spektrum reicht von reinen Bekanntmachungsplattformen, die zur Veröffentlichung von Bekanntmachungstexten öffentlicher Vergaben beziehungsweise offener Verfahren gegebenenfalls inklusive elektronischer Bereitstellung der Vergabeunterlagen dienen, bis hin zu Vergabeplattformen, die zusätzlich auf Bieterseite die elektronische Angebotsabgabe und auf Verwaltungsseite die Annahme und Aufbewahrung der Angebote unterstützt [Ru09]. Die Bedeutung der elektronischen Vergabe im öffentlichen Vergabewesen nimmt ständig zu. Beispielsweise nimmt das Beschaffungsamt des Bundesministeriums des Innern seit dem 01.01.2010 Angebote nur noch elektronisch entgegen. Desgleichen bauen die Bundesländer und die Kommunen die E-Vergabe ständig aus, so dass mittlerweile eine Vielzahl unterschiedlicher E-Vergabeplattformen in Deutschland existiert [La10].

1.2 Auswirkungen auf Auftraggeber und Bieter

Im kommunalen Bereich führt die Komplexität des Vergaberechts zu unterschiedlichen negativen Wirkungen. Die Fülle an Regelungen erhöht den Aufwand bei der Abwicklung von Vergabeverfahren. Erschwerend kommt hinzu, dass die Kenntnis über das Vergaberecht allein nicht ausreicht, rechtskonforme Vergabevorgänge durchzuführen. Zusätzlich bedarf es Kenntnisse von einschlägigen Vergabekammerentscheidungen oder Oberlandesgerichtsurteilen. Viele Vergabestellen fühlen sich deshalb überfordert. Dies trifft nicht nur auf kleinere Kommunen zu, die selten öffentliche Ausschreibungen durchführen, sondern auch auf große Kommunen in Verbindung mit selten auftretenden Beschaffungsvorgängen. Immer häufiger ziehen deshalb selbst große öffentliche Auftraggeber bei Ausschreibungen externe Vergaberechtsexperten hinzu, um die (finanziellen) Risiken, die sich aus Aufhebungen, Nachprüfungsverfahren und so weiter ergeben, zu reduzieren [RIL08]. Ein ähnliches Bild zeigt sich auf Seiten der Bewerber und Bieter. Die meisten Unternehmen, die sich erstmals auf öffentliche Ausschreibungen bewerben, scheitern aufgrund formaler Fehler. Viele belassen es bei einem einmaligen Versuch. Gerade kleine und mittelständische Unternehmen kapitulieren anhand der Fülle an formalen Vorgaben, Formularen und so weiter beim Bearbeiten und Abgeben eines Angebots. Den öffentlichen Auftraggebern entsteht dadurch ein großer Nachteil, weil das Fehlen leistungsfähiger Unternehmen den eigentlich gewünschten, breiten Wettbewerb sowie die Förderung des Mittelstandes einschränkt. Spezielle Auftragsberatungsstellen, beispielsweise auf Ebene der Industrie- und Handelskammern, die sowohl

Unternehmen als auch öffentliche Auftraggeber in allen Fragen des öffentlichen Auftragswesens unterstützen, bieten zwar eine wichtige Hilfestellung, kurieren aber letztendlich nur die Symptome [Da11]. Elektronische Vergabelösungen besitzen das Potenzial, die Komplexität des öffentlichen Vergabewesens für Auftraggeber und Bieter beherrschbar zu machen [GS02]. Bislang konnten diese Möglichkeiten noch nicht flächendeckend genutzt werden. Bewerber beziehungsweise Bieter müssen sich auf jeder einzelnen, häufig kostenpflichtigen Plattform separat anmelden und einarbeiten. Regelmäßig kritisieren sie, dass ein zentraler elektronischer Zugang zu allen Ausschreibungen des Bundes, der Länder und der Kommunen fehlt [BDI10]. Auch die weiterhin offenen Fragestellungen zum Einsatz der elektronischen Signatur bei elektronischen Ausschreibungen erschweren die Nutzung der E-Vergabe [SBA09]. In der Summe schrecken die hohen Kosten für die mehrfache Registrierung und Einarbeitung in unterschiedliche E-Vergabesysteme sowie die Beschaffung elektronischer Signaturen besonders kleine und mittelständische Unternehmen von der Nutzung der E-Vergabe ab.

2. Aktuelle Entwicklungen im öffentlichen Vergabewesen

2.1 Elektronische Vergaben am Beispiel des Vergabeportals der Metropolregion Rhein-Neckar

Das Bundesministerium für Wirtschaft und Technologie (BMWi) und der Bundesverband Materialwirtschaft, Einkauf und Logistik e.V. (BME) haben im Jahr 2010 ein besonders zukunftsweisendes Konzept für eine elektronische Vergabelösung mit dem Preis „Innovation schafft Vorsprung“ ausgezeichnet.

Unter der E-Vergabeplattform[6] „www.auftragsboerse.de“ stellt die Metropolregion Rhein-Neckar[7] alle Informationen zu aktuellen Ausschreibungen aus der Region online zur Verfügung. Auf Seiten der Bieter entfällt die mehrfache Anmeldung und Einarbeitung in unterschiedliche Bekanntmachungsplattformen. Zusätzlich stehen die Vergabeunterlagen der beteiligten Kommunen kostenlos zur Bearbeitung bereit. Bei Bedarf unterstützt ein so genanntes Bieterwerkzeug die Bieter beim Ausfüllen der Unterlagen. Es strukturiert durch Dialogmasken die Bearbeitung der unterschiedlichen Formulare, weist durch Plausibilitätsprüfungen auf Lücken oder Fehler hin und verhilft so zu einem vollständigen und formal korrekten Angebot. Ein wesentliches Element des Konzeptes bildet die Vereinheitlichung und ständige Aktualisierung der Formulare/Vordrucke, die die beteiligten Kommunen über die Ländergrenzen hinweg, anwenden. Insbesondere kleinen und mittelständischen Unternehmen soll damit der Zugang zu öffentlichen Ausschreibungen erleichtert werden.

[6] Mit dem Vergabeportal der Metropolregion Rhein-Neckar wird bewusst nicht das Ziel verfolgt, eine kommunale Einkaufsgemeinschaft aufzubauen. Um dies zu unterstreichen, verzichtet der Beitrag im Folgenden auf den gängigen Begriff „E-Procurement“ und verwendet nur die Begriffe „E-Vergabe“, „Vergabeplattform“ usw. Auch inhaltlich geht der Beitrag auf dieses Thema nicht ein.

[7] Die Metropolregion Rhein-Neckar umfasst sieben Landkreise und acht kreisfreie Städte in den drei Bundesländern Baden-Württemberg, Rheinland-Pfalz und Hessen. Die größten Städte sind Mannheim, Heidelberg und Ludwigshafen.

Auch auf Seiten der öffentlichen Aufraggeber entstehen durch die Nutzung der E-Vergabeplattform zahlreiche Vorteile. Sie bietet den Vergabestellen eine vollständig workflowbasierte elektronische Unterstützung bei der Vorbereitung, Durchführung und Dokumentation des Vergabeprozesses. Neben der Entlastung der Sachbearbeiter/-innen von Routinetätigkeiten entsteht die Chance zur Optimierung der internen Vergabeprozesse. Jede Kommune setzt dabei eigenständig die E-Vergabeplattform ein.

Die Metropolregion Rhein-Neckar hat diesen Entwicklungsprozess über die Zusammenarbeit im Arbeitskreis „Vergabe öffentlicher Aufträge“, an dem neben Experten aus kommunalen Vergabestellen auch Vertreter der Handwerkskammern und der Industrie- und Handelskammern der Region teilgenommen haben, koordiniert und die E-Vergabeplattform als Application Service Providing-Modell (ASP) zentral als Rahmenvertrag ausgeschrieben. Die Einführung der Software sowie die Abrechnung zwischen ASP-Anbieter und den einzelnen Kommunen werden jeweils bilateral geregelt [BD10].

2.2 Zentralisierung von Vergabevorgängen

Die hohe Komplexität des öffentlichen Vergabewesens und die damit verbundenen Risiken für öffentliche Auftraggeber führen zunehmend zu einer Überforderung der betroffenen Sachbearbeiter/-innen und damit zu einer steigenden Unzufriedenheit. Dies gilt vor allem für diejenigen, die hauptsächlich Fachaufgaben in ihrer Dienststellen wahrnehmen und sich nur am Rande mit dem Thema Vergabe beschäftigen müssen. Trotz zahlreicher Vorteile, die sich durch eine Zentralisierung der Vergabevorgänge ergeben könnten, organisieren die meisten öffentlichen Auftraggeber ihre Beschaffung dezentral [Bo11]. Lediglich einige große Kommunen, die eine entsprechende Anzahl an Vergabevorgängen pro Jahr durchführen, reagieren auf diese Situation vermehrt mit der Bildung von zentralen Einheiten. Je nach Kommune nehmen diese zentralen Einheiten unterschiedliche Aufgaben wahr. Folgende wesentliche Aufgaben lassen sich identifizieren:

- Beratung und Unterstützung bei der Durchführung von Vergabevorgängen
- Kompetenzaufbau, zum Beispiel Durchführung von Weiterbildungen zum Vergabewesen
- Abwicklung von kompletten Vergabevorgängen
- Bedarfsbündelung, zum Beispiel Standardisierung von Produkten und Ausschreibung von Rahmenverträgen

Bei der Beratung und Unterstützung bei der Durchführung von Vergabevorgängen wickeln die zentralen Einheiten keine Vergabeprozesse ab. Federführend bleibt die Dienststelle, bei der der Bedarf auftritt[8]. Die zentrale Einheit berät und gibt Empfehlungen, wie Vergabevorgänge abgewickelt werden können.

Beim Kompetenzaufbau geht es darum, Mitarbeiter und Mitarbeiterinnen in den Bedarfsstellen in die Lage zu versetzen, nach und nach auch komplexere Vergabevorgänge eigenständig durchführen zu können. Dies geschieht durch ein regelmäßig angebotenes

[8] So genannte Bedarfsstellen.

Fortbildungsprogramm und den Aufbau eines Wissensmanagements zum Thema Vergabewesen. Das Wissensmanagement umfasst unter anderem Informationsportale im Intranet und Internet sowie den Aufbau von FAQs aus der Beratungstätigkeit bis hin zum Einsatz von Web 2.0-Werkzeugen. Durch die Kombination der E-Learning-Angebote mit persönlichen Schulungen und praktischen Beratungen an aktuellen Vergabevorgängen entsteht integriertes Lernen (Blended Learning), das zusätzliche Chancen bietet [HK03].

Einige Kommunen lassen komplette Vergabevorgänge von zentralen Einheiten, so genannten zentralen Vergabestellen, durchführen. Dabei geht die Federführung oder zumindest ein Teil davon auf die zentrale Vergabestelle über. Die Abwicklung von kompletten Vergabevorgängen durch die zentrale Einheit birgt aber die Gefahr, dass es zu Spannungen zwischen zentraler Vergabestelle und Bedarfsstellen kommt. Hier bietet sich eine klare Trennung der Prozessschritte nach Entscheidungen über fachliche Fragen und Entscheidungen bezüglich Vergabe- und Vertragsrecht an. Die Zuständigkeit für fachliche Fragen liegt bei den Bedarfsstellen, die über das jeweilige fachliche Know-how verfügen. Die Entscheidungen bezüglich Vergabe- und Vertragsrecht benötigen das spezielle Know-how zu diesem Themengebiet. Insofern liegt die Zuständigkeit bei der zentralen Einheit, die durch die stadtweite Zuständigkeit auch die notwendige Größe, insbesondere aus personeller Sicht, besitzt und eine ständige Arbeitsfähigkeit (Vertretungsregelungen et cetera) gewährleistet.

Die Zentralisierung erhöht außerdem die Transparenz bezüglich der gesamten Beschaffungsaktivitäten einer Kommune. Ähnliche Bedarfe in verschiedenen Dienststellen werden sichtbar und erleichtern Bedarfsbündelung, zum Beispiel durch Standardisierung von Produkten und Ausschreibung von Rahmenverträgen.

Die beschriebene Zentralisierung eignet sich in erster Linie für größere Kommunen. Für kleine und mittlere Kommunen ist diese Vorgehensweise aufgrund der geringeren und unregelmäßiger auftretenden Anzahl von Vergabevorgängen weniger geeignet. Bei einer konsequenten Nutzung von Electronic Government und Shared Services im öffentlichen Vergabewesen könnten sie aber an den Vorteilen einer Zentralisierung partizipieren.

3 Shared Service Center zur Abwicklung öffentlicher Vergaben am Beispiel der Metropolregion Rhein-Neckar

3.1 E-Government und Shared Services

E-Government schafft die Vorrausetzungen für die Zusammenarbeit beziehungsweise Kollaboration unterschiedlicher Verwaltungseinheiten [Tr99]. Der Begriff Shared Services fasst die verschiedenen Konzepte der Kollaboration zusammen, angefangen von Shared Service Center, bei denen eine Einheit zentral alle Dienste erbringt, bis hin zu Shared Service Networks, bei denen mehrere Einheiten Dienste erbringen und gegebenenfalls auch gleichzeitig empfangen [BNK09]. Eine Verbreitung dieses Gedankens

in der kommunalen Praxis hat bis auf die klassische Zusammenarbeit in Zweckverbänden bisher kaum stattgefunden. Die Potenziale, die sich durch E-Government bieten, sind bei weiten nicht ausgeschöpft [BWT07]. Besonders für kleinere Kommunen eröffnet E-Government die Möglichkeit, Lücken in der eigenen Leistungsfähigkeit zu schließen, Prozesse zu vereinfachen und die Wirtschaftlichkeit zu erhöhen [Ca08]. Einer der Hauptgründe für den zurückhaltenden Einsatz von E-Government bei der interkommunalen Zusammenarbeit liegt in der kommunalen Selbstverwaltungsgarantie und Befürchtungen der jeweiligen Verwaltungsspitzen die eigenen Einflussmöglichkeiten zu beschränken [Sc07]. Lediglich die einheitliche Behördenrufnummer D 115 bildet auf dem Gebiet eine Ausnahme. Hier entstehen zunehmend Shared Services-Strukturen im kommunalen Bereich [Lu10].

Auch das öffentliche Vergabewesen bietet unter intensiver Nutzung der E-Vergabe ähnliche Zusammenarbeitsmöglichkeiten wie D 115. E-Vergabeplattformen und angeschlossene Vergabemanagementsysteme bilden alle bei Vergaben relevanten Prozesse von der Erstellung der Vergabeunterlagen über die Veröffentlichung der Bekanntmachung bis zum Zuschlag durchgängig elektronisch ab [TS05]. Berechtigungskonzepte grenzen die Rechte der einzelnen Benutzer zur Durchführung bestimmter Aufgaben und Vorgänge eindeutig ab und schaffen somit die Grundlagen für eine gemeinsame Sachbearbeitung [Me09]. Die Abbildung einer Shared Service-Struktur mit einer oder mehreren Stellen, die Dienstleitungen bei der Durchführung von Vergaben zentral anbieten, stellt technologisch und organisatorisch überschaubare Herausforderungen dar. Trotzdem treiben Kommunen die Implementierung von E-Vergabe-Lösungen nur zögerlich voran [WLS08]. Auf Bundesebene praktiziert das Beschaffungsamt des Bundesministeriums des Innern seit einigen Jahren erfolgreich ein solches Modell [Kl02]. Als Dienstleistungszentrum des Bundes bietet es standardisierbare Dienstleistungen, insbesondere im Bereich Einkauf/Beschaffung, zur Entlastung der einzelnen Bundesbehörden an. Das Dienstleistungsangebot reicht von der vergabe- oder vertragsrechtlichen Beratung bis zur Durchführung einer kompletten Beschaffung. Das im Beschaffungsamt gebündelte Expertenwissen verhilft den Kundenbehörden, Ressourcen zu sparen und sich besser auf Kernaufgaben zu konzentrieren [BI10].

Die bestehenden Hemmnisse bei einer verwaltungsübergreifenden Zusammenarbeit bei Beschaffungsprozessen im kommunalen Bereich können nur überwunden werden, wenn die beteiligten Kommunen die wesentlichen Entscheidungen im Vergabeverfahren weiterhin selbst treffen können. Dazu gehören in der Regel die Beschreibung des Bedarfes inklusive Erstellung des Leistungsverzeichnisses, die fachliche Prüfung der eingehenden Angebote und die eigentliche Vergabeentscheidung, welcher Bieter zum Zuge kommt. Alle anderen Prozessschritte von der Festlegung des Vergabeverfahren und Vergabeart über öffentliche Bekanntmachung, Submission und formelle Prüfung bis hin zur eigentlichen Zuschlagserteilung sind durch das Vergaberecht strikt geregelt und bieten kaum individuelle Gestaltungsmöglichkeiten. Insofern gibt es wenige Gründe diesbezüglich auf eine eigenständige Abwicklung dieser Prozessschritte zu bestehen. Auch bei einer Trennung zwischen fachlichen und rechtlichen Fragestellungen können Situationen im laufenden Vergabeverfahren entstehen, die eine enge Abstimmung erfordern. Hier müssen über eine reibungslose Zusammenarbeit im Vergabemanagementsys-

tem und durch die zentrale Vorhaltung aller Dokumente beziehungsweise Dokumentationen die Nachteile der räumlichen & organisatorischen Trennung kompensiert werden.

3.2 Umsetzungsmöglichkeiten am Beispiel der Metropolregion Rhein-Neckar

Die E-Vergabeplattform der Metropolregion Rhein-Neckar bietet für die Realisierung dieser Überlegungen ideale Voraussetzungen. Seit einigen Jahren arbeiten Kommunen und Kreise der drei Bundesländer beim Thema „Öffentliches Vergabewesen" erfolgreich zusammen und tauschen sich im Arbeitskreis „Vergabe öffentlicher Aufträge" intensiv über eigene Erfahrungen auf diesem Gebiet aus. Ein großer Teil der Kommunen der Region nutzt bereits die einheitliche E-Vergabeplattform mit standardisierten Vordrucken. Der nächste Schritt wäre der Aufbau einer Shared Services-Struktur in der Metropolregion Rhein-Neckar. Die zentrale Dienstleistung besteht in der rechtssicheren und rechtskonformen Durchführung von Vergabeverfahren. Dabei geht es nur um Fragestellungen zum Vergabe- und Vertragsrecht. Die Entscheidungen zu diesen Themengebieten benötigen spezielles Know-how, das dezentral in den (insbesondere kleineren und mittleren) Kommunen nicht oder nur unwirtschaftlich bereitgestellt werden kann. Insofern ist eine Zentralisierung dieses Bereichs aus regionaler Perspektive sinnvoll. Nur so entsteht die notwendige Größe, insbesondere aus personeller Sicht, die eine ständige Arbeitsfähigkeit (Vertretungsregelungen et cetera) gewährleistet. Die Zuständigkeit für die Beschreibung des Bedarfes und der Bewertung der Angebote inklusive Vergabeentscheidung liegt bei den einzelnen Kommunen, die über das jeweilige fachliche Know-how[9] verfügen (siehe Abbildung 1).

Die sich momentan im Einsatz befindliche E-Vergabeplattform inklusive Vergabemanagementsystem in der MRN, aber auch andere Produkte bieten technologisch alle Voraussetzungen, um die beschriebenen Strukturen abzubilden. Das Vergabemanagementsystem teilt den kompletten Vergabeprozess in einzelne Arbeitsschritte auf und weist sie über das hinterlegte Berechtigungskonzept den beteiligten Sachbearbeiter/-innen zu. Es koordiniert das gemeinsame Bearbeiten eines Vergabevorgangs, indem es die einzelnen Tätigkeiten der beteiligten Personen aufeinander abstimmt, den gemeinsamen Zugriff auf die Informationen regelt sowie Mehrfach- beziehungsweise sich widersprechende Tätigkeiten vermeidet. Schließlich kontrolliert es erfüllte und unerfüllte Tätigkeiten mit Plausibilitätsprüfungen, Terminüberwachungen und so weiter. Eine automatisierte Dokumentation der einzelnen Bearbeitungsschritte, bei Bedarf auch mit automatisierten Eintrag in die Vergabeakte, stellt die Nachvollziehbarkeit und Transparenz sicher [Zi11].

[9] Falls eine Kommune nicht über das fachliche Know-how verfügt, besteht die Möglichkeit, Architekten, Ingenieure oder andere Experten einzubeziehen.

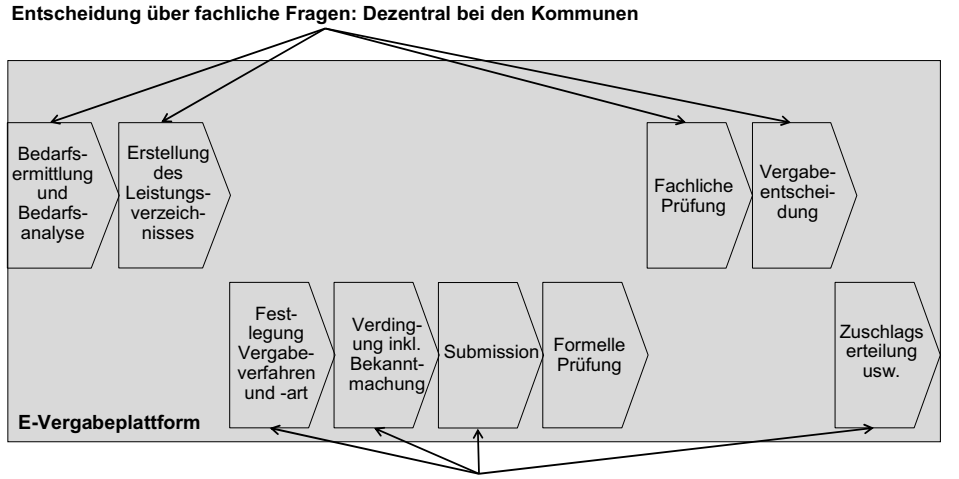

Abbildung 1: Zuständigkeiten für die einzelnen Arbeitsschritte

Neben der erhöhten Leistungsfähigkeit und Wirtschaftlichkeit liefert eine Zentralisierung auf regionaler Ebene auch einen wichtigen Beitrag zur Korruptionsverhütung und Korruptionsbekämpfung. Zum einen gewährleisten E-Vergabeplattform und Vergabemanagementsystem eine lückenlose, aktenmäßige Begründung aller Entscheidungen. Vollkommen automatisiert entsteht eine elektronische Dokumentation des Vergabeprozesses, die die Transparenz erhöht, Manipulationen erschwert und Prüfungen durch Revisionen, Rechnungsprüfungsämter und andere Prüfungseinrichtungen erleichtert [OE07]. Zum anderen sind Vorbereitung, Planung und Bedarfsbeschreibung einerseits (jeweilige Kommune) und die Durchführung des Vergabeverfahrens andererseits (Servicecenter) grundsätzlich organisatorisch getrennt. Eine Vorgabe, die die Bundesländer in den entsprechenden Vorschriften zur Korruptionsverhütung und –bekämpfung häufig machen.[10] Außerdem wird durch die zentrale Beantwortung von Rückfragen der Bieter während der Angebotsphase und deren zentrale Beantwortung über die E-Vergabeplattform eine ungleiche Behandlung der Bieter vermieden.

4 Rahmenbedingungen zur Organisation der Veränderungsprozesse

Klärungsbedarf besteht bei der organisatorischen und rechtlichen Umsetzung eines regionalen Servicecenters [Br06]. Die Vor- und Nachteile der Realisierungsmöglichkeiten als Shared Service Center oder als Shared Service Network müssen gegeneinander abgewogen werden. Einerseits wäre beispielsweise die Vorhaltung der notwendigen fachlichen Expertise in einem Shared Service Center einfacher zu realisieren. Anderer-

[10] Beispielsweise trifft die „Verwaltungsvorschrift der Landesregierung und der Ministerien zur Verhütung unrechtmäßiger und unlauterer Einwirkungen auf das Verwaltungshandeln und zur Verfolgung damit zusammenhängender Straftaten und Dienstvergehen“ in Baden-Württemberg entsprechende Regelungen.

seits bleibt trotz der Verständigung auf gemeinsame Vergabeformulare in der MRN weiterhin die Herausforderung, dass die rechtlichen Rahmenbedingungen in den drei Bundesländern unterschiedliche Entwicklungen nehmen können. Dies würde für den Aufbau eines Shared Service Networks sprechen mit mindestens einer dezentralen Stelle in jedem Bundesland. Die Rechtsgrundlage für die interkommunale Zusammenarbeit schaffen die jeweiligen Landesgesetze und die dazu erlassenen Verwaltungsvorschriften. Die Zuständigkeit von drei Bundesländern erhöht zwar die Komplexität, sie war bei der Realisierung des Vergabeportals aber kein unüberwindbares Hindernis. Die gängigsten Formen zur gemeinsamen Aufgabenwahrnehmung sind der Zweckverband und öffentlich-rechtliche Vereinbarungen, wobei auch neuere Varianten wie das „Kommunalunternehmen“ (zum Beispiel Gemeindeordnung Bayern) in die Überlegungen einzubeziehen sind. Je nach Form entstehen weitere datenschutzrechtliche, personalrechtliche, steuerrechtliche und vergaberechtliche Fragestellungen [Fr09]. Die Abwägung der einzelnen Chancen und Risiken kann nur im konkreten Fall erfolgen. Auch hier können die Erkenntnisse und Erfahrungen aus D 115-Projekten genutzt werden.

Bei zentralen Servicecenter Vergaben stellen sich darüber hinaus drei spezielle Themen. Zum einen besteht Klärungsbedarf bei Haftungsfragen. Öffentlicher Auftraggeber bleibt die jeweilige Kommune, bei der der Bedarf besteht. Sie bedient sich zur Durchführung einzelner Prozessschritte des Servicecenters. Wie wird zum Beispiel verfahren, wenn aufgrund von Fehlern des Servicecenters ein Vergabeverfahren aufgehoben wird? Zum anderen besteht die Notwendigkeit, ein Preismodell beziehungsweise ein Verfahren zur Aufteilung der Kosten für Beratungsleistungen und für die Durchführung der jeweiligen Vergabearten zu entwickeln. Schließlich ist zu klären, ob der Servicecenter noch weitere Aufgaben wahrnehmen soll. Beispielsweise könnten, das Einverständnis der beteiligten Kommunen vorausgesetzt, Leistungsbeschreibungen beziehungsweise -verzeichnisse ausgetauscht werden.

Literaturverzeichnis

[BD10] Brockmann, C; Dallinger, S.: E-Government bringt eine Region zusammen. In (Alcatel-Lucent Stiftung für Kommunikationsforschung et al. Hrsg.): Praxis des E-Government in Baden-Württemberg. Richard Boorberg Verlag, Stuttgart, 2010; S. 83-97.

[BDI10] Bundesverband der Deutschen Industrie e.V. (Hrsg.): Nationale Vergaberechtsreform. BDI-Drucksache 442. Berlin, 2010.

[BI10] Bundesministerium des Innern (Hrsg.): Abschlussbericht E-Government 2.0. Berlin, 2010.

[BNK09] Becker, J.; Niehaves, B.; Krause, A.: Shared Service Center vs. Shared Service Network. In (Wimmer, M. A. et al. Hrsg.): EGOV 2009. Springer-Verlag, Berlin und Heidelberg, 2009; S. 115–126.

[Bo11] Booz & Company (Hrsg.): Zum Entwicklungsstand des öffentlichen Einkaufs, Eine empirische Analyse in 16 Entwicklungsfeldern. Düsseldorf, 2011.

[Br06] Brüggemeier, M. et al.: Organisatorische Gestaltungspotenziale durch Electronic Government. ed. sigma, Berlin, 2006.

[BWT07] Bundesministerium für Wirtschaft und Technologie (Hrsg.): Öffentliches Beschaffungswesen, Wissenschaftlicher Beirat beim Bundesministerium für Wirtschaft und Technologie, Gutachten Nr. 2/07. Berlin, 2007.

[Ca08] Castelnovo, W.: E-Government for small local government organizations. In: (Mazzeo, A.; Bellini, R.; Motta, G. Hrsg.): E-Government; ICT Professionalism. Springer, Boston, 2008; S. 1-10.

[Da11] Daum, R.: Beschaffung zwischen Betriebswirtschaft und Recht. In: Innovative Verwaltung, 2011, Heft 9; S. 18-20.

[EC10] European Commission (Hrsg.): Evaluation of the 2004 action plan for electronic public procurement. Brüssel, 2010, http://ec.europa.eu/internal_market/consultations/docs/2010/e-procurement/evaluation-report_en.pdf (Abruf: 26.09.2011).

[Fr09] Franzius, C.: Flexible Organisationsmodell: Netzwerke, Organisationshoheit, Shard Services, Verwaltungsverbünde, Mischverwaltung. In (Hill, H.; Schliesky, U. Hrsg.): Herausforderung e-Government. Nomos-Verlag, Baden-Baden, 2009; S. 39-52.

[GS02] Gehrmann, F.; Schinzer, H.: Public E-Procurement – Potenziale und Rahmenbedingungen der netzbasierten Beschaffung für öffentliche Auftraggeber. In (Gehrmann, F.; Schinzer, H.; Tacke, A. Hrsg.): Public E-Procurement. Vahlen, München, 2002; S. 13-24.

[He05] Heinze, F.: Die elektronische Vergabe öffentlicher Aufträge. Peter Lang Verlag, Frankfurt am Main, 2006.

[HK03] Hummel, S.; Krcmar, H.: Blended Learning für E-Government. In (Baacke, E., Schröter, W. Hrsg.): Lernwege zum Electronic Government. Talheimer Verlag, Mössingen, 2003; 41-54.

[Kl02] Kleindiek, R.: BundOnline 2005 – Electronic Government Strategie des Bundes. In (Reinermann, H.; Lucke, J. v. Hrsg.): Electronic Government in Deutschland. Speyerer Forschungsberichte 226, Speyer, 2002; S. 118-129.

[La10] Laux, D.: Wirksamkeit der Nutzung, von E-Vergabe im Beschaffungsmanagement der öffentlichen Verwaltung. kassel university press, 2010.

[Lu10] Lucke, J. v.: Bürger und Unternehmen wollen elektronisch mit der Verwaltung kommunizieren. In (Alcatel-Lucent Stiftung für Kommunikationsforschung et al. Hrsg.): Praxis des E-Government in Baden-Württemberg. Richard Boorberg Verlag, Stuttgart, 2010; S. 455-461.

[Me09] Meier, A.: eDemocracy & eGovernment. Springer-Verlag, Berlin und Heidelberg, 2009.

[OE07] Organisation for economic co-operation an development (Hrsg.): Integrity in Public Procurement. OECD Publishing, Paris, 2007.

[RIL08] Rambøll Management; Institut für Mittelstandsforschung Bonn; Leinemann & Partner Rechtsanwälte (Hrsg.): Kostenmessung der Prozesse öffentlicher Liefer-, Dienstleistungs- und Bauaufträge aus Sicht der Wirtschaft und der öffentlichen Auftraggeber – Endbericht. 2008. Online: http://bmwi.de/BMWi/Navigation/Service/publikationen, did=254980.html Zugriff: 26.09.2011.

[Ru09] Ruff, A.: Public Electronic Procurement: Elektronische Vergabe und Beschaffung von Lieferungen und Leistungen der Kommunal-Verwaltung über Internet. GUC-Verlag, Lößnitz, 2009.

[Sa11] Sandberg, B.: Vergabefremde Ziele in der öffentlichen Beschaffung. In: Verwaltung & Management, 17. Jg., 2011, Heft 2; S. 59-66.

[Sc07] Schmitt, W. J.: Finanznot und e-Government – Nur Zusammenarbeit macht e-Government möglich. In (Bieler, F.; Schwarting, G. Hrsg.): e-Government / Perspektiven - Probleme – Lösungsansätze. Schmidt-Verlag, Berlin, 2007; S. 173-199.

[SBA09] Statistisches Bundesamt (Hrsg.): Informationsgesellschaft in Deutschland – Ausgabe 2009. Wiesbaden, 2009.

[Tr99] Traunmüller, R.: Annäherung an die Verwaltung aus Sicht der Informationstechnik: Technikpotentiale und Systemlösungen. In (Lenk, K.; Traunmüller, R. Hrsg.): Öffentliche Verwaltung und Informationstechnik. R. v. Decker´s Verlag, Heidelberg, 1999; S. 21-51.

[TS05] Thome, R.; Schinzer, H.: Konsultative Assistenzsysteme für E-Government. In: Wirtschaftsinformatik, 47. Jg., 2005, Heft 5; S. 326-336.
[WLS08] Wirtz, B. W.; Lütje, S.; Schierz, P.: Electronic Procurement in der öffentlichen Verwaltung. Speyerer Forschungsberichte 257, Speyer, 2008.
[WS10] Wietersheim, M. v.; Schranner, U.: Das neue Vergaberecht. Haufe-Verlag, Freiburg, 2010.
[Zi11] Zielke, D.: Doppelter Vorteil – Auswirkungen der E-Vergabe für Wirtschaft und Verwaltung. In: Kommune 21, 2011, Heft 7; S. 32 f.

Development of a European Framework for e-Government Competences

Sirko Schulz, Tino Schuppan

IfG.CC – The Potsdam eGovernment Competence Center
c/o University of Potsdam, Universitätskomplex III Babelsberg
August-Bebel-Straße 89, 14467 Potsdam, Germany
sschulz@ifg.cc / schuppan@ifg.cc

Abstract: The term e-government stands for an ICT enabled transformation of the public sector. New forms of collaboration and inter-organizational public service networks become feasible, to fulfill public tasks more efficiently and effectively. Even though e-government is being promoted by the EU, tangible results are rather scarce. The European Commission and the EU member countries therefore strive for a more coherent development of e-government within the EU. Nevertheless, it's being implemented very differently in the EU member countries. One reason for this diverse development seems to be that different competences for the personnel of public administrations are associated with e-government in the EU member countries. This article describes the first steps of the development of an e-government competence framework. This framework is initially being developed in the COMPATeGov project with public administrations from Bulgaria, Germany, Greece, and Romania. The article sums up the first results of a literature review on e-government competences, a survey, and focus group workshops. It outlines a first set of e-government competences and concludes with a forecast of the next steps in the project, in order to validate and facilitate the results.

1 Introduction and Problem Statement

E-government can be understood as an ICT-enabled transformation of the public sector to achieve better government (type-3, -4 definition of the [OECD03]). In this respect, it is more than just online government, which reduces e-government to the online delivery of public services (type-1 definition of the [OECD03]). Instead, this broader transformational perspective takes into account, that the public sector as a whole can be reorganized by making use of information and communication technologies (ICT). Hence, ICT has the potential to rethink which and how public services are being produced and which actors are being involved in the process. The consequential networking and cooperation are expected to have a transformative impact, albeit the term transformation is being used manifoldly in the e-government context (e.g. [Zu05]; [BH09]). O'Neill [O'N09] defines systemic transformation as a second tier of transformation: Accordingly, the application of ICT goes beyond the mere instrumental use of ICT (first tier) to

change organizational processes and practices; moreover it alters the relationships and behavior of the actors involved and thereby changes the model of public management itself (second tier) [O'N09]. This perspective enables for instance the separation of public services into parts which are conducted in the front office, where public services are delivered, and the back office, where they are produced. Thus ICT facilitates new organizational models, like e.g. shared service centers, which provide a large number of agencies with a standardized service, mostly a support process in the back office [Be03]. Another example are one stop agencies, which bundle a number of different services from a variety of agencies and offer them at one location ("front office") – online or offline [Le02]. With slightly different connotations, these transcending models are underlying the "joined-up" [Bo05] and "whole-of-government" [CL07]-approaches. These approaches address policy-making and -implementing issues across organizational boundaries to mitigate the effects of a fragmented public sector. E-government is a major enabler of these new forms of networked government [CBB05].

Promoting e-government has been a major effort in the European Union [MM09]. Considerable effort has especially been undertaken to measure the implementation of e-government. Different, more or less sophisticated maturity models have been used to display the status of e-government within the European Union (e.g. the limited model in [EC09]; for an overview see [Gr10]; [GM07]). Thus depending on the specific measures, the overall results are rather scarce and very diverse in the different EU countries. Therefore, the European Commission has undertaken various initiatives (e.g. EU Services Directive) to promote e-government. The results remain selective, what can be considered problematic in a Union aiming at a single internal market (see the Digital Single Market in [EC10].

Besides the different legal frameworks, cultural aspects and administrative traditions among the EU member countries [PB04], an obstacle constraining the implementation of a more coherent European e-government seems to be the heterogeneous approaches to e-government in the member countries (critical of a uniform reform approach is [Le06]). One aspect of the context of e-government reforms are the skills which are required of the public administration's personnel [He05]. As a consequence, it can be considered a barrier for a more coherent European e-government that there is no consistent understanding of the skills and competences associated with e-government. Often there is not even an established understanding of e-government competences at all [Sc10].

Because of the increasing importance of lifelong learning, the competency approach is enjoying larger recognition worldwide, as it focuses on the results of learning processes [Gn07]; [KSB07]. In Europe in particular, the competency concept has become important in establishing comparability between educational degrees issued in different countries [WDS06]. When applied in professional life, the competency approach takes into account what a person is able to do in a working context, regardless of how this competency has been acquired. Instead of paying attention exclusively to formal qualifications and degrees, which differ throughout Europe, skills, techniques, expertise, and know-how are becoming more important [EI05]; [WDS06]. While the qualification

concept is input-oriented, the competency concept is output-oriented, i.e., regardless of formal degrees.

However, despite increasing interest in the competency approach, it is a rather "fuzzy concept" [BK06]. In particular the terms competency and competence are often used inconsistently (see [Ho99]; [Ro95]. While the term "competence" can be defined as the ability to fulfill a task to certain, often specifically defined standard, in comparison competency designates the underlying attributes of a person, such as knowledge, skills, and abilities needed to fulfill competence standards [Ho99]. Regarding the focus of this research – the standardization of specifically defined competences – we therefore use the term competences when talking about concrete abilities; in contrast we use the term competency for the knowledge, skills, and competences required of a person [Sc10].

To date, in practice, the topic of e-government competences is – if at all – still being addressed in a very IT-dominated fashion. The same is true for the scientific community in public management and in administrative sciences [Gr10], which often very unilaterally still perceives e-government as an IT subject [EEE04]; [Ka04]; [MKM01]. Nevertheless, in practical projects and in the everyday work of public administration, it is becoming increasingly apparent that new competences are required which go beyond the simple use of an IT application, or even IT specialist and tool knowledge [OECD03]. A comprehensive change of competence requirements for all civil servant groups can be expected—and is already becoming apparent.

To address this problem the research questions at the core of this article ask which competences are considered e-government competences in different European countries? What differences actually exist between these countries? Which competences are specifically important from a transformational perspective on e-government?

To answer these questions, the article will be structured as follows: at the beginning, the methods employed will be briefly laid out. Second, the results of a survey and workshops with e-government experts will be presented in order to determine new competences. These results will then be analyzed and the necessary skills and competences structured in what can be considered a first draft of an e-government competence model. Furthermore, exemplary use-cases for an e-government competence model will be outlined. To conclude, an outlook will be given on how the results will be validated and specified in more detail.

2 Methods

Until now, e-government competences have hardly been discussed in the academic debate. Only a few academic articles addressing e-government-related competences or skills exist (e.g. [Le06], [Se05], [Sc10]), and even these often lack the focus of this article. Other contributions elaborate on organisational capabilities [PBP11], don't explicitly address e-government, but rather ICT in general [Ro03], or mention specific competences without yet integrating these into a holistic approach to e-government competences [He03]. Besides the shortcomings of the academic research, the question

of changing and newly arising competences in the context of e-government faces some significant challenges from practice:

- There is no agreed and established job profile for "e-government public personnel", on which to draw upon.
- The understanding of e-government in practice is at best mixed and rather incomplete.
- Given the dynamics in the field of e-government and the time lag to adjust competence level, it is necessary to reflect upon future competence requirements.

Therefore, the methodology of this article employs a multi-staged methodology: Competences have been derived from a literature analysis of the scarce previous research as well as newly arising e-government structures and processes. Based on this analysis, an initial set of e-government skills and competences has been derived, which served as the basis for an online survey. This survey has been conducted among e-government experts in Bulgaria, Germany, Greece, and Romania. These countries have been chosen, since they represent a sample of diverse administrative traditions and score differently in e-government benchmarking studies [EC09]. Hence, the country selection covers only four out of the 27 EU member countries, one of which is a Mediterranean, one is a central European and two are Eastern European countries. Major administrative cultures and traditions, like e.g. Scandinavian countries, are thus not included. This can be vindicated by the fact that the project is an initial attempt to develop a European competence framework.

The questionnaire used in the survey asked for the relevance of a skill or competence, the competence level necessary in the public sector, and the current competence level in general. The participants were asked to rate the importance of a specific skill on a four-tier scale, zero meaning a skill would not be important and three, a skill would be very important. The assessment had to be made for three different roles of public personnel: staff, mid-level management and senior management. The survey asked specifically for the competences necessary in e-government projects in order to gain an understanding of those competences required to make use of the transformative potential of e-government. Furthermore, statistical personal data was obtained from the participants at the end of the survey. Along with the questionnaire came a glossary that provided a short definition of the item in question. In total, 83 participants completed the questionnaire. The survey results have been validated and specified in more detail in workshops in the different project countries with e-government experts. The participants totalled to 62 experts who were either themselves public personnel, consultants, or scholars from the field of e-government. The results from the survey and the workshops have been consolidated and systematised. They will receive further specification and validation in upcoming workshops and online discussions as part of a project on e-government competences, the COMPATeGov project, which is funded by the European Commission. Together with academic institutions and public administrations in Bulgaria, Germany, Greece, and Romania this project develops a European e-government competence model. A competence model is not a "one size fits all"-approach that tries to force a uniform frame upon public administration across countries with different state structures, admin-

istrative cultures and traditions etc. Rather, it can be considered a construction kit that encompasses the relevant competence categories from which to pick and adapt the specific competence and its required level. The competence model will be used to develop an assessment tool for e-government competences, set up an online repository with relevant training materials adapted to one's individual training needs, and adapt corresponding vocational education and training (VET) offers.

3 Results

3.1 Skills and Competences for the staff level

The Skills considered the most important for e-government project staff across all researched countries are IT Literacy, Information Processing, IT Specialist, Process Management, and Organisational Design Skills (Table 1). The single-country results are – except for Romania – very similar, showing that there seems to be a pretty homogeneous understanding of e-government skills for project staff.

Skills for Project Staff	Bulgaria	Germany	Greece	Romania	Total
IT Literacy Skills	2,37	2,41	2,56	2,67	2,50
Information Processing Skills	1,95	1,59	2,12	2,64	2,07
IT Specialist Skills	1,83	1,88	2,04	2,41	2,04
Process Management Skills	1,63	2,12	1,80	2,05	1,90
Organisational Design Skills	1,58	2,12	1,56	1,86	1,78
Project Management Skills	1,47	2,00	1,36	2,05	1,72
Quality Management Skills	1,44	1,38	1,64	2,32	1,69
Change Management Skills	1,58	1,53	1,52	1,73	1,59
Management Accounting Skills	1,32	1,00	1,36	2,36	1,51
Juridic Skills	1,32	1,00	1,29	2,14	1,44
Risk Management Skills	1,26	1,06	1,32	2,09	1,43
IT Strategy Skills	1,32	1,24	1,08	1,45	1,27
Contract Management Skills	1,17	0,94	1,00	1,95	1,27
Marketing Skills	1,06	0,94	0,88	1,67	1,14
Media Skills	1,11	1,06	0,72	1,45	1,09
Policy Process Skills	1,00	0,88	1,24	0,62	0,94

Table 1: Relevant Skills for Project Staff

The personal and social competences assessed as very important for the staff involved in e-government projects were cooperation competence, communicative competence and self-control.

3.2 Skills and Competences for the project management

The Skills considered the most important for mid-level managers involved in e-government projects across all researched countries are Project Management, Process Management, Organisational Design, Risk Management, and IT Strategy Skills (Table 2). Again, there is not much of a difference between the single-country results, with at least four out of the five general top skills for project managers being identical in each country. Thus, there is a significantly homogeneous understanding of e-government skills for project managers.

Skills for Project Managers	Bulgaria	Germany	Greece	Romania	Total
Project Management Skills	2,84	2,81	2,76	3,00	2,85
Process Management Skills	2,68	2,63	2,60	2,90	2,70
Risk Management Skills	2,68	1,94	2,72	2,86	2,55
Organisational Design Skills	2,42	2,53	2,56	2,82	2,58
IT Strategy Skills	2,68	2,29	2,44	2,76	2,55
Information Processing Skills	2,56	1,88	2,56	2,73	2,43
Quality Management Skills	2,41	2,00	2,16	2,68	2,31
Contract Management Skills	2,53	1,73	2,08	2,68	2,26
Change Management Skills	2,47	2,06	2,44	2,64	2,40
IT Literacy Skills	2,53	2,06	2,92	2,52	2,51
Marketing Skills	1,95	1,44	1,64	2,45	1,87
Media Skills	2,12	1,76	1,80	2,32	2,00
Juridic Skills	1,95	1,65	2,12	2,24	1,99
IT Specialist Skills	1,78	1,38	2,36	2,05	1,89
Management Accounting Skills	2,11	1,71	2,12	2,05	1,99
Policy Process Skills	2,11	1,81	2,28	1,59	1,95

Table 2: Relevant Skills for Project Managers

Even though some of the most important skills for project managers mirror the skills considered relevant for staff, there are significant differences, e.g. the top three skills being completely different. Furthermore, even if the skill's title is identical, the associated skill levels and tasks for the different roles are not.

The personal and social competences assessed as very important for the mid-level managers involved in e-government projects were communicative competence, time-management and cooperation competence as well as leadership.

3.3 Skills and Competences for the senior management

The skills considered the most important for e-government senior managers across all project countries are IT Strategy, Organisational Design, Project Management, Risk Management, and Change Management Skills (Table 3). There is slightly more variance among the single countries, but the results nevertheless show solid consistency. At least three out of the five general top skills for project managers are mirrored in each country. Thus, there is a relative homogeneous understanding of e-government skills for senior managers.

There is a significant similarity between the most important skills for project managers and the skills considered relevant for senior managers; four out of the top five skills are identical. It was explained that the project managers are often recruited from the organisation's management ranks. In the public sector, different from the private sector, there basically is no separate caste of project managers. The project managers in the public sector often keep their responsibilities and tasks in the hierarchical structure and/or go back to their regular occupation, after the project is finished.

Skills for Senior Managers	Bulgaria	Germany	Greece	Romania	Total
IT Strategy Skills	2,63	2,12	2,96	2,79	2,62
Organisational Design Skills	2,47	2,24	2,92	2,76	2,60
Project Management Skills	2,68	1,82	2,76	2,90	2,54
Risk Management Skills	2,58	1,75	2,92	2,76	2,50
Change Management Skills	2,63	1,94	2,58	2,71	2,47
Contract Management Skills	2,29	1,71	2,92	2,81	2,43
Process Management Skills	2,63	1,75	2,48	2,85	2,43
Quality Management Skills	2,47	1,80	2,44	2,62	2,33
Information Processing Skills	2,44	1,59	2,44	2,57	2,26
Media Skills	2,12	1,71	2,68	2,48	2,24
Policy Process Skills	2,26	2,00	2,75	1,85	2,22
IT Literacy Skills	2,53	0,94	2,88	2,35	2,17
Juridic Skills	2,05	1,71	2,68	2,25	2,17
Marketing Skills	2,28	1,44	2,20	2,62	2,13
Management Accounting Skills	2,21	1,65	2,16	1,95	1,99
IT Specialist Skills	1,58	0,53	2,04	1,95	1,53

Table 3: Relevant Skills for Senior Managers

The social and personal competences estimated to be the most important for senior managers responsible for e-government were communicative and cooperation competence as well as leadership.

4 Analysis

The results have shown that apart from IT-related competences a large variety of different skills and competences are estimated to be important in the context of e-government (i.e., mixed competences). Thus it becomes apparent that particularly public managers involved with e-government also need knowledge about the possible applications and opportunities of IT architecture and operational process knowledge, so as to understand coming changes and make strategic decisions. The governance-related leadership literature especially neglects this aspect, either ignoring it or assuming, more or less explicitly, that operational knowledge is not necessary for strategic skills.

The results confirm that the working level is in particular affected in a way which goes beyond knowledge of IT applications. Staff at this level needs a new understanding of work processes and self-organisation skills. Project leaders face special challenges, because they must possess very profound interdisciplinary expert technical knowledge and increased social competences. Executives also require specialist knowledge - sometimes in great detail - to be able to push through projects and to ensure the necessary broader political support.

Looking toward future developments, it can be assumed that the relevance of isolated competences in IT application will decrease, in part because human-machine interactions will continue to improve. It can be expected that technical expertise will gain importance, because IT will become an integral, self-evident element of work in public administration. Already, every branch of public administration – security, law enforcement, social services and others – utilises IT. It is becoming clear that the changes in competence requirements at issue have much less to do with digitisation and much more to do with new procedures and processes of public administration. This also applies to executives. To date, however, there is a lack of consistent management and control concepts which address digital and spatially distributed work forms and the related competences.

Analysing the obtained results particularly from the workshops in detail, newly arising skills and competences can be distinguished from other skills and competences, which have been prevalent in the public sector and "merely" need to be applied to e-government. We thereby differentiate between these latter, which we term generic government skills and competences on the one hand and newly arising core e-government skills and competences on the other hand (Figure 1).

The so-called generic government skills and competences contain personal competences (creativity, self-control and -motivation, and self-management) and social competences (leadership, cooperation and communication). These competences gain higher relevance in this more networked and partly less hierarchical e-government working environment which requires more cooperation across organisational borders. They furthermore encompass policy and legal skills (policy process, administrative law and cultures, specialised law) and change-related skills (project and change management skills and implementation competence). These latter categories are also more or less generic competences that are required in the public administration, but which are necessary in order to implement the transformational changes.

Among the so-called core e-government skills and competences which can be grouped together, the e-government management skills and competences (risk management, quality management, performance management, and contract management), e-government design competences (organisational design, process design, IS design, IT specialist, and marketing skills), eCompetences (IT literacy, information processing, and media skills), and ePolicy competences (eStrategies and ePolicies, models and concepts, and information processing law) can be distinguished. These comprise rather new competences that arise in the context of e-government.

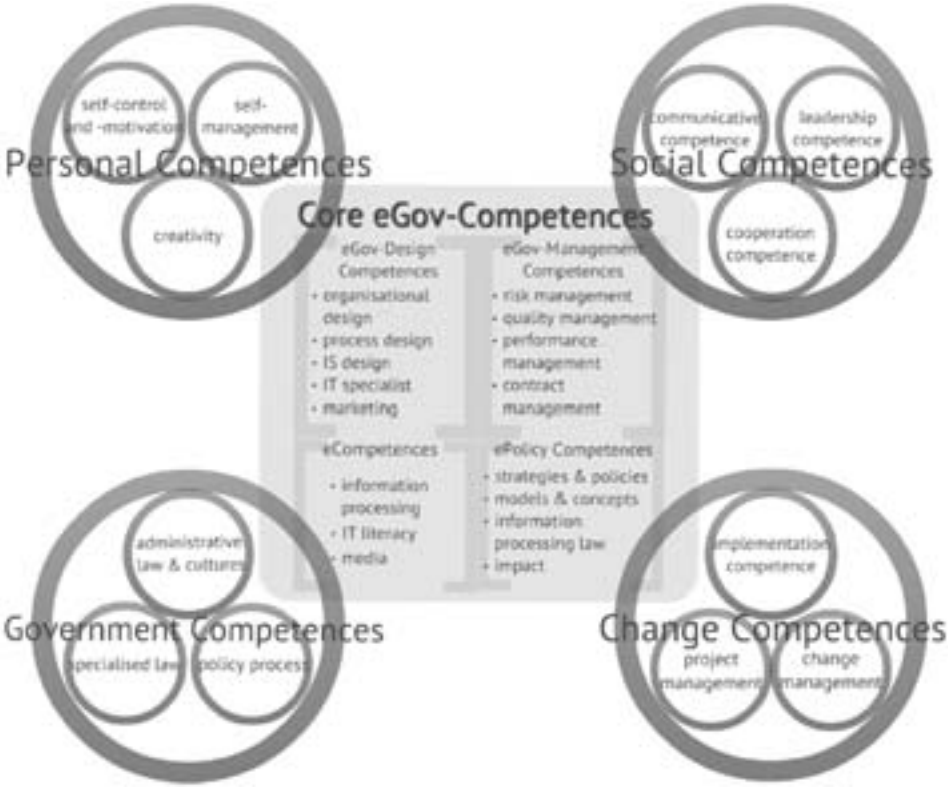

Figure 1: E-Government Competence Structure

In order to use a competence framework for competence development, a distinction between generic and core e-government competences is especially useful to analyse the competence gap which is presumably larger among the newly arising skills and competences. Such a systematisation of the necessary skills and competences can serve as the basis for practice and academia to design training programs and for work force planning efforts. "E-government work force planning efforts […] offer organizations the opportunity to assess their current work force capabilities, determine future work force requirements in the context of e-government[.], and implement strategies to eliminate gaps, both current and future, between work force capabilities and work force requirements."[Ar02] Considering the challenges the public sector faces in the upcoming years, with e.g. a large part of the public work force retiring and its scarce financial resources these efforts are especially necessary.

5 Summary and Outlook

Drawing on the literature, an initial set of e-government skills and competences has been assembled. These have been evaluated, complemented and specified in a survey and workshops in Bulgaria, Germany, Greece, and Romania. Comparing all these results for the different skills and competences assigned to the different roles in e-government transformation it is striking to see that even though e-government is developed quite differently in the four project countries, the necessary skills and competences are rather similar across all countries. Thus it can be stated that a shared understanding of e-government competences does exist. These e-government competences encompass a large variety of different skills and competences (i.e., mixed competences) which go far beyond a limited set of IT-related competences. Going back to the initial hypothesis, that different skills and competences are one factor contributing to different outcomes in how successful e-government has been implemented in a country, it becomes apparent, that at this stage of the research, the hypothesis does not stand. However, further research is necessary to analyse, whether the actual differences in competence levels can account for the how far a country has come in implementing e-government.

During the next stages of the project, these e-government skills and competences will be refined and the different competence levels which are necessary will be described in more detail. Further refinement and validation will be based on the first draft of the competence model. Therefore workshops with training centres and the liable authorities at the different levels of government will be conducted and online discussions will be held with e-government experts from academia and practice. Based on these further discussions, a curriculum will be developed and pilot sessions will be conducted. Parallel activities aim at disseminating the competence model to ensure its use by public administrations within the European Union.

References

[Ar02] Armstrong, A.: E-government Work Force Planning: A Pilot Study. In: The Journal of Government Financial Management 51; pp. 32-35.

[Be03] Bergeron, B.: Essentials of shared services. John Wiley & Sons, New York, 2003.

[BH09] Bloomfield, B.P.; Hayes, N.: Power and Organizational Transformation through Technology: Hybrids of Electronic Government. Organization Studies 30; pp. 461-487.

[Bo05] Bogdanor, V. (Ed.): Joined-Up Government. Oxford University Press, Oxford, 2005.

[BK02] Boon, J.; van der Klink, M.: Competencies: The triumph of a fuzzy concept. In: Academy of Human Resource Development Annual Conference. Proceedings Vol. 1; pp. 327-334.

[CBB05] Centeno C.; van Bavel, R.; Burgelman J.C.: A Prospective View of e-Government in the European Union. In: The Electronic Journal of e-Government 3; pp. 59-66.

[CL07] Christensen, T.; Laegreid, P.: The Whole-of-Government Approach to Public Sector Reform. In: Public Administration Review 67; pp. 1059-1066.

[EEE04] Elovaara, P.; Eriksén, S.; Ekelin, A.; Hansson, C.; Nilsson, M.; Winter, J.: Educational Programs in e-Government. In (Traunmüller, R. Ed.): Electronic Government. Third International Conference, EGOV 2004. LNCS 3183. Springer, Berlin, 2004; pp. 457-459.

[EC09] European Commission (ed.): Smarter, Faster, Better Government. 8th Benchmark Measurement.

[EC10] European Commission: A Digital Agenda for Europe. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. COM(2010) 245 final/2.

[EI05] European Institute for Public Administration: Organisational Changes, Skills and the Role of Leadership required by eGovernment, Luxembourg, 2005.

[GM07] Gil-Garcia, J.R.; Martinez-Moyano, I.J.: Understanding the evolution of e-government: The influence of systems of rules on public sector dynamics. In: Government Information Quarterly 24; pp. 266-290.

[Gn07] Gnahs, D.: Kompetenzen - Erwerb, Erfassung, Instrumente. W. Bertelsmann Verlag, Bielefeld, 2007.

[Gr10] Grönlund, A.: Ten Years of E-Government. The 'End of History' and New Beginning. In (Wimmer, M.A.; Chappelet, J-L.; Janssen, M.; Scholl, H.J. Eds.): Electronic Government. 9th International Conference, EGOV 2010. LNCS 6228; pp. 13-24.

[He03] Heeks, R.: Most e-Government-for-Development Projects Fail How Can Risks be Reduced? Paper 14, i-Government Working Paper Series, Institute for Development Policy and Management, University of Manchester, UK.

[He05] Heeks, R.: e-Government as a Carrier of Context. In: Journal of Public Policy 25; pp. 51-74.

[Ho99] Hoffmann, T.: The Meanings of Competency. In: Journal of European Industrial Training 23; pp. 275–285.

[Ka04] Kaiser, S.: Qualification Requirements in e-Government: The Need for Information Systems in Public Administration Education. In (Traunmüller, R. Ed): Electronic Government. Third International Conference, EGOV 2004. LNCS 3183. Springer, Berlin, 2004; pp. 464-467 .

[KSB07] van der Klink, M.; Schlusmans, K.; Boon, J.: Designing and Implementing Views on Competencies. In (Sicilia, M.-A. Ed.): Competencies in Organizational E-Learning: Concepts and Tools. IGI Global, Hershey/PA, 2007;pp. 221-233.

[Le06] Leitner, C.: eGovernment: People and Skills in Europe's Administration. In: Proceedings of the 39th Hawaii International Conference on System Sciences. Hawaii: IEEE; pp. 77-86.

[Le02] Lenk, K.: Electronic Service Delivery - A Driver of Public Sector Modernization. In: Information Polity 7; pp. 87-96.

[Le06] Lenk, K.: E-Government in Europe: Uniform solutions for all countries? In: Information Polity 11; pp. 189-196.

[MM09] Malmö Ministerial Declaration on eGovernment: Fifth Ministerial eGovernment Conference. Malmö, Sweden. http://www.egov2009.se/wp-content/uploads/Ministerial-Declaration-on-eGovernment.pdf accessed 28 September 2011.

[MKM01] Mundy, D.; Kanjo, C.; Mtema, P.: Meeting training needs for information age reform: shortcomings of current training provision. In (Heeks, R. Ed.): Reinventing Government in the Information Age: International practice in IT-enabled public sector reform. Routledge, London, 2001; pp. 271-292.

[OECD03] OECD: The E-Government Imperative. OECD e-Government Studies. OECD Publications, Paris, 2003.

[O'N09] O'Neill, R.: E-Government: Transformation of Public Governance in New Zealand? Victoria University of Wellington, Wellington, 2009.

[PBP09] Plattfaut, R.; Niehaves, B.; Pöppelbuß, J.; Becker, J.: Development of BPM Capabilities – Is Maturity the Right Path? In: Proceedings of the 19th European Conference on Information Systems (ECIS). Helsinki/Finland, 2011, Paper 27.

[PB04] Pollitt, C.; Bouckaert, G.: Public Management Reform. A Comparative Analysis, 2nd ed. Oxford University Press, New York, 2004.

[Ro95] Rowe, C.: Clarifying the use of competence and competency models in recruitment, assessment and staff development. In: Industrial and Commercial Training 27; pp. 12-17.

[Ro03] Ross, J.: Creating a Strategic IT Architecture Competency: Learning in Stages, CISR Working Paper No. 335, Center for Information Systems Research, Sloan School of Management Working Paper No. 4314-03.

[Sc10] Schuppan, T.: E-Government Competencies. Looking Beyond Technology. In (Shea, C.M.; Garson, G.D. Eds.): Handbook of Public Information Systems, 3rd ed. Taylor & Francis, Boca Raton, 2010; pp. 353-370.

[Se05] Settles, A.: What Skills are Needed in an E-World. E-Government Skills and Training Programs for the Public Sector. In (Khosrow-Pour, M. Ed.): Practicing E-Government: A Global Perspective. Idea Group Publishing, Hershey/PA, 2005; pp. 383-414.

[WDS06] Winterton, J.; Delamare-Le Deist, F.; Stringfellow, E.: Typology of knowledge, skills and competences: clarification of the concept and prototype. Office for Official Publications of the European Communities, Luxembourg, 2006.

[Zu05] Zuurmond, A.: Organisational Transformation Through the Internet. In: Journal of Public Policy 25; pp. 133-148.

Prozessmanagement

Prozessorientierte Verwaltung – Status quo und Forschungslücken

Jörg Becker[1], Sara Hofmann[1], Marlen Jurisch[2], Ralf Knackstedt[1], Helmut Krcmar[2], Michael Räckers[1], Irina Thome[1], Petra Wolf[2]

[1]Westfälische Wilhelms-Universität Münster
European Research Center for
Information Systems
Leonardo-Campus 3, 48149 Münster
{vorname.nachname}@ercis.uni-muenster.de

[2]Technische Universität München
Lehrstuhl für Wirtschaftsinformatik
Boltzmannstr. 3, 85748 Garching bei München
{marlen.jurisch|petra.wolf|krcmar}@in.tum.de

Abstract: Geschäftsprozesse rücken zunehmend ins Zentrum der Modernisierungsbemühungen in öffentlichen Verwaltungen. An vielen Standorten und in verschiedenen Wissenschaftsdisziplinen wird an dem Thema der prozessorientierten Verwaltung geforscht. Das Ziel der diesem Beitrag zugrunde liegenden Studie ist es, den Status quo der Forschung aufzuzeigen sowie Forschungslücken und Synergiepotenziale zu identifizieren. Die Auswertung von 155 Forschungsergebnissen aus den letzten zehn Jahren führt zu insgesamt 14 konkreten Handlungsempfehlungen, sowohl die Forschung selbst als auch die Art, wie Forschungsprojekte durchgeführt werden, betreffend. Als Instrument zur Datenanalyse wurde die Forschungslandkarte „Prozessorientierte Verwaltung" eingesetzt, eine browserbasierte Software, in der die Forschungsergebnisse zur prozessorientierten Verwaltung strukturiert gespeichert werden. Auf einer interaktiven Landkarte wird angezeigt, an welchen Standorten zu welchen Themen geforscht und entwickelt wird.

1 Einleitung

Geschäftsprozesse in öffentlichen Verwaltungen und zwischen Wirtschaft und Verwaltung sind Gegenstand vielfältiger Forschungsprojekte in den vergangenen Jahren (vgl. [Be10][WJK10]). Die verstärkte Orientierung in den deutschen Verwaltungen hin zu einer ablauforganisatorischen Betrachtung und damit einhergehend eine – zumindest teilweise – Abkehr von den Prinzipen des Verwaltungshandelns von Max Weber [We22] lässt sich im Wesentlichen an verwaltungsintern begründbaren Defiziten festmachen, deren Adressierung durch eine Betrachtung der Geschäftsprozesse möglich

scheint [BAF09]. Diese Bestrebungen lassen sich unter dem Begriff der Prozessorientierung subsumieren.

Das Thema der prozessorientierten Verwaltung birgt Forschungsfragen für viele unterschiedliche Wissenschaftsdisziplinen [Ha07]. Die einzelnen Disziplinen zeichnen sich durch eigene Terminologien, Projekt- und Publikationskulturen aus. Dies bedeutet, dass jede Disziplin ihre Forschungsergebnisse in eigenen Fachzeitschriften publiziert und auf speziellen Tagungen präsentiert, die von den anderen Disziplinen nur teilweise beziehungsweise gar nicht zur Kenntnis genommen werden [He10]. Dieser Umstand erschwert es, einen Überblick über die Forschungsergebnisse zur prozessorientierten Verwaltung zu erlangen. Drei Zielgruppen der Forschungsergebnisse können hier unterschieden werden:

1. *Verwaltungs- und Unternehmenspraxis*: Für die Mitarbeiter in Unternehmen und Verwaltungen ist es so gut wie unmöglich, alle für sie relevanten Forschungsergebnisse zu identifizieren. Problemlösungen, die gegebenenfalls schon entwickelt wurden, kommen so nicht zu einem flächendeckenden und schnellen Einsatz.
2. *Wissenschaft*: Auch in der Wissenschaft besteht die Gefahr, dass aufgrund der getrennten Begriffswelten und Publikationskulturen bereits erzielte Arbeitsergebnisse unbekannt bleiben. Die mehrfache Entwicklung ähnlicher Problemlösungsansätze und die Durchführung redundanter empirischer Untersuchungen sind die Folge. Synergiepotenziale von Arbeitsgruppen unterschiedlicher Disziplinen bleiben ungenutzt, interdisziplinäre Ansätze werden erschwert.
3. *Forschungsförderung*: Der Mangel an einem disziplinenübergreifenden Überblick über Ergebnisse der prozessorientierten Verwaltung erschwert es, bestehende Lücken in der Forschungsagenda und im Vergleich dazu übermäßig bearbeitete Schwerpunkte der Forschung gezielt zu identifizieren.

Um einen Überblick sowie eine disziplinenübergreifende Orientierungshilfe für die Forschung zu Prozessen in Verwaltungen und Prozessketten zwischen Verwaltungen und anderen Akteuren zu schaffen, wurde die Forschungslandkarte zur prozessorientierten Verwaltung erarbeitet [Be11]. Ziel dieses Beitrags ist es, ausgewählte Ergebnisse vorzustellen und auf dieser Basis spezifische Handlungsempfehlungen für die prozessorientierte Verwaltung abzuleiten.

Im Folgenden wird in Abschnitt 2 zunächst das methodische Vorgehen zur Datenerhebung beschrieben, die Ergebnisse der Auswertung der Datenbasis und konkrete Handlungsempfehlungen werden in Abschnitt 3 aufgezeigt. Abschnitt 4 fasst den Beitrag zusammen und gibt einen Ausblick auf zukünftige Forschung.

2 Methodisches Vorgehen zur Datenerhebung

Die Konzeption und Durchführung der Datenerhebung wurde in Anlehnung an das Vorgehen von vom Brocke et al. [Br09] in mehreren Schritten durchgeführt.

In der ersten Phase der Datenerhebung wurde multimethodisch gezielt nach Forschungsergebnissen zum Thema „Prozessorientierte Verwaltung“ gesucht. Dabei wurden folgende Kriterien angesetzt, um den gefundenen Beitrag in die Datenbasis aufzunehmen: (1) Das Forschungsergebnis musste aus dem Bereich der prozessorientierten Verwaltung stammen und (2) das Ergebnis musste sich auf Deutschland beziehen oder der Forscher musste in Deutschland forschen beziehungsweise arbeiten.

Für die anschließende, breite Datenerhebung wurden auf Basis der ersten Ergebnisse Suchbegriffe in deutscher und englischer Sprache generiert und durch eine Expertenbefragung ergänzt. Mit Hilfe dieser Suchbegriffe wurde in den Projekt- und Literaturdatenbanken nach weiteren einschlägigen Beiträgen recherchiert. Hierzu zählten Konferenzen aus dem Bereich der Wirtschaftsinformatik, Verwaltungsfachtagungen sowie E-Government-Konferenzen. Auf Basis der identifizierten Forschungsergebnisse wurde eine Schneeballsuche durchgeführt, welche über die Verknüpfung von bekannten Forschungsergebnissen, Projekten, Forschern und Publikationen weitere Informationen lieferte (beispielsweise Forschungsergebnisse aus identifizierten Projekten, welche nicht durch die gefundenen Publikationen abgedeckt wurden).

Zur Verifikation der erhobenen Daten wurden in einem letzten Schritt die identifizierten Forscher aus dem Themenfeld der prozessorientierten Verwaltung einbezogen. Zum Zweck der Qualitätssicherung der Datenbasis wurden sie gebeten, die über ihre Forschungstätigkeit erhobenen Daten im Forschungsportal zu überprüfen und gegebenenfalls zu aktualisieren.

Durch Auswertung der im Rahmen dieser Befragung ermittelten Verweise auf weitere Forscher beziehungsweise Institutionen konnte die Datenbasis erneut ausgeweitet werden. Bis zum Stichtag 14. April 2011 wurden 115 Projekte und 155 Forschungsergebnisse erfasst. Ebenso wurden 143 Organisation, 215 Personen und 104 Publikationen ermittelt. Unter Zuhilfenahme der Berichtsfunktion des genutzten Forschungsportals wurden die gesammelten Daten ausgewertet und Analysen erstellt.

3 Status quo und Forschungslücken

In diesem Abschnitt werden der aktuelle Stand der Forschung zur prozessorientierten Verwaltung sowie daraus abgeleitete Forschungslücken dargestellt, die sich aus den Auswertungen der Datenbasis ergeben. Dabei werden diese anhand der wichtigsten zukünftig zu adressierenden Felder strukturiert. Auf Basis der gewonnenen Erkenntnisse wurden Handlungsempfehlungen für zukünftige Forschungsprojekte abgeleitet. Insgesamt konnten 14 Forschungsfelder bzw. Handlungsbereiche identifiziert werden, die sich auf die Forschungsinhalte, aber auch auf strukturelle Aspekte der Forschung beziehen. In diesem Beitrag werden neben dem strukturellen Aspekt der *Vernetzung von Forschungsinstitutionen* insbesondere die Handlungsbereiche *Standardisierung und Harmonisierung, Prozessketten, Schnittstellen zu spezifischen Akteuren, Langfristigkeit und Kontinuität des Prozessmanagements, Integration der Finanzflusssicht in das Prozessmanagement* und *Prozessmanagement und Recht* vorgestellt. Die weiteren in der Studie identifizierten Forschungsfelder werden im Ausblick des Beitrags aufgegriffen.

Vernetzung von Forschungsinstitutionen
Die derzeitige Vernetzung von Forschungsinstitutionen im deutschsprachigen Raum, die sich mit der prozessorientierten Verwaltung beschäftigen, ist gering. So sind beispielsweise knapp 47% (67 der 143 Organisationen) der aufgelisteten Forschungsorganisationen nicht durch ein Forschungsergebnis mit einer anderen Institution vernetzt. Die Dichte des gesamten Netzwerkes beträgt 2.81%, gemessen als Anzahl der tatsächlich existierenden Kooperationen geteilt durch die Anzahl der theoretisch möglichen Kooperationsbeziehungen.

Die geographische Auswertung lässt sich durch eine Darstellung der Vernetzung der Forschungslandschaft in der prozessorientierten Verwaltung ergänzen (Abbildung 1). Der Großteil der 285 Verknüpfungen besteht aus schwachen Kooperationen, das heißt Institutionen, die über maximal zwei Forschungsergebnisse miteinander kooperieren. Die Intensität der Vernetzung von Forschungsinstitutionen der prozessorientierten Verwaltung kann dementsprechend als eher gering eingeschätzt werden.

Abbildung 1: Geographische Darstellung der institutionellen Vernetzung

Die Daten spiegeln damit eine verhältnismäßig stark isolierte Forschung im Bereich der prozessorientierten Verwaltung wider. Synergiepotenziale, die die Zusammenarbeit verschiedener Experten mit sich brächte, bleiben so ungenutzt. Durch eine verbesserte Kooperation zwischen verschiedenen Institutionen und Forschern würden die erzielten Resultate schneller kommuniziert und zur Anwendung gebracht sowie die Zahl redundanter Forschungsaktivitäten verringert.

Handlungsempfehlung 1: Die Forschungsinstitutionen, die im Themenfeld der prozessorientierten Verwaltung arbeiten, sollten verstärkt miteinander kollaborieren.

Standardisierung und Harmonisierung
Ein wichtiges Handlungsfeld, das sich aus der Analyse verschiedener Dimensionen ergibt, ist das der Standardisierung und Harmonisierung. Nur wenige Forschungsergebnisse haben die Entwicklung von Interoperabilitätsstandards sowie Harmonisierungsinitiativen zum Ziel. Generell werden wenige Standards eingesetzt beziehungsweise ist deren Einsatz schlecht dokumentiert. Bisherige Forschungsergebnisse haben wenig Einfluss auf Standardisierungen, was das Bild der vielen Insellösungen unterstützt [Ba01]. Dazu wurden bei der Erfassung der Daten für die vorgelegte Studie die Teildimensionen *IT-Sicherheitsstandard* (*OSCI-Transport 2.0, sonstige Sicherheitsstandards*), *Modellierungsstandard* (*BPMN, EPK, UML*), *XÖV* (*Ausländerwesen, DatML/ RAW Gewerbe, XBau, XDomea, XFinanz, XJustiz, XKasse, XKfz, XMeld, XPersonenstand, XPlanung, XSozial, XStatistik*), *Weitere Interoperabilitätsstandard* (*Fachspezifisch, Fachübergreifend, Fachunabhängig*) und *Sonstige Standards* unterschieden. Zusätzlich ist auch die freie Eingabe eines berücksichtigten Standards in einem Textfeld möglich.

Die Auswertung in Bezug auf genutzte Standards ergibt, dass bei 79% der Forschungsergebnisse keine Zuordnung zu einem spezifischen Standard vorgenommen werden konnte. Dies bedeutet, dass in den Informationen, die zu einem Forschungsergebnis gefunden werden konnten, keinerlei Bezug auf die Nutzung von Standards oder die Entwicklung beziehungsweise Beeinflussung von Standards genommen wurde. Ebenso haben die Forscher selbst, die in die Befüllung des Forschungsportals eingebunden wurden, keine Hinweise auf genutzte, entwickelte oder beeinflusste Standards vermerkt.

So adressiert lediglich 1 Forschungsergebnis (1%) einen IT-Sicherheitsstandard, 6 Forschungsergebnisse (4%) verwenden diverse Modellierungsstandards. Die XÖV-Standards finden ebenfalls in nur sehr wenigen Forschungsergebnissen (5%) Anwendung. Auch werden nur bei 5 Forschungsergebnissen Interoperabilitätsstandards adressiert. Auf die Teildimension „Sonstige Standards“ entfallen 11 Forschungsergebnisse. Generell ist nun die Frage zu stellen, ob die bisher verfügbaren Standards nicht praxistauglich sind und deshalb nicht verwendet beziehungsweise adressiert werden oder ob es auf der anderen Seite so viele Standards beziehungsweise vergleichbare Konzepte gibt, dass sich keine wirklichen Standards ausgebildet haben. Dies wäre in weiterführenden Untersuchungen zu beantworten und stellt eine offene Frage dar.

Ähnlich wie im Bereich der genutzten Standards verhält es sich bei der Frage nach dem Einfluss auf Standardisierungsverfahren aus den untersuchten Projekten heraus. 134 Forschungsergebnisse sind in keine Standardisierungs- beziehungsweise Normungsinitiative eingeflossen. 7 Forschungsergebnisse sind in nationale Verfahren (Deutschland) eingeflossen, davon 4 in XÖV und 3 in „sonstige Standardisierungsverfahren“. In multinationale Verfahren sind 4 Ergebnisse eingegangen, 2 davon in CEN (Europäisches Komitee für Normung), die weiteren in „sonstige multinationale Standardisierungsverfahren“.

Bei der zukünftigen Entwicklung von Richtlinien, Verordnungen und Gesetzen sollten Standardisierungs- und Harmonisierungsverfahren beteiligt sein. In der E-Government-Literatur wird ebenfalls festgestellt, dass ein Grund für den geringen Fortschritt vieler E-Government-Bemühungen die mangelnde Interoperabilität und Integration von Systemen ist [Kl04]. Die Zusammenarbeit zwischen verschiedenen Behörden, die in Zukunft immer wichtiger wird, lässt sich nur durch einheitliche Austauschstandards verwirklichen [Ja11]. Durch erhöhte Berücksichtigung von Standards und Harmonisierungsinitiativen in der Forschung könnte dieses Ziel wirksam unterstützt werden.

Handlungsempfehlung 2: Forschungsprojekte sollten vermehrt auf Standards zurückgreifen beziehungsweise an der Entwicklung von Standards mitwirken, um so zur Harmonisierung im Prozessmanagement beizutragen.

Prozessketten
Ein Forschungsfeld mit zunehmender Bedeutung sind Prozessketten. Diese Dimension verdeutlicht, inwieweit die Forschungsergebnisse im Bereich der prozessorientierten Verwaltung andere, neben der Verwaltung beteiligte Akteure in die Prozesse einbinden oder ob vornehmlich „Insellösungen" entstehen, die ausschließlich die Verwaltung berücksichtigen. Darüber hinaus wird ersichtlich, welche Prozesskettenausschnitte in der bisherigen Forschung besonders betrachtet werden, welche Beziehungen bisher vernachlässigt wurden und ob es viele Ergebnisse gibt, die die gesamte Prozesskette berücksichtigen.

Die Ergebnisse der Analyse zeigen, dass die Mehrheit der Forschungsergebnisse andere Akteure als nur die betrachtete Verwaltung selbst einbezieht. Nur 22 Forschungsergebnisse finden lediglich innerhalb einer Verwaltung Anwendung. Weitere 67 beziehen sich auf die Zusammenarbeit mehrerer Verwaltungen. Externe Akteure spielen in der Mehrzahl der Forschungsergebnisse eine Rolle: Unternehmen werden in 74 Forschungsergebnissen einbezogen, Bürger in 64 und soziale Einrichtungen in 25.

Ein anderes Bild ergeben die Daten in Bezug auf die Interoperabilität. Zu 49% der untersuchten Forschungsergebnisse wurde keine Angabe in der Dimension „Prozessketteninteroperabilität" gemacht beziehungsweise das Thema Interoperabilität spielte keine Rolle. Von den 48%, für die eine Klassifizierung vorliegt, befassen sich 15 Forschungsergebnisse mit staatsgrenzenübergreifenden Prozessketten. Weitere 31 haben die Angabe „ländergrenzenübergreifend". Den Schwerpunkt bilden mit 45 Nennungen fachbereichsgrenzenübergreifende Prozessketten. Nur sieben der Forschungsergebnisse befassen sich mit der Zusammenarbeit zwischen Arbeitsgruppen.

Die Daten zeigen, dass die Relevanz dieses vergleichsweise jungen Themas bereits von einigen Forschern erkannt wurde [WJK10]. Allerdings gibt es hier noch viel Potenzial, den Datenaustausch zwischen der öffentlichen Verwaltung und ihren Kunden zu verbessern. Bisherige Forschungsaktivitäten und -ergebnisse sind noch stärker zu vernetzen, um ausgehend von den identifizierten methodischen, organisatorischen, rechtlichen und technischen Fragestellungen vertiefte Forschungsarbeiten anzustoßen.

Darüber hinaus könnte die Analyse von Fachlichkeiten auf kommunaler sowie Bundes- und Landesebene, die besonders stark in Prozessketten eingebunden sind, zeigen, ob

Fachlichkeiten mit bestimmten Eigenschaften sich besonders für die Prozessketten-integration eignen. Zukünftige Forschungsprojekte sollten somit durch weitergehende Untersuchungen zur Verwirklichung des Potenzials durchgängiger Prozessketten beitragen.

Handlungsempfehlung 3: Die Arbeiten zur Entwicklung standardisierter, durchgängiger Prozessketten zwischen den Verwaltungen und weiteren Akteuren bedürfen weiterer Forschung.

Schnittstellen zu spezifischen Akteuren
Die Auswertung der Daten hat einen Mangel an Forschungsergebnissen aufgedeckt, die sich auf die Bedürfnisse spezieller Akteure beziehen. Die Analyse der Fachbezogenheit ergibt, dass sich 37% aller Forschungsergebnisse (58 Ergebnisse) auf alle Fachlichkeiten anwenden lassen. 29% aller Ergebnisse (45) lassen sich auf mehrere Fachlichkeiten anwenden und knapp 19% (29) beziehen sich ausschließlich auf eine einzelne Fachlichkeit.

Die Analyse der adressierten Fachlichkeiten speziell auf kommunaler Ebene ergibt, dass sich über 63% (98 Ergebnisse) aller Forschungsergebnisse keiner spezifischen Fachlichkeit zuordnen lassen. Es gibt elf Nennungen im Umweltschutz, sechs im Einwohnermeldewesen, jeweils fünf im Bereich des Bürgerservices und Feuer- beziehungsweise Zivilschutz, eine Nennung im Friedhofswesen, je drei Nennungen in den Fachlichkeiten Bauordnung/Bauverwaltung, Gesundheit sowie Gewerbe und jeweils zwei Nennungen im Bereich Soziales sowie in der zentralen Verwaltung. Darüber hinaus richtet sich jeweils ein Forschungsergebnis an die Fachlichkeiten Entsorgung, Hochbau- und Gebäudemanagement, Kämmerei, Kinder, Jugend und Familie, Kultur, Presse- und Öffentlichkeitsarbeit, Stadtplanung, Statistik und Wahlen sowie Steuern. Darüber hinaus gibt es elf weitere Nennungen im Bereich der sonstigen Fachlichkeiten auf kommunaler Ebene. Die hohe Anzahl Forschungsergebnisse, die auf alle Fachlichkeiten anwendbar sind, unterstreicht, dass viele Forschungsergebnisse verhältnismäßig unspezifisch ausgelegt sind und prinzipiell in verschiedensten Anwendungskontexten eingesetzt werden können.

Das betrifft zum einen die Besonderheiten einzelner Fachlichkeiten, die selten berücksichtigt werden, was sowohl auf kommunaler Ebene als auch auf Bundes- und Landesebene zutrifft. Dies ist nicht zwangsweise als schlecht zu beurteilen, da diese eher generisch angelegten Lösungen Bestrebungen der Standardisierung nicht nur von IT, sondern gegebenenfalls auch von Abläufen vereinfachen und auch die Wiederverwendung unterstützen. Allerdings zeigt die Analyse in den betreffenden Dimensionen, dass dies bisher nicht erfolgt.

Besonders deutlich aber wird der generelle Ansatz und daraus abgeleitete Mangel an spezifischen Forschungsergebnissen im Bereich der Schnittstellen zu Unternehmen. So wird nur wenig auf die Bedürfnisse von Kleinst-, kleinen und mittleren Unternehmen eingegangen. 76% der Forschungsergebnisse weisen gar keinen Bezug zu Unternehmen auf. Häufig wird die Unternehmenssicht allgemein betrachtet, ohne dass Unterschiede und Spezifika in den Anforderungen verschiedener Unternehmenstypen untersucht werden. Durch weitergehende Analysen hinsichtlich dieser speziellen Bedürfnisse und

Eigenschaften könnten zukünftige Forschungsprojekte ein besseres Verständnis der beteiligten Akteure und Unternehmen unterstützen.

Handlungsempfehlung 4: Besonderheiten der Schnittstellen zu spezifischen Akteuren innerhalb und außerhalb der Verwaltung sollten gezielter erforscht werden.

Langfristigkeit und Kontinuität des Prozessmanagements
Im Bereich des Prozessmanagements werden vor allem Prozessverbesserungen und Umsetzungen erarbeitet. Die Strategieentwicklung sowie auch das kontinuierliche Prozessmanagement werden in den erfassten Forschungsergebnissen kaum betrachtet (vgl. Abbildung 2).

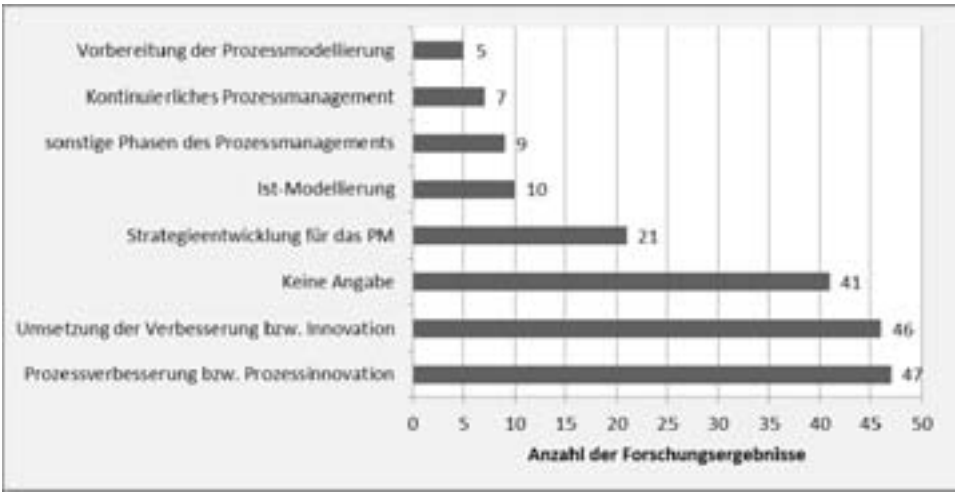

Abbildung 2: Phasen des Prozessmanagements

Für diese Schlussfolgerung spricht insbesondere, dass das kontinuierliche Prozessmanagement im Vergleich zu anderen Phasen des Prozessmanagements in der Forschungslandkarte selten von Forschungsergebnissen abgedeckt wird. Angesicht des inhaltlichen und methodischen Facettenreichtums der Verstetigung des Prozessmanagements tritt hier ein relativ deutliches Defizit in der bisherigen Forschung zu Tage. Insbesondere stellt sich die Frage, wie sich diese Lücke begründet. Wie die Auswertung weiterer Dimensionen es bereits nahelegt, kann vermuten werden, dass die prozessorientierte Verwaltung gegenwärtig noch stark von ad-hoc-Maßnahmen geprägt ist und deshalb Forschungsfragen des Prozessmanagements mit langfristiger beziehungsweise grundlegendender Bedeutung noch nicht in den Vordergrund drängen.

Für diese Diagnose sprechen auch die noch geringe Bedeutung der Vorbereitung der Prozessmodellierung und die allmählich in den Fokus rückende Strategieentwicklung. Es ist zu erwarten, dass mit zunehmender Reife des Prozessmanagements in Verwaltungen die genannten Themen vermehrt auf Interesse in der Forschung und Praxis treffen werden. Darüber hinaus benötigen einige Forschungsziele, wie beispielsweise die Einführung von Wissensmanagement oder die Förderung der Innovationsfähigkeit, ein

kontinuierliches Prozessmanagement als Basis [Da10]. Da für den nachhaltigen Erfolg von Projekten im Bereich der prozessorientierten Verwaltung das Prozessmanagement langfristig aufgestellt sein muss, besteht hier ein dringender Bedarf, die Strategieentwicklung im Bereich des Prozessmanagements sowie das vor allem sehr wichtige Verstetigen des Prozessmanagements zu vertiefen.

Handlungsempfehlung 5: Die Forschung zur prozessorientierten Verwaltung sollte zukünftig insbesondere die langfristige und kontinuierliche Etablierung des Prozessmanagements adressieren.

Integration der Finanzflusssicht in das Prozessmanagement
Im Rahmen der prozessorientierten Verwaltung dominiert bei den Forschungsergebnissen die technische Perspektive. Die überwiegende Mehrheit der Forschungsergebnisse (60%) hat Datenflüsse zum Gegenstand. Eine immer noch signifikante Menge von 20% beschäftigt sich mit Kontrollflüssen, die häufig mit einem entsprechenden Datenfluss einhergehen. Finanz- und Materialflüsse folgen mit zwölf beziehungsweise sieben Nennungen, was 8% beziehungsweise 5% der untersuchten Forschungsergebnisse ausmacht.

Die starke Konzentration auf Datenflüsse spiegelt den informations- und datengetriebenen Charakter von Verwaltungsdienstleistungen wider. Mit dem Datenfluss wird in der Regel zugleich ein wesentlicher Teil der Kontrollflüsse abgebildet. Ereignisse, die der Kontrolle eines Informationssystems unterliegen und zentrale Konstrukte der Prozesssteuerung und -kontrolle darstellen, werden regelmäßig durch Datenbanksysteme abgebildet. Insofern wird der geringeren Anzahl der Nennungen des Kontrollflusses bei der Klassifizierung der Forschungsergebnisse keine besondere Bedeutung beigemessen. Auch die geringe Betrachtung von Materialflüssen kann nicht notwendigerweise als gravierendes Defizit in der Forschung gewertet werden, da sich nur wenige Abläufe in Verwaltungen hauptsächlich mit materiellen Bewegungen befassen. Daher besteht keine Notwendigkeit, Forschung in diesem Bereich der Wertflüsse zu stärken. Allerdings wird dafür plädiert, zukünftig die Integration der Finanzsicht in das Prozessmanagement stärker voranzutreiben. Monetäre Bewegungen machen einen beträchtlichen Anteil am Verwaltungshandeln aus. Es ist zu vermuten, dass Finanzflüsse in Analogie zur Forschung im Bereich des Supply Chain Management erst in späteren Stadien der Untersuchungen eine Rolle spielen werden [HS01].

Handlungsempfehlung 6: Die Forschung zur prozessorientierten Verwaltung sollte zukünftig die Finanzflusssicht innerhalb der Prozesse in den Fokus rücken.

Prozessmanagement und Recht
Die juristische beziehungsweise regulatorische Perspektive wird in Forschungsergebnissen zur prozessorientierten Verwaltung selten eingenommen. Die Analyse der Forschungsergebnisse zeigt jedoch, dass zunehmend auch disziplinenübergreifende Ziele wie die Integration von IT und rechtlichen Aspekten wichtig werden. Die Intensitätsunterschiede, mit denen einzelne Richtlinien, Verordnungen und Gesetze berücksichtigt werden, können als Indiz gegen das Vorliegen einer systematischen Abstimmung von Prozessmanagement und Recht gesehen werden.

Die Statistik dieser Dimension ergibt, dass bei rund der Hälfte (51%) aller Forschungsergebnisse keine Zuordnung zu einer Richtlinie beziehungsweise Verordnung möglich war. Bei 18% der Forschungsergebnisse konnte gänzlich ausgeschlossen werden, dass sie eine Richtlinie, Verordnung oder Gesetz adressieren. Hingegen konnte knapp ein Viertel der Forschungsergebnisse direkt einer oder mehreren nationalen beziehungsweise europäischen Richtlinien beziehungsweise Verordnungen zugeordnet werden. 13 Forschungsergebnisse wurden keiner der vorgegebenen spezifischen Dimensionsausprägungen zugeordnet und fallen in die Kategorie „sonstige europäische Verordnungen, Gesetze etc."

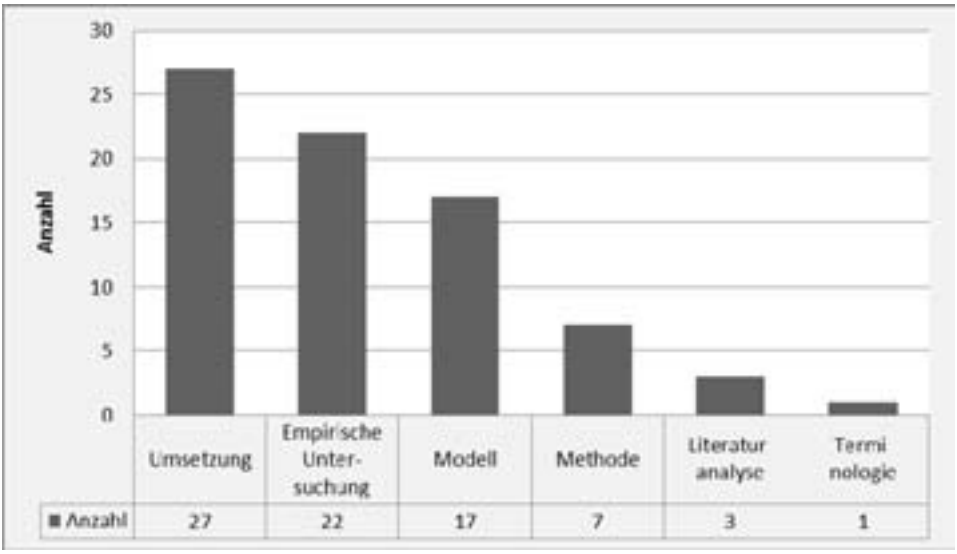

Abbildung 3: Durch Richtlinien angestoßene Forschungsergebnisse je Ergebnistyp

Die EU-DLR ist die am häufigsten referenzierte Richtlinie auf europäischer Ebene. Allerdings konnten bei den europäischen Richtlinien auch wieder neun Forschungsergebnisse keiner der vordefinierten Richtlinien zugeordnet werden und fallen deshalb in die Kategorie „andere europäische Richtlinien". Innerhalb der deutschen, nationalen Richtlinien ist auffällig, dass keines der Forschungsergebnisse auf die BITV zurückgeht. Hier fallen alle Ergebnisse in die Kategorie „sonstige nationale Richtlinien, Verordnungen, Gesetze etc.". Damit deckt das vorgegebene Klassifikationsschema auf den verschiedenen Ebenen insgesamt rund ein Zehntel der in den Forschungsergebnissen adressierten Richtlinien und Verordnungen nicht ab.

Darüber hinaus besteht ein relativ ausgeglichenes Verhältnis zwischen den adressierten nationalen (16) und europäischen (20) Richtlinien. Entwicklungsbegleitende Standardisierungen sind besonders wirkungsvoll, wenn sie mit der Verbindung von Prozessmanagement und Recht gekoppelt sind. Von daher ist eine frühzeitige Abstimmung zwischen Prozessmanagement und rechtlichen Rahmenbedingungen empfehlenswert.

Die Datenbasis zeigt ferner, dass einzelne Richtlinien bereits durchaus einen größeren Einfluss auf die Forschung nehmen können. Der Umstand, dass es sich bei den durch Richtlinien angestoßenen Forschungsergebnissen überwiegend um Umsetzungen handelt (vgl. Abbildung 3), legt aber den Schluss nahe, dass die Forschung gegenwärtig überwiegend reaktiv mit den Auswirkungen beziehungsweise der Einhaltung regulatorischer Vorgaben befasst ist.

Handlungsempfehlung 7: Rechtliche Aspekte sollten stärker zum Gegenstand der Prozessmanagementforschung gemacht werden.

4 Zusammenfassung und Ausblick

Ziel der Forschungslandkarte „Prozessorientierte Verwaltung" ist es, einen disziplinenübergreifenden Status quo der Forschungsaktivitäten in Deutschland aufzuzeigen. Dafür wurden erzielte Forschungsergebnisse systematisch identifiziert, klassifiziert und analysiert. Sowohl Praktikern als auch Wissenschaftlern gleichermaßen soll dies erleichtern, Problemlösungsbeiträge unterschiedlicher Disziplinen gezielt zu identifizieren und zu nutzen sowie Experten für die interdisziplinäre Bearbeitung von Fragestellungen aufzufinden. Durch die Ergebnisse wird deutlich, dass es zwar viele zielführende Methodenentwicklungen, Modelle, Umsetzungen oder Standards gibt, es auf der anderen Seite aber noch viele Probleme zu adressieren gilt. Hervorzuheben ist die bisher noch schwache Vernetzung der Forscher untereinander, die viele Synergiepotenziale brachliegen lässt.

Neben den in diesem Beitrag vorgestellten Handlungsbereichen konnten in der Gesamtstudie weitere Forschungslücken beziehungsweise Handlungsdefizite aufgedeckt werden, der Vollständigkeit sollen diese Handlungsdefizite hier gelistet werden, für eine Vertiefung sei auf [Be11] verwiesen.

So wird bisher kaum an *theoretischen Grundlagen* der prozessorientierten Verwaltung geforscht, überwiegende Forschungsergebnisse sind IT-technische Umsetzungen. Auch der *Einfluss der Forschung auf die Praxis* ist bisher gemessen an den erhobenen Daten eher gering, viele Forschungsergebnisse werden nur in geringem Umfang angewendet. Dies ist vor allem auf eine sehr geringe *Wiederverwendung von Forschungsergebnissen* zurückzuführen. Die meisten Ergebnisse werden nur einmal angewendet und nicht auf andere Verwaltungen übertragen. Während das *Risikomanagement* im betrieblichen Geschäftsprozessmanagement wichtig ist, ist es in der prozessorientierten Verwaltung bislang noch deutlich unterrepräsentiert. Ebenso verhält es sich mit der Berücksichtigung des *Arbeitsmarkts*. Doch um ein erfolgreiches Prozessmanagement in öffentlichen Verwaltungen aufzubauen, bedarf es gut ausgebildeter Fachkräfte.

Schlussendlich werden innerhalb der Forschungsprojekte zur prozessorientierten Verwaltung Aspekte des *Marketings* und des Vermarktens der Ergebnisse sowie Fragen der *Akzeptanz und Erfolgswirkung* der Projekte vernachlässigt. Gerade die letzten Aspekte aufgreifend ist es das Ziel, die Forschungslandkarte „Prozessorientierte Verwaltung" zu einer lebendigen Communityplattform zu entwickeln und so die Arbeit an den identifizierten Handlungsfeldern zu forcieren.

Literaturverzeichnis

[BAF09] Becker, J., Algermissen, L., Falk, T.: Prozessorientierte Verwaltungsmodernisierung – Prozessmanagement im Zeitalter von E-Government und New Public Management. 2. Aufl., Springer, Berlin u.a., 2009, S. 12 ff.

[Ba01] Bannister, F.: Dismantling the silos: extracting new value from IT investments in public administration. In: Information Systems Journal, 11 (3), 2001, S. 65-84.

[Br09] vom Brocke, J.; Simons, A.; Niehaves, B.; Riemer, K.; Plattfaut, R.; Cleven, A.: Reconstructing the Giant: On the Importance of Rigour in Documenting the Literature Search Process. In: Proceedings der European Conference on Information Systems (ECIS). Verona, Italy, 2009.

[Be10] Becker, J.; Pfeiffer, D.; Falk, T.; Räckers, M.: Semantic Business Process Analysis. In (vom Brocke, J. et al. Hrsg.): International Handbook on Business Process Management. Springer, Berlin et al., 2010; S. 187-211.

[Be11] Becker, J.; Heide, T.; Hofmann, S.; Jurisch, M.; Knackstedt, R.; Krcmar, H.; Ley, T.; Räckers, M.; Thome, I.; Wolf, P.: Forschungslandkarte „Prozessorientierte Verwaltung". Studie im Auftrag des Bundesministeriums des Innern. München/Münster 2011.

[Da10] Davenport, T.: Process Management for Knowledge Work. In (vom Brocke, J. et al. Hrsg.): International Handbook on Business Process Management. Springer, Berlin et al., 2010; S. 187-211.

[He10] Henckel, D., von Kuczkowski, K., Lau, P., Pahl-Weber, E., Stellmacher, F.: Interdisziplinarität – Transdisziplinarität. In: Planen- Bauen- Umwelt: Ein Handbuch. VS Verlag für Sozialwissenschaften, Wiesbaden, 2010.

[Ha07] Hach, H.: Evaluation und Optimierung kommunaler E-Government Prozesse. Dissertation, Flensburg, 2007.

[HS01] Holten, R., Schultz, M. B.: Integriertes Controlling für Aufbau, Betrieb und Anpassung von Supply Chains. In: Wirtschaftsinformatik 43 (2001) 6, S. 579-492.

[Ja11] Janssen, M.; Charalabidis, Y.; Kuk, G.; Cresswell, T.: Special Issue on E-government Interoperability, Infrastructure and Architecture: State-of-the-art and Challenges. In: Journal of Theoretical and Applied Electronic Commerce Research, 6, 2011.

[Kl04] Klischewski, R.: Information integration or process integration? How to achieve interoperability in administration. In: Proceedings 3rd International Conference on Electronic Government (EGOV), 2004.

[We22] Weber, M.: Wesen, Voraussetzung und Entfaltung der bürokratischen Herrschaft. In (Weber, M. Hrsg.): Wirtschaft und Gesellschaft. Mohr, Tübingen, 1922.

[WJK10] Wolf, P.; Jurisch, M.; Krcmar, H.: Analyse und Design von Prozessketten. In: (Wimmer, M. et al. Hrsg): Vernetzte IT für einen effektiven Staat – Gemeinsame Fachtagung Verwaltungsinformatik (FTVI) und Fachtagung Rechtsinformatik (FTRI) 2010 – Proceedings. Lecture Notes in Informatics (LNI), Bonn, 2010; S. 29-40.

Entwicklung eines Domänenmodells zur Identifikation und Analyse von Prozessketten

Marlen Jurisch, Vanessa Greger, Petra Wolf, Helmut Krcmar

Technische Universität München
Fakultät für Informatik, Lehrstuhl für Wirtschaftsinformatik - I17
Boltzmannstr. 3, D-85748 Garching bei München
{marlen.jurisch|vanessa.greger|petra.wolf|krcmar}@in.tum.de

Abstract: Um die Identifikation und Analyse von Informations- und Meldepflichten zu erleichtern, empfiehlt sich die Erstellung eines Domänenmodells für den jeweiligen Überwachungsbereich. Bisher sind jedoch in der Literatur kaum Ansätze für ein strukturiertes Sammeln und Aufbereiten von Informations- und Meldepflichten für weitere Analysen vorhanden. Die Autoren stellen im Rahmen dieses Beitrags ein Vorgehen für das Bilden eines Domänenmodells vor, mit dessen Hilfe die Informations- und Meldepflichten einer Domäne strukturiert visualisiert werden können, um so die Identifikation und Analyse von Prozessketten zu erleichtern. Zusätzlich werden die Grundelemente von Domänenmodellen vorgestellt und exemplarisch ein Domänenmodell im Bereich Umwelt - Emissionen präsentiert.[11]

1 Einführung

Unternehmen stehen bedingt durch unterschiedliche Informations- und Meldepflichten mit Verwaltungen in zahlreichen Kontakten, die auch als B2G-Kontakte bezeichnet werden [WJK10]. Im Zuge dessen müssen sie eine große Menge von Daten an verschiedene Verwaltungen übermitteln. Die dezentrale Bearbeitung von Behördenkontakten führt jedoch dazu, dass Unternehmen teilweise Daten redundant an unterschiedlichste Verwaltungseinheiten übermitteln müssen. Diese Daten werden außerdem oftmals dezentral und teilweise redundant im Unternehmen vorgehalten [Hu11]. Beim Sammeln und Übermitteln entsteht hierdurch für einzelne Unternehmensbereiche ein großer Aufwand, welcher sich in den Bürokratiekosten niederschlägt. Unternehmen und Verwaltungen streben deshalb zum einen die automatisierte Abwicklung der Informations- und Meldepflichten an, indem auf zentrale Datenbestände im Unternehmen zugegriffen wird und somit Aufwand und Bürokratiekosten reduziert werden [LR00; Hu11], und zum anderen die Reduktion von redundant zu übermittelnden Informationen und Daten [WJK10].

[11] Die Autoren bedanken sich beim Bundesministerium des Inneren für die Förderung des Lehrstuhls bei der Forschungsarbeit zum Thema „Prozessketten zwischen Wirtschaft und Verwaltung“ im Rahmen des P23R (Prozess-Daten-Beschleuniger) Projektes.

Die Grundlage für eine automatisierte Abwicklung von Informations- und Meldepflichten bildet die Identifikation und Analyse der Prozessketten mit dem Ziel, Verwaltungsprozesse in die Unternehmensprozesse zu integrieren [WJK10]. Prozessketten werden als „zielgerichtete Bündelung einzelner Transaktionsdienstleistungen entlang einer definierten Wertschöpfungskette“ [Bu07] definiert. Für die Unternehmer ergeben sich durch die Prozessketten Möglichkeiten zur Automatisierung bei der Überlieferung der Informations- und Meldepflichten. Hierdurch reduzieren sich Kommunikations- und Koordinationsaufwand für die Unternehmen. Dies hat wiederum Effizienzsteigerungen sowie Kosteneinsparungen zur Folge [Bu07; BVA09]. Durch die gezielte Analyse der Informations- und Meldepflichten erhöht sich sowohl für die Unternehmer als auch für die Verwaltungen die Transparenz über die anfallenden Informations- und Meldepflichten [Bu07; WJK10]. Auf Seiten der Verwaltungen soll außerdem eine Harmonisierung der Informations- und Meldepflichten erreicht und die Vergleichbarkeit der überlieferten Informationen erleichtert werden.

Um die Analyse der Informations- und Meldepflichten zu erleichtern, empfiehlt sich die Erstellung eines Domänenmodells für den jeweiligen Überwachungsbereich. Im Domänenmodell werden die relevanten Informations- und Meldepflichten einer bestimmten Domäne logisch zusammengefasst und visualisiert. Somit bietet ein Domänenmodell die Möglichkeit einer „visuellen Repräsentation der problemrelevanten Konzepte einer Domäne“ [La05]. Auf Basis eines Domänenmodells können die Informations- und Meldepflichten systematisch analysiert werden, um Prozessintegrationskandidaten zu identifizieren. Bisher sind in der Literatur kaum Ansätze für ein strukturiertes Sammeln und Aufbereiten der Informations- und Meldepflichten für weitere Analysen vorhanden [WJK10].

Ziel des vorliegenden Beitrags ist es, aufzuzeigen, wie der Ansatz der Domänenmodellierung zur Unterstützung der Identifikation und Analyse von Prozessketten eingesetzt werden kann. Zentrale Fragestellungen hierbei sind:

- Wie kann man die Informations- und Meldepflichten einer Domäne strukturiert aufbereiten, so dass die Identifikation und Analyse von Prozessketten erleichtert werden?
- Was sind Grundelemente eines Domänenmodells und welche Vorteile ergeben sich hierdurch bei der Identifikation und Analyse von Prozessketten?

Zur Beantwortung dieser Fragen gliedert sich dieser Beitrag wie folgt: Zuerst wird in Kapitel 2 das methodische Vorgehen beschrieben. In Kapitel 3 werden das Vorgehen bei der Bildung eines Domänenmodells sowie die damit verbundenen Ziele und Vorteile vorgestellt. Kapitel 4 beschreibt ein Domänenmodell am Beispiel Umwelt – Emissionen. Zum Schluss werden die gewonnenen Erkenntnisse diskutiert (Kapitel 5) und zusammengefasst (Kapitel 6).

2 Methodik

Als Grundlage für die Entwicklung eines Domänenmodells wurde zuerst eine Dokumentenanalyse durchgeführt [Ma02]. Hierbei wurden relevante Gesetze und Verordnungen aus dem Bereich Umwelt – Emissionen betrachtet. Hierzu gehören das Bundesimmissionsschutzgesetz, Bundesimmissionsschutzverordnungen, die Technische Anleitung Luft sowie das Europäische Schadstofffreisetzungs- und –verbringungsregister. Anschließend wurden mithilfe der Standardkostenmodell-Datenbank (SKM-Datenbank) die Informations- und Meldepflichten, welche sich für Unternehmer im Bereich Umwelt – Emissionen ergeben, identifiziert.

Neben der umfassenden Dokumentenanalyse wurden zusätzlich fünf semi-strukturierte Interviews mit Domänenexperten aus Bundes- und Landesverwaltungen in Deutschland durchgeführt. Die Interviewdauer lag jeweils zwischen 30 Minuten und 60 Minuten. Ziel der Interviews war es, das aufgestellte Domänenmodell von Experten aus dem Bereich Umwelt – Emissionen evaluieren und diskutieren zu lassen.

3 Domänenmodell

3.1 Ziele bei der Bildung eines Domänenmodells

Da die Ziele, welche mit einem Domänenmodell verfolgt werden, eng mit der Prozessintegration verbunden sind, wird zuerst eine Definition des Begriffs gegeben und auf die Vor- und Nachteile einer Prozessintegration kurz eingegangen.

In der Literatur findet sich keine einheitliche Definition des Integrationsbegriffs. Gemeinsame Grundlage für die Definitionen bildet jedoch die Herleitung aus dem lateinischen Wort *integrare*, welches wiederherstellen, ergänzen, wieder aufnehmen oder erneuern bedeutet. Die Definitionen unterscheiden sich hinsichtlich des Gegenstands, welcher integriert werden soll. Integrationsgegenstände können beispielsweise Daten, Prozesse oder Systeme sein [BP05; Sc07]. In der Literatur findet man bei Verwaltungen oftmals eine Unterscheidung zwischen einer Back-Office- und einer Front-Office-Integration der Prozesse. Bei den von den Autoren betrachteten B2G-Kontakten handelt es sich um letzteres, da die Interaktionen zwischen Verwaltungen und Unternehmen beziehungsweise Bürgern und nicht die Prozesse innerhalb der Verwaltung betrachtet werden [Be07]. Ziel einer Prozessintegration ist es, die unterschiedlichen Prozesse, welche sich aus den Informations- und Meldepflichten ergeben, zu koordinieren und zu einer übergeordneten Einheit zusammenzufassen [BP05; SK07].

Es wurde festgestellt, dass ein positiver Zusammenhang zwischen Integration und Performance besteht. Durch die Integration können Dienste und Prozesse schneller, effektiver und effizienter abgewickelt werden und bringen somit sowohl Verwaltungen als auch Unternehmen Vorteile [BP05; SK07]. Es darf aber nicht außer Acht gelassen werden, dass für eine Integration Ressourcen benötigt werden. Zudem entsteht durch die Integration oftmals ein zeitlicher und mitunter auch kostenintensiver Aufwand [BP05;

SK07]. Betrachtet man die Integration speziell von Verwaltungsprozessen, so ergeben sich weitere Einschränkungen. Diese entstehen beispielsweise durch gesetzliche Rahmenbedingungen, durch begrenzte Budgets oder durch den organisatorischen Aufbau der jeweiligen Verwaltung mit unterschiedlichen Entscheidungs- und Verantwortungsbereichen [SK07; Sh11].

Bis jetzt findet sich in der Literatur noch keine Handlungsvorgabe, wie die große Menge an Informations- und Meldepflichten aufbereitet werden kann, so dass aus diesen diejenigen Prozesse identifiziert werden können, welche das größte Integrationspotenzial aufweisen. Klassische Prozesskriterien reichen hier nicht aus, da eine gesamte Domäne betrachtet werden muss, um Prozesse für die Integration auszuwählen. [WJK10] stellten in ihrem Beitrag zur Analyse und Design von Prozessketten noch kein Verfahren für die strukturierte Aufbereitung von Informations- und Meldepflichten vor. Diese Lücke wird nun mit dem Domänenmodell im vorliegenden Beitrag geschlossen. Ein Domänenmodell bietet Möglichkeiten, einen Gesamtüberblick über sämtliche Informations- und Meldepflichten einer Domäne zu geben und diese strukturiert aufzubereiten, so dass in einem nächsten Schritt Integrationskandidaten ausgewählt werden können. Das Domänenmodell kann somit bei der Prozessintegration als unterstützendes Instrument dienen.

3.2 Vorgehen bei der Bildung eines Domänenmodells

Die Bildung des Domänenmodells ist eng mit dem Vorgehensmodell zur Identifikation und Analyse von Prozessketten verbunden [vgl. WJK10]. Abbildung 1 zeigt die drei Phasen des Vorgehensmodells. Die Bildung des Domänenmodells lässt sich der zweiten Phase zuordnen.

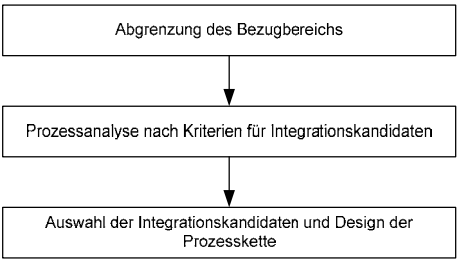

Abbildung 1: Vorgehensmodell zur Identifikation und Analyse von Prozessketten
(Quelle: [WJK10])

Ausgangsbasis bildet die Abgrenzung des Bezugsbereichs: Während dieser Phase werden die zu analysierenden Informations- und Meldepflichten nach einem festgesetzten Kriterium ausgewählt, zum Beispiel Informations- und Meldepflichten aus einer speziellen Domäne oder Informations- und Meldepflichten mit den höchsten Bürokratiekosten. Eine Unterstützung bei der Auswahl der Gesetze und Verordnungen bietet hierbei die SKM-Datenbank [WJK10]. Diese Datenbank ist eine öffentliche Plattform, in welcher vom Statistischen Bundesamt alle Informationspflichten für Unternehmen mit Merkmalen, wie gesetzliche Grundlagen, Kosten oder Fallzahlen, gesammelt sind [OAOJ]. Es empfiehlt sich das Abspeichern der ausgewählten Informations- und Mel-

depflichten mit prozessrelevanten Merkmalen, zum Beispiel beteiligte Akteure, ausgetauschte Informationen oder anfallende Bürokratiekosten, in einer Prozessbibliothek. Diese erleichtert im Laufe der nächsten Schritte die weitere Analyse, da sie eine strukturierte Filterung nach spezifischen Merkmalsausprägungen ermöglicht [OA11].

In einem nächsten Schritt werden die Prozesse nach dem Kriterium *inhaltliche Übereinstimmung beziehungsweise Ähnlichkeit* analysiert. Im Zuge der inhaltlichen Analyse wird auch die Typologie des B2G-Kontaktes, zum Beispiel Meldung oder Bericht, betrachtet. Inhaltlich ähnliche Informations- und Meldepflichten werden dann zu sogenannten Prozesskategorien zusammengefasst [WJK10]. Die große Anzahl an unstrukturiert vorliegenden Informations- und Meldepflichten wird somit in kleine, überschaubare Kategorien eingeteilt, so dass hier eine erste Aufbereitung für weitere Analysen und letztendlich für die Auswahl der Integrationskandidaten stattfindet.

Anschließend werden die Prozesskategorien zu Überwachungsgegenständen gebündelt (Abbildung 2). Die Überwachungsgegenstände verknüpfen die Prozesskategorien logisch und ordnen sie einem übergeordneten Bereich zu. Ziel hierbei ist es, einzelne Prozesskategorien nicht mehr isoliert zu betrachten, sondern Zusammenhänge aufzuzeigen. Beispielsweise werden bei Informations- und Meldepflichten innerhalb eines Überwachungsgegenstands ähnliche Daten in meist auch einer ähnlichen Form übermittelt.

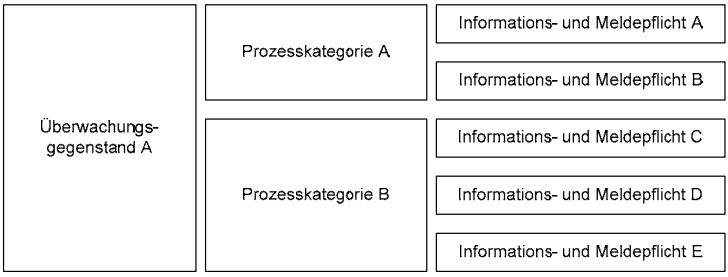

Abbildung 2: Aufbau Überwachungsgegenstand

Diese Überwachungsgegenstände werden dann im Domänenmodell entlang des Überwachungsprozesses angeordnet. Für das Domänenmodell empfiehlt es sich, den zu überwachenden Bereich abzubilden. In [Kr00] wurden bereits verschiedene Überwachungsmerkmale während eines Produktionsprozesses, zum Beispiel Abwasser oder Emissionen, identifiziert. Diese Überwachungsmerkmale können jeweils als Modell entlang eines Produktionsprozesses abgebildet und die identifizierten Überwachungsgegenstände darin eingeordnet werden. Hierdurch sind die Informations- und Meldepflichten strukturiert entlang des Produktionsprozesses an der Stelle eingeordnet, an welcher sie anfallen.

Auf der Grundlage des Domänenmodells können abschließend Integrationskandidaten identifiziert werden, auf deren Basis Prozessketten gestaltet werden. In die Gestaltung der Prozessketten werden sowohl fachliche Anforderungen als auch rechtliche Rahmenbedingungen aufgenommen [WJK10].

4 Beispiel eines Domänenmodells im Bereich Umwelt

Die Bedeutung der Reduktion und Vermeidung von Emissionen ist für den Umweltschutz enorm. Während des Produktions- und Verbrennungsprozesses treten meist unzählige Stoffe in die Umwelt aus und belasten diese. Chronische Krankheiten sind oftmals die Folge von Emissionen [BWT10; Um11]. Daher ist es wichtig, diesen Bereich stetig zu überwachen, um bei einer zu hohen Umweltbelastung durch Emissionen rechtzeitig und gezielt Gegenmaßnahmen einleiten zu können. Emissionen wurden auch von [Kr00] als Überwachungsmerkmal in einem Referenzmodell für Umweltsysteme identifiziert. Dieses unterteilt den Umweltbereich in unterschiedliche Überwachungsbereiche, zum Beispiel Boden, Wasser oder Luft. Die Notwendigkeit, diesen Bereich zu überwachen, resultiert in einer großen Anzahl an unterschiedlichen Informations- und Meldepflichten. Aus diesen Gründen wurde der Schwerpunkt auf die Domäne Emissionen gelegt.

Nach der Abgrenzung des Bezugsbereichs ergaben sich aus dem Bereich Umwelt – Emissionen insgesamt 71 unterschiedliche Informations- und Meldepflichten, welche mithilfe der SKM-Datenbank des Statistischen Bundesamts Deutschland [OAOJ] und den relevanten Gesetzen und Vorschriften identifiziert wurden. Diese wurden mit für die weitere Analyse relevanten Merkmalen, zum Beispiel zu übermittelnde Informationen, beteiligte Akteure, Fallzahlen oder Bürokratiekosten, in einer Prozessbibliothek gesammelt. Die Informations- und Meldepflichten wurden wie beschrieben zu Prozesskategorien und anschließend zu Überwachungsgegenständen zusammengefasst. Das Bilden des Domänenmodells fand hierbei bereits parallel zu der Bündelung zu den Überwachungsgegenständen statt. Dies gewährleistete, dass sämtliche Prozesskategorien in das Domänenmodell aufgenommen werden konnten.

Das Domänenmodell im Bereich Umwelt – Emissionen wird entlang des Stoffstroms, das heißt des Prozesses, welchen die Stoffe während des Produktions- und Verbrennungsprozesses durchlaufen, abgebildet (Abbildung 3). Der Produktionsablauf unterteilt sich in den Brennstoffzufuhr-, den Verbrennungs- sowie den Emissionsprozess. In allen Phasen beobachten die Unternehmen die Prozesse und messen, schätzen oder berechnen anfallende Daten. Die hieraus gewonnenen Ergebnisse werden an die zuständigen Behörden berichtet beziehungsweise gemeldet.

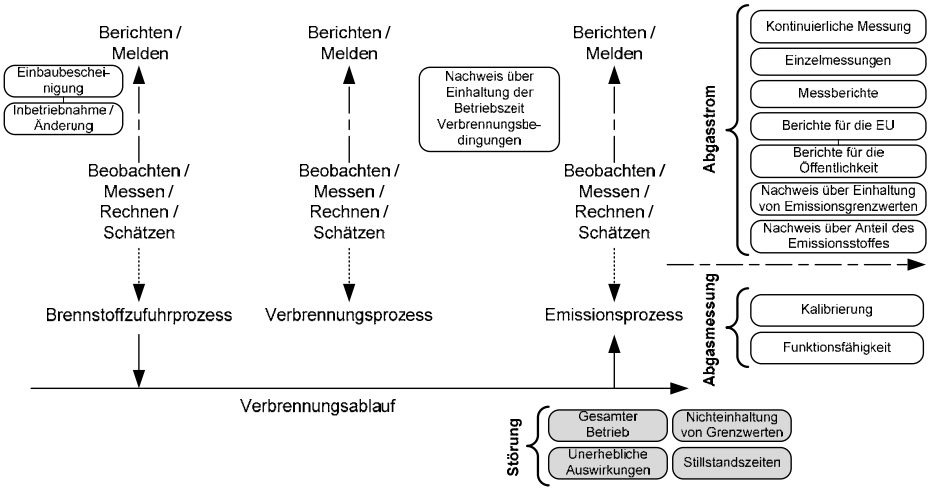

Abbildung 3: Domänenmodell entlang des Stoffstroms

Insgesamt ergaben sich nach dem Zusammenfassen der Informations- und Meldepflichten sechs unterschiedliche Überwachungsgegenstände, welche in den Prozessablauf eingeordnet wurden: Einbaubescheinigung, Inbetriebnahme & Änderung, Nachweis über Einhaltung der Betriebszeit & Verbrennungsbedingungen, Abgasstrom, Abgasmessung sowie Störung. Die einzelnen Überwachungsgegenstände teilen sich wiederum in 19 Prozesskategorien auf, welche jeweils bis zu 11 Informations- und Meldepflichten beinhalten. Für die Überwachungsgegenstände Abgasstrom, Abgasmessung und Störung sind die einzelnen Prozesskategorien in Abbildung 3 exemplarisch aufgeführt.

Aus dem Domänenmodell wird ersichtlich, dass zwischen den einzelnen Prozesskategorien Zusammenhänge bestehen. Beispielsweise müssen Nachweise über die Einhaltung von Emissionsgrenzwerten erbracht werden. Werden die Grenzwerte nicht eingehalten, so treten in diesem Bereich Störungen auf. Der Überwachungsgegenstand Abgasstrom enthält, wie in der Abbildung zu erkennen ist, die meisten Prozesskategorien und auch die größte Anzahl an Informations- und Meldepflichten. Somit bietet sich dieser Überwachungsgegenstand für weitere Analysen zur Bildung von Prozessketten an, da das Erstellen dieser Messberichte für die Unternehmen die meiste Zeit in Anspruch nimmt und somit hohe Kosten verursacht. Aus diesen Gründen wurden die Messberichte für weitere Analysen ausgewählt.

Betrachtet man die Prozesskategorie jährliche Messberichte, so erkennt man, dass es sich bei den zu liefernden Informationen um eine Aggregation der Messergebnisse aus den Prozesskategorien Einzelmessungen sowie kontinuierliche Messungen handelt. Die Prozesskategorien greifen somit auf gleiche oder ähnliche Datenbestände zurück. Hierdurch eignen sich diese Prozesse für eine Integration. Eine automatisierte Abwicklung dieser Informations- und Meldepflichten ist möglich. Dies führt letztendlich zu einer Reduktion des Aufwandes für die Unternehmen.

5 Diskussion

Durch die grafische Darstellung als Domänenmodell können Integrationskandidaten einfach vorgestellt und kommuniziert werden. Die Prozesskategorien sind nicht nur abstrakte Begriffe, sondern werden konkret an der jeweiligen Stelle innerhalb des Domänenmodells eingeordnet. Dies hilft aufzuzeigen, an welcher Stelle im Produktionsprozess die jeweiligen Informations- und Meldepflichten anfallen. Durch die Überwachungsgegenstände kann somit das Verständnis über das Zusammenspiel zwischen den Prozesskategorien maßgeblich verbessert werden. Die Prozesskategorien werden nicht mehr länger isoliert betrachtet, sondern durch das Zusammenfassen in Überwachungsgegenständen in Beziehung zueinander gesetzt.

Das Domänenmodell zeigt zudem durch das Zusammenfassen auf, welche Informations- und Meldepflichten auf ähnliche oder gleiche Daten zurückgreifen. Dieses Wissen kann von den Unternehmen zur automatisierten Abwicklung der Informations- und Meldepflichten genutzt werden. Da Datenbestände dann nicht mehr redundant an mehreren Orten im Unternehmen, sondern nur noch zentral an einer Stelle vorgehalten werden müssen, reduziert sich für die Unternehmen der Aufwand beim Sammeln der Daten [Ev02; BJW11].

Ein weiterer Vorteil ergibt sich für den Fall, dass geänderte gesetzliche Verordnungen oder neue EU-Richtlinien neue Informations- und Meldepflichten für die Unternehmen nach sich ziehen. Mithilfe des Domänenmodells können diese schnell der jeweiligen Prozesskategorie zugeordnet werden. Durch die Einordnung der Überwachungsgegenstände in das Domänenmodell kann eine erste grobe Zuordnung ohne genaue Kenntnis der gesamten Prozesskategorien erfolgen. Erst nachdem die neue Berichtspflicht einem Überwachungsgegenstand zugeordnet wurde, müssen die darin enthaltenen Prozesskategorien genauer betrachtet und gegebenenfalls eine neue Prozesskategorie gebildet werden. Das Domänenmodell ist somit nicht statisch, sondern entwickelt sich dynamisch durch neue, meist rechtliche Anforderungen weiter.

Das Domänenmodell kann abschließend als Referenzmodell für Bereiche mit ähnlichen Informations- und Meldepflichten dienen. Die aus einem Domänenmodell gewonnenen Erkenntnisse über Standardisierungsmöglichkeiten können gegebenenfalls auf andere Bereiche übertragen werden. Dies vereinfacht das Bilden von Prozessketten und reduziert den Aufwand [LL69]. Das gebildete Domänenmodell eignet sich für den Einsatz im Bereich Emissionen. Es ist davon auszugehen, dass in anderen Schadstoffbereichen, welche während des Produktionsprozesses bei einer industriellen Anlage entstehen, ähnliche Überwachungsgegenstände zu finden sind und somit ähnliche Domänenmodelle gebildet werden können. Daher ist in einem nächsten Schritt die Übertragbarkeit des Domänenmodells auf andere Überwachungsbereiche, zum Beispiel Abwasser oder Boden, zu überprüfen.

Es ist jedoch zu beachten, dass Informations- und Meldepflichten erst identifiziert werden müssen, bevor das Domänenmodell gebildet wird. Es erleichtert zwar das Einordnen neuer Informations- und Meldepflichten. Jedoch müssen für eine kontinuierliche Weiterentwicklung gesetzliche Änderungen noch manuell gefunden und zugeordnet werden. Langfristig müsste hier ein Weg gefunden werden, dies automatisch auszuführen.

6 Zusammenfassung

In diesem Beitrag wird das Vorgehen zur Bildung eines Domänenmodells vorgestellt. Dieses unterstützt die Identifikation und Analyse von Prozessketten, mit welchen Verwaltungsprozesse in unternehmensinterne Prozesse integriert werden können. Zur Bildung des Domänenmodells wird dem Vorgehensmodell zur Analyse und Gestaltung von Prozessketten gefolgt. Ausgangsbasis bildet die genaue inhaltliche Analyse aller relevanten Informations- und Meldepflichten. Hierbei müssen vor allem die ausgetauschten Informationselemente sowie der Kontakttyp betrachtet werden. Die Informations- und Meldepflichten können anschließend in Prozesskategorien zusammengefasst werden, welche gebündelt zu Überwachungsgegenständen in das Domänenmodell aufgenommen werden.

Die Autoren stellen außerdem die Ziele und Chancen vor, welche sich durch ein Domänenmodell ergeben. Mithilfe des Domänenmodells können Möglichkeiten zur Harmonisierung, zum Abbau der Bürokratiekosten, zur Effizienzsteigerung sowie zur Nutzung gemeinsamer Datenbestände aufgezeigt werden. Die Bildung eines Domänenmodells wird anhand eines Beispiels aus dem Bereich Umwelt – Emissionen illustriert. Zudem zeigt dieses Beispiel, wie Zusammenhänge und weitere Analysemöglichkeiten durch ein Domänenmodell erkannt werden können.

Literaturverzeichnis

[Be07] Bekkers, V.: The governance of back-office integration – organizing co-operation between information domains. In: Public Management Review, Vol. 9, Nr. 3, 2007; S. 377-400.

[BJW11] Bharosa, N.; Janssen, M.; Winne, N.: Managing the transformation to Standard Business Reporting – principles and lessons learned from the Netherlands. In: 12th Annual International Conference on Digital Government Research, Maryland, 2011.

[BP05] Barki, H.; Pinnsoneault, A.: A model of organizational integration, implementation effort, and performance. In: Organization Science, Vol. 16, Nr. 2, 2005; S. 165-179.

[Bu07] Bundesministerium des Innern: Konzept – Handlungsfeld Prozessketten im Programm E-Government 2.0 – Kurzfassung. In: http://www.cio.bund.de/SharedDocs/Publikationen/DE/E-Government/prozessketten_konzept_download.pdf?__blob=publicationFile, zugegriffen am: 18.08.2011.

[BVA09] Berente, N.; Vandenbosch, B.; Aubert, B.: Information flows and business process integration. In: Business Process Management Journal, Vol. 15, Nr. 1, 2009; S. 119-141.

[BWT10] Becker, U.; Winter, M.; Tschöke, H.: Effiziente Minderung der Luftschadstoffemissionen des Verkehrs. In: (AVL Deutschland GmbH Hrsg.): Beiträge – 6. Internationales Forum Abgas- und Partikel-Emissionen, Ludwigsburg, 2010, S. 6-15

[Ev02] Evgeniou, T.: Information integration and information strategies for adaptive enterprises. In: European Management Journal, Vol. 20, Nr. 5, 2002; S. 486-494.

[Hu11] Hulstijn, J. et al.: Public Process Management – a method for introducing Standard Business Reporting. In: 12th Annual International Conference on Digital Government Research, Maryland, 2011.

[JWK10] Jurisch, M.; Wolf, P.; Krcmar, H.: Toward a formal approach to process bundling in public administrations. In: IFIP International Federation for Information Processing 2010, S. 412-423.

[Kr00] Krcmar, H. et al.: Informationssysteme für das Umweltmanagement – das Referenzmodell Eco-Integral. Oldenbourg Verlag, München Wien 2000.

[La05] Larman, C.: UML und Patterns angewendet- objektorientierte Softwareentwicklung. Mitp-Verlag, Heidelberg, 2005.

[LL69] Lawrence, P.; Lorsch, J.: Organization and Environment. Harvard Business School Press, Boston, 1969.

[LR00] Lucke, J.; Reinermann, H.: Speyerer Definition von Electronic Government – Ergebnisse des Forschungsprojektes Regieren und Verwalten im Informationszeitalter. Forschungsinstitut für öffentliche Verwaltung, Speyer, 2000.

[Ma02] Mayring, P.: Einführung in die qualitative Sozialforschung. Beltz Verlag, Weinheim / Basel, 2002.

[OAOJ] O.A.: Zahlen und Fakten zum Bürokratieabbau. In: http://www.bundesregierung.de/Content/DE/StatischeSeiten/Breg/Buerokratieabbau/zahlen-und-fakten-zum-buerokratieabbau.html, zugegriffen am: 18.08.2011.

[OA11] O.A.: Nationale Prozessbibliothek – Prozesstag für die öffentliche Verwaltung. In: Behördenspiegel, Vol. 27, Nr. 8, 2011, S. 16.

[Sc07] Schneider, C.: E-Government-Integration – Konzeption einer serviceorientierten Integrationsarchitektur zur Digitalisierung von Verwaltungsprozessen. OXYGON Verlag, Würzburg, 2007.

[Sh11] Sharafi, A.; Jurisch, M.; Ikas, C.; Wolf, P.; Krcmar, H.: Bundling Processes between Private and Public Organizations – a Qualitative Study. In: Information Resources Management Journal (IRMJ), Vol. 24, Nr. 2, 2011; S. 28-45.

[SK07] Scholl, H.; Klischewski, R.: E-Government integration and interoperability – framing the research agenda. In: Journal of Public Administration, Vol. 30, Nr. 8, 2007; S. 889-920.

[Um11] Umweltbundesamt: Luftbelastungssituation 2010 – vorläufige Auswertung. In: http://www.umweltdaten.de/publikationen/fpdf-l/4063.pdf, zugegriffen am: 24.07.201

[WJK10] Wolf, P.; Jurisch, M.; Krcmar, H.: Analyse und Design von Prozessketten. In: (Wimmer, M. et al. Hrsg): Vernetzte IT für einen effektiven Staat – Gemeinsame Fachtagung Verwaltungsinformatik (FTVI) und Fachtagung Rechtsinformatik (FTRI) 2010 - Proceedings. Lecture Notes in Informatics (LNI), Bonn, 2010; S. 29-40.

Fachkonzeptionelle Modellierung von Berichtspflichten in Finanzaufsicht und Verwaltung mit dem H2-Toolset

Jörg Becker, Ralf Knackstedt, Mathias Eggert, Stefan Fleischer

Westfälische Wilhelms-Universität Münster
European Research Center for Information Systems (ERCIS)
Leonardo-Campus 3, 48149 Münster
{vorname.nachname}@ercis.uni-muenster.de

Abstract: Bankrechtliche Meldepflichten sind nicht erst seit der Finanzkrise ein relevantes Forschungsfeld. Jedoch werden insbesondere Methoden zur Unterstützung eines rechts- und regelkonformen Berichtswesens derzeit in der Forschung unzureichend betrachtet. Mit der Entwicklung einer Methode zur Modellierung und Analyse von Berichtsregulierungen mit dem Fokus auf den Finanzsektor wird ein Weg aufgezeigt, um die rechtskonforme Berichtsgestaltung in Banken zu unterstützen. Die entwickelte Methode zeichnet sich insbesondere durch die Analysefähigkeit von Berichtskonstrukten aus, welche bei Modell- und Gesetzesänderungen Anwendung findet.

1 Management von Berichtspflichten in Finanzaufsicht und Verwaltung

Berichtspflichten werden vom Gesetzgeber in vielfältiger Weise auferlegt. Umweltinformationsgesetze (wie beispielsweise im Bundesland Nordrhein-Westfalen) sollen Bürger mittels Kennzahlen (zum Beispiel über den Zustand von Gewässern oder der Luft) über relevante Umwelttatbestände informieren. In der öffentlichen Verwaltung sind „Kennzahlen zur Zielerreichung zu bestimmen." § 11 Satz 1 Kommunalhaushaltsverordnung. Von Finanzdienstleistern verlangt das Gesetz nach dem Aufbau eines angemessenen Berichtswesens (vgl. zum Beispiel § 281 Abs. 3, Satz 1 SolvV). Relevante Regulierungen für das Berichtswesen finden sich in unterschiedlichen Quellen, was den Überblick über die einzuhaltenden Regulierungen besonders erschwert. Relevante Berichtsregulierungen des Finanzsektors werden beispielsweise formuliert in der Anzeigenverordnung, im Bundesbankgesetz, in der Groß- und Millionenkreditverordnung, im Investment- und Kreditwesengesetz oder in der Liquiditätsverordnung.

Der Beitrag diskutiert die Erweiterung bestehender Modellierungsansätze für das Berichtswesen, mit dem Ziel, die Gebundenheit des Berichtswesens an rechtliche Vorschriften zu explizieren und die daraus resultierende Modellbasis automatisiert auswertbar zu gestalten. In bestehenden Modellierungsansätzen werden diese Aspekte der Umsetzung regulatorischer Vorgaben im Berichtswesen nur unzureichend beachtet. Die

vorgestellten Erweiterungen tragen dazu bei, eine zeitnahe Reaktion auf sich ändernde Gesetze zu ermöglichen und nachweisen zu können. Dabei wird mit dem Finanzsektor als Anwendungsdomäne der am stärksten regulierte Bereich fokussiert [ASI10].

Die bestehenden Forschungsarbeiten werden zunächst erläutert (Abschnitt 2), bevor in einer argumentativen, auf Rechtsbeispielen basierenden Analyse die Anforderungen an eine innovative Methode entwickelt werden (Abschnitt 3). Die Umsetzung dieser Anforderungen erfolgt über die Adaption einer bestehenden Modellierungstechnik und funktionaler Erweiterung eines zugehörigen Modellierungswerkzeugs (Abschnitt 4). In weiterführenden Untersuchungen ist die Evaluation um abschließend erörterte, zusätzliche Aspekte zu ergänzen (Abschnitt 5).

2 Vorarbeiten

2.1 Bestehende Modellierungsmethoden zur fachkonzeptionellen Spezifikation im Data Warehousing

Die Rechtsmodellierung fokussiert sich derzeit vor allem auf die Modellierung von Verwaltungsprozessen [zum Beispiel AO05; FWB10] und Verträgen [zum Beispiel Ma10]. Ansätze zur Modellierung von Berichtspflichten und den damit verbundenen Data-Warehouse-Systemen werden unzureichend betrachtet. Klassische Ansätze der fachkonzeptionellen Modellierung von Data Warehouses lehnen sich eng an Modellierungssprachen an, wie zum Beispiel das Entity-Relationship-Modell [Ch76] oder die Objekttypenmethode [We81], die für die Fachkonzeption operativer Anwendungen etabliert sind, die auf relationalen Datenbanken basieren. Darüber hinaus wurden neue Modellierungstechniken entwickelt, die sich nicht an bestehenden anlehnen; ein anderer Entwicklungsstrang greift das Paradigma der objektorientierten Softwareentwicklung für die Fachkonzeption von Data-Warehouse-Systemen auf (vgl. [Bö01]).

Allen diesen Ansätzen gemeinsam ist, dass der Berichtsinhalt in Form eines mehrdimensionalen Raumes konzipiert wird, der durch Hierarchien von Bezugsobjekten (Produktgruppen, Regionen, Kunden et cetera) sowie Kennzahlen (Umsatz, Deckungsbeitrag et cetera) aufgespannt wird. Die Räume beschreiben die Datenbestände (zum Beispiel Umsätze bestimmter Produktgruppen et cetera), die das Berichtswesen insbesondere in Form von OLAP-Berichten auswertbar machen sollen (insbesondere Aggregation oder Disaggregation entlang der Hierarchien, sowie Bildung von Teilmengen des Datenbestandes). Die einzelnen Data-Warehouse-Modellierungstechniken, wie beispielsweise ME/RM [SBH98], ADAPT [Bu98] und DFM [GMR98], verwenden teilweise unterschiedliche Bezeichnungen für gleiche oder ähnliche Konstrukte. Zu den verbreiteten Unterschieden zählt, ob die Modellierung von Bezugsobjektinstanzen, durch die ausgedrückt werden kann, aus welchen Bezugsobjekten eine Hierarchiestufe konkret zusammengesetzt wird (zum Beispiel „Januar 2010“, „Februar 2010“ et cetera als Ausprägungen der Hierarchiestufe „Monat“) darstellbar ist. Auch unterscheiden sich die Ansätze darin, ob sie *Bezugsobjektattribute* abbilden, um beispielsweise für die Instanzen der Hierarchiestufe „Kunde“ Stammdaten, wie zum Beispiel „Adresse“, „Geburtsdatum“, definieren zu können, die im Rahmen der Berichterstattung abfragbar sein

sollen. Neben diesen Details sind sie sich in der Verfolgung der Metapher des aus Bezugsobjekten und Kennzahlen aufgespannten Datenraumes allerdings ähnlich.

Fortgeschrittene Ansätze wurden von *Goeken und Knackstedt* [GK08, GK09] sowie *Feja et al.* [FWB10] vorgeschlagen. *Goeken und Knackstedt* haben in ihrem Ansatz bereits erste Entwicklungen vorangetrieben, um Berichtsregulierungen für den Finanzsektor zu modellieren [GK08, GK09]. Dabei konnte gezeigt werden, dass Berichtsregulierungen, welche Banken im Rahmen der MiFID auferlegt wurden, über eine Spracherweiterung des ME/RM-Ansatzes modelliert werden können. Der Ansatz geht jedoch nicht auf die Annotation von Gesetzen und deren Analysierbarkeit ein. *Feja et al.* haben hingegen eine Spracherweiterung für die EPK entwickelt, welche die Annotation von Datenschutzanforderungen an Modellelemente erlaubt [FWB10]. Der Ansatz betrachtet schwerpunktmäßig die Prozessmodellierung. Beispielsweise wird die Kennzeichnung personenbezogener Daten erlaubt, was Folgen für deren weitere Nutzung hat [FWB10]. Offen hingegen bleibt die Modellierung konkreter Berichte auf Grundlage von gesetzlichen Bestimmungen. Sofern Dokumentenmanagement-Systeme die Zugriffs- und Nutzungskontrolle von Dokumenten und damit auch Berichten (im Sinne von *Müller et al.* [MAH10]) unterstützen, können auch sie als fortgeschrittener Ansatz bezeichnet werden. Eine fachkonzeptionelle Modellierung dieser Zugriffs- und Nutzungskontrollen von Berichten wird allerdings nicht adressiert.

Die vorgestellten Ansätze zeigen, dass der Bereich der Reporting-Compliance insgesamt und die Rechtsanalyse im Speziellen ein noch nicht stark betrachtetes Forschungsfeld darstellen. Der Forschungsfokus im Bereich des Compliance-Managements liegt auf der Prozessmodellierung und betrachtet die Compliance von Daten- und Berichtsmodellen nicht oder nur am Rande. Diese Forschungslücke zu adressieren, ist Ziel dieses Beitrags.

Zu einer wesentlichen Eigenschaft einer Modellierungstechnik zählt die Unterstützung durch ein Modellierungstool, ohne das eine adäquate Modellverwaltung nicht gewährleistet werden kann. Die Auswahl einer geeigneten Modellierungssprache und eines geeigneten Modellierungstools ist faktisch obligatorisch in einem Data-Warehouse-Projekt. Die bestehenden Modellierungstechniken unterscheiden sich insbesondere darin, inwieweit sie durch Modellierungswerkzeuge unterstützt werden. Während die Verwaltung in einem datenbankbasierten Repository automatisierte Analysen auf den Modellen ermöglicht, ist die Analysefähigkeit eingeschränkt, falls für die Modellierungstechnik zum Beispiel lediglich Symbolschablonen in einem grafischen Softwarewerkzeug, wie beispielsweise Visio, bereitgestellt werden. Die vorhandenen Modellierungsumgebungen beeinflussen dabei auch die Adaptierbarkeit einer Modellierungsmethode, um – wie in unserem Fall – die besonderen Anforderungen von gesetzlichen Berichtspflichten an die Modellierung erfüllen zu können.

2.2 H2 for Reporting als ausgewählte Modellierungsmethode

Die exemplarische Umsetzung der in diesem Beitrag vorgestellten Methode zur Modellierung und Analyse von Berichtsregulierungen wurde anhand der Modellierungssprache *H2 for Reporting* (H2fR) unter Verwendung und Erweiterung des Meta-Modellierungs-Werkzeugs *H2-Toolset* realisiert (vgl. [BFJ07]). Die Gründe für diese Entscheidung waren die folgenden:

- Die *Modellierungssprache* H2fR unterstützt die üblichen Elemente der Berichtsmodellierung. H2fR [BFJ07] zeichnet sich gegenüber anderen Modellierungstechniken dadurch aus, dass mit ihr neben dem auszuwertenden Datenraum auch die Tabellenstruktur beim Aufbau eines Berichts spezifiziert werden kann, die anschließend vom Benutzer gegebenenfalls weiter manipuliert wird (zum Beispiel in Form des Austauschs einzelner in der Tabelle angegebener Kennzahlen und in Form der üblichen OLAP-Operationen „slicing“, „dicing“ et cetera).
- Als *Meta-Modellierungs-Werkzeug* unterstützt das H2-Toolset neben der eigentlichen Modellierung von H2fR auch die Definition neuer sowie die Adaption bestehender Modellierungssprachen. Die bereits im H2-Toolset angelegte Sprache H2fR lässt sich somit werkzeuggestützt erweitern, um den zuvor identifizierten Anforderungen gerecht zu werden.
- Die *Plugin-Architektur* des H2-Toolsets ermöglicht zudem die flexible Erweiterung des Funktionsumfangs des H2-Toolsets. Import- und Exportschnittstellen, Analysewerkzeuge, Transformations- und Weiterverarbeitungsmechanismen stellen einen typischen Ausschnitt aus der Palette existierender H2-Toolset-Plugins dar. Ebenso die Analyse von Berichtsregulierungen lässt sich über ein in das H2-Toolset eingebundenes Auswertungs-Plugin realisieren, das auf Modellen der (entsprechend erweiterten) Modellierungssprache H2fR operiert.

Das Fachkonzept des softwarebasierten Meta-Modellierungs-Werkzeugs H2-Toolset ist vereinfacht in Abbildung 1 dargestellt. Als zentrales Konstrukt dient die Modellierungssprache, die durch eine Menge von Kontexten beschrieben wird. Die Kontexte sind der Sprache eindeutig zugeordnet und lassen sich als Menge von Vorschriften – sogenannte Kontextregeln – zur Modellerstellung interpretieren. Die Objekttypen einer Sprache bilden das Fundament eines jeden Modells, wobei die Struktur der Objekttypen zueinander über die Kontextregeln definiert wird. Objekttypen der Sprache H2fR sind Dimension, Bezugsobjekt, Dimensionsausschnitt, Kennzahl, Kennzahlensystem, Navigationsraum, Bericht, Zeile, Spalte, Filter, Faktberechnung und Berechnungsausdruck. Die konkreten Modellelemente stellen letztlich Ausprägungen (oder Instanzen) der Objekttypen dar und sind letzteren dementsprechend eindeutig zugeordnet. Beispiele für Ausprägungen des Objekttyps „Dimension“ sind Zeit, Produkt und Kunde. Die hierarchische Anordnung der Modellelemente in Unter- oder Überordnungen wird über die Modellstruktur abgebildet. Dabei entspricht diese Struktur den über die Kontextregeln spezifizierten Beschränkungen. Dies wird über Regelzuordnungen sichergestellt und dient nicht allein der syntaktischen Korrektheit des Modells: Die Regelzuordnungen geben ferner Aufschluss über den Kontext eines Modellausschnitts. Die Kontexte unterteilen demnach das Gesamtmodell in einzelne Ausschnitte, in denen die Modellelemen-

te je nach Kontextregeln jeweils unterschiedliche Unter- oder Überordnungen zueinander aufweisen können, und stellen somit verschiedene Perspektiven auf das Gesamtmodell dar.

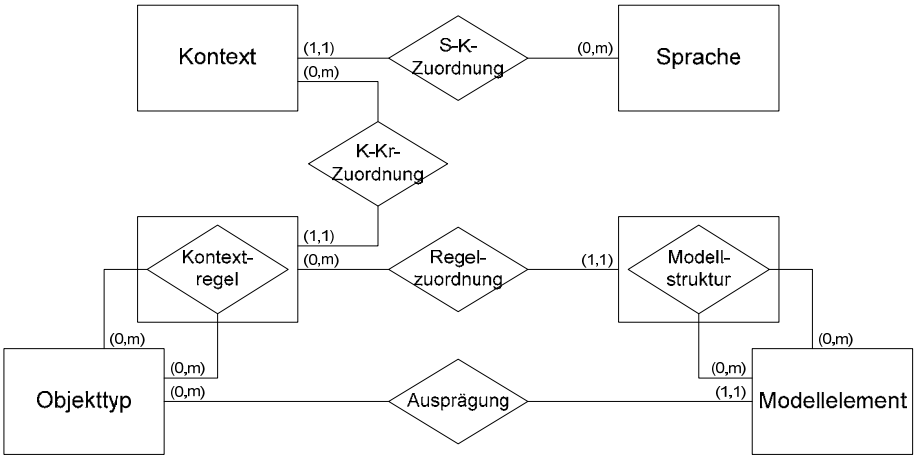

Abbildung 1: Fachkonzept des H2-Toolsets

Die Sprache H2fR wurde im H2-Toolset mittels der Kontexte „Dimensionen“, „Dimensionsausschnitte“, „Kennzahlen“, „Kennzahlensysteme“, „Navigationsräume“ und „Berichte“ definiert. Die Kontexte in ihrer Gesamtheit bilden die Sprachdefinition von H2fR. In Abbildung 2 ist entsprechend das Metamodell von H2fR dargestellt.

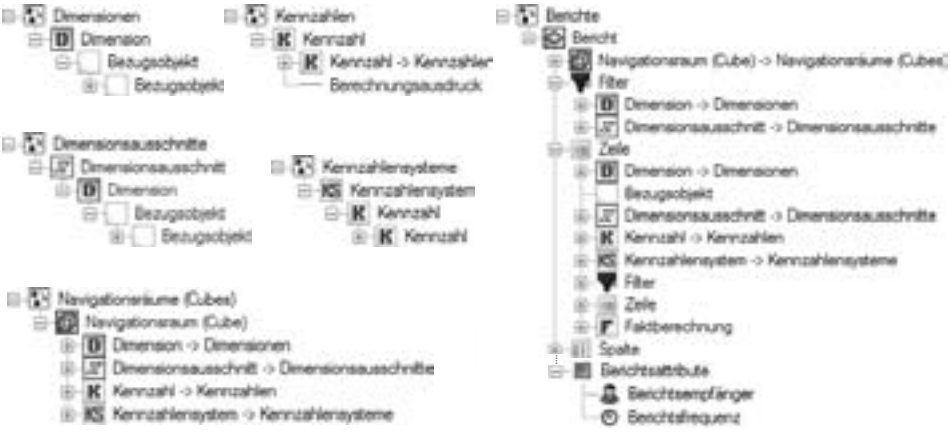

Abbildung 2: Definition der Modellierungssprache H2fR

Das Metamodell folgt der Metapher des Datenwürfels in Form von sogenannten Navigationsräumen (Cubes). Sie werden aufgespannt, indem einem Navigationsraum ein oder mehrere Dimensionen und Dimensionsausschnitte zugeordnet werden. Dimensionen stellen dabei Hierarchien von Bezugsobjekten dar. Dimensionsausschnitte sind genau einer Dimension zugeordnet. Sie entstehen, indem aus den Bezugsobjekten der Dimension eine Auswahl getroffen wird. Der Navigationsraum drückt aus, dass der durch Dimensionen und Dimensionsausschnitte aufgespannte mehrdimensionale Raum über Kennzahlen und Kennzahlensysteme ausgewertet werden soll. Für Kennzahlen lassen sich Berechnungsausdrücke vorgeben. Mehrere Kennzahlen lassen sich sachlogisch in hierarchischen Kennzahlensystemen gliedern. Der Navigationsraum entspricht damit der üblichen Modellstruktur, mit der im Data Warehousing fachkonzeptionelle Anforderungen definiert werden. Der Kontext „Berichte“ erweitert diese Spezifikationsmöglichkeiten, indem über Zeilen- und Spaltenkonstrukte das Layout einer Berichtstabelle definiert werden kann, die einen Ausschnitt aus dem gesamten Navigationsraum darstellt, den der Bericht analysierbar macht. Neben dem zugrundeliegenden Navigationsraum und den Zeilen- und Spaltenstrukturen kann auch ein Filter definiert werden, über den eine Datenteilmenge abgegrenzt werden kann, auf die sich die Informationsbasis der Berichtstabelle beschränken soll (zum Beispiel nur Daten eines bestimmten Jahres als Ausschnitt einer Zeit-Dimension). Darüber hinaus können die Berichtsempfänger und die Berichtsfrequenz als Berichtsattribute angegeben werden.

3 Anforderungsanalyse

Die fachkonzeptionelle Modellierung gesetzlicher Berichtspflichten soll ermöglichen, festzustellen, welche Berichtselemente aufgrund welcher Regulierungen eingeführt wurden oder durch welche Regulierungen bestimmte Berichtselemente legitimiert oder vorgeschrieben sind. Die Anforderungen an eine entsprechende Modellierungssprache werden im Folgenden argumentativ und anhand von Beispielen hergeleitet.

Der Begriff *Regulierung* wird im Folgenden für Gesetze, Richtlinien, Vorschriften und Empfehlungen et cetera verwendet, die in Unternehmen für die Gestaltung des Berichtswesens relevant sind. Bei den Regulierungen kann es sich entweder um *externe* oder um *interne* Regulierungen handeln. Externe Regulierungen werden Unternehmen in Form von Gesetzen und Verordnungen vorgeschrieben. Über die externen Regulierungen hinaus kann das Berichtswesen auch durch unternehmensinterne Vorschriften geregelt werden. Um den detaillierten Aufbau von Regulierungen beschreiben zu können, ist es notwendig, Regulierungen und Regulierungselemente zueinander in Beziehung zu setzen. Relevante *Typen* der *Regulierungselementbeziehungen* sind:

- *Setzt sich zusammen aus*: Mittels dieser Beziehung lassen sich die Gliederungen der Regulierungen und ihrer Elemente abbilden. Ein Gesetz gliedert sich beispielsweise in Paragraphen, die wiederum aus Absätzen bestehen, et cetera
- *Setzt um*: Diese Beziehung verdeutlicht, dass einzelne Regulierungen/ Regulierungselemente der Konkretisierung oder Umsetzung anderer Regulierungen/Regulierungselemente dienen. Über diesen Beziehungstyp lässt sich abbilden, dass nationale Gesetze Europäische Richtlinien umsetzen.

Ein weiterer viel versprechender Ansatz, die Verständlichkeit von Regulierungen zu erhöhen, besteht darin, die Regulierungen/Regulierungselemente gemäß ihrer *deontischen Funktion* zu klassifizieren (zur deontischen Logik vgl. [Ri01, Vw51]). Dieser Ansatz sieht vor, zu explizieren, ob es sich bei einem Regulierungselement um eine *Vorschrift*, ein *Verbot*, eine *Ausnahme* von einer Vorschrift oder eine *Erlaubnis* handelt. Regulierungselemente, die diesen deontischen Funktionen nicht zuordenbar sind, dienen der Definition, welche Sachverhalte unter einem bestimmten juristischen Begriff zu verstehen sind (*Qualifikation*) oder der Zuordnung von Befugnissen zu ausführenden Institutionen (*Macht*) (vgl. zu diesem Visualisierungsansatz Mahler [Ma10]).

Die Regulierungselemente sind Berichten und deren Elementen zuzuordnen. Der zugehörige Beziehungstyp wird *Gültigkeit* genannt und kann über Gültigkeitszeiträume und geographische sowie sektorale/branchenspezifische Einschränkungen näher beschrieben werden. Die zu beschreibenden Aspekte des Berichtswesens übernehmen wir von den etablierten Ansätzen der fachkonzeptionellen Modellierung von Data-Warehouse-Systemen (vgl. Abschnitt 2). Im Folgenden wird anhand der Solvabilitätsverordnung (SolvV) gezeigt, dass die jeweiligen Berichtselementtypen für die Rechtsanalyse des Berichtswesens relevant sind:

- *Bezugsobjekte:* § 2 Abs. 3, Satz 2 SolvV beschreibt Instanzen der „Marktrisikopositionen".
- *Dimension:* § 55 Abs. 2, Satz 1 SolvV: „Die IRBA-Positionen nach § 71 sind den IRBA-Forderungsklassen nach den §§ 73 bis 83 zuzuordnen." Eine IRBA-Forderungsklasse enthält dabei *n* IRBA-Positionen.
- *Bezugsobjektattribute:* § 334 SolvV: Institute müssen bei Verbriefungstransaktionen beispielsweise den Namen der bei der Verbriefung eingesetzten Ratingagentur offenlegen.
- *Kennzahl:* § 307 Abs. 3, Satz 1, Nr. 3 SolvV: "…Vermögensgegenstände und Verbindlichkeiten, der Nettoertrag und die Geschäftstätigkeiten …" müssen aus einem Bericht über Investmentanteile hervorgehen.
- *Kennzahlensystem:* In § 2 Abs. 2 SolvV werden die Voraussetzungen für die Erfüllung der Eigenkapitalanforderungen benannt. Um diese Anforderung modellseitig abzubilden, ist es erforderlich ein Kennzahlensystem zu erstellen.
- *Bericht:* Das Gesetz schreibt die Erstellung von konkreten Berichten vor. Ein Beispiel hierfür liefert § 335 Abs. 2 SolvV.
- *Berichtslayout:* Im Meldebogen 2 der Anlage 3 gefordert, dass die bilanziellen Adressenausfallrisikopositionen und Aufrechnungspositionen nach § 12 Abs. 2 SolvV zeilenweise dargestellt werden sollen.
- *Berichtsattribut:* In § 6 Abs. 1, Satz 1 SolvV: „Institute haben der Deutschen Bundesbank zu den Anforderungen nach § 2 Abs. 2 bis 4 und 6 […] Meldungen […] einzureichen". Der Berichtsempfänger „Bundesbank" ist hier eine Berichtseigenschaft.

Parallel zu der Modellierbarkeit der Berichtselemente, die durch die Berichtsregulierungen vorgegeben werden, muss ein adäquater Ansatz auch rechtsanalytische Auswertungen erfüllen können. Dabei ist die Analyse von Modellelementen, die von einer Regulierungsänderung betroffen sind, eine zentrale Anforderung (*Analyse aus Sicht der Gesetze*, *Typ 1*). Aus der Perspektive eines bestehenden Berichtswesens betrachtet muss eine Auswertung von Berichtsmodellen auch in die andere Richtung ermöglicht werden (*Analyse aus Sicht der Berichte*, *Typ 2*):

- *Analyse aus Sicht der Gesetze (Typ 1):* Eine dynamische Legislative, wie sie insbesondere im Finanzsektor anzutreffen ist, führt zu einer permanenten Änderung der Berichtsregulierung, was sich auf das Compliance-Management innerhalb von Unternehmen auswirkt. Es muss ständig sichergestellt werden, dass die Berichte den aktuellen gesetzlichen Vorgaben entsprechen, da anderenfalls eine strafbare Zuwiderhandlung erfolgt. Die Analyse von Modellelementen, welche von einer Regulierungsänderung betroffen sind, zu ermöglichen ist somit eine Analyseanforderung an Berichtsmodellanalyseansätze.
- *Analyse aus Sicht der Berichte (Typ 2):* Aus der Perspektive eines rechtskonformen Berichtswesens betrachtet, muss eine Auswertung von Berichtsmodellen auch in die andere Richtung ermöglicht werden. Ändern sich innerhalb des Unternehmens Berichtselemente, beispielsweise auf Grund von einer veränderten Kennzahlberechnung, so muss eine Ermittlung aller betroffenen Berichtsregulierungen ermöglicht werden, um die Rechtskonformität der Modelländerung überprüfen zu können. Folglich besteht eine weitere Analyseanforderung in der Auswertbarkeit der zu den Berichtsmodellelementen zugeordneten Berichtsregulierungen.

Darüber hinaus besteht noch eine Vielzahl weiterer Anforderungen an die Analysefähigkeit von Berichtsmodellen. Die Unterscheidung von internen und externen Berichtsregulierungen lässt Rückschlüsse auf den Verlauf der Regulierungsdichte zu. Je mehr externe Regulierungen durch interne ersetzt werden, desto konkreter werden die generischen gesetzlichen Anforderungen ausgelegt und damit individuell an das Unternehmen angepasst. Aus dem Verhältnis zwischen externen und internen Regulierungen wird somit deutlich, wie stark das Unternehme Gesetze interpretiert und umsetzt. Zudem kann durch die Erstellung von Berichtsmodellen mit Bezug zu Regulierungen die informationelle Basis geschaffen werden, um einen validen Vergleich der Regulierungsdichte von Branchen zu erstellen.

Die Durchführung dieser Analysen ist nur möglich, wenn entsprechende Informationen auch in den Modellen vorgehalten werden und das verwendete Modellierungswerkzeug entsprechende Analysefunktionalität unterstützt.

4 Methodenanpassung

In diesem Abschnitt wird die Modellierungssprache H2fR bezüglich der Abbildung und Analyse von Berichtsregulierungen auf Basis der identifizierten Anforderungen erweitert. Diese Erweiterung um entsprechende Sprachkonstrukte umfasst die folgenden fünf Aspekte:

- *Definition von Regulierungen:* Ein neuer grundlegender Kontext Regulierungen ermöglicht die Spezifikation von externen und internen Regulierungen sowie ihre Beziehungen zueinander. Hierfür wurde eine Menge neuer Objekttypen eingeführt, die neben einer allgemeinen Form der Regulierung jeweils unterschiedliche deontische Funktionen (Vorschrift, Verbot, Ausnahme, Erlaubnis) repräsentieren. Über den allgemeinen Objekttypen Regulierung werden Gesetze auf oberster Aggregationsstufe oder einzelne Definitionen (Qualifikation, Macht) abgebildet. Ferner lässt sich über einen neuen, speziellen Kantentypen „Setzt um“ die Konkretisierung oder Umsetzung einer Regulierung oder eines Regulierungselements abbilden. Der gewöhnliche, reguläre Kantentyp impliziert den Regulierungselementbeziehungstypen „Setzt sich zusammen aus“.
- *Definition von Gültigkeiten:* Die in dem neuen Kontext definierten Regulierungen lassen sich in den sechs bisherigen Kontexten referenzieren, um einen Bezug der Berichtselemente zu entsprechenden Gesetzen und Verordnungen et cetera herzustellen und somit die Anforderung der „Gültigkeit“ zu adressieren. Referenzierte Regulierungen im Kontext „Berichte“ bedeuten eine Regulierungsabhängigkeit der Berichtselemente bezüglich des jeweiligen Berichts (zum Beispiel die Ausweisung des Kundenkontos und des Kontostands nach § 9 Abs. 2 WpDVerOV). Referenzierte Regulierungen in einem der fünf übrigen Kontexte betreffen die Berichtselemente im allgemeinen Sinne. (zum Beispiel Identifizierungsmöglichkeiten von Kunden über den Namen oder Definition der Kennzahlen „Nettoertrag“ und „Verbindlichkeiten“).
- *Attribuierung von Gültigkeiten:* Ein neuer Objekttyp „Gültigkeitsattribut“ ermöglicht die Abbildung unterschiedlicher Behandlungen von Berichtselementen oder ganzen Berichten, zum Beispiel um zwischen Kreditinstituten und Finanzdienstleistungsinstituten oder zwischen Geschäftskunden und Privatkunden unterscheiden zu können. Für alle etwaig regulierungsabhängigen Modellelemente lassen sich Konfigurationsterme definieren. Letztere können ihrerseits wiederum mit Regulierungen in Relation gesetzt werden, um den Zusammenhang gesetzlich zu fundieren.
- *Attribuierung von Bezugsobjekten:* Ein neuer Objekttyp „Bezugsobjektattribut“ kann im Kontext „Dimensionen“ als Ausprägung an bestehende Bezugsobjekte modelliert werden, um einigen Gesetzen folgend das Vorhandensein oder die Zusammensetzung gewisser Daten abzubilden. Hierzu zählt beispielsweise die bereits angesprochene Identifizierungsmöglichkeit von Kunden. Modellele-

mente des neuen Objekttypen „Bezugsobjektattribut“ lassen sich ebenfalls mit Regulierungen in Beziehung setzen.

- *Attribuierung von Berichten:* Einige der bisher über Attribute realisierten Spezifika von Berichtsdefinitionen finden über die Ausprägung neuer Objekttypen Verwendung, um diese ebenfalls mit Konfigurationstermen und/oder Regulierungen in Relation setzen zu können. Dies betrifft insbesondere Berichtsempfänger, Periodizität (Frequenz, Frist oder auslösendes Ereignis) sowie Medium (oder Format), die nun als Modellelemente konkreter Bestandteil des Modells sein können.

Ein Ausschnitt der um den Aspekt der Berichtsregulierungen erweiterten Modellierungssprache H2fR ist in Abbildung 3 dargestellt, wobei die Erweiterungen mit grauen Ellipsen gekennzeichnet wurden.

In der Anforderungsanalyse (Abschnitt 3) wurden Typen von Analysen identifiziert, die im Rahmen des Compliance-Managements für das Berichtswesen von Bedeutung sind. Zu deren Umsetzung wurde ein Plugin für das H2-Toolset entwickelt. Dabei handelt es sich um ein generisches Analyse-Plugin, das nicht dediziert für die Analyse von Berichtsregulierungen konzipiert wurde. Es ist ein sprachunabhängig operierendes Auswertungswerkzeug, das zu einem gegebenen Modellelement alle verbundenen Modellelemente bezüglich eines oder mehrerer ausgewählter Objekttypen ermittelt und in einer Liste zusammenfasst. Die Analysen vom Typ 1 und Typ 2 können auf Basis dieses generischen Plugins realisiert werden. In Abbildung 4 ist die Analysefunktionalität exemplarisch dargestellt. Rechts in Abbildung 4 werden alle zu der Dimension „Kunde“ existierenden rechtlichen Verordnungen angegeben, links werden alle zu § 8 Abs. 2 WpDVerOV gehörenden Modellelemente angezeigt. Die Abfrageergebnisse werden jeweils dynamisch auf der Basis der Inhalte des Modells erzeugt.

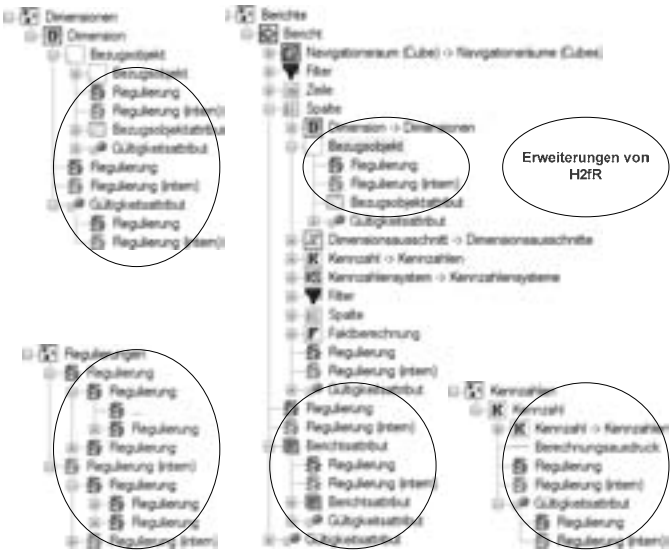

Abbildung 3: Definitionsausschnitt der erweiterten Modellierungssprache H2fR

Abbildung 4: Analyse aus Sicht der Gesetze (Typ 1) und Analyse aus Sicht der Berichte (Typ 2)

5 Zusammenfassung und Ausblick

Der Beitrag beschreibt einen Ansatz, um gesetzliche Grundlagen in Berichtsmodelle zu integrieren und diese Zusammenhänge auswertbar zu machen. Es wurde gezeigt, dass die durch das Metamodell beschriebene Datenbasis entsprechender Modelle unterschiedliche Analysen der gesetzlichen Regulierungen ermöglicht. Bisherige Modellierungstechniken haben ein Defizit hinsichtlich Darstellbarkeit und Auswertbarkeit von gesetzlichen Anforderungen. Diese Lücke zu schließen, ist Ziel der vorgestellten Methode.

Der Ansatz bedarf einer umfangreichen Evaluation, welche aus mehreren Schritten besteht. Neben der bereits erfolgten Umsetzung der exemplarischen Gesetzesmodellierung und ersten beispielhaften Analysen ist geplant, das Modell zu erweitern und in einer Praxisumgebung zu evaluieren. Die Relevanz in ersten Gesprächen mit Compliance-Experten im Finanzsektor wurde bereits bestätigt. In diesem Zuge gilt es, die Unterstützung des Compliance-Managements durch qualitative und quantitative Untersuchungen eingehend zu überprüfen. Geplant sind ferner eine Erweiterung um Überwachungsaspekte, wie sie im Ansatz von [FWB10] vorgestellt werden, eine Erweiterung hinsichtlich einer Nutzungskontrolle der Berichte, welche von [MAH10] gefordert wird, sowie eine Ausweitung der Analysemöglichkeiten. Über den Anwendungsfall im behördlichen Meldewesen hinaus lässt die Methode eine effizientere Berichtsgestaltung von Haushaltsplänen, Haushaltsabschlüssen und der Verwaltungssteuerung erwarten. Sowohl die erstellten Modelle als auch die adäquate Werkzeugunterstützung bilden einen Beitrag zum Compliance-Management im Reporting. Um in Zukunft Hypothesen zur Steigerung der Effizienz des Compliance-Managements und einer verbesserten Rechtskonformität im Berichtswesen aufstellen und evaluieren zu können, werden Methoden benötigt, die sowohl die Modellerstellung als auch die Modellanalyse aus der Rechtsperspektive ermöglichen. Die vorgestellte Arbeit bildet dafür eine unerlässliche Voraussetzung.

Literaturverzeichnis

[AO05] Alpar, P.; Olbrich, S.: Legal Requirements and Modelling of Processes in e-Government. The Electronic Journal of e-Government, 3 (3), 2005, S. 107-116.

[ASI10] Abdullah, N.; Sadiq, S.; Indulska, M.: Emerging Challenges in Information Systems Research for Regulatory Compliance Management. In Proceedings of the 22nd International Conference on Advanced Information Systems Engineering (CAiSE'10). Hammamet, Tunesien, 2010.

[BFJ07] Becker, J.; Fleischer, S.; Janiesch, C.; Knackstedt, R.; Müller-Wienbergen, F.; Seidel, S.: H2 for Reporting: Analyse, Konzeption und kontinuierliches Metadatenmanagement von Management-Informationssystemen. In (Becker, J.; Grob, H. L.; Hellingrath, B.; Klein, S.; Kuchen, H.; Müller-Funk, U.; Vossen, G. Hrsg.): Arbeitsberichte des Instituts für Wirtschaftsinformatik, Münster, 2007.

[Bö01] Böhnlein, M.: Konstruktion semantischer Data-Warehouse-Schemata. 1. Auflage Edition. Deutscher Universitäts-Verlag, Wiesbaden, 2001.

[Bu98] Bulos, D.: OLAP Database Design – A New Dimension. In (Chamoni, P.; Gluchowski, P. Hrsg.): Analytische Informationssysteme: Data Warehouse, On-Line Analytical Processing, Data Mining, Springer-Verlag, Berlin, 1998.

[Ch76] Chen, P. P.-S.: The Entity-Relationship-Model – Toward a Unified View of Data. ACM Transactions on Database Systems, 1 (1976), 1976, S. 9-36.

[FWB10] Feja, S.; Witt, S.; Brosche, A.; Speck, A.; C., P.: Modellierung und Validierung von Datenschutzanforderungen in Prozessmodellen. In Proceedings of the Fachtagung Verwaltungsinformatik und Fachtagung Rechtsinformatik (FTVI), LNI 162 GI 2010, 2010, S. 155-166.

[GK08] Goeken, M.; Knackstedt, R.: Referenzmodellgestütztes Compliance Reporting am Beispiel der EU-Finanzmarktrichtlinie MiFID. HMD – Praxis der Wirtschaftsinformatik, 263, 2008, S. 47-57.

[GK09] Goeken, M.; Knackstedt, R.: Multidimensionale Referenzmodelle zur Unterstützung des Compliancemanagements Grundlagen – Sprache – Anwendung. In Proceedings of the 9. Internationale Tagung Wirtschaftsinformatik. Wien, Austria, 2009, S. 359-368.

[GMR98] Golfarelli, M.; Maio, D.; Rizzi, S.: The Dimensional Fact Model – A Conceptual Model for Data Warehouse. International Journal of Cooperative Information Systems, 7 (2-3), 1998, S. 215-246.

[Ma10] Mahler, T.: Legal risk Management: Developing and Evaluation elements of a Method for Proactive Legal Analyses, With a Particular Focus on Contracts. PhD Thesis, Faculty of Law, University of Oslo, 2010.

[MAH10] Müller, G.; Accorsi, R.; Höhn, S.; Sackmann, S.: Sichere Nutzungskontrolle für mehr Transparenz in Finanzmärkten. Informatik-Spektrum, 33 (1), 2010, S. 3-13.

[Ri01] Risto, H.: Deontic Logic. In: (Goble, L. Hrsg.): The Blackwell Guide to Philosophical Logic, Blackwell, 2001.

[SBH98] Sapia, C.; Blaschka, M.; Höfling, G.; Dinter, B.: Extending the E/R Model for the Multidimensional Paradigm. In Proceedings of the International Workshop on Data Warehouse and Data Mining (DWDM'98). Singapur, 1998, S. 105-116.

[Vw51] von Wright, G. H.: Deontic Logic. Mind, 60 (237), 1951, S. 1-15.

[We81] Wedekind, H.: Datenbanksysteme I – Eine konstruktive Einführung in die Datenverarbeitung in Wirtschaft und Verwaltung. 2. Auflage Edition, Mannheim u. a., 1981.

Rechtsinformatik

Vier Augen, zwei Behörden und eine Technik für künftige Biometrie-basierte Kriminalitätsbekämpfung

Matthias Pocs

Universität Kassel
Projektgruppe verfassungsverträgliche Technikgestaltung
Wilhelmshöher Allee 64-66, 34109 Kassel
matthias.pocs@uni-kassel.de

Abstract: Biometrische Fahndungstechnik wird gegenwärtig erforscht. Sie verspricht, potenzielle Terroristen und andere Kriminelle aufzuspüren, aber birgt auch neuartige Risiken. Ein Szenario ist die vorsorgliche biometrische Datenerfassung, mit der Flugzeugabstürze und ähnliches aufgeklärt werden könnten. Um den Schutz des Grundrechts auf informationelle Selbstbestimmung sicherzustellen, schlägt dieser Beitrag eine Technikgestaltung für die Pseudonymisierung vor. Die Technikgestaltung soll eine sichere, offene, „smarte" und vernetzte Verwaltungskultur fördern.[12]

1 Einleitung

Polizeibehörden setzen schon gegenwärtig biometrische Technik ein. So hat zum Beispiel das Bundeskriminalamt die Gesichtserkennung getestet [BKA07], 2001 wurde in Tampa (Florida) ein Gesichtserkennungssystem eingesetzt [Ga10] und Iriserkennung wird routinemäßig beim Grenzübergang in die Vereinigten Arabischen Emirate genutzt [DM04]. Entsprechende Forschung wird gefördert, zum Beispiel Fingerspurenscanning an Gepäckstücken [Hi11], Gangerkennung [Bo11] und Verhaltensanalyse aus der Videoüberwachung [FP09].

Aufgrund dieser Entwicklungen ist es vorstellbar, dass künftig Gesetze erlassen werden, die eine vorsorgliche Datenerfassung - also vor Verursachung einer Gefahr oder Begehung einer Straftat - erlauben. Ein mögliches künftiges Szenario, in dem biometrische Daten von Bedeutung sind, könnte wie folgt aussehen: Am Flughafen könnten Gesichtsaufnahmen von Videoüberwachungskameras automatisiert erfasst werden. Sollte dann der Absturz des Flugzeugs herbeigeführt oder das Flugzeug entführt werden, könnten die vorsorglich erfassten Daten auf bereits bekannte Daten aus einer Datenbank (von Kontaktpersonen, Kriminellen oder ähnliches) durchsucht werden.

[12] Danksagung für die Anregungen zu technischen Aspekten an Maik Schott (Arbeitsgruppe Multimedia and Security, Otto von Guericke Universität Magdeburg).

Solche vorsorglichen Datenerfassungen stellen das Recht vor neue Herausforderungen [DPS11] [Po12] [Po11a] [Hi11] [HDP10], insbesondere weil biometrische Charakteristika (und damit personenbezogene Daten) erfasst werden, ohne dass der Betroffene einen Anlass dafür geschaffen hat, sowie eine Vielzahl von Personen davon betroffen ist. Dieser Beitrag untersucht daher, ob die Verfassung eine Regelung zur Pseudonymisierung vorschreibt und wie die Technikgestaltung konkret geregelt werden sollte. Er untersucht nicht das allgemeine Verhältnis zwischen den Zielen der Kriminalitätsbekämpfung und dem Eingriff in Grundrechte, sondern greift einen Vorschlag für die Technikgestaltung heraus. Die wissenschaftliche Leistung dieses Beitrags ist die Konkretisierung rechtlicher Anforderungen für eine verfassungsverträgliche Technikgestaltung anhand der spezifischen Technik der Pseudonymisierung.

Die untersuchte Pseudonymisierung beruht darauf, dass die Daten in sogenannten „Pseudoidentitäten“ und „Hilfsdaten“ zerlegt werden (mittels „Biometric Template Protection“) und nur die Datenschutzbehörde die Hilfsdaten aufbewahrt. Dadurch soll eine sichere, offene, ‚smarte‘ und vernetzte Verwaltungskultur gefördert werden: die „informationelle Gewaltenteilung“ schafft Transparenz und Kontrolle, Biometric Template Protection ist sicher und ‚smart‘ und für die Übermittlung der Hilfsdaten muss die Datenschutzbehörde mit der Polizei (monodirektional) eine vernetzte Architektur und organisationsübergreifende Prozesskette verfügbar sein.

Nach dieser Einleitung werden im zweiten Abschnitt die technischen Besonderheiten künftiger biometrischer Systeme und ein Szenario für den Systemeinsatz beschrieben. Im dritten Abschnitt wird untersucht, wie die besondere Technik der Pseudonymisierung rechtliche Ziele der Verfassung fördert. Im vierten Abschnitt werden Gestaltungsvorschläge für die Technik entwickelt, die für das spezifische Szenario der Kriminalitätsbekämpfung bestimmt ist. Im fünften Abschnitt schließt dieser Beitrag mit einem kurzen Fazit.

2 Künftige Biometrie und ihre Chancen und Risiken

Biometrische Anwendungen für die Kriminalitätsbekämpfung
Der Einsatz künftiger biometrischer Systeme für die Kriminalitätsbekämpfung stellt das Recht vor neue Herausforderungen, weil er sich vom Einsatz herkömmlicher Systeme zur biometrischen Zugriffs-, Zugangs-, Zutritts- und Ausweiskontrolle unterscheidet. Die künftigen Anwendungen zeichnet insbesondere aus, dass die biometrischen Charakteristika in unkontrollierten Umgebungen, in welchen der Betroffene nicht mitwirken muss, automatisiert erfasst werden.

Zunächst ist zwischen Mustererkennung einerseits und andererseits Biometrie im engeren Sinne zu unterscheiden. Bei Technologien der Mustererkennung (Optik, Photonik, Signalverarbeitung und so weiter) werden nur die rohen biometrischen Daten in Form von Bildern erfasst. Dazu gehören zum Beispiel Forschungsprojekte wie “Digi-Dak” [Hi11], bei denen die Spuren von Fingerabdrücken, die bei der Gepäckabfertigung an Koffern hinterlassen werden, gescannt werden. Hier ist ein automatischer Abgleich jedoch technisch nicht möglich. Bei Technologien der Biometrie im engeren Sinne

hingegen werden nicht nur Bilder erhoben, sondern auch Merkmale aus den Rohdaten extrahiert. Dadurch können erfasste Daten automatisiert mit biometrischen Referenzen abgeglichen werden. Der Ansatz der Biometric Template Protection damit der Technikgestaltung, die in diesem Beitrag vorgeschlagen wird, funktioniert nur bei Technologien der Biometrie im engeren Sinne.

Das für diesen Beitrag konkret zu realisierende Szenario kann dabei aus technischer Sicht, wie folgt beschrieben werden: Aufnahmen von Videoüberwachungskameras werden automatisiert auf Gesichter untersucht und vorsorglich erfasst. Dabei werden die Gesichter in Pseudoidentitäten (PI) (nach [BB08]) überführt. Die Hilfsdaten („Auxiliary Data"; nach [BB08]), also im simpelsten Fall die Systemparameter, unter denen die PI berechnet wurden oder ein kryptografischer Schlüssel oder ähnliches, werden ebenfalls gespeichert.

Anschließend werden die Hilfsdaten zu allen erstellten PI an einen Treuhänder, in diesem Fall eine Datenschutzbehörde, gesendet und für die Dauer eines Fluges verwahrt. Die PI werden für dieselbe Dauer bei der Polizeidienststelle hinterlegt. Sollte nun während des Fluges ein gesetzlich bestimmter Vorfall eintreten (herbeigeführter Absturz, Entführung, Reise von Mitgliedern der organisierten Kriminalität oder ähnliches), sollen die vorsorglich gespeicherten PI die Identifikation beteiligter, bekannter Krimineller ermöglichen. Dafür greift die Polizeidienststelle auf die biometrische Referenzdatenbank zu und erlangt Zugriff auf die zu den PI gehörigen Hilfsdaten von der Datenschutzbehörde. Nun erzeugt die Polizeidienststelle zu den Referenzdaten mittels der Hilfsdaten ebenfalls PI, welche dann mit den am Flughafen erfassten PI verglichen werden.

Die vorsorgliche biometrische Datenerfassung erweitert das bisherige polizeiliche Instrumentarium, da ihretwegen Daten zur Kriminalitätsaufklärung verfügbar werden. Ziel ist es, Hinweise zum Aufdecken von kriminellen Netzwerken zu gewinnen. Die Referenzen, mit denen die am Flughafen erfassten Daten verglichen werden, stammen aus einer früheren Sicherung von Gesichtsbildern an überwachten Orten und Erstellung von Lichtbildern von Kriminellen. Über die Orte und Kriminellen werden häufig kriminologische Profile erstellt. Im Fall der terroristischen und organisierten Kriminalität können solche Profile offenlegen, mit wem der Fluggast in Kontakt stand. Außerdem können sich Fluggäste in der Eingangshalle des Flughafens mit anderen Mitgliedern des kriminellen Netzwerks getroffen haben; dies legt auch offen, mit wem der Fluggast in Kontakt stand. Der Vorfall auf dem Flugzeug kann somit mit anderen Gesichtsbildern oder bekannten Kriminellen zusammenhängen.

Bisher sind rechtliche Regelungen zum Schutz von Personen, die von biometrischen Systemen betroffen sind, nur für die Verifikation (zum Beispiel für die Zutrittskontrolle), jedoch nicht für die Identifikation auf vorsorglich erfassten Daten für die Kriminalitätsaufklärung entwickelt worden. Dieser Beitrag untersucht einen bestimmten Schutzmechanismus und szenarienspezifische Maßnahmen. Durch die institutionelle Trennung zwischen Datenschutzbehörde und Polizei wird nicht nur das Schlüsselmanagement anspruchsvoll, sondern es muss auch die Systemadministration auf dieser Ebene diskutiert werden muss, damit die Polizei nicht etwa das Verschlüsselungs-

programm einseitig ändern kann. Die szenarienspezifischen Maßnahmen beinhalten unter anderem eine automatisierte Löschung nach Landung des Flugzeugs.

Rechtliche Chancen und Risiken
Der Einsatz von Systemen zur automatisierten Erfassung biometrischer Charakteristika zwecks Fahndungsabgleich bietet Chancen und birgt Risiken. Einerseits können mit dem Einsatz die Begehung von Straftaten und Verursachung von Gefahren verhindert werden. Andererseits birgt der Systemeinsatz spezifische Risiken [DPS11] [Po12] [Po11a] [Po11b] [Hi11] [HDP10]:

- Offenbarung sensibler Informationen aus Roh- und Template-Daten ([WP03], Nr. 3.7),
- Verknüpfung mehrerer Datenbanken zu einem Persönlichkeitsprofil aufgrund der Einzigartigkeit,
- … Universalität (jeder hat biometrische Charakteristika) und
- ... lebenslangen Gültigkeit biometrischer Charakteristika ([WP03], Nr. 3.2),
- Gewinnung von Informationen über Aufenthaltsort, Zeit und Zielort,
- Falschtreffer (es sei denn, der Abgleich ist im Ganzen zur Erfassung anlassbezogen),
- heimliche Datenerfassung (Fingerabdrücke und Gesichter hinterlassen Spuren ([WP03], Nr. 3.2)),
- unbefugter Datenzugriff („Identitätsdiebstahl“),
- zweckfremder Datenzugriff (zum Beispiel Ahndung von Ordnungswidrigkeiten oder Bildung von Profilen über Kontaktpersonen (ausführlich [Po11a]),
- Folgemaßnahmen durch die Polizei am Einsatzort sowie
- Sicherheitsparadox bei konkurrierenden Kontrollen.

Insbesondere ist zu befürchten, dass eine Vielzahl von Personen identifizierbar wird, ohne einen Anlass für die Datenerfassung geschaffen zu haben. Daher ist zu untersuchen, inwieweit das Grundrecht auf informationelle Selbstbestimmung Regelungen zur Pseudonymisierung von vorsorglich erfassten biometrischen Daten vorschreibt.

Verfassungsverträgliche Technikgestaltung
Wissenschaft und Technik können insbesondere durch Regelung der Technikgestaltung geleitet werden. Die Konkretisierung rechtlicher Anforderungen für eine verfassungsverträgliche Technikgestaltung (KORA) ist eine rechtswissenschaftliche Methode, um Vorschläge für die Technikgestaltung zu entwickeln. Dies zielt darauf ab, vorhersagbare Risiken der Technikanwendungen zu vermeiden und zusätzliche Chancen zu nutzen. Dazu werden konkrete Anforderungen für Techniksysteme von rechtlichen Vorgaben in einem bestimmten mehrstufigen Prozess abgeleitet.

Diese Stufen beinhalten die Ableitung (1.) rechtlicher Anforderungen aus rechtlichen Vorgaben, (2.) rechtlicher Kriterien aus diesen Anforderungen, (3.) technischer Ziele

aus diesen Kriterien und (4.) technischer Gestaltungsvorschläge aus diesen Zielen. Während die ersten beiden Stufen in der Sprache des Rechts geprüft werden, werden die beiden letzten Stufen in der Sprache der Technik geprüft [Ha93] [Pr11]. Daher müssen erst rechtliche Kriterien erforscht werden, um Gestaltungsvorschläge aus der Verfassung abzuleiten. Um den Rahmen dieses Beitrags nicht zu sprengen, werden die ersten beiden Stufen mit der rechtlichen Analyse (Abschnitt 3) zusammengelegt.

Die Kriterien sind allgemeingültig, weil sie aus der Verfassung - der höchsten deutschen Rechtsquelle - abgeleitet werden. Verträglichkeit technischer Systeme mit der Verfassung wird verbessert, wenn sie die Ziele der Verfassung fördern. Die Methode legt das Zusammenwirken von sozialen, technischen und rechtlichen Systemen zugrunde und zeigt Möglichkeiten, eine verfassungsverträgliche Technikgestaltung zu verwirklichen, in Zusammenarbeit mit Technikentwicklern, -betreibern und -nutzern [Pr11].

Die verfassungsrechtlichen Kriterien (Abschnitt 3) bilden den Stand der Rechtswissenschaft und folgen aus den Entscheidungen des Bundesverfassungsgerichts zum Grundrecht auf informationelle Selbstbestimmung und dem Datenschutzrecht, welches das Grundrecht näher bestimmt. Die Kriterien sind im Wesentlichen gleichrangig. Allerdings bietet die Rechtswissenschaft noch keine detailliertere Gewichtung der Kriterien; ein solches Verdienst war gerade der Grund für die Einführung der Methode KORA. Die wissenschaftliche Leistung dieses Beitrags ist die Konkretisierung rechtlicher Anforderungen. Anforderungen werden in diesem Beitrag für die spezifische Technik der Pseudonymisierung konkretisiert.

3 Verfassungsmäßigkeit der künftigen Biometrie

Die Rechtmäßigkeit künftiger biometrischer Systeme setzt voraus, dass die verfassungsmäßigen Anforderungen des Grundgesetzes erfüllt werden. Im Folgenden wird die Verfassungsmäßigkeit des Systemeinsatzes bezüglich der Zerlegung in PI und Hilfsdaten geprüft, um zu ermitteln, ob und welche Regelungen grundrechtlich gefordert sind und wie sie die Ziele der Verfassung fördert.

Im Folgenden wird untersucht, wie die spezifische Technik der Pseudonymisierung die Ziele der Verfassung fördert. Dazu wurde eine Fokussierung vorgenommen. Die Verfassungsmäßigkeit wird zwar in den rechtswissenschaftlich üblichen Schritten geprüft (Eingriff, Normenbestimmtheit, Erforderlichkeit, Verhältnismäßigkeit bezüglich des Gefühls des Überwachtwerdens und so weiter), aber nicht um allgemeine Fragen des Verhältnisses von (künftiger biometrischer) Überwachungstechnik zu Eingriffen in Persönlichkeitsrechte zu beantworten - dafür reicht der Rahmen dieses Beitrags nicht aus (einen Überblick geben [DPS11] [Po12] [Po11a] [Hi11] [HDP10]). Vielmehr greift dieser Beitrag einen einzelnen Aspekt der Technikgestaltung heraus und betrachtet nur diejenigen Kriterien, die mit der spezifischen Technik der Pseudonymisierung in Zusammenhang stehen.

Personenbezug
Ein künftiger Systemeinsatz und das ihn erlaubende Gesetz greifen in das Grundrecht auf informationelle Selbstbestimmung gemäß Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 Grundgesetz ein, weil personenbezogene Daten (biometrische und Fahndungsdaten) i. S. v. § 3 Bundesdatenschutzgesetz und Art. 2 Buchst. a i. V. m. EG 26 EU-Datenschutzrichtlinie verarbeitet werden. Für die Umkehrung der Pseudonymisierung ohne zweckgemäße Mitarbeit der Datenschutzbehörde dürfen insbesondere keine Mittel verfügbar sein, die vernünftigerweise entweder von der verantwortlichen Stelle oder von einem Dritten eingesetzt werden könnten, beziehungsweise muss der Aufwand an Zeit, Kosten und Arbeitskraft unverhältnismäßig groß sein. Ein Kriterium des Personenbezugs ist das Zusatzwissen (etwa über Gesichter und Fingerabdrücke in Fahndungs- und erkennungsdienstlichen Dateien).

Aufgrund der spezifischen Risiken des biometrischen Fahndungssystems ist die Pseudonymisierung auf hoher organisatorischer Ebene durchzusetzen, da die Stelle das Zusatzwissen nicht besitzen und auch nicht mit vertretbarem Aufwand erlangen darf. Eine rein innerbehördliche Lösung stellt eine Pseudonymisierung nicht sicher. Für die Stelle, die die PI speichert, wäre die Kooperation mit der Stelle, die die das Zusatzwissen hat, und andersherum dann nämlich nicht unverhältnismäßig aufwendig. Zudem sind die Daten bei einer rein innerbehördlichen Lösung für die Leitung der Behörde, deren Teil die verantwortliche Stelle ist, oder übergeordnete Behörden nicht pseudonym, weil beide Stellen von den Weisungen des Behördenleiters nicht völlig unabhängig sind.

Daher wird gefordert, die Datenteile in getrennten Dateien in unabhängigen öffentlichen Einrichtungen zu speichern (für dienst- und anschlussbezogene Daten der Vorratsdatenspeicherung [Zi09]). Idealerweise ist eine der Einrichtungen die Datenschutzbehörde, da sie im Lichte von Art. 28 EU-Datenschutzrichtlinie nicht nur von der Polizei unabhängig, sondern völlig unabhängig ist [Eu10]. Im Übrigen gilt das Prinzip der Datenvermeidung auch für die Datenschutzbehörde oder andere „Treuhänder“. Bei der Zerlegung in PI und Hilfsdaten verarbeiten - im Gegensatz zur Telekommunikation-Vorratsdatenspeicherung - weder die Polizei noch die Datenschutzbehörde personenbezogene Daten.

Normenbestimmtheit
Zudem muss das Gesetz Anlass, Zwecke und Grenzen des Zugriffs auf die vorsorglich erfassten biometrischen Daten festlegen [BV08(1)]. Zudem muss das Gesetz festlegen, dass die erfassten biometrischen Daten in PI und Hilfsdaten zerlegt und die Hilfsdaten der Datenschutzbehörde mittels Vernetzung zur exklusiven Aufbewahrung übermittelt werden.

Außerdem werden die biometrischen Roh- und Templatedaten gelöscht. Auch ohne solche Daten können kriminelle Netzwerke aufgedeckt werden. Zwar wären solche Daten für die Beweissicherung notwendig, aber der Systemeinsatz dient nicht dazu, revisionsfeste Beweise für Strafverfahren zu gewinnen, sondern wird nur durchgeführt, um Hinweise zu erlangen, mit denen kriminelle Netzwerke aufgedeckt werden können. Die Technikgestaltung wird so gewählt, dass so wenige Daten gespeichert werden, wie es die Zweckbestimmung erlaubt. Im Umkehrschluss muss das Gesetz auch festlegen, dass biometrische Treffer nicht als Beweis oder Indiz für Strafverfahren, sondern nur als

Anhaltspunkt verwertet werden, der die Eröffnung eines polizeilichen Ermittlungsverfahrens begründet.

Verhältnismäßigkeit
Die verfolgten Zwecke sind legitim, weil sie der Strafverfolgung und Gefahrenabwehr dienen. Der Einsatz ist zumindest nicht offensichtlich ungeeignet, wenn die Eingriffe im Einzelfall Erfolg haben können [BV09]. Wie die Kfz-Kennzeichenerfassung zeigt, ist die Übermittlung von Referenzen aus dem Zentralsystem in die Erfassungsgeräte nicht zu aufwendig [He07]; nichts Anderes kann für die Übermittlung der Hilfsdaten gelten. Auch etwa eine unzuverlässige Übermittlung der Hilfsdaten beseitigt die Eignung nicht, da die Eingriffe im Einzelfall Erfolg haben können. Im Gegenteil, die Tatsache, dass durch Zerlegung in PI und Hilfsdaten die technische Performanz gesteigert wird, spricht für die Eignung. Der Systemeinsatz kann erforderlich sein [BV08(2)]. Nur in solchen Fällen ist der Systemeinsatz zulässig. Die Frage kann offenbleiben, da jedenfalls die Pseudonymisierung die Erforderlichkeit nicht beseitigt.

Schließlich müssen der Grundrechtseingriff und die Zwecke, die mit dem Systemeinsatz erreicht werden sollen, miteinander abgewogen werden. In seiner Gesamtheit hat der Systemeinsatz ein hohes Eingriffsgewicht. Wie erwähnt wird im Falle nur geprüft, ob die Pseudonymisierung das Eingriffsgewicht verringert. Dafür werden die Kriterien, die das Bundesverfassungsgericht (für Überwachungstechniken) ausdrücklich anerkannt hat, betrachtet.

Streubreite
Ein Systemeinsatz hat eine hohe Streubreite (Vielzahl von Betroffenen, die keinen Anlass für die Datenverarbeitung geschaffen haben) [BV08(3)]. Die Streubreite wird auf ein Minimum verringert, wenn sich die Datenschutzbehörde erst beteiligen muss, bevor der Personenbezug hergestellt werden kann. Nicht die Gesamtheit aller Flüge in einem unbegrenzten Zeitraum ist betroffen, sondern nur ein einziger Flug.

Transparenz
Das System muss transparent und kontrollfähig sein. Eine solche Systemtransparenz kann unterschiedlich fortgeschritten gestaltet werden. Die erste Stufe der Systemtransparenz wird durch die Beteiligung von Datenschutzbehörden erreicht. Daher wird die Datenschutzbehörde in der EU-Datenschutzrichtlinie über Art. 18, 20, 22 und 28 Abs. 3 beteiligt. Für Fahndungsmaßnahmen ist typisch, dass Transparenz gegenüber den Betroffenen und die Betroffenenrechte beschränkt werden müssen; daher ist die unabhängige Kontrolle durch die Datenschutzbehörden umso wichtiger [BV01].

Eine zweite Stufe ist die Beteiligung eines unabhängigen „Treuhänders“, nach der eine Datenverwendung nur unter Mitwirkung dieser Stelle möglich ist. So ist zum Beispiel bei der Telekommunikation-Vorratsdatenspeicherung verfassungsrechtlich anerkannt, dass die Trennung der Speicherung durch private Telekommunikationsunternehmen und des Abrufs durch Polizeibehörden Transparenz und Kontrolle der Datenverwendung fördert [BV10(1)]. Vereinzelt wird auch für die Fingerabdruckidentifizierung vorgeschlagen, dass das AFIS statt bei der Polizei bei einer „informationellen Verrechnungsstelle“ verwaltet wird und der Polizei nur im Trefferverfahren die Entscheidung über die

Übereinstimmung einer Fingerabdruckspur und Referenz mitgeteilt wird [Wo03]. Dies erinnert an die Praxis von Eurodac, nach der die Meldebehörden nur im Trefferfall Asylbewerber identifizieren kann.

Eine dritte Stufe der Beteiligung ist, wenn weder der Datenverwender noch der „Treuhänder" personenbezogene Daten speichert. Dies folgt insbesondere aus dem Systemdatenschutz. Danach wird die das System kontrollierende Stelle von der es anwendenden Stelle institutionell getrennt. Die kontrollierende Stelle trägt die technische Verantwortung, indem sie das System zugriffsbereit hält und die Einhaltung der Systemvorschriften sicherstellt. Sie kann auf die personenbezogenen Daten jedoch nicht zugreifen. Die das System anwendende Stelle trägt die fachliche Verantwortung und verarbeitet die personenbezogenen Daten. Um Berechtigungen des Zugriffs auf bestimmte Daten zu erhalten, müssen sie erst bei der unabhängigen Einrichtung, die die technische Verantwortung über das System trägt, beantragt werden [Po76].

Die Pseudonymisierung mittels exklusiver Aufbewahrung der Hilfsdaten bei der Datenschutzbehörde schafft die fortgeschrittenste Stufe der Systemtransparenz und hebt somit das Prinzip der Transparenz auf ein besonders hohes Niveau. Die Technikgestaltung bietet damit die beste Gewähr, dass offengelegt wird, in welchen Fällen der Personenbezug hergestellt wird und somit einzelne Personen polizeilichen Maßnahmen ausgesetzt werden können.

Gefühl des Überwachtwerdens
Der Systemeinsatz könnte auch ein Gefühl des Überwachtwerdens hervorrufen. Ein solches Gefühl kann durch eine hohe Streubreite geschaffen werden [BV08(4)]. Im Umkehrschluss bedeutet dies, dass mit der spezifischen Technik der Pseudonymisierung nicht nur eine hohe Streubreite vermieden wird, sondern auch - begünstigt durch eine vertrauenswürdige Datentrennung auf hoher institutioneller Ebene - die Möglichkeit des Gefühls des Überwachtwerdens verringert wird.

Verhaltensanpassung
Darüber hinaus könnte der Grundrechtseingriff aufgrund des Systemeinsatzes dazu führen, dass Betroffene ihr Verhalten anpassen. Ein solcher Eingriff entspricht funktional Eingriffen in andere Grundrechte [BV08(5)]. Mit der spezifischen Technik der Pseudonymisierung können Betroffene darauf vertrauen, dass sie personenbezogenen Maßnahmen durch die Polizei oder personenbezogenen Nachteilen aufgrund von „Identitätsdiebstahl" nicht ausgesetzt werden. Daher werden die Möglichkeit von Eingriffen in andere Grundrechte und eine Verhaltensanpassung verringert.

Datensparsamkeit
Jede Gestaltung einer Technik, die zur Zweckerreichung geeignet ist, kann am Ziel [BV10(2)] ausgerichtet werden, keine personenbezogenen, sondern nur pseudonymisierte Daten zu verarbeiten und die Datenteile auf (völlig) unabhängige Einrichtungen zu verteilen. Auch der Treuhänder, die Datenschutzbehörde, erhält und verarbeitet keine personenbezogenen Daten.

Zweckbindung
Das Prinzip der Zweckbindung wird durch das Prinzip der informationellen Gewaltenteilung konkretisiert [BV83]. Dieses Prinzip ist verfassungsrechtlich anerkannt [BV83] [De85] [Si84] [He90] [Po83] [Di00] und in § 9 Satz 1 i. V. m. Nr. 8 der Anlage des BDSG ausgedrückt. Das Prinzip der informationellen Gewaltenteilung verlangt insbesondere von der Behörde oder dem Behördenteil, ihren beziehungsweise seinen Aufgabenbereich mit dem jeweiligen Datenbestand von dem Aufgabenbereich anderer Behördenteile zu trennen. Das Prinzip folgt aus dem Systemdatenschutz. Ursprünglich meinte das Prinzip der informationellen Gewaltenteilung die Trennung der das System kontrollierenden Stelle von der es anwendenden Stelle (siehe oben).

Dieser ursprüngliche Begriff der informationellen Gewaltenteilung gilt insbesondere für vorsorglich erfasste Daten. Solche Daten zeichnet aus, dass sie nur ausnahmsweise für die Zweckerfüllung benötigt werden. Daher ist bezüglich des Großteils der Daten festzustellen, dass die Datentrennung den Personenbezug verhindert. Die Behörden können nicht ohne Mitarbeit der jeweils anderen Behörde personenbezogene Daten verarbeiten. Dies fördert das Prinzip der informationellen Gewaltenteilung und Zweckbindung.

Datensicherheit
Neben unbefugten Zugriffen auf die Datenbank bei der Polizei sind auch unbefugte Zugriffe auf die Datenbank der Datenschutzbehörde denkbar, die durch die Zerlegung der Daten in PI und Hilfsdaten ausgeschlossen wird. Die Zerlegung der Daten in PI und Hilfsdaten erfüllt die Vorgabe des Vier-Augen-Prinzips, der asymmetrischen Verschlüsselung und des Need-To-Know-Prinzips und ermöglicht eine revisionssichere Protokollierung [BV10(3)]. Insbesondere das Vier-Augen-Prinzip wird erfüllt, nach dem zwei Personen nur gemeinsam berechtigt sein sollen, auf riskante Daten zuzugreifen, und einander somit kontrollieren können.

Jeder Datensatz wird mit einem eigenen Schlüssel erzeugt. Daher bietet die Pseudonymisierung gegenüber dem allgemeinen Zugriffsschutz den Vorteil, dass ein erfolgreicher Angriff auf einen Schlüssel nicht den Zugriff auf alle Datensätze ermöglicht, sondern nur auf einen Datensatz. Der Aufwand, um auf die Vielzahl der Datensätze zuzugreifen, wird entsprechend vergrößert.

4 Technikgestaltung: Template Protection für die künftige Biometrie

Wie bereits zuvor erwähnt, soll in diesem Beitrag ein Konzept vorgeschlagen werden, dass mithilfe der „Biometric Template Protection“ und vorsorglicher biometrischer Datenerfassung eine Identifikation (im Gegensatz zur Verifikation) erlaubt. Wie ein solches biometrie- und kryptoprotokollbasiertes Konzept grundsätzlich arbeiten kann und welche speziellen Herausforderungen bei der konkreten Implementation der entsprechenden Algorithmen zu bewältigen sind, kann in [UU04] nachgelesen werden. Die hier vorgestellte technische Betrachtungsweise bezieht sich dabei eher auf die Anforderungen eines komplexen Systems in einem bestimmten Szenario (siehe Abschnitt 2), das ein solches Konzept als Basis verwendet. Die korrekte und sichere Funktionsweise des

ausgewählten Ansatzes zur „Biometric Template Protection“ wird als vorausgesetzt angesehen.

Gesichtserfassung
Erster Schritt für die Erzeugung sämtlicher gewünschter PI ist die Erfassung der Gesichtsdaten aus den Aufnahmen der Videoüberwachungskameras. Außerdem sollte die Gesichtserfassung nicht direkt durch eine Stelle übernommen werden, die gleichzeitig auch direkten Zugriff auf die biometrische Referenzdatenbank besitzt. Das bedeutet, selbst wenn die Gesichtserfassung durch eine Polizeistelle durchgeführt wird, darf ihr nicht gleichzeitig auch ein Zugriffsrecht auf die bei der Polizei gespeicherten biometrischen Daten eingeräumt werden. Erst die Stelle, die die PI zugesandt bekommt, hat dann auch Zugriffsrecht auf die entsprechende Referenzdatenbank, darf allerdings im Gegensatz zu der Daten erfassenden Stelle wiederum keinen Zugriff auf die (nicht dauerhaft) gesicherten Rohdaten erlangen.

Sind die biometrischen Daten erfasst, muss daraufhin eine Merkmalsextraktion durch das System durchgeführt werden, um aus den so erlangten Merkmalsvektoren die eigentlichen PI erzeugen zu können. Für das dafür spezifisch genutzte Verfahren gibt es unterschiedliche Ansätze. Grundsätzlich entsprechen die „Biometric Template Protection“ Systeme aber immer den in [BB08] definierten Architekturen. Dabei wird üblicherweise eine biometrische Authentifizierung ermöglicht, ohne dabei aber tatsächliche biometrische Rohdaten, das heißt Daten, die direkt Auskunft über die Eigenschaften des zugrunde liegenden biometrischen Charakteristikums geben, in irgendeiner Form abspeichern zu müssen. Dabei wird ein im Enrolment aufgenommener Merkmalsvektor eines biometrischen Charakteristikums mithilfe von bestimmten Hilfsdaten in eine pseudonymisierte, digitale Repräsentation übertragen. Die Hilfsdaten selbst können dabei, abhängig von der Implementation, unterschiedlichster Art sein. So sind diese Hilfsdaten im einfachsten Fall, wie in [GK06], schlicht die Systemparameter, unter denen das System die PI berechnet hat oder aber auch echte kryptografische Schlüssel, wie zum Beispiel in [BSW07]. Zusätzlich dazu könnte bei einem System, in dem der zur Berechnung der PI verwendete Algorithmus austauschbar ist, noch zusätzlich ein Identifikator für diesen mit in die Hilfsdaten eingefügt werden.

An dieser Stelle ist es wichtig zu erwähnen, dass aus der PI keinerlei Informationen über das tatsächliche, zugrunde liegende biometrische Charakteristikum ableitbar sind. In einem System zur Verifikation würden dann die PI und die dazugehörigen Hilfsdaten auf einem geeigneten Medium zusammen abgespeichert werden. Die Merkmalsvektoren der erfassten biometrischen Merkmale werden dann sicher gelöscht (auch der Arbeitsspeicher sollte ausreichend klein sein).

Dieser Teil des grundsätzlichen Ablaufs der „Biometric Template Protection“ entspricht für das hier vorgeschlagene System auch größtenteils der allgemeinen Architektur nach [BB08]. Der einzig gravierende Unterschied für die vorsorgliche biometrische Datenerfassung besteht darin, dass die erzeugten PI und die dazugehörigen Hilfsdaten nicht zusammen abgespeichert werden. Die PI gehen dabei sicher digital signiert und ver-

schlüsselt an die Polizei, wohingegen die dazugehörigen Hilfsdaten ebenso digital signiert und verschlüsselt an die Datenschutzbehörde übertragen werden.

Die PI und Hilfsdaten bleiben nun für eine feste Zeitspanne bei den entsprechenden Instanzen abgespeichert, bis sie automatisiert gelöscht werden sollten. Die Zeitspanne sollte die tatsächliche Flugdauer und einen weiteren Tag umfassen, damit die Polizei etwaige Maßnahmen zur Sicherung der Fluggäste oder anderen Betroffenen und danach der Informationssicherung ergreifen können. Hinzu kommt die Dauer für den Aufenthalt im überwachten Raum, bevor Fluggäste einchecken und an Bord gehen. Aus Gründen der Effektivität des Rechtsschutzes sollte nicht eine von anderen Variablen abhängige (tatsächliche Flugdauer), sondern eine einheitliche Zeitspanne (zum Beispiel fünf Tage) gewählt werden.

Identifikation
Sollte es nun notwendig werden, die vorsorglich erfassten Gesichter auf mögliche Übereinstimmungen mit biometrischen Referenzdaten zu untersuchen, müssen dafür die zuvor separierten PI und die dazugehörigen Hilfsdaten wieder zusammengeführt werden. Zu diesem Zweck müssen die bei der Datenschutzbehörde gespeicherten Hilfsdaten an die untersuchende Polizeistelle übersendet werden. Diese wäre dann in der Lage, mithilfe der Hilfsdaten PI zu den biometrischen Referenzdaten zu berechnen. Kann eine solche neu berechnete PI auch in dem von Flughafen erzeugten Datensatz ausfindig gemacht werden (Zuordnung), ist die Wahrscheinlichkeit hoch, dass der jeweilige Verdächtige zum betrachteten Zeitpunkt von der Kamera aufgenommen worden ist.

Nur diejenigen PI und Hilfsdaten dürfen zusammengeführt werden, die mit dem gesetzlich bestimmten Vorfalls während eines Flugs im Zusammenhang stehen. Um dies feststellen zu können, müssen daher Metadaten über die Kamera, die Zeit und gegebenenfalls den Flug mit den PI und Hilfsdaten in einem Datensatz/-Format erhoben und gespeichert werden. Aufgrund der unterschiedlich hohen Streubreite sollte auch festgehalten werden, ob sich die Kamera am jeweiligen Gate (welcher gezielt mit dem Flug im Zusammenhang steht) oder in der Eingangshalle des Flughafens befindet.

Nachdem die PI zu den Referenzdaten erfolgreich berechnet worden sind, sind die Hilfsdaten frühestmöglich zu löschen. Die Hilfsdaten ermöglichen es der Polizeistelle, in Zukunft erhobene biometrische Daten mit gespeicherten Daten abzugleichen mit der Folge, dass dem Betroffenen zusätzliche Informationen (Flugzeit und -ziel beziehungsweise Kriminalhistorie und Fahndungsausschreibung) zugeordnet werden können. Dies ist nicht von der gesetzlichen Zweckbestimmung gedeckt. Daher müssen die Hilfsdaten gelöscht werden, sobald die Datensätze erfolgreich abgeglichen worden sind, oder gar nicht erst offenbart werden. Dies könnte zum Beispiel mittels eines geschützten „Match-On-Card“-Systems realisiert werden, das die Hilfsdaten geheim hält, den Abgleich durchführt und dem Systembediener nur die Zuordnung mitteilt.

Infrastrukturbetrachtungen
Um das vorgeschlagene System und vor allem die im nächsten Unterabschnitt vorgeschlagenen Sicherheitsmechanismen auch realisieren zu können, sind grundsätzlich auch einige infrastrukturelle Gegebenheiten notwendig. So ist für die Sicherung der

digitalen Kommunikation inklusive des sicheren Schlüsselaustauschs und der digitalen Signatur grundsätzlich eine „Public-Key-Infrastructure“ (PKI) empfehlenswert, mithilfe deren eine Zertifizierung der zur Kommunikation verwendeten Schlüssel überhaupt erst möglich wird.

Da zu erwarten ist, dass die zur Berechnung der PI genutzte Applikation über die Zeit gesehen häufiger einer Versionsaktualisierung unterzogen wird, muss auch grundsätzlich eine zentrale Versionsprotokollierung und -verwaltung durchgeführt werden. Diese dient dem Zweck der vollständigen Nachvollziehbarkeit aller Programmänderungen und der Archivierung von nicht aktuellen Versionen, die notwendig sein könnten, um Datensätze älterer Versionen korrekt verarbeiten zu können. Da die Daten erfassenden und verarbeitenden Instanzen - aus offensichtlichen Gründen - keine Möglichkeit zur Abänderung oder Vervielfältigung der verwendeten Anwendungen besitzen sollten, müsste diese Aufgabe durch eine zusätzliche Instanz ohne Zugriffsrecht auf personenbezogene Daten ausgeübt werden, deren Abänderungen aber trotzdem systemglobal verifiziert werden sollten.

Um alle Vorgänge im System auch zeitlich erfassen zu können, muss in jedem Fall auch ein zentraler vertrauenswürdiger Zeitgeber/-dienst verfügbar sein, der für alle Instanzen eine systemglobale Zeitmessung ermöglicht. Außerdem wird dieser Zeitgeber ebenfalls benötigt, um die Einhaltung der Speicherfristen für alle Instanzen überprüfbar und ausführbar zu realisieren. Für die notwendigen vertrauenswürdigen Zeitstempel das die Daten zu einem konkreten Zeitpunkt vorlag kann das Time-Stamp Protocol (RFC 3161) verwendet werden, das garantiert das Daten vor einem bestimmten Zeitpunkt vorlagen und nicht erst später hinzugekommen sind.

Sicherheitsmechanismen
Im Rahmen des vorgestellten Systems ist es notwendig, verschiedenste Sicherheitsmechanismen zu realisieren, die die sichere Kommunikation und Speicherung gewährleisten.

Der erste Teil in diesem System, der unter allen Umständen durch verschiedene Sicherheitsmechanismen geschützt werden muss, ist die Erfassung der biometrischen Gesichtsdaten vor der Verarbeitung zu den entsprechenden PI. An dieser Stelle ist es essenziell, dass die aus einem Gesichtsdatensatz extrahierten Merkmalsdaten unmittelbar nach der Erzeugung der entsprechenden PI vollständig und forensisch sicher gelöscht werden, um sicherzustellen, dass zu einem späteren Zeitpunkt eine Rekonstruktion des biometrischen Charakteristikums oder Teilen davon ausgeschlossen werden kann.

Da die erzeugten PI und die dazugehörigen Hilfsdaten zwischen den Instanzen kommuniziert werden, sind natürlich grundsätzliche integritäts- und authentizitätssichernde Maßnahmen zu ergreifen. Das bedeutet, die PI und Hilfsdaten werden grundsätzlich nur digital signiert zwischen den Instanzen kommuniziert. Prinzipiell enthalten die Daten für einen potenziellen Angreifer ohne Zugriff auf die Referenzdaten zwar keinen wirklichen Informationsgehalt, bei einer Anwendung mit dieser datenschutztechnischen Relevanz sollten die Daten jedoch nur verschlüsselt kommuniziert werden.

Die Speicherung der Daten bei der entsprechenden Instanz sollte dann ebenfalls nur in verschlüsselter Form erfolgen, um mehrere verschiedene Sicherheitsaspekte abzusichern. Zum einen ist das Schutzziel der Verschlüsselung an dieser Stelle natürlich die Vertraulichkeit. Wie zwar bereits erwähnt bieten die PI sowie die Hilfsdaten allein keinen wirklichen sensiblen Informationsgehalt, sollten aber trotzdem geschützt werden. Innentäter könnten nämlich die PI und Hilfsdaten wieder zusammenführen. In diesem Sinne ist es zudem notwendig, dass PI und Hilfsdaten mit unterschiedlichen Schlüsseln verschlüsselt werden. Rein aus Gründen der Performanz wäre es an dieser Stelle sinnvoll, einen symmetrischen Verschlüsselungsalgorithmus für die Sicherung der gespeicherten Daten zu nutzen. Das zweite Schutzziel, das die Verwendung von kryptografischen Protokollen an dieser Stelle verfolgt, ist die Absicherung gegen unberechtigte Veränderung, also die Integrität der gespeicherten Daten. Dafür kann implizit die Verschlüsselung genutzt werden, da nach einer Modifikation der (verschlüsselten) Daten, die Entschlüsselung ungültige Werte beziehungsweise Datenstrukturen zurückgibt. Dies setzt jedoch die Verwendung von Datenformaten voraus bei denen derartige Fehler erkannt werden können. Besser wäre eine digitale Signatur, mit der in jedem Fall Veränderungen erkannt werden können. Aus beiden Gründen muss die Zugriffskontrolle auch die Authentizität natürlicher Personen kontrollieren (zum Beispiel passwortbasierte personengebundene Zugriffsrechte).

Die beiden Verschlüsselungsschritte - zum einen für die Kommunikation und zum anderen für die Speicherung - sollten zusammengefasst werden, damit die Daten zu keinem Zeitpunkt im Klartext vorliegen. Dem kann entgegengewirkt werden, indem die Daten vor der Kommunikation verschlüsselt werden, wodurch eine dann zusätzliche Verschlüsselung auf Transport- oder Anwendungsschicht nicht mehr notwendig ist und diese verschlüsselten Daten dann so wie sie sind gespeichert werden. Zudem spart dies einen Verschlüsselungsdurchgang.

Bezüglich der digitalen Signaturen ist zu beachten, dass für jede Signatur eine zeitaufwendige asymmetrische Verschlüsselung notwendig ist, sowie je eine Kommunikation mit dem Zeitdienst für den Zeitstempel. Bei einer sehr großen Anzahl an Daten kann dies reduziert werden, in dem die Daten in Gruppen eingeteilt und über diese Gruppen, evtl. mit Hilfe von Hashbäumen, die Signatur berechnet wird (RFC 4998).

Ein weiterer Mechanismus, der um das gesamte System gespannt werden sollte, ist eine lückenlose Protokollierung sämtlicher im System ablaufender Vorgänge. Dies umfasst natürlich die ausreichend detaillierte Beschreibung dieser Vorgänge sowie ihre Chronologie. Dabei wäre es denkbar, die Kommunikation zwischen den Instanzen durch unabhängige, automatische, nicht abschaltbare, lokale Protokollierung bei jeder Instanz zu dokumentieren. Sollte es dann notwendig werden, diese Protokolle auszuwerten, kann über eine Konsistenzprüfung aller lokalen Protokolle, also einem Vergleich aller Protokolle miteinander, ihre globale Richtigkeit überprüft werden. Außerdem könnten die Protokolldaten direkt in einem Datensatz mit den signierten biometrischen Daten gespeichert werden.

Um die Gesichtserfassung an sich protokollieren zu können, bleibt ebenfalls nur die Möglichkeit einer fest implementierten, nicht abschaltbaren, automatischen Protokollierung nach der Erfassung jedes Gesichts. Das Gleiche gilt für die Abänderung und Aktualisierung der verwendeten Applikationen.

Die Sicherheit sämtlicher digitaler Signaturen und Verschlüsselungen setzen die Sicherheit des verwendeten spezifischen Algorithmus sowie den sicheren Austausch alle verwendeten Schlüssel voraus. Aus dieser Sicht ist es also angebracht, Algorithmen und Protokolle zu verwenden, von denen ein hoher sicherheitstechnischer Standard angenommen wird und die für die Verwendung in Hochsicherheitsbereichen (durch das BSI [BS08]) ausdrücklich empfohlen werden.

5 Fazit

Die Erfassung biometrischer Daten zur Vorsorge für die Kriminalitätsaufklärung ist nur in engen Grenzen zulässig. Wenn sie jedoch in einem konkreten Fall geeignet und erforderlich ist, ist die Technikgestaltung zu regeln. Dieser Beitrag zeigt, dass die Technik gestaltbar ist und insbesondere eine effektive Pseudonymisierung von vorsorglich erfassten biometrischen Daten ermöglicht.

Nur nach Umsetzung der technischen und rechtlichen Gestaltungsvorschläge ist ausreichend sicher, dass Betroffene nicht befürchten müssen, personenbezogenen Maßnahmen der Polizei ausgesetzt zu werden. Dies ist ein wichtiger Aspekt, um die Verfassungsverträglichkeit des Systemeinsatzes herzustellen. Dies liegt insbesondere daran, dass die zwei Hindernisse für die Biometrie - Einzigartigkeit biometrischer Charakteristika und Gewinnbarkeit von Gesundheitsdaten/ethnischen Daten - überwunden werden.

Die Gesellschaft kann mit dem neuartigen Risiko künftiger biometrischer Systeme zur Kriminalitätsbekämpfung umgehen. Ein solcher verfassungsverträglicher Umgang ist auch notwendig, denn der vernünftige Bürger ist an beidem interessiert: Schutz vor Gefahren und Straftaten sowie Schutz vor Folgen des Missbrauchs informationeller Macht und nachlässigen Umgangs mit Technik. Wenn diese und andere Gestaltungsmöglichkeiten genutzt werden, kann das Fundament für eine Zukunft der Terroristen- und Kriminalitätsbekämpfung gelegt werden, die sich die Gesellschaft wünscht.

Literaturverzeichnis

[BB08] Breebaart, J., Busch, C., Grave, J., Kindt, E.: A Reference Architecture for Biometric Template Protection based on Pseudo Identities. In (Brömme, A.; Busch, C.; Hühnlein, D. Hrsg.): BIOSIG 2008, 2008, S. 25-37, Lecture Notes in Informatics 137, Gesellschaft für Informatik

[BKA07] Bericht des BKA zur "Fotofahndung", 2/2007.

[Bo11] Bouchrika I. u. a., Journal of Forensic Sciences 2011, 882.

[BS08] BSI Technische Richtlinie: Kryptographische Verfahren: Empfehlungen und Schlüssellängen. BSI TR-02102, Version 1.0, 20.06.2008.

[BSW07] Boult, T.; Scheirer, W. und Woodworth, R.: Revocable fingerprint biotokens: accuracy and security analysis. In Proc. IEEE Inter. Conf. on Comput. Vis. & Patt. Recog, USA, 2007.

[BV83] So zum Beispiel in BVerfGE 65, 1 (69).

[BV01] BVerfGE 100, 313 (361 f.); 65, 1 (46 f.).

[BV08] (1) So zum Beispiel BVerfGE 120, 378 (424); (2): BVerfGE 120, 378 (428); (3): BVerfGE 120, 378 (402); 115, 320 (354 f.); 107, 299 (328); (4): BVerfGE 120, 378 (403); 113, 29 (46); 65, 1 (42); (5): BVerfGE 120, 378 (406); 116, 202 (222); 113, 63 (76).

[BV09] So zum Beispiel BVerfGE 120, 274.

[BV10] (1): BVerfGE 125, 260 (Abs. 214); (2): BVerfGE 125, 260 (Abs. 270); (3): BVerfGE 125, 260, Abs. 223; Fox, DuD 2008, 375.

[De85] Denninger, E.: KJ 1985, 215 (239 ff.).

[Di00] Di Fabio, U. in: Maunz, T.; Dürig, G. GG, Art. 2 Abs. 1, Rn 184.

[DM04] Daugman, J.; Malhas, I.: International Airport Review 2/2004.

[DPS11] Desoi, M.; Pocs, M. und Stach, B.: Biometric Systems in Future Crime Prevention Scenarios – How to Reduce Identifiability of Personal Data. In (Brömme, A.; Busch, C. Hrsg.): BIOSIG 2011. Proceedings - International Conference of the Biometrics Special Interest Group, Bonn 2011, S. 259-266.

[Eu10] EuGH, Urteil v. 9.3.2010, C-518/07.

[FP09] FP7-Projekte: ADABTS (RCN: 91158), SAMURAI (89343), SUBITO (89391); BMBF-Projekte: ADIS (FKZ: 13N10977-9); CamInSens (13N10814); APFEL (13N10795-801).

[Ga10] Gates, K.: Culture Unbound 2/2010, S. 67; in Newham, T., The Observer, 11.10.1998, S. 5.

[GK06] GenKey: System, portable device and method for digital authenticating, crypting and signing by generating short-lived cryptokeys. US Patent 2006/0198514A1.

[Ha93] Hammer, V.; Pordesch, U.; Roßnagel, A.: Betriebliche Telefon- und ISDN-Anlagen rechtsgemäß gestaltet. Heidelberg, New York, 1993.

[HDP10] Hornung, G.; Desoi M.; Pocs M.: Biometric Systems in future preventive Scenarios – Legal Issues and Challenges. In: Brömme, A.; Busch, C.: BIOSIG 2010, Bonn 2010, S. 83-94.

[He90] Heußner in: FS Simon, S. 233 ff.; BB 1990, 1281 (1283).

[He07] Hessische Staatskanzlei, 31.5.2007, http://www.daten-speicherung.de/data/Schriftsatz_Staatskanzlei_2007-06-01.pdf, S. 2.

[Hi11] Hildebrandt, M.; Pocs, M.; Dittmann, J.; Ulrich, M.; Merkel, R.; Fries, T.: Privacy preserving challenges: New Design Aspects for Latent Fingerprint Detection Systems with contact-less Sensors for Future Preventive Applications in Airport Luggage Handling. In: Proceedings of BioID 2011, Springer Lecture Notes on Computer Sciences (LNCS) Vol. 6583, Berlin 2011, S. 286.

[Po76] Podlech, A. in: Steinmüller, W.: Informationsrecht und Informationspolitik, München 1976, S. 211.
[Po83] Podlech, A.: Alternativkommentar zum Grundgesetz, Art. 2 Abs. 1, Rn 80.
[Po11a] Pocs, M.: Gestaltung von Fahndungsdateien - Verfassungsverträglichkeit biometrischer Systeme. Datenschutz und Datensicherheit (DuD) 2011, S. 163-168.
[Po11b] Pocs, M.: Abgleich im Erfassungsgerät. In: Schartner, P./Taeger, J. (Hrsg.): Tagungsband D-A-CH Security 2011, syssec 2011, 346-360.
[Po12] Pocs, M.: Constitutionally Compatible Design of Future Biometric Systems for Crime Prevention. In (Friedewald, M.;Pohoryles, R.; Sharan, Y. Hrsg.): Innovation - European Journal of Social Science Research, Spezialausgabe „Privacy and Technology“, Routledge, Juni 2012 (i. E.).
[Pr11] provet (Projektgruppe verfassungsverträgliche Technikgestaltung) unter der Leitung von Prof. Dr. Alexander Roßnagel. http://provet.uni-kassel.de
[Si84] Simitis, S.: NJW 1984, 398 (402 f.), NJW 1997, 1902 (1902 f.).
[UU04] Uludag, U.; Pankanti, S.; Prabhakar S.; Jain, A.K.: Biometric Cryptosystems: Issues and Challenges. Proceedings of the IEEE 92(6): 948-960 (2004).
[Wo03] Woodward, J.D. in: Woodward, J.D.; Orlans, N.; Higgins, M.: Biometrics. Identity Assurance in the Information Age, New York 2003, S. 327.
[WP03] Artikel-29-Datenschutzgruppe: Stellungnahme zur Biometrie (WP80) 2003.
[Zi09] Ziebarth, W.: DuD 2009, 25, S. 29; zustimmend Roßnagel A. u.a.: DuD 2009, 536, S. 539.

Sicherheitseigenschaften neuerer Systeme zur E-Mail-Kommunikation zwischen Bürgern und Behörden

Jörn Freiheit

Hochschule für Technik und Wirtschaft Berlin
Wilhelminenhofstr. 75A, 12459 Berlin
Joern.Freiheit@HTW-Berlin.de

Abstract: Bei der Kommunikation mit Behörden und der Justiz wird nach wie vor der herkömmliche Brief bevorzugt, obwohl sowohl für Privatpersonen als auch für Unternehmen die Briefpost fast vollständig durch E-Mails abgelöst worden ist. Preis und Geschwindigkeit der E-Mail sind dem herkömmlichen Brief deutlich überlegen, doch datenschutzrechtliche Aspekte haben bis heute verhindert, dass mit Behörden rechtsverbindlich per E-Mail kommuniziert werden kann. Hier soll mit Neuentwicklungen wie dem e-Postbrief, De-Mail oder dem Elektronischen Gerichts- und Verwaltungspostfach (EGVP) Abhilfe geschaffen werden. Die Aspekte Vertraulichkeit, Integrität und Authentizität in diesen Neuentwicklungen und die Praktikabilität für die elektronische Kommunikation zwischen Bürgern und Behörden werden in diesem Papier diskutiert.

1 Einleitung

Für die sichere und einfache elektronische Kommunikation zwischen Bürgern, Behörden und Unternehmen wurden in den vergangenen Jahren neue Produkte entwickelt und zur Verfügung gestellt. Dazu gehören De-Mail, der e-Postbrief und das Elektronische Gerichts- und Verwaltungspostfach (EGVP). Allen diesen Systemen ist jedoch gemein, dass ihre Einführung mit hohen Anlaufschwierigkeiten verbunden ist. So wurde die Einführung von De-Mail auf Ende 2011 verschoben, da der Akkreditierungsprozess der privaten De-Mail-Provider aufwändiger als vermutet ist. Darüber hinaus kritisieren Datenschützer, dass eine durchgehende Verschlüsselung einer De-Mail vom Absender bis zum Empfänger nicht verbindlich ist [Le11, Sch11]. Über den e-Postbrief hat im August 2011 das Landgericht Bonn geurteilt, dass die Aussage der Deutschen Post, „der E-Postbrief ist so sicher und verbindlich wie der Brief“, unwahr ist. Darüber hinaus wurde durch das Landgericht Bonn auch die Werbebehauptung der Deutschen Post: “der E-Postbrief überträgt die Vorteile des klassischen Briefs in das Internet und bietet damit auch in der elektronischen Welt eine verbindliche, vertrauliche und verlässliche Schriftkommunikation” verboten[13]. Das elektronische Gerichts- und Verwaltungspostfach wird als Eigenentwicklung der Justiz derzeit ausschließlich innerhalb der Justiz zur Kommunikation zwischen Gerichten, Staatsanwaltschaften, Anwälten und Notaren verwendet und ist von den genannten drei Verfahren bereits das „dienstälteste“. Es wird,

[13] Landgericht Bonn, Urteil vom 30. Juni 2011 – 14 O 17/11

im Gegensatz zu den beiden anderen Verfahren, von der Justiz kostenfrei zur Verfügung gestellt. In einigen Verfahren (Handelsregistersachen, Mahnsachen) ist das EGVP per Gesetz als ausschließlicher Kommunikationsweg mit der Justiz vorgeschrieben. Papiereingänge werden in diesen Sachen nicht akzeptiert. In Verfahren, in denen die Übermittlung per EGVP freiwillig erfolgt, wird es jedoch nur von einer sehr überschaubaren Anzahl von Rechtsanwälten genutzt.

In diesem Papier sollen diese Kommunikationsinfrastrukturen bezüglich ihrer *Sicherheitseigenschaften* diskutiert werden. Dazu wird zunächst in Abschnitt 2 allgemein erläutert, welche Anforderungen an eine sichere E-Mail-Kommunikation zwischen Bürgern, Behörden und Unternehmen gestellt werden müssen. Abschnitt 3 beschreibt etablierte technische Möglichkeiten der sicheren E-Mail-Kommunikation und diskutiert deren Praktikabilität. In Abschnitt 4 werden die Systeme De-Mail, e-Postbrief und EGVP näher beschrieben und unter den in Abschnitt 2 identifizierten Sicherheitsanforderungen bewertet.

2 Allgemeine Anforderungen an die sichere E-Mail-Kommunikation

In diesem Abschnitt werden die unterschiedlichen Anforderungen beschrieben, die eine *sichere* E-Mail-Kommunikation nach heutigem Stand der Wissenschaft erfüllen muss. Eine E-Mail-Kommunikation ist sicher, wenn sie vertraulich ist, die Kommunikationspartner eindeutig identifizierbar sind und die Integrität der übermittelten Daten beziehungsweise Dokumente garantiert wird. Dies bedeutet grob zusammengefasst, dass Daten, die per E-Mail versendet werden, nicht von Unbefugten gelesen (Vertraulichkeit) und nicht geändert (Integrität) werden können und dass die Daten tatsächlich von dem vorgegebenen Autor beziehungsweise Absender stammen (Authentizität). Neben diesen drei Anforderungen können weitere Anforderungen an eine sichere E-Mail-Kommunikation gestellt werden, wie zum Beispiel dass ein E-Mail-Dienst stets verfügbar sein muss oder Fehlermeldungen bei Unzustellbarkeit versendet werden. Auf diese weiteren, technischen Anforderungen, wird in diesem Papier jedoch nicht eingegangen.

2.1 Vertraulichkeit

„Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen dürfen ausschließlich Befugten in der zulässigen Weise zugänglich sein.“ [BSI]

Hierbei ist zu betonen, dass die Vertraulichkeit verletzt ist, wenn Unbefugten die Daten in einer lesbaren Form zugänglich sind, das heißt wenn die Daten durch Unbefugte auswert-bar und weiterverwendbar sind. Die Vertraulichkeit ist umgekehrt nicht verletzt, wenn Unbefugte Zugang zu den Daten erhalten, diese aber, zum Beispiel durch Verschlüsselung (siehe Abschnitt 3.1), nicht lesbar und weiterverwendbar sind. Neben dieser Anforderung an die Lesbarkeit und Weiterverwendbarkeit von Daten ist klarzustellen, wer als *unbefugt* im Sinne der Vertraulichkeit gilt. Eine sehr restriktive Eingrenzung dieses Begriffes, zum Beispiel die Festlegung, dass die einzig Befugten bei der

sicheren E-Mail-Kommunikation ausschließlich Absender und Empfänger sind, führt in der Praxis häufig zu Vertraulichkeitsverletzungen, die rein theoretischer Natur sind (siehe Abschnitte 4.1 und 4.2).

2.2 Integrität

Integrität bezeichnet laut Glossar des Bundesamtes für Sicherheit in der Informationstechnik (BSI) die Sicherstellung der Korrektheit, das heißt Unversehrtheit von Daten. Der Verlust der Integrität kann bedeuten, „dass diese unerlaubt verändert, Angaben zum Autor verfälscht oder Zeitangaben zur Erstellung manipuliert wurden." [BSI]. Werden also Daten per E-Mail versendet, so muss zur Wahrung der Integrität sichergestellt werden, dass diese genauso beim Empfänger angekommen, wie sie der Absender versendet hat. Die Sicherstellung der Integrität ist eine zentrale Anforderung für den sicheren Versand elektronischer Daten in der Justiz.

Es sei an dieser Stelle betont, dass es genügt, wenn die Integrität einer Nachricht beziehungsweise ihre Verletzung nachträglich festgestellt werden kann. Das bedeutet, dass der Schutz der Integrität nicht zwingend erfordert, dass es keine Möglichkeit gibt, die Integrität zu verletzen. Vielmehr muss sichergestellt werden, dass die Verletzung der Integrität im Zweifel nachgewiesen werden kann (siehe Abschnitt 2.2). Werkzeuge zum Schutz der Integrität ermöglichen somit das sichere Erkennen der Wahrung beziehungsweise der Verletzung der Integrität.

2.3 Authentizität

„Mit dem Begriff Authentizität wird die Eigenschaft bezeichnet, die gewährleistet, dass ein Kommunikationspartner tatsächlich derjenige ist, der er vorgibt zu sein. Bei authentischen Informationen ist sichergestellt, dass sie von der angegebenen Quelle erstellt wurden." [BSI]

Eine E-Mail-Kommunikation ist demnach dann authentisch, wenn der Absender auch tatsächlich die Person ist, die er vorgibt zu sein. Die Verletzung der Authentizität wird insbesondere bei den als *Phishing* bekannten Attacken praktiziert (siehe auch Kapitel 1.3.2 bei [Eck09]). Tatsächlich ist der Nachweis über die Identität des Absenders bei der elektronischen Kommunikation schwierig zu führen. Dies liegt unter anderem auch daran, dass die Anforderungen an die Authentizität im Falle der elektronischen Kommunikation häufig strenger sind, als man dies beispielsweise von der herkömmlichen Briefkommunikation kennt, bei der man zunächst von der Korrektheit der vorgegebenen Identität des Absenders ausgeht, wenn der Brief handschriftlich unterzeichnet wurde. In Anlehnung an die handschriftliche Unterschrift wurde die elektronische Signatur entwickelt, die einen Nachweis der Authentizität ermöglicht (siehe Abschnitt 3.2).

3 Technische Möglichkeiten für eine sichere E-Mail-Kommunikation

Um die Anforderungen an die sichere E-Mail-Kommunikation zu erfüllen, wurden technische Verfahren entwickelt, die im Folgenden diskutiert werden. Dabei wird insbesondere darauf eingegangen, welche der Anforderungen Integrität, Vertraulichkeit und Authentizität durch die jeweiligen technischen Verfahren gewährleistet werden und welche Besonderheiten in der praktischen Anwendung der jeweiligen Verfahren zu berücksichtigen sind.

3.1 Verschlüsselung

Mit der sogenannten *Verschlüsselung* werden die Daten und/oder Nachrichten mithilfe kryptografischer Verfahren in eine Folge von Zeichen überführt, die ohne Bedeutung und ohne Rückschlussmöglichkeit auf den tatsächlichen Inhalt ist. Das Entschlüsseln dieser Folge von Zeichen kann ohne einen Schlüssel nicht erfolgen. Die Qualität der Verschlüsselung hängt davon ab, wie leicht beziehungsweise schwer es mithilfe gegenwärtiger technischer Hilfsmittel möglich ist, den zur Entschlüsselung benötigten Schlüssel unberechtigterweise herauszufinden. Sichere Verfahren benötigen zur Schlüsselermittlung selbst bei Verwendung aller heute verfügbaren Rechnerkapazitäten viele Jahre. Einen Überblick über die jeweils als gegenwärtig sicher eingestuften kryptografischen Verfahren zur Verschlüsselung gibt die Bundesnetzagentur in einem jährlich aktualisierten Katalog heraus [BNA].

3.1.1 Ablauf

Zur Verschlüsselung ist ein Paar von Schlüsseln notwendig. Der eine Schlüssel wird zum Ver- und der andere Schlüssel zum Entschlüsseln verwendet. Es wird zwischen *symmetrischen* und *asymmetrischen* Verfahren unterschieden. Bei den symmetrischen Verfahren sind die Schlüssel zum Ver- und Entschlüsseln gleich (oder lassen sich leicht voneinander ableiten). Bei den asymmetrischen Verfahren werden unterschiedliche Schlüssel zum Ver- und Entschlüsseln verwendet. Asymmetrische Verfahren werden zum Verschlüsseln von E-Mails verwendet. Das asymmetrische Ver- und Entschlüsseln zwischen zwei Kommunikationspartnern A und B läuft dabei grob wie folgt ab:

1. A und B erzeugen jeweils ein Schlüsselpaar ($S_A^{Ö}$, S_A^{P}) und ($S_B^{Ö}$, S_B^{P}). Dabei sind $S_A^{Ö}$ und $S_B^{Ö}$ die *öffentlichen* Schlüssel von A und B und S_A^{P} und S_B^{P} die *privaten* Schlüssel von A und B.
2. A schickt seinen öffentlichen Schlüssel $S_A^{Ö}$ an B und B schickt seinen öffentlichen Schlüssel $S_B^{Ö}$ an A.
3. A verschlüsselt die für B vorgesehene E-Mail E_K (E-Mail als Klartext) mithilfe des öffentlichen Schlüssels $S_B^{Ö}$ von B. Es entsteht eine verschlüsselte E-Mail E_V=verschlüsselt(E_K, $S_B^{Ö}$). Diese verschlüsselte E-Mail E_V wird von A an B versendet.
4. B empfängt die E-Mail E_V und entschlüsselt diese mithilfe seines privaten Schlüssels S_B^{P}. Durch das Entschlüsseln erhält B die ursprüngliche E-Mail wieder im Klartext E_K=entschlüsselt(E_V, S_B^{P}).

5. Will B nun A antworten, so verwendet er zum Verschlüsseln den öffentlichen Schlüssel $S_A^{Ö}$ von A und A entschlüsselt die von B erhaltene verschlüsselte E-Mail mithilfe seines privaten Schlüssels S_A^{P}.

3.1.2 Schlüsselaustausch

Generell muss also zum Verschlüsseln einer E-Mail der öffentliche Schlüssel des Empfängers bekannt sein. Dieser muss in den Besitz des Absenders gelangen. Dies stellt in der Praxis oft eine hohe Hürde dar, da entweder der Empfänger gar keinen öffentlichen Schlüssel besitzt oder aber dieser nur aufwändig (zum Beispiel durch Suche auf Zertifikatsservern oder auf der persönlichen Webseite des Empfängers) zu beschaffen ist. Ein weiterer praktischer Nachteil der Verschlüsselung besteht darin, dass die E-Mail nur vom Empfänger selbst (mithilfe seines privaten Schlüssels) entschlüsselt werden kann. Dies ist insbesondere in größeren Organisationen, in denen der Zugriff auf E-Mail-Konten oft delegiert wird, problematisch. Das Senden verschlüsselter E-Mails an mehrere Empfänger ist nicht möglich (und auch nicht sinnvoll), da das Verschlüsseln stets für genau einen Empfänger (die Person, die den passenden privaten Schlüssel besitzt) geschieht. Darüber hinaus ist die Verwaltung sowohl des eigenen privaten Schlüssels als auch der fremden öffentlichen Schlüssel aufwändig. Einerseits wäre ein Verlust (oder das Bekanntwerden) des eigenen privaten Schlüssels fatal, andererseits führt eine redundante Speicherung des privaten Schlüssels an mehreren Sicherungsspeicherorten zu einem erhöhten Risiko. Das Entziehen des öffentlichen Schlüssels, das durch den Verlust des privaten Schlüssels notwendig wird, ist kompliziert und wird bei Risikobetrachtungen häufig vernachlässigt.

3.1.3 Werkzeuge

Das Bundesamt für Sicherheit in der Informationstechnik stellt ein kostenloses Werkzeug zur Verschlüsselung von E-Mails bereit. Dieses Werkzeug Gpg4win kann in E-Mail-Programme, wie zum Beispiel Microsoft Outlook eingebunden werden. Gpg4win basiert auf dem ebenfalls frei erhältlichen Werkzeug GnuPG.

Sowohl De-Mail, der e-Postbrief als auch das EGVP verwenden Verschlüsselungen zum E-Mail-Austausch. Es unterscheiden sich diese Verfahren jedoch darin, ob standardmäßig eine durchgehende Verschlüsselung vom Absender bis zum Empfänger erfolgt. Dies ist nur beim EGVP der Fall (siehe Abschnitt 4).

3.1.4 Bewertung

Verschlüsselungsverfahren wahren die Integrität und die Vertraulichkeit der übersandten Daten. Die Authentizität jedoch ist nur mittelbar gewahrt. Zwar werden bei der Erstellung der Schlüsselpaare vertrauenswürdige Zertifikatsstellen (je nach Zertifikat wird eine Hierarchiekette des Vertrauens oder ein Netz des Vertrauens verwendet) eingebunden, die dabei gemachten Angaben über beispielsweise den Namen des Nutzers werden jedoch nicht geprüft.

Für einen allgemeinen Einsatz in der Verwaltung und Justiz sind die Verschlüsselungsverfahren aufgrund der genannten praktischen Nachteile nicht geeignet.

3.2 Elektronische Signatur

Bereits seit 1997 gibt es gesetzliche Rahmenbedingungen für den Einsatz elektronischer Signaturen in Deutschland. Von besonderer Bedeutung ist dabei die *qualifizierte elektronische Signatur*, die die höchsten Sicherheitsanforderungen an eine elektronische Signatur stellt. Die qualifizierte elektronische Signatur ist eine mit einem privaten Schlüssel verschlüsselte Datei, die Informationen über ein, dieser qualifizierten elektronischen Signatur zugeordnetem Dokument enthält. Die qualifizierte elektronische Signatur kann nur mit dem öffentlichen Schlüssel entschlüsselt werden, der zu dem zur Verschlüsselung der Signatur verwendeten privaten Schlüssel gehört. Das Schlüsselpaar aus privatem und öffentlichem Schlüssel wurde dabei von einer Zertifizierungsstelle erzeugt, bei der die Identität des Schlüsselpaarinhabers hinterlegt ist. Mit der qualifizierten elektronischen Signatur ist somit die Authentizität sichergestellt. Sie kann auch jederzeit bei den Trustcentern, die die Signatur ausgestellt haben, nachgeprüft werden.

Die in der qualifizierten elektronischen Signatur enthaltenen Informationen über das signierte Dokument sichern darüber hinaus die Integrität des Dokumentes. Dies wird dadurch sichergestellt, dass ein sogenannter Hashwert für das Dokument erstellt wird. Hashwertberechnungen werden verwendet, um große Datenmengen, zum Beispiel elektronische Dokumente oder elektronische Akten, auf einen kleinen, eindeutigen Wert abzubilden. Dieser Hashwert liefert mithilfe kryptografischer Verfahren eine eindeutige Prüfsumme für dieses Dokument. Wird das Dokument geändert, so ändert sich auch die Prüfsumme (der Hashwert).

Das Verfahren zur qualifizierten elektronischen Signatur besteht aus drei Teilschritten:

1. dem Ausstellen einer Signaturkarte,
2. dem Signieren einer Datei oder eines Dokumentes sowie
3. dem Prüfen der Signatur.

3.2.1 Das Ausstellen der Signaturkarte

Um qualifiziert elektronisch signieren zu können, ist eine Signaturkarte erforderlich. Diese wird von einem Trustcenter ausgestellt. Das Trustcenter prüft die Identität der die Signaturkarte beantragenden natürlichen Person. Dies kann beispielsweise über das Post-Ident-Verfahren erfolgen. Nach Prüfung der Identität des Antragstellers generiert das Trustcenter ein Schlüsselpaar[14], das aus einem öffentlichen und einem privaten Schlüssel besteht. Das Trustcenter speichert die zu diesem Schlüsselpaar zugehörige

[14] Auf Basis von Zufallszahlengeneratoren (siehe Bundesnetzagentur, Übersicht über geeignete Algorithmen, Mai 2011, online abrufbar unter http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Sachgebiete/QES/Veroeffentlichungen/Algorithmen/2011_2_AlgoKatpdf.pdf?__blob=publicationFile)

Identität. Der öffentliche Schlüssel wird durch das Trustcenter in einem öffentlichen Verzeichnis zum Abruf bereitgestellt.[15]

3.2.2 Das Signieren einer Datei

Das Signieren einer Datei erfolgt in zwei Schritten. Zunächst wird der Hashwert dieser Datei mithilfe eines Verfahrens zur Hashwertberechnung[16] gebildet. Für jede Datei ist dieser Hashwert eindeutig. Eine Änderung an der Datei bewirkt auch einen neuen Hashwert. Das Verfahren der Hashwertberechnung ist eine Funktion der Signaturanwendungskomponente[17] (Soft- und Hardware zur Erzeugung und Prüfung qualifizierter elektronischer Signaturen).

In einem zweiten Schritt wird der Hashwert mithilfe kryptographischer Verfahren (den sogenannten Signaturverfahren)[18] mit dem privaten Schlüssel, der auf der Signaturkarte gespeichert ist, verbunden. Dazu ist die Eingabe einer PIN am Kartenlesegerät notwendig, um die Authentizität des Signierenden zu sichern. Die Kombination aus Hashwert und privatem Schlüssel ist die qualifizierte elektronische Signatur. Die Signaturverfahren sind ebenfalls Funktionen der Signaturanwendungskomponente.

Im Ergebnis liegen nach dem Signieren einer Datei demnach zwei Dateien vor; die signierte Datei und die Signatur, die den Hashwert der signierten Datei und den persönlichen Schlüssel des Signierenden enthält.

Zum Anbringen einer qualifizierten elektronischen Signatur sind nach § 2 SigG eine den Anforderungen des Signaturgesetzes entsprechende sichere Signaturerstellungseinheit (Signaturkarte und Kartenleser) sowie eine Signaturanwendungskomponente (die Software) erforderlich. Für die Software muss entweder eine Prüfung und Bestätigung nach Signaturgesetz erfolgt sein oder die Bundesnetzagentur hat eine entsprechende Herstellererklärung des Softwareanbieters veröffentlicht.[19]

---

[15] Tatsächlich werden nicht nur der öffentliche Schlüssel, sondern gleichzeitig auch noch die Identität desjenigen bereitgestellt, der den zu dem öffentlichen Schlüssel korrespondierenden privaten Schlüssel besitzt. Diese Kombination aus öffentlichem Schlüssel und Identitätsinformationen wird „Zertifikat“ genannt. "Qualifizierte Zertifikate" sind nach § 2 SigG „elektronische Bescheinigungen, mit denen Signaturprüfschlüssel einer natürlichen Person zugeordnet werden und die Identität dieser Person bestätigt wird.“ Diese Zertifikate müssen die „Voraussetzungen des § 7 erfüllen und von Zertifizierungsdiensteanbietern ausgestellt werden, die mindestens die Anforderungen nach den §§ 4 bis 14 oder § 23 dieses Gesetzes und der sich darauf beziehenden Vorschriften der Rechtsverordnung nach § 24 erfüllen.“

[16] In der von der Bundesnetzagentur am 20. Mai 2011 veröffentlichten Übersicht über geeignete Algorithmen zur elektronischen Signatur sind die Verfahren SHA-256, SHA-384, SHA-512 als bis 2017 geeignet (das heißt sicher) aufgeführt (SHA = secure hash algorithm, die Zahl gibt die Länge des Hashwertes in bit an)

[17] Siehe § 2 Nr. 11 SigG

[18] In der von der Bundesnetzagentur am 20. Mai 2011 veröffentlichten Übersicht über geeignete Algorithmen zur elektronischen Signatur sind RSA-Verfahren mit den Parametern 1976 bit (Mindestwert) beziehungsweise 2048 bit (empfohlen), DSA-Verfahren mit den Parametern 2048 bit und 256 bit sowie DSA-Varianten mit dem Parameter q=250 bit als bis 2017 geeignet (das heißt sicher) aufgeführt.

[19] Nach § 17 Absatz 4 SigG

3.2.3 Das Prüfen einer Signatur

Auch das Prüfen einer Signatur ist ein zweistufiges Verfahren. Zunächst wird von der zu prüfenden Datei ein Hashwert mit dem gleichen Verfahren gebildet, wie es bei der Erstellung der Signatur verwendet wurde. Danach wird die Signatur mithilfe des öffentlichen Schlüssels entschlüsselt. Dies gelingt nur, wenn der vorgebliche Signierende auch tatsächlich derjenige war, der die Signatur erstellt, das heißt wenn sein privater Schlüssel zum Signieren verwendet wurde. Nur dann ist es auch möglich mit dem dazugehörigen öffentlichen Schlüssel, die Signatur zu entschlüsseln. Nach dem Entschlüsseln der Signatur ist der beim Signieren erstellte Hashwert lesbar und kann mit dem im ersten Schritt gebildeten Hashwert verglichen werden. Sind beide Hashwerte gleich, so wurde die Datei seit dem Signieren nicht mehr verändert. Für das Prüfen von Signaturen stehen diverse auch kostenfreie Programme bereit.

3.2.4 Bewertung

Obwohl für das Verfahren der qualifizierten elektronischen Signatur seit bereits fast 15 Jahren eine rechtliche Grundlage existiert, hat es sich noch nicht durchgesetzt und wird aufgrund der aufwändigen praktischen Handhabung kritisiert [BLK11]. Dies hängt insbesondere damit zusammen, dass der Einsatz der qualifizierten elektronischen Signatur in Behörden nicht den herkömmlichen Büroabläufen angepasst ist. Die qualifizierte elektronische Signatur ist genau einer Person, nicht jedoch einer Behörde zugeordnet, was einerseits einen organisatorischen Mehraufwand in einer Behörde zulasten eines Einzelnen bedeutet und andererseits oft über das Ziel hinausgeht, wenn nämlich die absendende Person im Gegensatz zur absendenden Behörde unwichtig ist. Darüber hinaus ist bei der Archivierung von mit der qualifizierten elektronischen Signatur signierten Dokumenten zu beachten, dass Zertifikate ablaufen und ein spätes Prüfen der Signatur und der Integrität der damit assoziierten Dokumente einen zusätzlichen Organisationsaufwand (zum Beispiel durch Übersignieren) hervorruft.

So wurde beispielsweise in dem (allerdings nicht vom Bundesrat zugestimmten) Steuervereinfachungsgesetz 2011 vorgesehen, die Anforderungen an elektronische Rechnungen derart zu vereinfachen, dass eine qualifizierte elektronische Signatur unter einer solchen elektronischen Rechnung nicht mehr notwendig ist.

Generell gilt zu beachten, dass die Verwendung qualifizierter elektronischer Signaturen die mit diesen Verfahren versehenen Dateien *nicht* vor Änderungen schützen, sondern diese nur nachweisbar machen. Insbesondere bietet die qualifizierte elektronische Signatur keinen Schutz der Vertraulichkeit, da das signierte Dokument nicht verschlüsselt wird. Die Gewährleistung der Sicherheit der elektronischen Kommunikation unter ausschließlichem Einsatz der qualifizierten elektronischen Signatur ist somit nicht gegeben.

Sowohl De-Mail, der e-Postbrief als auch das EGVP unterstützen den Einsatz qualifizierter elektronischer Signaturen. Bei De-Mail und dem e-Postbrief kommen qualifizierte elektronische Signaturen optional zum Einsatz, wenn der Absender einer E-Mail zusätzlich durch den Provider bestätigt wird und wenn eine Empfangsbestätigung (Einschreiben) erforderlich ist. Beim EGVP werden qualifizierte elektronische Signaturen

automatisch ausgestellt. Beim EGVP werden auch automatisch Empfangsbestätigungen übersandt.

4 Neuentwicklungen für die sichere E-Mail-Kommunikation

Aufgrund der beschriebenen Nachteile der bereits bekannten und in Abschnitt 3 beschriebenen technischen Möglichkeiten zur sicheren E-Mail-Kommunikation sind in den letzten Jahren Verfahren und Infrastrukturen entwickelt worden, die eine sichere E-Mail-Kommunikation zwischen Privatpersonen und Behörden ermöglichen sollen. Diese werden im Folgenden diskutiert.

4.1 De-Mail

De-Mail wurde am Bundesministerium des Innern entwickelt. Die oberste Aufsichtsbehörde des De-Mail-Systems ist das Bundesamt für Sicherheit in der Informationstechnik. Im Mai 2011 trat das De-Mail-Gesetz [DeMG] in Kraft. Das Gesetz sieht vor, einen „sicheren, vertraulichen und nachweisbaren Geschäftsverkehr für jedermann im Internet“ sicherzustellen. Dazu werden private E-Mail-Provider zertifiziert und als De-Mail-Provider akkreditiert. Dieser aufwändige Zertifizierungs- und Akkreditierungsprozess hat offiziell zu einer Verzögerung des Starts von De-Mail geführt, der nunmehr für Ende 2011 geplant ist. Von Oktober 2009 bis März 2010 wurde De-Mail in einem Pilotprojekt in Friedrichshafen mit den E-Mail-Providern Deutsche Telekom, GMX, T-Systems und WEB.DE von Behörden, Bürgern und Unternehmen getestet.

De-Mail ist kein zentral betriebener Dienst. Vielmehr können sich beliebig viele private E-Mail-Provider als De-Mail-Diensteanbieter nach § 17 De-Mail-Gesetz vom Bundesamt für Sicherheit in der Informationstechnik zertifizieren und akkreditieren lassen. Dies bedeutet auch, dass kein zentrales Verzeichnis aller De-Mail-Nutzer existiert, sondern dass jeder De-Mail-Diensteanbieter seine eigenen De-Mail-Nutzer nach den Vorgaben von § 3 des De-Mail-Gesetzes verwaltet.

De-Mail steht allen Bürgern, Behörden und Unternehmen kostenpflichtig zur Verfügung. Datenschützer kritisieren De-Mail teilweise heftig [Le11, Sch11]. Ihre Kritik ist, dass eine Ende-zu-Ende-Verschlüsselung, das heißt die durchgehende Verschlüsselung vom Absender bis zum Empfänger einer Nachricht, in De-Mail nicht verpflichtend ist. Dem ist einerseits entgegenzuhalten, dass die Ende-zu-Ende-Verschlüsselung in De-Mail möglich ist, wenn Empfänger und Absender dem Speichern ihrer öffentlichen Schlüssel im De-Mail-System zugestimmt haben. Andererseits erfolgt das Ent- und erneute Verschlüsseln beim Provider automatisiert und in einem Zeitraum von „wenigen Millisekunden bis zu einer Sekunde“ [BSIb]. Es bleibt darüber hinaus offen, ob ein zertifizierter und akkreditierter De-Mail-Provider ein Unbefugter im Sinne der Definition der Vertraulichkeit ist. Es erscheint vielmehr gerechtfertigt, Nachrichten automatisiert auf Viren oder ähnliche Gefährdungen zu prüfen, solange sichergestellt wird, wie es im Zertifizierungs- und Akkreditierungsprozess geprüft wird, dass eine Kenntnis-

nahme, Speicherung und Änderung der Nachrichteninhalte durch Dritte ausgeschlossen ist.

Vielmehr ist die Sicherung der Integrität der übersandten Nachrichten und Daten insofern problematischer, als durch das automatisierte Ent- und Verschlüsseln der Nachricht, dem Prüfen auf Viren und dem dazu notwendigen temporärem Zwischenspeichern die Prüfsumme (der Hashwert) über die Daten bereits verändert werden könnte, obwohl die Inhaltsdaten nicht geändert wurden. Nach § 5 Absatz 3 De-Mail-Gesetz ist der De-Mail-Diensteanbieter jedoch verpflichtet, die Integrität der Daten sicherzustellen, auch dann, wenn eine Ende-zu-Ende-Verschlüsselung durch den Nutzer nicht verwendet wird. Es bleibt bis zur Einführung von De-Mail abzuwarten, ob die Sicherung der Integrität automatisiert prüfbar bleibt oder ob die Sicherung der Integrität aufgrund der technischen Umsetzung der rechtlichen Anforderungen zweifelsfrei angenommen werden kann.

Zur Registrierung beim De-Mail-System muss der zukünftige Nutzer sich eindeutig identifizieren. Der Provider, bei dem sich der Nutzer registriert, kann somit eindeutig ein Postfach einer Identität zuordnen. Dies gilt auch dann, wenn für die De-Mail-Adresse ein Pseudonym verwendet wird. Unter der Annahme, dass eine Anmeldung an das De-Mail-System nur mithilfe von Nutzername und Passwort als nicht sicher gilt, ist die Anmeldung an De-Mail über das gesicherte Verfahren nach § 4 De-Mail-Gesetz, das heißt die Verwendung von „zwei geeigneten und voneinander unabhängigen Sicherungsmitteln“, zu verlangen, um die Authentizität sicherzustellen.

Die Praktikabilität von De-Mail wird insbesondere durch Plug-Ins unterstützt, die eine Verwendung von De-Mail in herkömmlichen E-Mail-Programmen, wie zum Beispiel Microsoft Outlook, ermöglicht [Men].

4.2 e-Postbrief

Der e-Postbrief wird durch die Deutsche Post AG bereits seit Juli 2010 zur Verfügung gestellt. Der e-Postbriefdienst und somit auch die Verwaltung der e-Postbrief-Nutzer-Adressen werden zentral betrieben. Ein e-Postbrief kostet 0,55 Euro, mit Einschreiben 2,15 Euro. Die Deutsche Post hat angekündigt, als De-Mail-Provider zu agieren, sobald De-Mail eingeführt wird.

Die Kommunikation erfolgt verschlüsselt. Dabei wird TLS (Transport Security Layer) verwendet, ein Verschlüsselungsprotokoll zur Datenübertragung. Wie bei De-Mail wird auch hier die Nachricht beim Provider ent- und wieder verschlüsselt. Auch für den e-Postbrief eine Ende-zu-Ende-Verschlüsselung möglich.

Im Gegensatz zu De-Mail unterliegt der e-Postbrief jedoch nicht den gesetzlichen Anforderungen des De-Mail-Gesetzes. Bei dem e-Postbriefdienst handelt es sich um ein hybrides Verfahren. Das bedeutet, dass ein e-Postbrief, dessen Empfänger keine e-Postadresse besitzt, ausgedruckt und als herkömmlicher Papierbrief dem Empfänger zugestellt wird. Bei diesem Prozess ist die Vertraulichkeit nicht gewahrt. Die Deutsche Post unterliegt als Betreiber des e-Postbriefes auch keiner Akkreditierung und ist auch

nicht gesetzlich verpflichtet, die Integrität zu wahren. In einem Urteil des Landgerichtes Bonn vom August 2011 wurde entschieden, dass die Aussage der Deutschen Post, „der E-Postbrief ist so sicher und verbindlich wie der Brief", unwahr ist [LGBo].

Die Registrierung bei e-Postbrief erfolgt über das Post-Ident-Verfahren. Für die Anmeldung gibt es, wie bei De-Mail, zwei Sicherheitsstufen. Die normale Anmeldung erfolgt durch Benutzername und Passwort. Bei der hohen Sicherheitsstufe wird zusätzlich die Eingabe einer mobilen TAN abgefragt. Die Authentizität ist somit bei dem e-Postbrief gewahrt.

Die Praktikabilität des e-Postbriefes wird dadurch erschwert, dass eine Integration des e-Postbriefes in herkömmliche E-Mail-Programme derzeit noch nicht möglich ist, so dass für das Empfangen und Versenden von e-Postbriefen stets die Webanwendung der Post AG in einem Browser geöffnet werden muss.

4.3 EGVP

Das Elektronische Gerichts- und Verzeichnispostfach (EGVP), das durch die Bundesländer und den Bund im Verbund für die Justiz entwickelt wurde, steht in der aktuellen Version 2.6 Gerichten, Staatsanwaltschaften, Notaren und Anwälten kostenfrei zur elektronischen Kommunikation zur Verfügung und wird gegenwärtig von rund 40 000 Nutzern verwendet. Für Handelsregistereinträge und in Mahnsachen ist die Verwendung des EGVP verbindlich. Monatlich werden über das EGVP rund 400 000 Nachrichten versendet.

Um das EGVP nutzen zu können, ist die Installation eines separaten Clients erforderlich. Eine Einbindung in etablierte E-Mail-Programme, wie zum Beispiel Microsoft Outlook oder Thunderbird ist nur mit einem kostenpflichtigen Plug-In, das am Markt erhältlich ist, möglich. Mithilfe der ab November 2011 erhältlichen EGVP-Version „Enterprise" soll eine Einbindung des EGVP-Clients in Fachverfahren möglich werden, so dass keine separate Installation des EGVP-Clients mehr notwendig ist.

Zur Gewährleistung der Vertraulichkeit werden die Nachrichten im EGVP Ende-zu-Ende verschlüsselt. Als Übertragungsprotokoll der Kommunikation wird OSCI verwendet. Die Verwaltung der Nutzer und deren Schlüssel erfolgt mithilfe des Registrierungsdienstes S.A.F.E. (Secure Access to Federated e-Justice/e-Government), der in der aktuellen Version 1.4 ebenfalls kostenfrei angesprochen werden kann und in Zukunft nicht nur als Registrierungsdienst für das EGVP, sondern darüber hinaus auch für weitere Anwendungen, wie zum Beispiel das Zentrale Testamentsregister, verwendet wird. Die Integrität der Nachrichten kann mithilfe der qualifizierten elektronischen Signatur, die an jede Nachricht angefügt werden kann, überprüft werden.

Der Benutzerkreis des EGVP ist geschlossen. Es wird unterschieden zwischen Nutzern, die ein sogenanntes EGVP-Backend (zum Beispiel Gerichte) besitzen und solche mit einem EGVP-Bürgerclient (zum Beispiel Rechtsanwälte und Notare). Ein Versenden von Nachrichten ist nur zwischen Backends, zwischen Backends und Clients, nicht jedoch zwischen Clients möglich. Ein Registrieren bei EGVP kann ohne den Nachweis

der Identität erfolgen. Die Anmeldung erfolgt mit Softwarezertifikaten. Das EGVP ermöglicht als Signaturanwendungskomponente das Anbringen von Signaturen an Nachrichten. Die Authentizität ist beim EGVP somit nur gewährleistet, wenn die Nachricht qualifiziert elektronisch signiert wurde.

Auf dem IT-Gipfel 2012 wurde eine Zusammenarbeit von EGVP und De-Mail vereinbart [Bec11]. Dabei sollen die Nutzerkreise dieser Systeme gegenseitig geöffnet werden, so dass eine gegenseitige Adressierung und somit eine Kommunikation zwischen den Systemen ermöglicht wird.

5 Zusammenfassung und Ausblick

Die in diesem Papier diskutierten neuen Infrastrukturen für eine sichere E-Mail-Kommunikation erfüllen prinzipiell die Anforderungen an die Sicherheit. Das EGVP ist aufgrund der Ende-zu-Ende-Kommunikation im Zusammenspiel mit der qualifizierten elektronischen Signatur bezüglich der Wahrung der Integrität, Authentizität und der Vertraulichkeit am stärksten. Nachteile des EGVP liegen aufgrund der fehlenden Überprüfung der registrierten Identitäten und des einfachen Anmeldevorgangs am EGVP-Client, da die zusätzliche Anbringung einer qualifizierten elektronischen Signatur erforderlich ist, um die Authentizität zu sichern. Das EGVP steht grundsätzlich auch für die Kommunikation mit Verwaltungsbehörden zur Verfügung. Allerdings sind nach derzeitigem Stand nur wenige Verwaltungen oder öffentliche Einrichtungen (zum Beispiel IHKs) über das EGVP erreichbar.

Für die Kommunikation zwischen Bürger und Verwaltungen wurden die vorgestellten Infrastrukturen De-Mail und der e-Postbrief entwickelt. Diesen beiden fehlt eine verbindlich zu nutzende Ende-zu-Ende-Verschlüsselung. Bei beiden Verfahren ist diese jedoch optional verwendbar. Es ist jedoch fraglich, ob die maschinell und im Sekundenbruchteil durchgeführte Ent- und Verschlüsselung einen Bruch der Vertraulichkeit darstellt. Akkreditierte Diensteanbieter sind vielmehr verpflichtet, die Vertraulichkeit zu gewährleisten. Dasselbe gilt für die Sicherstellung der Integrität der übersendeten Nachrichten und Daten. Hierbei ist jedoch zu beachten, dass diesbezüglich nur sichergestellt werden muss, dass die Integrität der versendeten Nachrichten und Daten verletzt, das heißt dass sie während der Übertragung geändert wurden. Hierbei bleibt jedoch offen, wie sichergestellt werden soll, dass positive Fehler vermieden werden, das heißt eine geänderte Prüfsumme suggeriert eine Änderung der Daten ohne dass tatsächliche eine inhaltliche Änderung passierte. Im Gegenteil zum EGVP werden bei der Registrierung für De-Mail und e-Postbrief die Identitäten geprüft. De-Mail ist im Vergleich zum e-Postbrief insofern praktikabler, als dass für De-Mail bereits heute Integrationsmöglichkeiten in herkömmliche E-Mail-Programme verfügbar sind. Eine parallele Verwendung von Webanwendungen im Browser wird dadurch vermieden. Dies wird auch mit der entstehenden EGVP-Enterprise-Version möglich, wobei das EGVP dabei in Fachverfahren integriert wird.

Literaturverzeichnis

[Bac11] Bachmann, R.: „E-Mail Plugin für De-Mail vorerst nur für Firmen“, 2011, Blog-Beitrag, online abrufbar unter http://baetschman.ralfbachmann.de/2011/02/

[Bec11] Beck-Aktuell: „IT-Gipfel 2011: De-Mail soll Kommunikation mit Gerichten erleichtern“, 2011, online abrufbar unter http://beck-aktuell.beck.de/news/it-gipfel-2011-de-mail-soll-kommunikation-mit-gerichten-erleichtern

[BLK11] Bericht der Bund-Länder-Kommission, Unterarbeitsgruppe: „Konsequenzen der Ausweitung des elektronischen Rechtsverkehrs in kontradiktorischen Verfahren“, 2011, S.6

[BSI] Bundesamt für Sicherheit in der Informationstechnik. Glossar der IT-Grundschutz-Kataloge. Online abrufbar unter https://www.bsi.bund.de/DE/Themen/weitereThemen/ITGrundschutzKataloge/Inhalt/Glossar/glossar_node.html

[BSIb] Bundesamt für Sicherheit in der Informationstechnik, De-Mail verbessert die Sicherheit in der E-Mail-Kommunikation. BSI: Kritik an der Sicherheit der De-Mail ist unbegründet, 2010, online abrufbar unter https://www.bsi.bund.de/ContentBSI/Presse/Pressemitteilungen/Presse2010/De_Mail_Sicherheit_E_Mail_230710.html

[BNA] Bundesnetzagentur. Algorithmenkatalog. Online abrufbar unter http://www.bundesnetzagentur.de/cln_1912/DE/Sachgebiete/QES/Veroeffentlichungen/Algorithmen/algorithmen_node.html

[DeMG] De-Mail-Gesetz, 2011, online abrufbar unter http://www.gesetze-im-internet.de/de-mail-g/index.html

[Eck09] Eckert, C.: IT-Sicherheit. Konzepte, Verfahren, Protokolle. 6. Auflage, Oldenbourg Verlag, München, 2009

[Lap11] Lapp, T., EGVP funktioniert nicht mal innerhalb der Justiz, Beck-Blog, 2011. Online abrufbar unter http://blog.beck.de/2011/09/06/egvp-funktioniert-nicht-mal-innerhalb-der-justiz

[Le11] Lechtenbörger, J., Zur Sicherheit von De-Mail, Datenschutz und Datensicherheit 4, 2011

[LGBo] Landgericht Bonn, Urteil vom 30. Juni 2011 – 14 O 17/11

[Men] Mentana-Claimsoft AG, Homepage des Unternehmens zu DeMail: http://mentana-claimsoft.de/de-mail-fuer-unternehmen.html

[Sch11] Schaar, P.: De-Mail: Wer sicher gehen will, sollte verschlüsseln!, Mitteilung des Bundebeauftragten für Datenschutz und Informationsfreiheit, 12/2011. Online abrufbar unter http://www.bfdi.bund.de/DE/Oeffentlichkeitsarbeit/Pressemitteilungen/2011/12_InkrafttretenDEMailGesetz.html?nn=408908

Die Entwicklung der BSI-Richtlinie für das rechtssichere ersetzende Scannen

Astrid Schumacher[1], Olga Grigorjew[2], Detlef Hühnlein[3], Silke Jandt[2]

[1]Bundesamt für Sicherheit in der Informationstechnik,
Godesberger Allee 185-189, 53175 Bonn
astrid.schumacher@bsi.bund.de

[2]Universität Kassel
Projektgruppe verfassungsverträgliche Technikgestaltung (provet),
Wilhelmshöher Allee 64-66, 34109 Kassel
{olga.grigorjew|silke.jandt}@uni-kassel.de

[3]ecsec GmbH
Sudetenstraße 16, 96247 Michelau
detlef.huehnlein@ecsec.de

Abstract: Die Notwendigkeit Papierdokumente zu digitalisieren, wird immer drängender. Sowohl im behördlichen als auch privat-wirtschaftlichen Umfeld werden zunehmend Dokumente auch in digitalen Dokumenten- und Vorgangsbearbeitungs- sowie Aufbewahrungssystemen verarbeitet. Gleichzeitig nimmt das Bedürfnis zu, die Papierdokumente anschließend zu vernichten, um kostenintensive Papierarchive auflösen zu können. Während ein Scanprodukt in rechtlicher Hinsicht niemals denselben Beweiswert wie das originäre Papierdokument haben kann, ist eine Annäherung durchaus möglich. Dies setzt voraus, dass das digitale Endprodukt in einem insbesondere für ein Gericht nachvollziehbaren Scanprozess unter gleichbleibenden qualitativ hochwertigen und abgesicherten Bedingungen entstanden ist. Die dafür notwendigen technischen sowie organisatorischen Anforderungen werden in der derzeit projektierten Technischen Richtlinie (TR) des Bundesamtes für Sicherheit in der Informationstechnik (BSI) beschrieben.

1 Einleitung

In Verwaltung, Justiz und privatwirtschaftlichen Unternehmen (zum Beispiel im Gesundheitswesen, der Versicherungswirtschaft sowie im Steuer- und Buchführungswesen) werden im Zuge der fortschreitenden Digitalisierung zunehmend elektronische Dokumentenmanagement- und Vorgangsbearbeitungssysteme eingesetzt. Zur Umsetzung des elektronischen Rechts- und Geschäftsverkehrs mehren sich Rechtsvorschriften, die die elektronische Aktenführung zulassen oder vorschreiben. Der parallele Umgang mit Papierdokumenten ist aber nach wie vor erforderlich und wird es auch zukünftig sein, da die Digitalisierung von Altbeständen längst noch nicht abgeschlossen ist und weiterhin Neueingänge in Papier erfolgen werden. Die Originale werden bislang in

einer Vielzahl von Fällen weiter aufbewahrt, um gegebenenfalls folgenreiche Konflikte mit gesetzlichen Dokumentations- und Aufbewahrungsvorschriften zu vermeiden. Gleichzeitig werden sie zur Erleichterung der internen Aktenbearbeitung häufig eingescannt. Die Aufbewahrung der Papieroriginale stellt eine hohe finanzielle und organisatorische Belastung der betroffenen Stellen dar. In rechtlicher Hinsicht bestehen - neben der in verschiedenen Rechtsgebieten sehr unterschiedlichen Regelungen zur Zulässigkeit des ersetzenden Scannens - Unsicherheiten aufgrund uneinheitlich ausgestalteter technisch-organisatorischer Anforderungen. Das Recht kann immer allenfalls abstrakte rechtliche Anforderungen stellen. Trotz zahlreicher Bemühungen, zum Beispiel im Bereich der steuerrelevanten und kaufmännischen Unterlagen, bleibt die technische Umsetzung weitestgehend dem Anwender überlassen. Aufgrund vielfältiger Scanlösungen am Markt, die bei der Umsetzung von Sicherheitsvorgaben stark variieren oder aus einer ganzheitlichen informationstechnischen Betrachtung heraus unvollständig sind, führt dies zu Unsicherheit in der praktischen Anwendung.

Die Technische Richtlinie (TR) hat das Ziel, diese Lücke zwischen abstrakten und uneinheitlichen rechtlichen Anforderungen und der zuverlässigen technischen Realisierung des Scannens zu schließen. Auf Basis der bereits existierenden Empfehlungen[20] führt die TR entlang eines strukturierten Scanprozesses die sicherheitsrelevanten technischen und organisatorischen Maßnahmen, die beim ersetzenden Scannen zu berücksichtigen sind, zusammen. Dabei werden die Ziele der Informationssicherheit und der Rechtssicherheit gleichermaßen berücksichtigt. Die TR dient daher zum einen dem Anwender im behördlichen und privaten Bereich zur Erleichterung der Auswahl von Scan-Lösungen, indem eine Vereinheitlichung der Anforderungen und Sicherheitsmaßnahmen angestrebt wird. Zum anderen werden Herstellern und Dienstleistern notwendige Spezifikationen an die Hand gegeben, mittels derer diese ihre Leistungen TR-konform gestalten und anbieten können.

2 Rechtliche Aspekte des ersetzenden Scannens

Technisch erfolgt beim Scannen von Papierdokumenten eine Umwandlung von analogen in elektronische Daten, und das Medium wechselt von Papier zu elektronischen Datenspeichern. Rechtlich bedeutsam ist dieser Vorgang, weil dadurch die dem Papier immanente Sicherheitsmerkmale zum Integritäts- und Authentizitätsschutz verloren gehen und das elektronische Dokument neuen Risiken ausgesetzt ist. In diesem Zusammenhang stellen sich für das ersetzende Scannen aus rechtlicher Sicht im Wesentlichen drei Fragen: Erstens ist das ersetzende Scannen im Hinblick auf die gesetzlichen oder vertraglichen Dokumentations-, Aktenführungs- und Aufbewahrungspflichten zulässig und erfüllen die Scanprodukte diese Pflichten, so dass die Papierdokumente vernichtet werden dürfen. Sofern die Zulässigkeit bejaht werden kann, schließt sich zweitens die Frage an, ob bestimmte rechtliche, technische und organisatorische Anforderungen an den Scanprozess und das Scanprodukt zu stellen sind. Schließlich ist drittens zu fragen,

[20] Wie zum Beispiel [DOMEA], [IDW-FAIT3], [PK-DML, [GoBS], [GdPDU] und weiteren, deren Gültigkeit durch diese TR nicht beeinträchtigt wird.

welche Beweiswirkung das Scanprodukt hat, wenn es anstelle des Originals in ein Gerichtsverfahren als Beweis eingebracht wird [SCATE08:63][BMWi-HL-571:9].

Die rechtliche Zulässigkeit des ersetzenden Scannens ist nicht Gegenstand der Entwicklung der TR, sondern Voraussetzung für ihre Anwendung. In Bezug auf die Beweissicherheit steht nicht die abstrakte rechtliche Bewertung, sondern die konkrete Bewertung der technisch-organisatorischen Umsetzungsalternativen im Fokus der TR.

Rechtliche Anforderungen an das ersetzende Scannen sind entsprechend den Regelungen zur rechtlichen Zulässigkeit anwendungsspezifisch normiert. Der Gesetzgeber hat den Status des Papieroriginals maßgeblich für die Bestimmung der Anforderungen an die Ausgestaltung des ersetzenden Scannens festgelegt [SCATE08:80]. Soweit gesetzliche Vorschriften das ersetzende Scannen von Papierdokumenten – bei gleichzeitig bestehenden Dokumentations- und Aufbewahrungspflichten – erlauben, steht die Erlaubnis unter dem Vorbehalt der Umsetzung fachspezifischer gesetzlicher Anforderungen. Nur wenn diese gesetzlichen Vorschriften eingehalten werden, dürfen die Papierorginale vernichtet werden [BMWi-HL-571:16].

In folgenden Anwendungsgebieten sind derzeit gesetzliche Regelungen normiert, die ein ersetzendes Scannen ausdrücklich erlauben:

- Gerichtsakten (§ 299a ZPO für Prozessakten; § 298a ZPO für eingereichte Dokumente);
- Verwaltungsunterlagen (§ 6 RegR für Dokumente der Bundesministerien);
- Sozialversicherungsunterlagen (§ 110a Abs. 2 SGB IV; Sondervorschrift § 110d SGB IV für Dokumente, die der öffentlich rechtlichen Verwaltungstätigkeit zugrunde liegen);
- Röntgendokumentation (§ 28 Abs. 4 RöntgenVO);
- Kaufmännische Buchführungsunterlagen (§ 239 Abs. 4 HGB für Handelsbücher; § 257 Abs. 3 HGB für sonstige Unterlagen);
- Besteuerungsunterlagen (§ 147 Abs. 2 AO).

Obwohl sich die rechtlichen Anforderungen an das ersetzende Scannen von Papierdokumenten hinsichtlich Inhalt und Wortlaut unterscheiden, weisen diese eine weitgehende Homogenität hinsichtlich der gesetzlichen Anforderungen an den Scanprozess und das Scanprodukt auf:[21]

- Bildliche und inhaltliche Übereinstimmung zwischen dem Papieroriginal und dem Scanprodukt;
- Übereinstimmungsnachweis;
- Schutz vor Informationsveränderungen und Informationsverlusten;
- Dauerhafte Datenträger.

[21] Eine Ausnahme bildet hier § 110d SGB IV, da hier eine qualifizierte elektronische Signatur für den Übereinstimmungsnachweis gefordert wird [BMWi-HL-571:17].

3 Entwicklung und erste Ergebnisse der TR

Für die Entwicklung der TR wurde eine Markt-, Struktur-, Schutzbedarfs- und Bedrohungsanalyse für ein „typisches Scansystem“ und für den „generischen Scanprozess“ durchgeführt, der die Schritte Dokumentenvorbereitung, das eigentliche Scannen, die Nachverarbeitung und schließlich die Integritätssicherung umfasst (siehe Abbildung 1).

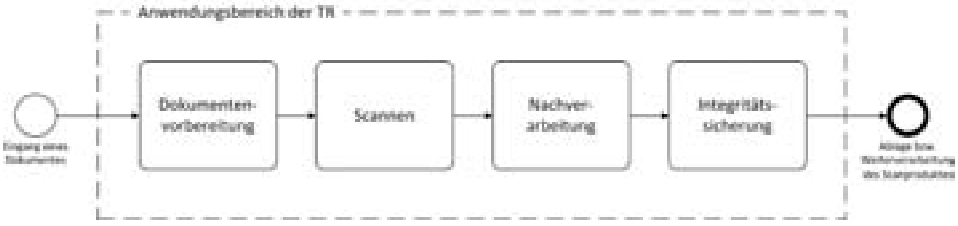

Abbildung 4: Der „generische Scanprozess“

Hieraus wurde ein modularer Anforderungs- und Maßnahmenkatalog entwickelt. Die Einhaltung der dort formulierten Anforderungen kann durch eine neutrale Stelle geprüft und objektiv bestätigt werden (Zertifizierung).

Die hierbei genutzte Methodik ist in informeller Weise an die internationalen Standards [ISO27001], [ISO27005], das IT-Sicherheitshandbuch [BSI-IT-SiHB] und die IT-Grundschutz-Vorgehensweise (siehe [BSI-100-2], [BSI-100-3]) des BSI angelehnt und umfasst die im Folgenden kurz erläuterten Aufgaben.

3.1 Struktur-, Schutzbedarfs- und Bedrohungsanalyse

Auf Basis des durch Abstraktion aus der Praxis abgeleiteten „generischen Scanprozesses“ und des „typischen Scansystemes“ wurden die im weiteren Verlauf zu betrachtenden Objekte identifiziert. Hierbei wurden insbesondere die relevanten Datenobjekte (Schriftgut, Scanprodukte, Sicherungsmittel, Protokolle et cetera), IT-Systeme, Netze und Anwendungen betrachtet.

Für diese identifizierten Objekte wurde in zwei Schritten eine detaillierte fachliche und technische Schutzbedarfsanalyse durchgeführt.

Im Rahmen der *fachlichen Schutzbedarfsanalyse* wurde zunächst ausgehend von den rechtlichen Anforderungen der Schutzbedarf der Datenobjekte ermittelt, wobei die differenzierten Sicherheitsziele „Integrität“, „Authentizität“, „Vollständigkeit“, „Nachvollziehbarkeit“, „Verfügbarkeit“, „Lesbarkeit“, „Verkehrsfähigkeit“, „Vertraulichkeit“ und „Löschbarkeit“ betrachtet wurden.

Die fachliche Schutzbedarfsanalyse für den Dokumententyp „*Gerichtsakten*“ führt zum Beispiel zu dem Ergebnis, dass folgende Kriterien für die Ausgestaltung der Aufbewahrung von Gerichtsakten, die im Scanprozess zu berücksichtigen sind:

- umfassender und effektiver Rechtsschutz,
- funktionsfähige Rechtspflege,
- das Recht auf Akteneinsicht sowie
- die Fortbildung des Rechts.

Darüber hinaus existieren noch weitere Kriterien, die allerdings nur bei einer Einzelfallbezogenen Schutzbedarfsanalyse herangezogen werden können, wie zum Beispiel das Prozessrisiko. Diese Kriterien wurden aus den Anforderungen abgeleitet, die an einen wirkungsvollen Rechtsschutz, denen die Gerichtsakten letztlich dienen, zu stellen sind. Dieser ergibt sich aus dem Rechtsstaatsprinzip des Art. 20 Abs. 1 GG sowie der Garantie des umfassenden und des effektiven Rechtsschutzes nach Art. 19 Abs. 4 GG durch unabhängige Gerichte [BVErfGE 54:277,291][Wi10:54][SCATE08:67]. Im Interesse einer funktionsfähigen Rechtspflege bestehen für die Gerichtsbarkeit eine umfassende Aktenführungspflicht sowie die Pflicht zur Aufbewahrung von Akten. Diese Verpflichtungen ergeben sich aus dem Recht der Verfahrensbeteiligten auf Information über den Verfahrensstoff. Dieses Recht lässt sich ausschließlich durch sorgfältige und nachvollziehbare Aktenführung und die Gewährung der Akteneinsicht[22] verwirklichen. Die Aufbewahrung von Gerichtsakten soll darüber hinaus zur Wahrung der Rechtseinheit und zur Fortbildung des Rechts dienen (§ 2 Abs. 2 SchrG). Die Zivilprozessordnung enthält ergänzende Vorschriften zur Führung und Aufbewahrung von Prozessakten. Es wird grundsätzlich zwischen Akten im laufenden Verfahren und Akten von rechtskräftig abgeschlossenen Verfahren differenziert. Gemäß § 298a Abs. 2 ZPO können die in Papierform eingereichten Unterlagen im laufenden Prozess zur Ersetzung der Urschrift in ein elektronisches Dokument umgewandelt werden. Nach § 298a Abs. 3 ZPO ist hierfür Voraussetzung, dass das elektronische Dokument einen Vermerk über die verantwortliche Person und den Zeitpunkt der Übertragung enthält. Darüber hinaus werden keine weiteren Anforderungen an die Ausgestaltung des Vermerks gestellt [Wi10:54]; [Greger in [Zö07], § 298a Rn.1, 2]. Die Originaldokumente sind nach § 298a Abs. 2 S. 2 ZPO mindestens bis zum rechtskräftigen Abschluss des Gerichtsverfahrens aufzubewahren, falls sie noch in Papierform benötigt werden.

Nach rechtskräftigem Abschluss eines Verfahrens können Prozessakten gemäß § 299a ZPO zur Ersetzung der Originale nicht nur auf einem Bildträger (Mikrofilm), sondern auch auf anderen Datenträgern wiedergegeben werden, sofern die Übertragung nach ordnungsgemäßen Grundsätzen erfolgt und ein schriftlicher Nachweis darüber vorliegt, dass die Wiedergabe mit der Urschrift übereinstimmt.[23]

[22] Dieses Recht ergibt sich unmittelbar aus dem Recht auf rechtliches Gehör (Art. 103 Abs. 1 GG) und informationelle Selbstbestimmung.

[23] In diesem Fall können die Gerichte den Prozessbeteiligten anstelle der Urschriften Ausfertigungen, Auszüge und Abschriften von dem Bild- und Datenträger erteilen.

Werden diese Voraussetzungen erfüllt, können die Papierakten vernichtet werden.[24] Somit besteht zwar eine grundsätzliche Möglichkeit für das ersetzende Scannen von Gerichtsakten, jedoch ist ihre konkrete Ausgestaltung durch den Gesetzgeber nicht vorgegeben worden [SCATE08:67].

Danach wurde in der *technischen Schutzbedarfsanalyse* der Schutzbedarf der IT-Systeme, Anwendungen und Kommunikationsbeziehungen hinsichtlich der Grundwerte „Integrität", „Verfügbarkeit" und „Vertraulichkeit" bestimmt.

Um die einfache Wiederverwendbarkeit der Ergebnisse im IT-Grundschutz-Kontext [BSI-100-2] zu gewährleisten, wurde der jeweilige Schutzbedarf in Abhängigkeit des Schutzbedarfs des ursprünglichen Papierdokumentes ausgedrückt und die differenzierten Sicherheitsziele wurden den oben genannten Grundwerten zugeordnet.

Bei der Bedrohungsanalyse wurden für die einzelnen Datenobjekte, IT-Systeme, Anwendungen und Kommunikationsverbindungen entsprechende Gefährdungen und Schwachstellen ermittelt. Hierbei wurden entlang des „generischen Scanprozesses" etwaige Bedrohungen ermittelt und geeignete Gegenmaßnahmen vorgeschlagen, die den identifizierten Gefährdungen entgegenwirken können. Dabei wurde auf anwendbare IT-Grundschutz-Bausteine[25] aufgebaut und bei Bedarf eine entsprechende Präzisierung und Ergänzung vorgenommen. Hierdurch ist ein für das ersetzende Scannen spezifischer Maßnahmenkatalog entstanden, der neben den generischen Gefährdungen und Maßnahmen aus dem IT-Grundschutzhandbuch auch eine Vielzahl von zusätzlichen anwendungsspezifischen Bedrohungen und Maßnahmen enthält.

Unter den spezifischen Bedrohungen in der *Dokumentenvorbereitung* finden sich beispielsweise die Manipulation oder die Vernichtung des Originals sowie das versehentliche Umdrehen einzelner Blätter in einem Scan-Stapel.

Beim *Scannen* könnten beispielsweise Fehler bei der Erfassung des Scangutes oder gezielte Manipulationen der Scan-Workstation oder des Scanners auftreten.

Bei der *Nachverarbeitung* könnte beispielsweise eine falsche Zuordnung der Index- und Metadaten erfolgen, wodurch das zukünftige Auffinden der Scanprodukte erschwert oder gar unmöglich gemacht werden würde.

Die *Integritätssicherung* könnte schließlich gar nicht oder mit ungeeigneten Sicherungsmitteln erfolgen und die eingesetzten kryptographischen Mechanismen könnten im Laufe der Zeit ihre Sicherheitseignung verlieren. Aus all diesen Gefährdungen ergibt sich ein mehr oder weniger großes Risiko, das den Beweiswert des Scanproduktes schmälern kann.

[24] Huber in [Mu2011], § 299a Rn. 1-2.

[25] Dies umfasst insbesondere die Bausteine 1.5 (Datenschutz), 1.6 (Schutz vor Schadprogrammen), 1.11 (Outsourcing), 1.12 (Archivierung), 3.101 (Allgemeiner Server), 3.201 (Allgemeiner Client), 3.406 (Drucker, Kopierer und Multifunktionsgeräte) sowie 5.7 (Datenbanken).

3.2 Modularer Anforderungskatalog

Um diesen Risiken entgegen zu wirken, wurden entsprechende technische und organisatorische Sicherheitsmaßnahmen festgelegt, die den identifizierten Gefährdungen entgegenwirken. Aus diesen Sicherheitsmaßnahmen wurden Anforderungen abgeleitet, die bei der richtlinienkonformen Ausgestaltung des Scanprozesses berücksichtigt werden müssen, sollen oder können. Um ein für den jeweiligen Anwendungsfall und damit für das konkrete Fachverfahren angemessenes Sicherheitsniveau erreichen zu können, wurde der Maßnahmenkatalog in einer modularen Weise aufgebaut. Bei der Entwicklung der TR wurde bewusst dieser Weg gewählt, damit der Anwender die für seinen konkreten Einsatzbereich angemessene Sicherheitsstufe wählen und dadurch die in betriebswirtschaftlicher Hinsicht effizienteste Lösung realisieren kann.

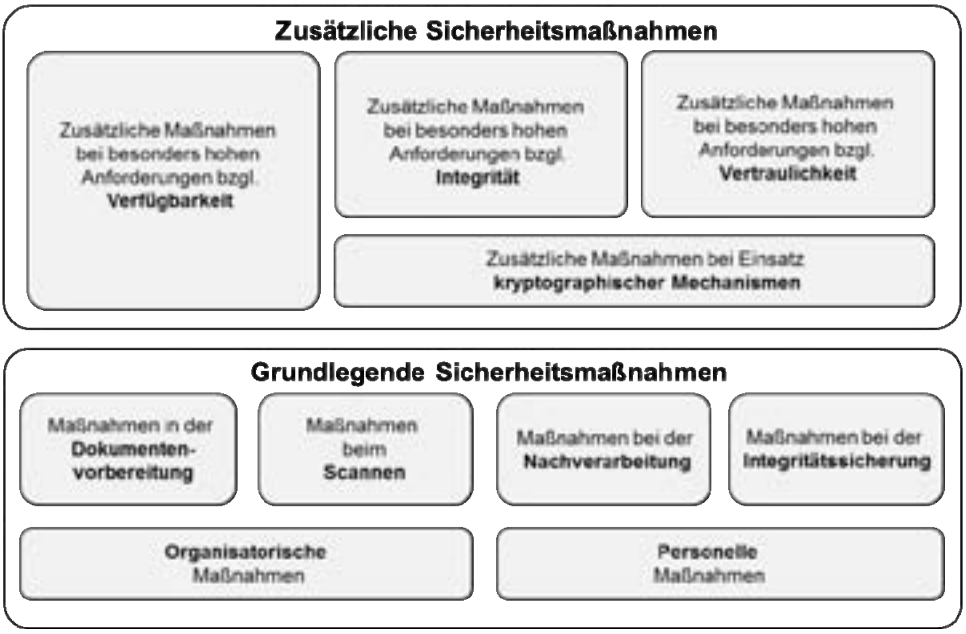

Abbildung 5: Der modulare Maßnahmenkatalog im Überblick

Der Maßnahmenkatalog sieht zunächst *grundlegende Sicherheitsmaßnahmen* vor, die für eine richtlinienkonforme Ausgestaltung des Scanprozesses notwendig sind. Diese umfassen übergreifende und somit in allen Phasen des Scanprozesses wirksame organisatorische Maßnahmen, wie zum Beispiel Festlegung von Verantwortlichkeiten und Funktionstrennung sowie personelle Maßnahmen, wie zum Beispiel Verpflichtung zur Einhaltung von Gesetzen, Sensibilisierung und Schulung der Mitarbeiter.

Darüber hinaus sieht die Richtlinie spezifische Maßnahmen in den verschiedenen Phasen des Scanprozesses vor. Dies umfasst beispielsweise:

- *Sicherheitsmaßnahmen in der Dokumentenvorbereitung*, wie die sorgfältige Vorbereitung der Papierdokumente, die Kennzeichnung der Dokumente bezüglich Sensitivität oder die Beschränkung des Zugriffs auf sensible Papierdokumente;

- *Sicherheitsmaßnahmen beim Scannen*, wie das sorgfältige Scannen, die Verwendung geeigneter Scan-Einstellungen, die Nutzung von Metainformationen aus der Dokumentenvorbereitung, die Durchführung geeigneter Schritte zur Qualitätssicherung sowie verschiedene Maßnahmen für Drucker, Kopierer, Scanner und Multifunktionsgeräte, wie zum Beispiel
    - die Definition von Kriterien für die Beschaffung und die geeignete Auswahl,
    - die geeignete Aufstellung und Inbetriebnahme,
    - die Änderung voreingestellter Passwörter,
    - die sorgfältige Durchführung von Konfigurationsänderungen,
    - die Beschränkung des Zugriffs und die Verwendung von sicheren Zugriffsmechanismen bei Fernadministration,
    - die geeignete Protokollierung und Auswertung,
    - die Netztrennung beim Einsatz von Multifunktionsgeräten und
    - die sichere Außerbetriebnahme.
- *Sicherheitsmaßnahmen bei der Nachbereitung*, wie die Durchführung von geeigneten Maßnahmen zur Qualitätssicherung und Nachbearbeitung und schließlich

- *Sicherheitsmaßnahmen bei der Integritätssicherung*, wie die Nutzung geeigneter Dienste und Systeme für den Integritätsschutz. Während die oben erläuterten Maßnahmen für ein grundlegendes Schutzniveau sorgen, können in bestimmten Anwendungsszenarien *zusätzliche Sicherheitsmaßnahmen* zum Schutz der Verfügbarkeit, Integrität und Vertraulichkeit empfehlenswert oder unmittelbar notwendig sein.

Beispielsweise empfiehlt sich für Sozialversicherungsträger (vgl. § 110d SGB IV) oder beim Scannen besonders schützenswerter Dokumente der Einsatz qualifizierter elektronischer Signaturen für die Integritätssicherung. In entsprechender Weise kann ein besonders hohes Maß an Vertraulichkeit durch Einsatz von geeigneten Verschlüsselungsmechanismen erreicht werden. In den beiden genannten Fällen sind darüber hinaus zusätzliche Maßnahmen für das Schlüsselmanagement, die Auswahl geeigneter kryptographischer Produkte und nicht zuletzt Aspekte der Nachsignatur beziehungsweise der Umschlüsselung zu beachten.

4 Zusammenfassung und Ausblick

Damit die Umsetzung der Vorgaben durch eine neutrale Stelle geprüft und bestätigt werden kann, wird schließlich aus dem Anforderungskatalog eine entsprechende Prüfspezifikation abgeleitet, die als Grundlage für zukünftige Prüfungen im Rahmen einer Zertifizierung dienen soll. Mit der damit möglichen Vergleichbarkeit von angebotenen Scanlösungen wird die Transparenz am Markt erhöht. Die TR kann zudem nach dem Vorbild zum Beispiel des elektronischen Personalausweises [PAuswV, Anhang 4] und De-Mail [§ 18 II De-Mail-G.] als zukünftiger Referenzpunkt für Rechtsvorschriften dienen, in denen auf die Einhaltung technisch-organisatorischer Anforderungen nach dem Stand der Technik, der bei Erfüllung der Anforderungen der TR vermutet wird, verwiesen wird.

Schließlich können die hier entwickelten Anforderungen an eine angemessen sichere und verbindliche Scanlösung als Mindeststandard nach § 8 I BSIG das Basis-Sicherheitsniveau für Scanprozesse, bei denen das Original nach Abschluss des Scannens vernichtet wird, zur Vereinheitlichung derartiger Abläufe beitragen. Die in der Praxis aufgeworfenen und aus der skizzierten uneinheitlichen Rechts- und Sachlage resultierenden Fragestellungen werden somit durch die TR im Hinblick auf die technisch-organisatorische Umsetzung adressiert. Gleichzeitig praktikable und rechtsverbindliche Lösungen werden damit einfacher umsetzbar. Durch den strukturierten modularen Ansatz mit an die jeweilige Fachanwendung anzupassenden sinnvollen Sicherheitsmaßnahmen trägt die TR zur notwendigen Vereinheitlichung der heterogenen Landschaft und zur Rechtssicherheit beim ersetzenden Scannen bei.

Literaturverzeichnis

[BMWi-HL-571]
Bundesministerium für Wirtschaft und Technologie Handlungsleitfaden zum Scannen von Papierdokumenten, BMWi - Dokumentation Nr. 571, 2008

[BSI-100-2]
Bundesamt für Sicherheit in der Informationstechnik (BSI): BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise

[BSI-100-3]
Bundesamt für Sicherheit in der Informationstechnik (BSI): BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz

[BSI-GSKat]
Bundesamt für Sicherheit in der Informationstechnik (BSI): IT-Grundschutz-Kataloge, 2011

[BSI-IT-SiHB]
Bundesamt für Sicherheit in der Informationstechnik (BSI): IT-Sicherheitshandbuch – Handbuch für die sichere Anwendung der Informationstechnik, 1992

[DOMEA]
KBSt: DOMEA-Konzept – Erweiterungsmodul zum DOMEA-Organisationskonzept 2.0, Scan-Prozesse, Schriftenreihe der KBSt, Band 64, Oktober 2004

[GdPDU]
Bundesministerium der Finanzen: Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU), BMF-Schreiben vom 16. Juli 2001 - IV D 2 - S 0316 - 136/01 -

[GoBS] Bundesministerium der Finanzen: Grundsätze ordnung-mäßiger DV-gestützter Buchführungssysteme (GoBS), Schreiben des Bundesministeriums der Finanzen an die obersten Finanzbehörden der Länder vom 7. November 1995 – IV A 8 – S 0316 – 52/95 – BStBl 1995 I S. 738

[IDW-FAIT3]
IDW RS FAIT 3: Grundsätze ordnungsmäßiger Buchführung beim Einsatz elektronischer Archivierungsverfahren, 2006

[ISO27001]
ISO/IEC 27001: Information technology – Security techniques – Information security management systems – Requirements, International Standard, 2005

[ISO27005]
ISO/IEC 27005: Information technology – Security techniques – Information security risk management, International Standard, 2008.

[Mu11] H. J. Musielak: ZPO-Kommentar, 8. Auflage, Franz Vahlen Verlag, 2011

[PK-DML]
Verband Organisations- und Informationssysteme (VOI): PK-DML Prüfkriterien für Dokumentenmanagement-Lösungen, 3. Auflage, 2008

[SCATE08]
A. Roßnagel, S. Fischer-Dieskau, S. Jandt, D. Wilke: Scannen von Papierdokumenten – Anforderungen, Trends und Empfehlungen, Band 18 der Reihe „Der elektronische Rechtsverkehr“, Nomos, 2008.

[Wi10] D. Wilke: Die rechtssichere Transformation von Dokumenten, Rechtliche Anforderungen an die Technikgestaltung und rechtlicher Anpassungsbedarf, Kassel 2010.

[Zö07] R. Zöller: Zivilprozessordnung, Kommentar, 26. neubearbeitete Auflage, Otto Schmidt Verlag, 2007.

Jörn von Lucke et al. (Hrsg.):
Auf dem Weg zu einer offenen, smarten und vernetzten Verwaltungskultur
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2012 137

Elektronische Identitäten – Öffentliche und private Initiativen

Erich Schweighofer, Walter Hötzendorfer

Universität Wien
Arbeitsgruppe Rechtsinformatik
Schottenbastei 10-16/2/5, 1010 Wien
{vorname.nachname}@univie.ac.at

Abstract: In der virtuellen Welt bedarf es eines umfassenden Identitätsmanagements. Den hohen Anforderungen des öffentlichen Sektors hinsichtlich der Eindeutigkeit der Identität werden die praxisnäheren privaten Federation-Modelle mit einer hohen Flexibilität sowie Relativität und Vielschichtigkeit der Identität gegenübergestellt. Die – notwendige und realisierbare – Integration beider Ansätze wird behandelt und es werden offene Forschungsfragen im Zusammenhang mit privaten Federation-Modellen besprochen. Auf Initiative österreichischer Unternehmen arbeitet derzeit eine Gruppe an der Entwicklung und Umsetzung eines privatwirtschaftlich geprägten Federation-Modells sowie an der Integration bestehender öffentlicher und privater Lösungen.

1 Einleitung

Während in der realen Welt die Identität einer natürlichen Person auf dem Menschen an sich beruht und von staatlicher Seite nur Hilfsmittel in Form von Personalausweisen angeboten werden müssen, bedarf es in der virtuellen Welt eines umfassenden Identitätsmanagements. Identitätsmanagement umfasst die Sammlung, Authentifizierung und Nutzung von Identitäten und damit verbundenen Informationen [HSC08].

Elektronische oder digitale Identitäten können definiert werden als „Sammlungen von digitalen Informationen, die zu einem Individuum oder einer Organisation gehören." [HM06, S. 543] Sie sind digitale Repräsentationen eines Teils der gesamten Identität einer Person (Teilidentitäten). Die einzelnen gespeicherten Informationen über einen Nutzer, die zusammen eine solche elektronische Identität bilden, werden als Attribute bezeichnet [PH10]. Für die virtuelle Welt gilt, dass es ohne die elektronische Identität praktisch keine Handlungsmöglichkeit gibt. Eine Person kann mehrere elektronische Identitäten besitzen. Gerade im Internet gibt es eine große Vielfalt an Identitäten, die Möglichkeiten reichen von der österreichischen Bürgerkarte mit eindeutiger Identifikation und Authentifizierung mittels Smartcard oder Handy-Signatur bis zur kurzfristig zugeordneten dynamischen IP-Adresse.

Die große Zahl von Identitäten verursacht hohe Kosten in der Wartung und bringt Datenschutzprobleme und das Risiko von fehlerhaften und inkonsistenten Daten mit sich. Daher gibt es vielerlei Anstrengungen, elektronische Identitäten zu schaffen, die für mehrere und nicht nur ein einzelnes Service im Internet verwendet werden können. Wichtige Beispiele sind von öffentlicher Seite die österreichische Bürgerkarte und in Deutschland der neue Personalausweis; von privater Seite Microsoft Passport, OpenID, Liberty Alliance Project, Facebook, Google et cetera.

Ziel des Ansatzes der in Kapitel 3 erläuterten Identity Federation ist die Verwendbarkeit bestehender Identitäten über Organisationsgrenzen hinweg, in Zusammenarbeit von Identitätsprovidern, Serviceprovidern und Attributsprovidern. Für jeden Geschäftsfall wird nur die unbedingt nötige Identität offengelegt und jede Person kann auch unter Personentypen oder Pseudonymen auftreten. Diesem entscheidenden Mehrwert an Datenschutz steht aber kein Verlust an Rechtssicherheit gegenüber: Im Streitfall wird der „Schleier" des Personentypus oder des Pseudonyms gelüftet.

2 Öffentliches Identitätsmanagement am Beispiel Österreichs

Die Ausgabe von Identitätsdokumenten ist seit langem eine wichtige staatliche Aufgabe. Die technologischen Möglichkeiten der Einbeziehung eines direkten Links zur jeweiligen Person haben sich nunmehr wesentlich erweitert: Beschreibung, Bild, Fingerabdrücke, et cetera. Neuere Identitätsdokumente sind maschinenlesbar und verfügen oft über einen RFID-Chip.[26] Das öffentliche Identitätsmanagement ist dadurch gekennzeichnet, dass der Eindeutigkeit der Personenbindung ein großer Stellenwert eingeräumt wird. In Österreich besteht das System Bürgerkarte, das technisch als Smartcard oder als Handy-Signatur ausgestaltet ist. Für kooperative Anwendungen werden derzeit in diesem Zusammenhang das Unternehmensserviceportal sowie das Bürgerserviceportal aufgebaut.

2.1 Bürgerkarte

Die Bürgerkarte ist eine logische Einheit, die technologisch unabhängig die Personenbindung mit einer qualifizierten elektronischen Signatur verbindet [§ 2 Z. 10 öE-GovG] [Ku08]. Bei natürlichen Personen erfolgt die eindeutige Identifikation mit der an das Zentrale Melderegister geknüpften Stammzahl, bei juristischen beziehungsweise nicht gemeldeten Personen mit der Ordnungsnummer des Firmenbuchs, Vereinsregisters oder des Ergänzungsregisters. Der Vorteil dieser Verknüpfung liegt in der Eindeutigkeit im Vergleich zu den mehrfach verwendeten Personennamen, die auch in Kombination mit dem Geburtsdatum häufig nicht eindeutig sind. Die Bürgerkarte wird im Standardfall auf der e-card (Sozialversicherungskarte) gespeichert. Die Authentifizierung erfolgt über eine qualifizierte elektronische Signatur; vornehmlich nunmehr als Handy-Signatur.

[26] Beispiele dafür sind der neue Personalausweis in Deutschland [Bo10] und das biometrische Großprojekt UID in Indien [Ec11].

2.2 Handy-Signatur

Die wesentliche Neuerung der Handy-Signatur besteht in der der sicheren Signaturerstellungseinheit (SSEE), mit welcher die elektronische Unterschrift erfolgt. Diese befindet sich nicht mehr in Form der Smartcard beim Nutzer, sondern auf einem Hochsicherheitsserver und wird mit einem per SMS an das Handy zugesandten Einmalpasswort vom Signator ausgelöst [Sc10] [KR10].[27] Die Handy-Signatur entspricht damit zwei Trends der IT: mehr Benutzerfreundlichkeit und Cloud Computing.

Die SSEE muss gewährleisten, dass die Signaturschlüssel praktisch nur einmal auftreten können, mit hinreichender Sicherheit nicht abgeleitet werden können, ihre Geheimhaltung hinreichend gewährleistet ist und die Signatur vor Fälschungen bei Verwendung der jeweils verfügbaren Technologie geschützt ist. Vom rechtmäßigen Unterzeichner müssen SSEE vor der Verwendung durch andere verlässlich geschützt werden können [Anhang III SigRL].

Bei der Handy-Signatur besteht die Signaturerstellungseinheit aus einem Rechner (HSM-Server), in dem sich ein Hardware Security Modul (HSM) vom Typ nShield 500e F31 befindet. Zu diesem Rechner in einem Safe im Hochsicherheitsbereich des Rechenzentrums hat nur spezielles Sicherheitspersonal Zugriff. Der Signator muss sich beim Hochsicherheitsrechner durch seine Mobilfunknummer und ein Signaturpasswort identifizieren; die Signaturerstellungseinheit wird sodann entschlüsselt. Zum Auslösen einer qualifizierten elektronischen Signatur wird an die Mobilfunknummer eine SMS mit einem vom HSM generierten, zeitlich begrenzt gültigen Einmalpasswort gesendet. Das Einmalpasswort ist über eine Signatur des HSM mit dem Hashwert der zu signierenden Daten verknüpft.

Die bisher im Zusammenhang mit der Bürgerkarte propagierten Komponenten der Signaturerstellung benötigt der Nutzer nicht mehr. Es ist nur mehr ein Handy erforderlich; die anderen Komponenten befinden sich im HSM. Kartenleser, Signatursoftware und Chipkarte sind nicht mehr notwendig.[28] Am „biometric touch“ wird nichts geändert; nach wie vor ist Geheimhaltung bestimmten Wissens und Besitz bestimmter Komponenten der stärkste Link zu einer bestimmten Person. Ohne Entschlüsselung der Signaturerstellungseinheit durch den Signator ist diese nicht verwendbar.

Die Handy-Signatur entspricht noch einem weiteren Trend, jenem zum Mobiltelefon als Universalinstrument des Menschen. Das Handy ist in Verbindung mit strengen Datensicherheitsauflagen sowie bei Verwendung von mobilen Transaktionscodes geeignet, den erforderlichen Link mit dem Signator sicherzustellen, sodass mittels sicherer Signaturerstellungseinheiten auf einem Hochsicherheitsserver rechtsverbindlich signiert werden kann. Weitere Sicherheitsmaßnahmen sind aus öffentlicher Sicht nicht erforderlich,

[27] Anbieter der Handy-Signatur ist A-Trust (http://www.a-trust.at). Vgl. zu den Sicherheitsauflagen die entsprechende Belehrung (https://www.a-trust.at/docs/belehrung/a-sign-premium-mobile/a-sign-premium-mobile-Belehrung.pdf, Zugriff am 15.01.2012).

[28] Auch die Online-Aktivierung der Bürgerkartenfunktion in Form der Handy-Signatur (mit postalischer Rückantwort) ist nunmehr möglich, sodass dies auch von zuhause aus durchgeführt werden kann [Fu11].

können aber je nach Nutzer durch Vereinbarung mit dem Signaturprovider vorgesehen werden [Sc10].[29]

2.3 Unternehmensserviceportal

Als Schnittstelle zur Wirtschaft wird vonseiten des Bundes das Unternehmensserviceportal als elektronisches Portal der österreichischen Wirtschaft aufgebaut.[30] Mit diesem zentralen Internetserviceportal für Unternehmen soll der elektronische Austausch von Informationen (Transaktionen) sowie die Bereitstellung von Informationen unterstützt werden. Ein wesentliches Ziel ist die Verringerung von Verwaltungslasten aus Informationsverpflichtungen. Mit der einmaligen Registrierung soll eine Vielzahl von Anwendungen der Verwaltung genutzt werden können. Die Verwendung einer eigenen einheitlichen Registrierungsnummer ist vorgesehen. Derzeit läuft ein Pilotbetrieb mit ausgewählten Unternehmen und Anwendungen.

Durch die Vielzahl von Meldeverpflichtungen, die Einbindung von E-Government-Anwendungen sowie die einheitliche Registrierungsnummer wird eine im Vergleich zum Firmenbuch verbesserte Identifikation von Unternehmen geboten. Neben der verbesserten Datenqualität liegt ein wesentlicher Vorteil auch darin, dass – im Gegensatz zur Stammzahl privater Personen – die Registernummer, Firmenbuchnummer, et cetera öffentlich ist und daher einheitlich verwendet werden kann. Je nach Bedarf kann in Verbindung mit einer Handysignatur, einer fortgeschrittenen Signatur, aber auch einfachen Signaturen eine hohe Transaktionssicherheit erreicht werden.

2.4 Bürgerserviceportal

Die Bundesministerien müssen für das Bürgerserviceportal HELP.gv.at möglichst verständliche und aktuelle Informationen zu Rechtsvorschriften und deren Entwürfen bereitstellen, um Bürger bei der Erfüllung von Informationspflichten zu unterstützen.

Eine Registrierung von Bürgern sowie die Einbindung von E-Government-Anwendungen in das Bürgerserviceportal sind aus Datenschutzgründen derzeit nicht vorgesehen. Die Option MyHELP als **personalisierte Version** von HELP bietet nur eine personenbezogene Unterstützung bei Informationen, Formularen und Behörden. Hierfür sind Daten zur persönlichen Lebenssituation einzugeben.

Die eindeutige Identifikation kann in der jeweiligen Geschäftsbeziehung erfolgen. Das österreichische E-Government-Gesetz [öE-GovG] verbietet aus Datenschutzgründen die Speicherung der einheitlichen Stammzahl. Nur das einem von 26 öffentlichen Anwendungsbereichen zuzuordnende, aus der Stammzahl der betroffenen Person und der Bereichskennung abgeleitete, auf diese nicht rückführbare bereichsspezifische Personenkennzeichen (bPK) darf verwendet werden. Im privaten Bereich tritt anstelle der

[29] Bei Verwendung von Smartphones ist es erforderlich, dass ein entsprechender Datensicherheitsstandard gegeben ist oder jedenfalls für die Transaktion ein vom Smartphone unabhängiger Rechner verwendet wird.
[30] https://www.usp.gv.at/Portal.Node/usp/public (Zugriff am 15.01.2012).

Bereichskennung die Stammzahl des Auftraggebers des privaten Bereichs [§ 14 öE-GovG].

3 Private Federation-Modelle

Der Großteil der Identifikations- und Authentifizierungsvorgänge im Internet erfolgt – ohne Einbeziehung der eben beschriebenen öffentlichen Systeme – zwischen Privaten, in der Regel zwischen Serviceprovidern und deren Nutzern. Jeder Serviceprovider verwaltet dazu üblicherweise Daten über seine Nutzer in Form von Nutzerkonten, welche die Nutzer beim erstmaligen Kontakt durch Eingabe selbstbehaupteter Daten angelegt haben [OM07]. Die laufende Identifikation und Authentifizierung der Nutzer erfolgt mittels Benutzername und Passwort. Die meisten der existierenden elektronischen Identitäten werden somit – in Form dieser Nutzerkonten – von Privatunternehmen verwaltet.

3.1 Grundlagen der Identity Federation

Ziel von privatwirtschaftlich geprägten Federation-Modellen ist es, diesen Status quo zu nützen und zugleich weiterzuentwickeln, indem sie die organisationsübergreifende Verwendung dieser elektronischen Identitäten ermöglichen. „Identity federation can thus be defined as a set of agreements, standards and technologies that enable SPs to recognise user identities and entitlements from other SPs.“ [JZS07, S. 147] Grundprinzip der Identity Federation ist also, dass der Nutzer nicht bei allen neu zu nutzenden Serviceprovidern eine elektronische Identität (ein Nutzerkonto) anlegt. Vielmehr veranlasst er, dass ihn Organisation A, bei der er bereits eine elektronische Identität angelegt hat, gegenüber Organisation B, deren Service er nutzen möchte, identifiziert, und dass Organisation A an Organisation B die zur Service-Nutzung benötigten Attribute des Nutzers übermittelt [Hi11]. Organisation A kann beispielsweise ein Serviceprovider sein, dessen Service(s) der Nutzer bereits verwendet, oder aber ein eigenständiger Identitätsprovider, dessen Hauptzweck die Authentifizierung von Nutzern sowie die Abwicklung des eben geschilderten Procedere ist und der ein besonderes Vertrauen seitens der Nutzer und der übrigen Teilnehmer einer Federation genießt. Das Konzept der Identity Federation schließt somit auch jenes der einmaligen Authentifizierung (Single-sign-on, SSO) [OM07, S. 344f.] mit ein, geht aber aufgrund seines organisationsübergreifenden Charakters und des Austauschs von Attributen weit darüber hinaus.

Die Umsetzung des Konzepts der Identity Federation bedarf eines institutionellen Rahmens, eines gemeinsamen Regelwerks und vertraglicher Beziehungen zwischen den beteiligten Organisationen. Das solcherart gebildete Netzwerk von Organisationen kann als Identity Ecosystem oder kurz als Federation bezeichnet werden, die einzelnen Organisationen als deren Teilnehmer.

Der Terminus Identity Ecosystem entstammt der National Strategy for Trusted Identities in Cyberspace (NSTIC) des Weißen Hauses. Diese definiert ein Identity Ecosystem als „an online environment where individuals and organizations can trust each other because they follow agreed-upon standards and processes to identify and authenticate their

digital identities—and the digital identities of organizations and devices. Similar to ecosystems that exist in nature, it will require disparate organizations and individuals to function together and fulfill unique roles and responsibilities, with an overarching set of standards and rules. The Identity Ecosystem will offer, but will not mandate, stronger identification and authentication while protecting privacy by limiting the amount of information that individuals must disclose." [Ns11, S. 21]

Für ein eng verwandtes Konzept wurde von der Liberty Alliance, deren Bestrebungen zur Förderung der Identity Federation nunmehr von der Kantara Initiative fortgesetzt werden, der Begriff Circle of Trust geprägt [OM07]. In Anlehnung an die drei von der Liberty Alliance unterschiedenen Modelle von Circles of Trust [Sh07] können drei verschiedene Organisationskonzepte einer Federation definiert werden, das konsortiale, das zentralisierte und das kollaborative Modell. Im kollaborativen Modell erstellen die Gründer der Federation gemeinsam deren Regelwerk und schaffen eine eigenständige zentrale Organisationseinheit, welche für die Weiterentwicklung und Einhaltung der Regeln sowie für den laufenden Betrieb der Federation sorgt. Eine konsortiale Federation besteht demgegenüber aus einem kleineren, beständigeren Kreis von Teilnehmern, die miteinander einen multilateralen Vertrag schließen. Charakteristikum des zentralisierten Modells ist die Dominanz des einzigen Gründers der Federation. Diesem Modell ähneln die beschriebenen Ansätze des öffentlichen Identitätsmanagements. Im Vergleich sind kollaborative Federations am besten skalierbar, da weder ihre Organisationsstruktur die Größe limitiert, noch ihr universeller Anspruch durch die Dominanz eines Teilnehmers konterkariert wird.

Trotz hoher Skalierbarkeit des kollaborativen Ansatzes ist nicht zu erwarten, dass sich in Zukunft eine einzelne große Federation entwickelt, welche die Nutzung aller erdenklichen Services im Internet ermöglicht. Stattdessen ist davon auszugehen, dass nebeneinander – ausgehend von bestimmten, zunächst möglicherweise eng gefassten Anwendungsdomänen – zahlreiche Federations entstehen. Um deren Interoperabilität zu gewährleisten bedarf es gemeinsamer Standards sowie eines Metamodells, mit welchem die Gemeinsamkeiten und Unterschiede verschiedener Federation-Modelle formalisiert werden können.

3.2 Stärken privater Federation-Modelle

Obwohl das Themengebiet Identity Federation im Rahmen der genannten Initiativen und zahlreicher Forschungsprojekte[31] insbesondere aus technischer Sicht bereits ausführlich erforscht wurde, sind den Autoren existierende kollaborative Federations außerhalb sehr enger Nischen nicht bekannt. Die Einführung solcher Federations brächte allerdings im Vergleich zum Status quo, der am Beginn von Kapitel 3 beschrieben wurde, viele Vorteile und insbesondere ein erhöhtes Datenschutz- und Datensicherheitsniveau mit sich [Ns11]. Die Nutzer würden sich die zeitraubende Registrierung und Wartung ihrer Identität bei den verschiedenen Serviceprovidern ersparen. Die derzeit übliche redundante Datenspeicherung bei den einzelnen Serviceprovidern vervielfacht zu-

[31] Insbesondere sind die einschlägigen von der EU in FP6 und FP7 geförderten Projekte, wie etwa FIDIS, PRIME, PrimeLife und TAS3 zu nennen.

dem die Angriffsfläche für unautorisierten Datenzugriff und die Vielzahl an benötigten Zugangsdaten birgt die Gefahr des sorglosen Umgangs mit Passwörtern durch die Nutzer.

Identity Federation führt somit potenziell zu höherer Datensicherheit und bietet den Serviceprovidern ein vertrauenswürdiges Identifikations- und Authentifizierungssystem sowie konsistente und aktuelle Nutzerdaten. Federations könnten überdies neue Nutzungsmöglichkeiten des Internets schaffen, weil die Nutzer ein Attribut wie beispielsweise ihr Alter nicht nur wie bisher behaupten, sondern belegen können, indem sie die Übertragung des Attributs von einem Attributsprovider veranlassen.

Im Regelwerk einer Federation kann für die Richtigkeit einer übertragenen Information (Identität, Attribut) eine Haftung der übertragenden Organisation und allenfalls des als Mittler zwischen den beteiligten Organisationen stehenden Identitätsproviders definiert werden. Die Haftung kann für mehrere abgestufte Sicherheitsniveaus unterschiedlich hoch festgelegt werden, sodass der eine Information bereitstellende Teilnehmer einer Federation abhängig von deren Sicherheitsniveau in unterschiedlichem Ausmaß für deren Richtigkeit haftet. Jeder Serviceprovider kann in der Folge das angemessene Sicherheitsniveau wählen, welches er von einem Nutzer für eine bestimmte Information verlangt und jeder Identitätsprovider kann selbst festlegen, welche Mittel der Authentifizierung er von den Nutzern für die jeweiligen Sicherheitsniveaus fordert, von Benutzername und Passwort für das niedrigste Niveau, bis hin zur Bürgerkarte oder etwa einer vom Identitätsprovider selbst ausgegebenen Smartcard für das höchste Niveau.

Die derzeitigen Datenschutzprobleme im Internet ergeben sich hauptsächlich daraus, dass gegenwärtig bei jedem Serviceprovider, dessen Service(s) man nutzen möchte, eine elektronische Identität angelegt werden muss. Die Nutzer können nicht mehr überblicken, wer welche Daten über sie gespeichert hat. Zudem müssen häufig mehr Daten angegeben werden, als für die Service-Nutzung erforderlich sind. In einer Federation ist hingegen jedes Attribut im Idealfall nur bei einer einzigen Organisation gespeichert, die als Attributsprovider fungiert und das jeweilige Attribut bei Bedarf an andere Teilnehmer der Federation übermitteln kann. Die Attribute eines Nutzers sind somit insgesamt auf mehrere Teilnehmer verteilt und werden nur im Bedarfsfall auf Veranlassung des Nutzers zusammengeführt. Eine Federation ermöglicht somit mehr Datensparsamkeit und verschafft den Nutzern Kontrolle und Nachvollziehbarkeit der Verwendung ihrer personenbezogenen Daten.[32] Zudem kann eine Federation so ausgestaltet werden, dass anonyme Transaktionen möglich sind und die Quelle einer Information dem Empfänger nicht zwangsläufig bekannt werden muss, die Transaktion im Schadensfall aber nachvollzogen werden kann.

[32] Wie dies gestaltet werden könnte, wird in [SJ10] beschrieben.

Anonyme Transaktionen entsprechen dem gewohnten Geschäftsverkehr, denn abseits des Internets ist es häufig nicht erforderlich, seine Identität offenzulegen, etwa bei einem Barkauf. Diese „Lebensnähe“ sowie eine möglichst nutzerfreundliche und nachvollziehbare Gestaltung einer Federation und der angebotenen Authentifizierungsmöglichkeiten, könnte die – bisher zurückhaltende – Nutzung des Internets für sicherheitssensible Anwendungen einerseits, andererseits auch für Transaktionen, deren Durchführung im Internet den Nutzern bisher zu kompliziert erschien, revolutionieren.

4 Integration öffentlichen und privaten Identitätsmanagements

Die beiden beschriebenen Systeme des Identitätsmanagements schließen sich keinesfalls gegenseitig aus, sondern können einander ergänzen. Identitätsprovider innerhalb einer Federation benötigen Mechanismen der Identifikation und Authentifizierung ihrer Nutzer. Ein Identitätsprovider kann mehrere solcher Mechanismen unterstützen, die verschiedenen Sicherheitsniveaus entsprechen können. Diese Mechanismen werden vom Nutzer bestimmt (zum Beispiel Nutzername und Passwort, Mobiltelefon/M-TAN), vom Identitätsprovider selbst ausgegeben (zum Beispiel Smartcard), oder sind öffentlich-rechtlicher Natur (Bürgerkarte).

Letzteres bedeutet, dass sich der Nutzer innerhalb einer Federation im Sinne des SSO bei einem Identitätsprovider, der dies unterstützt, identifiziert und authentifiziert und mittels dieses Identitätsproviders seine Bürgerkarten-Identität in der gesamten Federation nutzen kann. Dies wird ermöglicht, da § 14 des österreichischen E-Government-Gesetzes [öE-GovG] die Verwendung der Bürgerkartenfunktion im privaten Bereich unterstützt. Zu diesem Zweck wird aus der Stammzahl des Identitätsproviders und jener des Nutzers ein bPK gebildet, welches den Nutzer im Verhältnis zum Identitätsprovider eindeutig identifiziert. Festzuhalten ist, dass der Identitätsprovider weder aus diesem bPK noch auf andere Art Verknüpfungen zur übrigen Verwendung der Bürgerkartenfunktion durch den jeweiligen Nutzer im öffentlichen oder privaten Bereich herstellen kann.

Die Nutzung der Bürgerkarte ist in Österreich bisher weit hinter den Erwartungen geblieben [Sc10].[33] Ein Grund dafür könnte im privaten Bereich der erhebliche Aufwand sein, den die Bereitstellung einer Bürgerkartenumgebung für Serviceprovider mit sich bringt. Setzen sich private Federations durch, könnte dies die Verbreitung und Nutzung der Bürgerkarte fördern, denn durch die beschriebene Möglichkeit der Verwendung der Bürgerkartenfunktion innerhalb einer Federation mittels eines Identitätsproviders wird dieses Problem gelöst: Nicht mehr die einzelnen Serviceprovider, sondern nur noch

[33] Ob die bereits erwähnte neue Möglichkeit der Online-Aktivierung der Bürgerkartenfunktion in Form der Handy-Signatur [Fu11] dies ändern wird, bleibt abzuwarten.

mindestens) ein Identitätsprovider muss die für die Verwendung der Bürgerkarte notwendige technische Umgebung bereitstellen.[34]

Die Integration öffentlichen und privaten Identitätsmanagements ist nicht auf die Nutzung vom Staat ausgegebener elektronischer Identitäten für privatwirtschaftliche Services beschränkt. Mahler beschreibt den umgekehrten Fall am Beispiel des norwegischen E-Government-Identitätsportals („ID-porten“) [Ma12]. Über das System dieses Portals erkennen staatliche Stellen elektronische Identitäten an, die von Identitätsprovidern des privaten Sektors ausgegeben wurden. Dies setzt einen Vertrag des betreffenden Identitätsproviders mit der norwegischen E-Government-Behörde voraus und beinhaltet die Einstufung jeder elektronischen Identität in einen von vier „Assurance Levels“.

5 Umsetzung in der Praxis

Der Boden für eine technische Realisierung privater Federation-Modelle wurde durch bisherige Projekte bereits weitgehend aufbereitet.[35] Die Etablierung einer privatwirtschaftlich geprägten, kollaborativen Federation bringt aber zahlreiche weitere Herausforderungen mit sich. So muss die Federation den rechtlichen Bestimmungen, insbesondere dem Datenschutzrecht entsprechen, und erfordert ein fundiertes internes Regelwerk, in welches organisatorische, wirtschaftliche und juristische Überlegungen einfließen.

Eine Federation kann sich überdies nur etablieren, wenn unter den gegebenen sozioökonomischen Bedingungen für alle (potenziellen) Teilnehmer und Nutzer ein ausreichend großer Anreiz besteht, sich daran zu beteiligen. Dazu muss die Federation so gestaltet sein, dass die – oben beschriebenen – Vorteile einer Federation für jeden einzelnen Teilnehmer die Kosten übersteigen, die ihre Realisierung mit sich bringt. Zudem müssen diese Vorteile potenziellen Nutzern auch bekannt gemacht werden.

Auf Initiative österreichischer Unternehmen hat sich unter dem Akronym EUSTIC eine Gruppe zusammengefunden, die an einem Federation-Modell inklusive technischen Prototypen sowie an Anwendungsfällen und Geschäftsmodellen einer Federation arbeitet.[36] In dieser Initiative haben die Autoren die Rolle inne, die technische Umsetzung mit den rechtlichen Vorschriften in Einklang zu bringen, am internen Regelwerk mitzuarbeiten und insbesondere auch den Datenschutz im Vergleich zu derzeitigen Anwen-

[34] Die Bürgerkarte dient in diesem Szenario als sicheres Mittel zur Identifikation und Authentifizierung, erfüllt aber in Bezug auf die Serviceprovider nicht mehr die Funktion einer eigenhändigen Unterschrift im Sinne des § 4 Abs. 1 des österreichischen Signaturgesetzes [öSigG]. Diese Funktion spielt allerdings im Geschäftsverkehr im Internet bisher ohnehin eine geringe Rolle.

[35] Siehe dazu die Ergebnisse der bereits angesprochenen von der EU in FP6 und FP7 geförderten Projekte sowie die Technologien, die bereits in den in Kapitel 2 beschriebenen staatlichen Lösungen eingesetzt werden, und Standards wie insbesondere die Security Assertion Markup Language (SAML). Zum Einsatz von SAML siehe [SJ10] sowie die dort zitierte Literatur.

[36] EUSTIC (Enterprise- and User-oriented Strategy for Trust and Identity in Cyberspace) ist ein Vorhaben von 21 europäischen Projektpartnern und weiteren 60 Partnern in der anwendungsorientierten EUSTIC Partner Alliance. Siehe http://eustic.eu beziehungsweise http://www.univie.ac.at/RI/EUSTIC.

dungen (Facebook, Google et cetera) wesentlich zu verbessern. Als nächster Schritt ist die sozioökonomische Erprobung unter wissenschaftlicher Beteiligung geplant.

In der Wirtschaftskammer Österreich wird derzeit an einem Wirtschaftsportalverbund (WPV) gearbeitet.[37] Es sollen Spezifikationen und Musterverträge für ein „Trust Framework" erstellt werden. Dies entspricht dem Konzept der Federation. Die Einbeziehung öffentlicher Ansätze wie des Unternehmensserviceportals wird als wichtiger Teil dieses Vertrauensnetzwerks angesehen.

6 Schlussfolgerungen und zukünftige Forschung

Während die Bürgerkarte Identifikation, Authentifizierung und Nichtabstreitbarkeit auf einem gesetzlich – sehr hoch – festgelegten Sicherheitsniveau bietet, allerdings bei geringer Flexibilität, strebt Identity Federation verschiedene, das heißt alle denkbaren Sicherheitsniveaus an und zielt – unabhängig von spezifischen Identifikations- und Authentifizierungsmethoden – auf den (nutzerbestimmten) Austausch von Attributen entsprechend dem jeweiligen Bedarf an Sicherheit und Vertrauen ab. Aufgrund der verschiedenen Sicherheitsniveaus und Authentifizierungsmechanismen kann jede Aktivität eines Nutzers innerhalb einer Federation mit dem für diese Aktivität angemessenen Sicherheitsniveau durchgeführt werden. Die Teilnehmer einer Federation können wiederum darauf vertrauen, dass die Identitäten und Attribute der Nutzer dem jeweils geforderten Sicherheitsniveau genügen und dies mit einer entsprechenden Haftung verbunden ist.

Im Konzept der Identity Federation sind Identitäten relativ und vielschichtig. Von der strikten Personenbindung des österreichischen E-Government-Modells kann hier vielfach abgesehen werden. Es wird auf die Verhältnismäßigkeit zwischen der Notwendigkeit von strikter Personenbindung und Authentifizierung und dem Zweck der jeweiligen geschäftlichen oder privaten Beziehung abgestellt. Dem einheitlichen Modell des öffentlichen Sektors wird ein vielschichtiges und hochgradig vernetztes Federation-Modell gegenübergestellt.

Private Federation-Modelle befinden sich derzeit im Konzeptions- und Entwicklungsstadium. Bis zu deren Marktreife sind noch zahlreiche Forschungsfragen zu lösen. Ökonomisch ist vor allem zu untersuchen, wie eine Federation insgesamt, sowie aus der Sicht jedes einzelnen Teilnehmers wirtschaftlich betrieben werden kann, und wie man die Phase des Aufbaus einer Federation gestaltet, sodass ausreichend Teilnehmer einen wirtschaftlichen Anreiz haben, sich an der Federation zu beteiligen.

Juristisch besteht die Herausforderung vor allem in der Vielzahl von Rechtsgebieten, die bei der Konzeption einer Federation zu beachten und somit im Detail zu untersuchen sind. Zentrale Fragen sind die datenschutzrechtskonforme Ausgestaltung der Datenflüsse in einer Federation, die Haftung einzelner Teilnehmer einer Federation gegenüber anderen Teilnehmern sowie gegenüber den Nutzern, und welche gewerberechtlichen,

[37] http://reloaded.wko.at/wk/format_detail.wk?angid=1&stid=573341&dstid=1637 (Zugriff am 15.01.2012).

wettbewerbsrechtlichen und weiteren Bestimmungen Teilnehmer einer Federation zu beachten haben. Im europäischen Binnenmarkt müssen mehrere Rechtsordnungen berücksichtigt als die Fragen des grenzüberschreitenden Charakters, wie insbes. nach dem anwendbaren Recht, der Streitschlichtung sowie der Äquivalenz der jeweiligen elektronischen Identitäten geklärt werden.

Auch ein geeigneter Organisationsrahmen einer Federation, etwa in Form einer eigenen Trägerorganisation, muss gefunden werden, sodass ein detailliertes internes Regelwerk einer Federation definiert und dessen Einhaltung kontrolliert werden kann. Ein System ausschließlich bilateraler Verträge zwischen den einzelnen Teilnehmern ist dazu aus der Sicht der Autoren keine hinreichende Lösung, da nur eine zentrale Organisationseinheit basierend auf klar definierten Rechtsregeln, Politiken und Standards effizient für Compliance und Streitschlichtung sorgen kann. Diese Standards und das damit zusammenhängende, oben angesprochene Thema der Interoperabilität von Federations sind schließlich weitere Forschungsfelder, die hier zu nennen sind.

Mehrere Initiativen beschäftigen sich derzeit intensiv mit Lösungsansätzen zu den genannten Fragen, um das Thema Identity Federation voranzutreiben. Eine weitere Hürde ist die Etablierung einer Federation in der Praxis, denn diese erfordert, dass zahlreiche – zum Teil konkurrierende – Stakeholder an einem Strang ziehen. Den Autoren sind allerdings zahlreiche Unternehmen mit sehr konkreten Anwendungsfällen bekannt, die sich an Federations beteiligen möchten und auf ein einsatzfähiges Federation-Konzept warten, beziehungsweise sich an der Entwicklung eines solchen Konzepts beteiligen. Der Umgang mit elektronischen Identitäten im Internet könnte sich also schon bald nachhaltig verändern.

Literaturverzeichnis

[Bo10] Borges, G.: Der neue Personalausweis und der elektronische Identitätsnachweis. In: Neue Juristische Wochenschrift (NJW) 2010; S. 3334-3339.

[Ec11] The Economist: Reform by numbers: Opposition to the world's biggest biometric identity scheme is growing. In: The Economist, 14.01.2012; S. 39-40.

[Fu11] Futurezone.at: Handy-Signatur jetzt mit Online-Anmeldung. Futurezone.at, 2011. http://futurezone.at/digitallife/5135-handy-signatur-jetzt-mit-online-anmeldung.php (Zugriff am 15.01.2012).

[Hi11] Hitachi ID Systems: Identity Management Terminology. Hitachi ID Systems, Inc., 2011. http://hitachi-id.com/access-certifier/docs/identity-management-terminology.html (Zugriff am 15.01.2012).

[HM06] Hansen, M.; Meints, M.: Digitale Identitäten – Überblick und aktuelle Trends. In: Datenschutz und Datensicherheit 30, 2006; S. 543-547.

[HSC08] Hansen, M.; Schwartz, A.; Cooper, A.: Privacy and Identity Management. In: IEEE Security & Privacy 6 (2), 2008; S. 38-45.

[JZS07] Jøsang, A.; Zomai, M.; Suriadi S.: Usability and privacy in identity management architectures. In (Brankovic, L.; Coddington, P.; Roddick, J.F.; Steketee, C.; Warren, J.R.; Wendelborn, A. Hrsg.): ACSW '07 Proceedings of the fifth Australasian symposium on ACSW frontiers - Volume 68, Australian Computer Society, Inc., Darlinghurst, 2007; S. 143-152.

[KR10] Kustor, P.; Rössler, Th.: Mobile qualifizierte elektronische Signatur: technisches Konzept und rechtliche Bewertung. In (Schweighofer, E.; Geist, A.; Staufer, I. Hrsg.): Globale Sicherheit und proaktiver Staat – Die Rolle der Rechtsinformatik, Tagungsband des 13. Internationalen Rechtsinformatik Symposions IRIS 2010, gewidmet Roland Traunmüller. books@ocg.at, Österreichische Computer Gesellschaft, Wien, 2. Auflage 2010; S. 295-306.

[Ku08] Kustor, P.: Novellierungen im Signatur- und E-Government-Recht 2007. In (Schweighofer, E. et al. Hrsg.): Komplexitätsgrenzen der Rechtsinformatik, Tagungsband des 11. Internationalen Rechtsinformatik Symposions IRIS 2008. Boorberg Verlag, Stuttgart, 2008; S. 42-48.

[Ma12] Mahler, T.: Governance Models for Interoperable Electronic Identities. In: Journal of International Commercial Law and Technology (JICTL), Forthcoming; University of Oslo Faculty of Law Research Paper No. 2011-37.

[Ns11] NSTIC: NSTIC Strategy Document. The White House, 2011. http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf (Zugriff am 15.01.2012).

[öE-GovG] Bundesgesetz über Regelungen zur Erleichterung des elektronischen Verkehrs mit öffentlichen Stellen (E-Government-Gesetz - E-GovG), BGBl. I Nr. 10/2004, in der geltenden Fassung, zuletzt geändert: BGBl. I Nr. 111/2010. Elektronisch verfügbar: http://www.ris.bka.gv.at.

[OM07] Olsen, T.; Mahler T.: Identity management and data protection law: Risk, responsibility and compliance in 'Circles of Trust' – Part I + II. In: Computer Law & Security Report 23, 2007; S. 342-351, 415-426.

[öSigG] Bundesgesetz über elektronische Signaturen (Signaturgesetz - SigG), BGBl. I Nr. 190/1999, in der geltenden Fassung, zuletzt geändert: BGBl. I Nr. 75/2010. Elektronisch verfügbar: http://www.ris.bka.gv.at.

[PH10] Pfitzmann, A.; Hansen, M.: A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management Version v0.34. Technische Universität Dresden, Dresden, 2010. http://dud.inf.tu-dresden.de/Anon_Terminology.shtml (Zugriff am 15.01.2012).

[Sc10] Schweighofer, E.: Sind Handysignaturen qualifizierte elektronische Signaturen? In (Wimmer, M. et al. Hrsg.): Fachtagung Verwaltungsinformatik FTVI Fachtagung Rechtsinformatik FTRI 2010, Arbeitsberichte. Universität Koblenz-Landau, Koblenz, 2010; S. 78-81.

[Sh07] Sheckler, V. (Hrsg.): Liberty Alliance Contractual Framework Outline for Circles of Trust. Liberty Alliance Project, 2007, http://www.projectliberty.org/liberty/content/download/2962/19808/file/Liberty%20Legal%20Frameworks.pdf (Zugriff am 15.01.2012).

[SigRL] Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen (Signaturrichtlinie), ABl L 013, 12 vom 19.01.2000. Elektronisch verfügbar: http://eur-lex.europa.eu.

[SJ10] Scudder, J.; Jøsang, A.: Personal Federation Control with the Identity Dashboard. In (de Leeuw, E.; Fischer-Hübner, S.; Fritsch, L. Hrsg.): Policies and Research in Identity Management. Springer, Berlin, Heidelberg und New York, 2010; S. 85-99.

Autorenindex

GI-Edition Lecture Notes in Informatics

P-1 Gregor Engels, Andreas Oberweis, Albert Zündorf (Hrsg.): Modellierung 2001.

P-2 Mikhail Godlevsky, Heinrich C. Mayr (Hrsg.): Information Systems Technology and its Applications, ISTA'2001.

P-3 Ana M. Moreno, Reind P. van de Riet (Hrsg.): Applications of Natural Lan-guage to Information Systems, NLDB'2001.

P-4 H. Wörn, J. Mühling, C. Vahl, H.-P. Meinzer (Hrsg.): Rechner- und sensorgestützte Chirurgie; Workshop des SFB 414.

P-5 Andy Schürr (Hg.): OMER – Object-Oriented Modeling of Embedded Real-Time Systems.

P-6 Hans-Jürgen Appelrath, Rolf Beyer, Uwe Marquardt, Heinrich C. Mayr, Claudia Steinberger (Hrsg.): Unternehmen Hochschule, UH'2001.

P-7 Andy Evans, Robert France, Ana Moreira, Bernhard Rumpe (Hrsg.): Practical UML-Based Rigorous Development Methods – Countering or Integrating the extremists, pUML'2001.

P-8 Reinhard Keil-Slawik, Johannes Magenheim (Hrsg.): Informatikunterricht und Medienbildung, INFOS'2001.

P-9 Jan von Knop, Wilhelm Haverkamp (Hrsg.): Innovative Anwendungen in Kommunikationsnetzen, 15. DFN Arbeitstagung.

P-10 Mirjam Minor, Steffen Staab (Hrsg.): 1st German Workshop on Experience Management: Sharing Experiences about the Sharing Experience.

P-11 Michael Weber, Frank Kargl (Hrsg.): Mobile Ad-Hoc Netzwerke, WMAN 2002.

P-12 Martin Glinz, Günther Müller-Luschnat (Hrsg.): Modellierung 2002.

P-13 Jan von Knop, Peter Schirmbacher and Viljan Mahni_ (Hrsg.): The Changing Universities – The Role of Technology.

P-14 Robert Tolksdorf, Rainer Eckstein (Hrsg.): XML-Technologien für das Semantic Web – XSW 2002.

P-15 Hans-Bernd Bludau, Andreas Koop (Hrsg.): Mobile Computing in Medicine.

P-16 J. Felix Hampe, Gerhard Schwabe (Hrsg.): Mobile and Collaborative Business 2002.

P-17 Jan von Knop, Wilhelm Haverkamp (Hrsg.): Zukunft der Netze –Die Verletzbarkeit meistern, 16. DFN Arbeitstagung.

P-18 Elmar J. Sinz, Markus Plaha (Hrsg.): Modellierung betrieblicher Informationssysteme – MobIS 2002.

P-19 Sigrid Schubert, Bernd Reusch, Norbert Jesse (Hrsg.): Informatik bewegt – Informatik 2002 – 32. Jahrestagung der Gesellschaft für Informatik e.V. (GI) 30.Sept.-3. Okt. 2002 in Dortmund.

P-20 Sigrid Schubert, Bernd Reusch, Norbert Jesse (Hrsg.): Informatik bewegt – Informatik 2002 – 32. Jahrestagung der Gesellschaft für Informatik e.V. (GI) 30.Sept.-3. Okt. 2002 in Dortmund (Ergänzungsband).

P-21 Jörg Desel, Mathias Weske (Hrsg.): Promise 2002: Prozessorientierte Methoden und Werkzeuge für die Entwicklung von Informationssystemen.

P-22 Sigrid Schubert, Johannes Magenheim, Peter Hubwieser, Torsten Brinda (Hrsg.): Forschungsbeiträge zur "Didaktik der Informatik" – Theorie, Praxis, Evaluation.

P-23 Thorsten Spitta, Jens Borchers, Harry M. Sneed (Hrsg.): Software Management 2002 – Fortschritt durch Beständigkeit

P-24 Rainer Eckstein, Robert Tolksdorf (Hrsg.): XMIDX 2003 – XML-Technologien für Middleware – Middleware für XML-Anwendungen

P-25 Key Pousttchi, Klaus Turowski (Hrsg.): Mobile Commerce – Anwendungen und Perspektiven – 3. Workshop Mobile Commerce, Universität Augsburg, 04.02.2003

P-26 Gerhard Weikum, Harald Schöning, Erhard Rahm (Hrsg.): BTW 2003: Datenbanksysteme für Business, Technologie und Web

P-27 Michael Kroll, Hans-Gerd Lipinski, Kay Melzer (Hrsg.): Mobiles Computing in der Medizin

P-28 Ulrich Reimer, Andreas Abecker, Steffen Staab, Gerd Stumme (Hrsg.): WM 2003: Professionelles Wissensmanagement – Er-fahrungen und Visionen

P-29 Antje Düsterhöft, Bernhard Thalheim (Eds.): NLDB'2003: Natural Language Processing and Information Systems

P-30 Mikhail Godlevsky, Stephen Liddle, Heinrich C. Mayr (Eds.): Information Systems Technology and its Applications

P-31 Arslan Brömme, Christoph Busch (Eds.): BIOSIG 2003: Biometrics and Electronic Signatures

P-32 Peter Hubwieser (Hrsg.): Informatische Fachkonzepte im Unterricht – INFOS 2003

P-33 Andreas Geyer-Schulz, Alfred Taudes (Hrsg.): Informationswirtschaft: Ein Sektor mit Zukunft

P-34 Klaus Dittrich, Wolfgang König, Andreas Oberweis, Kai Rannenberg, Wolfgang Wahlster (Hrsg.): Informatik 2003 – Innovative Informatikanwendungen (Band 1)

P-35 Klaus Dittrich, Wolfgang König, Andreas Oberweis, Kai Rannenberg, Wolfgang Wahlster (Hrsg.): Informatik 2003 – Innovative Informatikanwendungen (Band 2)

P-36 Rüdiger Grimm, Hubert B. Keller, Kai Rannenberg (Hrsg.): Informatik 2003 – Mit Sicherheit Informatik

P-37 Arndt Bode, Jörg Desel, Sabine Rathmayer, Martin Wessner (Hrsg.): DeLFI 2003: e-Learning Fachtagung Informatik

P-38 E.J. Sinz, M. Plaha, P. Neckel (Hrsg.): Modellierung betrieblicher Informationssysteme – MobIS 2003

P-39 Jens Nedon, Sandra Frings, Oliver Göbel (Hrsg.): IT-Incident Management & IT-Forensics – IMF 2003

P-40 Michael Rebstock (Hrsg.): Modellierung betrieblicher Informationssysteme – MobIS 2004

P-41 Uwe Brinkschulte, Jürgen Becker, Dietmar Fey, Karl-Erwin Großpietsch, Christian Hochberger, Erik Maehle, Thomas Runkler (Edts.): ARCS 2004 – Organic and Pervasive Computing

P-42 Key Pousttchi, Klaus Turowski (Hrsg.): Mobile Economy – Transaktionen und Prozesse, Anwendungen und Dienste

P-43 Birgitta König-Ries, Michael Klein, Philipp Obreiter (Hrsg.): Persistance, Scalability, Transactions – Database Mechanisms for Mobile Applications

P-44 Jan von Knop, Wilhelm Haverkamp, Eike Jessen (Hrsg.): Security, E-Learning. E-Services

P-45 Bernhard Rumpe, Wofgang Hesse (Hrsg.): Modellierung 2004

P-46 Ulrich Flegel, Michael Meier (Hrsg.): Detection of Intrusions of Malware & Vulnerability Assessment

P-47 Alexander Prosser, Robert Krimmer (Hrsg.): Electronic Voting in Europe – Technology, Law, Politics and Society

P-48 Anatoly Doroshenko, Terry Halpin, Stephen W. Liddle, Heinrich C. Mayr (Hrsg.): Information Systems Technology and its Applications

P-49 G. Schiefer, P. Wagner, M. Morgenstern, U. Rickert (Hrsg.): Integration und Datensicherheit – Anforderungen, Konflikte und Perspektiven

P-50 Peter Dadam, Manfred Reichert (Hrsg.): INFORMATIK 2004 – Informatik verbindet (Band 1) Beiträge der 34. Jahrestagung der Gesellschaft für Informatik e.V. (GI), 20.-24. September 2004 in Ulm

P-51 Peter Dadam, Manfred Reichert (Hrsg.): INFORMATIK 2004 – Informatik verbindet (Band 2) Beiträge der 34. Jahrestagung der Gesellschaft für Informatik e.V. (GI), 20.-24. September 2004 in Ulm

P-52 Gregor Engels, Silke Seehusen (Hrsg.): DELFI 2004 – Tagungsband der 2. e-Learning Fachtagung Informatik

P-53 Robert Giegerich, Jens Stoye (Hrsg.): German Conference on Bioinformatics – GCB 2004

P-54 Jens Borchers, Ralf Kneuper (Hrsg.): Softwaremanagement 2004 – Outsourcing und Integration

P-55 Jan von Knop, Wilhelm Haverkamp, Eike Jessen (Hrsg.): E-Science und Grid Adhoc-Netze Medienintegration

P-56 Fernand Feltz, Andreas Oberweis, Benoit Otjacques (Hrsg.): EMISA 2004 – Informationssysteme im E-Business und E-Government

P-57 Klaus Turowski (Hrsg.): Architekturen, Komponenten, Anwendungen

P-58 Sami Beydeda, Volker Gruhn, Johannes Mayer, Ralf Reussner, Franz Schweiggert (Hrsg.): Testing of Component-Based Systems and Software Quality

P-59 J. Felix Hampe, Franz Lehner, Key Pousttchi, Kai Ranneberg, Klaus Turowski (Hrsg.): Mobile Business – Processes, Platforms, Payments

P-60 Steffen Friedrich (Hrsg.): Unterrichtskonzepte für inforrmatische Bildung

P-61 Paul Müller, Reinhard Gotzhein, Jens B. Schmitt (Hrsg.): Kommunikation in verteilten Systemen

P-62 Federrath, Hannes (Hrsg.): „Sicherheit 2005“ – Sicherheit – Schutz und Zuverlässigkeit

P-63 Roland Kaschek, Heinrich C. Mayr, Stephen Liddle (Hrsg.): Information Systems – Technology and ist Applications

P-64 Peter Liggesmeyer, Klaus Pohl, Michael Goedicke (Hrsg.): Software Engineering 2005

P-65 Gottfried Vossen, Frank Leymann, Peter Lockemann, Wolffried Stucky (Hrsg.): Datenbanksysteme in Business, Technologie und Web

P-66 Jörg M. Haake, Ulrike Lucke, Djamshid Tavangarian (Hrsg.): DeLFI 2005: 3. deutsche e-Learning Fachtagung Informatik

P-67 Armin B. Cremers, Rainer Manthey, Peter Martini, Volker Steinhage (Hrsg.): INFORMATIK 2005 – Informatik LIVE (Band 1)

P-68 Armin B. Cremers, Rainer Manthey, Peter Martini, Volker Steinhage (Hrsg.): INFORMATIK 2005 – Informatik LIVE (Band 2)

P-69 Robert Hirschfeld, Ryszard Kowalcyk, Andreas Polze, Matthias Weske (Hrsg.): NODe 2005, GSEM 2005

P-70 Klaus Turowski, Johannes-Maria Zaha (Hrsg.): Component-oriented Enterprise Application (COAE 2005)

P-71 Andrew Torda, Stefan Kurz, Matthias Rarey (Hrsg.): German Conference on Bioinformatics 2005

P-72 Klaus P. Jantke, Klaus-Peter Fähnrich, Wolfgang S. Wittig (Hrsg.): Marktplatz Internet: Von e-Learning bis e-Payment

P-73 Jan von Knop, Wilhelm Haverkamp, Eike Jessen (Hrsg.): “Heute schon das Morgen sehen“

P-74 Christopher Wolf, Stefan Lucks, Po-Wah Yau (Hrsg.): WEWoRC 2005 – Western European Workshop on Research in Cryptology

P-75 Jörg Desel, Ulrich Frank (Hrsg.): Enterprise Modelling and Information Systems Architecture

P-76 Thomas Kirste, Birgitta König-Riess, Key Pousttchi, Klaus Turowski (Hrsg.): Mobile Informationssysteme – Potentiale, Hindernisse, Einsatz

P-77 Jana Dittmann (Hrsg.): SICHERHEIT 2006

P-78 K.-O. Wenkel, P. Wagner, M. Morgenstern, K. Luzi, P. Eisermann (Hrsg.): Land- und Ernährungswirtschaft im Wandel

P-79 Bettina Biel, Matthias Book, Volker Gruhn (Hrsg.): Softwareengineering 2006

P-80 Mareike Schoop, Christian Huemer, Michael Rebstock, Martin Bichler (Hrsg.): Service-Oriented Electronic Commerce

P-81 Wolfgang Karl, Jürgen Becker, Karl-Erwin Großpietsch, Christian Hochberger, Erik Maehle (Hrsg.): ARCS´06

P-82 Heinrich C. Mayr, Ruth Breu (Hrsg.): Modellierung 2006

P-83 Daniel Huson, Oliver Kohlbacher, Andrei Lupas, Kay Nieselt and Andreas Zell (eds.): German Conference on Bioinformatics

P-84 Dimitris Karagiannis, Heinrich C. Mayr, (Hrsg.): Information Systems Technology and its Applications

P-85 Witold Abramowicz, Heinrich C. Mayr, (Hrsg.): Business Information Systems

P-86 Robert Krimmer (Ed.): Electronic Voting 2006

P-87 Max Mühlhäuser, Guido Rößling, Ralf Steinmetz (Hrsg.): DELFI 2006: 4. e-Learning Fachtagung Informatik

P-88 Robert Hirschfeld, Andreas Polze, Ryszard Kowalczyk (Hrsg.): NODe 2006, GSEM 2006

P-90 Joachim Schelp, Robert Winter, Ulrich Frank, Bodo Rieger, Klaus Turowski (Hrsg.): Integration, Informationslogistik und Architektur

P-91 Henrik Stormer, Andreas Meier, Michael Schumacher (Eds.): European Conference on eHealth 2006

P-92 Fernand Feltz, Benoît Otjacques, Andreas Oberweis, Nicolas Poussing (Eds.): AIM 2006

P-93 Christian Hochberger, Rüdiger Liskowsky (Eds.): INFORMATIK 2006 – Informatik für Menschen, Band 1

P-94 Christian Hochberger, Rüdiger Liskowsky (Eds.): INFORMATIK 2006 – Informatik für Menschen, Band 2

P-95 Matthias Weske, Markus Nüttgens (Eds.): EMISA 2005: Methoden, Konzepte und Technologien für die Entwicklung von dienstbasierten Informationssystemen

P-96 Saartje Brockmans, Jürgen Jung, York Sure (Eds.): Meta-Modelling and Ontologies

P-97 Oliver Göbel, Dirk Schadt, Sandra Frings, Hardo Hase, Detlef Günther, Jens Nedon (Eds.): IT-Incident Mangament & IT-Forensics – IMF 2006

P-98 Hans Brandt-Pook, Werner Simonsmeier und Thorsten Spitta (Hrsg.): Beratung in der Softwareentwicklung – Modelle, Methoden, Best Practices

P-99 Andreas Schwill, Carsten Schulte, Marco Thomas (Hrsg.): Didaktik der Informatik

P-100 Peter Forbrig, Günter Siegel, Markus Schneider (Hrsg.): HDI 2006: Hochschuldidaktik der Informatik

P-101 Stefan Böttinger, Ludwig Theuvsen, Susanne Rank, Marlies Morgenstern (Hrsg.): Agrarinformatik im Spannungsfeld zwischen Regionalisierung und globalen Wertschöpfungsketten

P-102 Otto Spaniol (Eds.): Mobile Services and Personalized Environments

P-103 Alfons Kemper, Harald Schöning, Thomas Rose, Matthias Jarke, Thomas Seidl, Christoph Quix, Christoph Brochhaus (Hrsg.): Datenbanksysteme in Business, Technologie und Web (BTW 2007)

P-104 Birgitta König-Ries, Franz Lehner, Rainer Malaka, Can Türker (Hrsg.) MMS 2007: Mobilität und mobile Informationssysteme

P-105 Wolf-Gideon Bleek, Jörg Raasch, Heinz Züllighoven (Hrsg.) Software Engineering 2007

P-106 Wolf-Gideon Bleek, Henning Schwentner, Heinz Züllighoven (Hrsg.) Software Engineering 2007 – Beiträge zu den Workshops

P-107 Heinrich C. Mayr, Dimitris Karagiannis (eds.) Information Systems Technology and its Applications

P-108 Arslan Brömme, Christoph Busch, Detlef Hühnlein (eds.) BIOSIG 2007: Biometrics and Electronic Signatures

P-109 Rainer Koschke, Otthein Herzog, Karl-Heinz Rödiger, Marc Ronthaler (Hrsg.) INFORMATIK 2007 Informatik trifft Logistik Band 1

P-110 Rainer Koschke, Otthein Herzog, Karl-Heinz Rödiger, Marc Ronthaler (Hrsg.) INFORMATIK 2007 Informatik trifft Logistik Band 2

P-111 Christian Eibl, Johannes Magenheim, Sigrid Schubert, Martin Wessner (Hrsg.) DeLFI 2007: 5. e-Learning Fachtagung Informatik

P-112 Sigrid Schubert (Hrsg.) Didaktik der Informatik in Theorie und Praxis

P-113 Sören Auer, Christian Bizer, Claudia Müller, Anna V. Zhdanova (Eds.) The Social Semantic Web 2007 Proceedings of the 1st Conference on Social Semantic Web (CSSW)

P-114 Sandra Frings, Oliver Göbel, Detlef Günther, Hardo G. Hase, Jens Nedon, Dirk Schadt, Arslan Brömme (Eds.) IMF2007 IT-incident management & IT-forensics Proceedings of the 3rd International Conference on IT-Incident Management & IT-Forensics

P-115 Claudia Falter, Alexander Schliep, Joachim Selbig, Martin Vingron and Dirk Walther (Eds.) German conference on bioinformatics GCB 2007

P-116 Witold Abramowicz, Leszek Maciszek (Eds.) Business Process and Services Computing 1st International Working Conference on Business Process and Services Computing BPSC 2007

P-117 Ryszard Kowalczyk (Ed.) Grid service engineering and manegement The 4th International Conference on Grid Service Engineering and Management GSEM 2007

P-118 Andreas Hein, Wilfried Thoben, Hans-Jürgen Appelrath, Peter Jensch (Eds.) European Conference on ehealth 2007

P-119 Manfred Reichert, Stefan Strecker, Klaus Turowski (Eds.) Enterprise Modelling and Information Systems Architectures Concepts and Applications

P-120 Adam Pawlak, Kurt Sandkuhl, Wojciech Cholewa, Leandro Soares Indrusiak (Eds.) Coordination of Collaborative Engineering - State of the Art and Future Challenges

P-121 Korbinian Herrmann, Bernd Bruegge (Hrsg.) Software Engineering 2008 Fachtagung des GI-Fachbereichs Softwaretechnik

P-122 Walid Maalej, Bernd Bruegge (Hrsg.) Software Engineering 2008 - Workshopband Fachtagung des GI-Fachbereichs Softwaretechnik

P-123 Michael H. Breitner, Martin Breunig, Elgar Fleisch, Ley Pousttchi, Klaus Turowski (Hrsg.)
Mobile und Ubiquitäre Informationssysteme – Technologien, Prozesse, Marktfähigkeit
Proceedings zur 3. Konferenz Mobile und Ubiquitäre Informationssysteme (MMS 2008)

P-124 Wolfgang E. Nagel, Rolf Hoffmann, Andreas Koch (Eds.)
9th Workshop on Parallel Systems and Algorithms (PASA)
Workshop of the GI/ITG Speciel Interest Groups PARS and PARVA

P-125 Rolf A.E. Müller, Hans-H. Sundermeier, Ludwig Theuvsen, Stephanie Schütze, Marlies Morgenstern (Hrsg.)
Unternehmens-IT:
Führungsinstrument oder Verwaltungsbürde
Referate der 28. GIL Jahrestagung

P-126 Rainer Gimnich, Uwe Kaiser, Jochen Quante, Andreas Winter (Hrsg.)
10th Workshop Software Reengineering (WSR 2008)

P-127 Thomas Kühne, Wolfgang Reisig, Friedrich Steimann (Hrsg.)
Modellierung 2008

P-128 Ammar Alkassar, Jörg Siekmann (Hrsg.)
Sicherheit 2008
Sicherheit, Schutz und Zuverlässigkeit
Beiträge der 4. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V. (GI)
2.-4. April 2008
Saarbrücken, Germany

P-129 Wolfgang Hesse, Andreas Oberweis (Eds.)
Sigsand-Europe 2008
Proceedings of the Third AIS SIGSAND European Symposium on Analysis, Design, Use and Societal Impact of Information Systems

P-130 Paul Müller, Bernhard Neumair, Gabi Dreo Rodosek (Hrsg.)
1. DFN-Forum Kommunikations-technologien Beiträge der Fachtagung

P-131 Robert Krimmer, Rüdiger Grimm (Eds.)
3rd International Conference on Electronic Voting 2008
Co-organized by Council of Europe, Gesellschaft für Informatik and E-Voting. CC

P-132 Silke Seehusen, Ulrike Lucke, Stefan Fischer (Hrsg.)
DeLFI 2008:
Die 6. e-Learning Fachtagung Informatik

P-133 Heinz-Gerd Hegering, Axel Lehmann, Hans Jürgen Ohlbach, Christian Scheideler (Hrsg.)
INFORMATIK 2008
Beherrschbare Systeme – dank Informatik
Band 1

P-134 Heinz-Gerd Hegering, Axel Lehmann, Hans Jürgen Ohlbach, Christian Scheideler (Hrsg.)
INFORMATIK 2008
Beherrschbare Systeme – dank Informatik
Band 2

P-135 Torsten Brinda, Michael Fothe, Peter Hubwieser, Kirsten Schlüter (Hrsg.)
Didaktik der Informatik –
Aktuelle Forschungsergebnisse

P-136 Andreas Beyer, Michael Schroeder (Eds.)
German Conference on Bioinformatics GCB 2008

P-137 Arslan Brömme, Christoph Busch, Detlef Hühnlein (Eds.)
BIOSIG 2008: Biometrics and Electronic Signatures

P-138 Barbara Dinter, Robert Winter, Peter Chamoni, Norbert Gronau, Klaus Turowski (Hrsg.)
Synergien durch Integration und Informationslogistik
Proceedings zur DW2008

P-139 Georg Herzwurm, Martin Mikusz (Hrsg.)
Industrialisierung des Software-Managements
Fachtagung des GI-Fachausschusses Management der Anwendungsentwicklung und -wartung im Fachbereich Wirtschaftsinformatik

P-140 Oliver Göbel, Sandra Frings, Detlef Günther, Jens Nedon, Dirk Schadt (Eds.)
IMF 2008 - IT Incident Management & IT Forensics

P-141 Peter Loos, Markus Nüttgens, Klaus Turowski, Dirk Werth (Hrsg.)
Modellierung betrieblicher Informations-systeme (MobIS 2008)
Modellierung zwischen SOA und Compliance Management

P-142 R. Bill, P. Korduan, L. Theuvsen, M. Morgenstern (Hrsg.)
Anforderungen an die Agrarinformatik durch Globalisierung und Klimaveränderung

P-143 Peter Liggesmeyer, Gregor Engels, Jürgen Münch, Jörg Dörr, Norman Riegel (Hrsg.)
Software Engineering 2009
Fachtagung des GI-Fachbereichs Softwaretechnik

P-144 Johann-Christoph Freytag, Thomas Ruf, Wolfgang Lehner, Gottfried Vossen (Hrsg.)
Datenbanksysteme in Business, Technologie und Web (BTW)

P-145 Knut Hinkelmann, Holger Wache (Eds.)
WM2009: 5th Conference on Professional Knowledge Management

P-146 Markus Bick, Martin Breunig, Hagen Höpfner (Hrsg.)
Mobile und Ubiquitäre Informationssysteme – Entwicklung, Implementierung und Anwendung
4. Konferenz Mobile und Ubiquitäre Informationssysteme (MMS 2009)

P-147 Witold Abramowicz, Leszek Maciaszek, Ryszard Kowalczyk, Andreas Speck (Eds.)
Business Process, Services Computing and Intelligent Service Management
BPSC 2009 · ISM 2009 · YRW-MBP 2009

P-148 Christian Erfurth, Gerald Eichler, Volkmar Schau (Eds.)
9th International Conference on Innovative Internet Community Systems
I^{2}CS 2009

P-149 Paul Müller, Bernhard Neumair, Gabi Dreo Rodosek (Hrsg.)
2. DFN-Forum Kommunikationstechnologien
Beiträge der Fachtagung

P-150 Jürgen Münch, Peter Liggesmeyer (Hrsg.)
Software Engineering
2009 - Workshopband

P-151 Armin Heinzl, Peter Dadam, Stefan Kirn, Peter Lockemann (Eds.)
PRIMIUM
Process Innovation for Enterprise Software

P-152 Jan Mendling, Stefanie Rinderle-Ma, Werner Esswein (Eds.)
Enterprise Modelling and Information Systems Architectures
Proceedings of the 3rd Int'l Workshop EMISA 2009

P-153 Andreas Schwill, Nicolas Apostolopoulos (Hrsg.)
Lernen im Digitalen Zeitalter
DeLFI 2009 – Die 7. E-Learning Fachtagung Informatik

P-154 Stefan Fischer, Erik Maehle Rüdiger Reischuk (Hrsg.)
INFORMATIK 2009
Im Focus das Leben

P-155 Arslan Brömme, Christoph Busch, Detlef Hühnlein (Eds.)
BIOSIG 2009:
Biometrics and Electronic Signatures
Proceedings of the Special Interest Group on Biometrics and Electronic Signatures

P-156 Bernhard Koerber (Hrsg.)
Zukunft braucht Herkunft
25 Jahre »INFOS – Informatik und Schule«

P-157 Ivo Grosse, Steffen Neumann, Stefan Posch, Falk Schreiber, Peter Stadler (Eds.)
German Conference on Bioinformatics 2009

P-158 W. Claupein, L. Theuvsen, A. Kämpf, M. Morgenstern (Hrsg.)
Precision Agriculture Reloaded – Informationsgestützte Landwirtschaft

P-159 Gregor Engels, Markus Luckey, Wilhelm Schäfer (Hrsg.)
Software Engineering 2010

P-160 Gregor Engels, Markus Luckey, Alexander Pretschner, Ralf Reussner (Hrsg.)
Software Engineering 2010 – Workshopband
(inkl. Doktorandensymposium)

P-161 Gregor Engels, Dimitris Karagiannis Heinrich C. Mayr (Hrsg.)
Modellierung 2010

P-162 Maria A. Wimmer, Uwe Brinkhoff, Siegfried Kaiser, Dagmar Lück-Schneider, Erich Schweighofer, Andreas Wiebe (Hrsg.)
Vernetzte IT für einen effektiven Staat
Gemeinsame Fachtagung Verwaltungsinformatik (FTVI) und Fachtagung Rechtsinformatik (FTRI) 2010

P-163 Markus Bick, Stefan Eulgem, Elgar Fleisch, J. Felix Hampe, Birgitta König-Ries, Franz Lehner, Key Pousttchi, Kai Rannenberg (Hrsg.)
Mobile und Ubiquitäre Informationssysteme
Technologien, Anwendungen und Dienste zur Unterstützung von mobiler Kollaboration

P-164 Arslan Brömme, Christoph Busch (Eds.)
BIOSIG 2010: Biometrics and Electronic Signatures Proceedings of the Special Interest Group on Biometrics and Electronic Signatures

P-165 Gerald Eichler, Peter Kropf, Ulrike Lechner, Phayung Meesad, Herwig Unger (Eds.)
10th International Conference on Innovative Internet Community Systems (I^2CS) – Jubilee Edition 2010 –

P-166 Paul Müller, Bernhard Neumair, Gabi Dreo Rodosek (Hrsg.)
3. DFN-Forum Kommunikationstechnologien
Beiträge der Fachtagung

P-167 Robert Krimmer, Rüdiger Grimm (Eds.)
4th International Conference on Electronic Voting 2010
co-organized by the Council of Europe, Gesellschaft für Informatik and E-Voting.CC

P-168 Ira Diethelm, Christina Dörge, Claudia Hildebrandt, Carsten Schulte (Hrsg.)
Didaktik der Informatik
Möglichkeiten empirischer Forschungsmethoden und Perspektiven der Fachdidaktik

P-169 Michael Kerres, Nadine Ojstersek Ulrik Schroeder, Ulrich Hoppe (Hrsg.)
DeLFI 2010 - 8. Tagung der Fachgruppe E-Learning der Gesellschaft für Informatik e.V.

P-170 Felix C. Freiling (Hrsg.)
Sicherheit 2010
Sicherheit, Schutz und Zuverlässigkeit

P-171 Werner Esswein, Klaus Turowski, Martin Juhrisch (Hrsg.)
Modellierung betrieblicher Informationssysteme (MobIS 2010)
Modellgestütztes Management

P-172 Stefan Klink, Agnes Koschmider Marco Mevius, Andreas Oberweis (Hrsg.)
EMISA 2010
Einflussfaktoren auf die Entwicklung flexibler, integrierter Informationssysteme
Beiträge des Workshops der GI-Fachgruppe EMISA (Entwicklungsmethoden für Informationssysteme und deren Anwendung)

P-173 Dietmar Schomburg, Andreas Grote (Eds.)
German Conference on Bioinformatics 2010

P-174 Arslan Brömme, Torsten Eymann, Detlef Hühnlein, Heiko Roßnagel, Paul Schmücker (Hrsg.)
perspeGKtive 2010
Workshop „Innovative und sichere Informationstechnologie für das Gesundheitswesen von morgen“

P-175 Klaus-Peter Fähnrich, Bogdan Franczyk (Hrsg.)
INFORMATIK 2010
Service Science – Neue Perspektiven für die Informatik
Band 1

P-176 Klaus-Peter Fähnrich, Bogdan Franczyk (Hrsg.)
INFORMATIK 2010
Service Science – Neue Perspektiven für die Informatik
Band 2

P-177 Witold Abramowicz, Rainer Alt, Klaus-Peter Fähnrich, Bogdan Franczyk, Leszek A. Maciaszek (Eds.)
INFORMATIK 2010
Business Process and Service Science – Proceedings of ISSS and BPSC

P-178 Wolfram Pietsch, Benedikt Krams (Hrsg.)
Vom Projekt zum Produkt
Fachtagung des GI-Fachausschusses Management der Anwendungsentwicklung und -wartung im Fachbereich Wirtschafts-informatik (WI-MAW), Aachen, 2010

P-179 Stefan Gruner, Bernhard Rumpe (Eds.)
FM+AM`2010
Second International Workshop on Formal Methods and Agile Methods

P-180 Theo Härder, Wolfgang Lehner, Bernhard Mitschang, Harald Schöning, Holger Schwarz (Hrsg.)
Datenbanksysteme für Business, Technologie und Web (BTW)
14. Fachtagung des GI-Fachbereichs „Datenbanken und Informationssysteme“ (DBIS)

P-181 Michael Clasen, Otto Schätzel, Brigitte Theuvsen (Hrsg.)
Qualität und Effizienz durch informationsgestützte Landwirtschaft, Fokus: Moderne Weinwirtschaft

P-182 Ronald Maier (Hrsg.)
6th Conference on Professional Knowledge Management
From Knowledge to Action

P-183 Ralf Reussner, Matthias Grund, Andreas Oberweis, Walter Tichy (Hrsg.)
Software Engineering 2011
Fachtagung des GI-Fachbereichs Softwaretechnik

P-184 Ralf Reussner, Alexander Pretschner, Stefan Jähnichen (Hrsg.)
Software Engineering 2011
Workshopband
(inkl. Doktorandensymposium)

P-185 Hagen Höpfner, Günther Specht, Thomas Ritz, Christian Bunse (Hrsg.)
MMS 2011: Mobile und ubiquitäre Informationssysteme Proceedings zur 6. Konferenz Mobile und Ubiquitäre Informationssysteme (MMS 2011)

P-186 Gerald Eichler, Axel Küpper, Volkmar Schau, Hacène Fouchal, Herwig Unger (Eds.)
11th International Conference on Innovative Internet Community Systems (I^2CS)

P-187 Paul Müller, Bernhard Neumair, Gabi Dreo Rodosek (Hrsg.)
4. DFN-Forum Kommunikations-technologien, Beiträge der Fachtagung 20. Juni bis 21. Juni 2011 Bonn

P-188 Holger Rohland, Andrea Kienle, Steffen Friedrich (Hrsg.)
DeLFI 2011 – Die 9. e-Learning Fachtagung Informatik
der Gesellschaft für Informatik e.V.
5.–8. September 2011, Dresden

P-189 Thomas, Marco (Hrsg.)
Informatik in Bildung und Beruf
INFOS 2011
14. GI-Fachtagung Informatik und Schule

P-190 Markus Nüttgens, Oliver Thomas, Barbara Weber (Eds.)
Enterprise Modelling and Information Systems Architectures (EMISA 2011)

P-191 Arslan Brömme, Christoph Busch (Eds.)
BIOSIG 2011
International Conference of the Biometrics Special Interest Group

P-192 Hans-Ulrich Heiß, Peter Pepper, Holger Schlingloff, Jörg Schneider (Hrsg.)
INFORMATIK 2011
Informatik schafft Communities

P-193 Wolfgang Lehner, Gunther Piller (Hrsg.)
IMDM 2011

P-194 M. Clasen, G. Fröhlich, H. Bernhardt, K. Hildebrand, B. Theuvsen (Hrsg.)
Informationstechnologie für eine nachhaltige Landbewirtschaftung
Fokus Forstwirtschaft

P-195 Neeraj Suri, Michael Waidner (Hrsg.)
Sicherheit 2012
Sicherheit, Schutz und Zuverlässigkeit
Beiträge der 6. Jahrestagung des Fachbereichs Sicherheit der
Gesellschaft für Informatik e.V. (GI)

P-197 Jörn von Lucke, Christian P. Geiger, Siegfried Kaiser, Erich Schweighofer, Maria A. Wimmer (Hrsg.)
Auf dem Weg zu einer offenen, smarten und vernetzten Verwaltungskultur
Gemeinsame Fachtagung Verwaltungsinformatik (FTVI) und Fachtagung Rechtsinformatik (FTRI) 2012

P-198 Stefan Jähnichen, Axel Küpper, Sahin Albayrak (Hrsg.)
Software Engineering 2012
Fachtagung des GI-Fachbereichs Softwaretechnik

P-200 Gero Mühl, Jan Richling, Andreas Herkersdorf (Hrsg.)
ARCS 2012 Workshops

The titles can be purchased at:

Köllen Druck + Verlag GmbH
Ernst-Robert-Curtius-Str. 14 · D-53117 Bonn
Fax: +49 (0)228/9898222
E-Mail: druckverlag@koellen.de