Schlussbericht

Vorhabenbezeichnung:

InfraNorm - Normungs- und Standardisierungspotenzial im Bereich des Schutzes von Verkehrsinfrastrukturen, Teilvorhaben: Normungshandbuch

Förderkennzeichen: 13N10915

Laufzeit des Vorhabens: März 2010 bis Februar 2013

Ausführende Stelle:

Technische Universität Berlin, Institut für Technologie und Management,
FG Innovationsökonomie, Herr Prof. Dr. Knut Blind

Gefördert vom
Bundesministerium
für Bildung
und Forschung

Inhaltsverzeichnis

Darstellungsverzeichnis

1 Einführende Aspekte in kurzer Darstellung

1.1 Aufgabenstellung

InfraNorms Teilvorhaben an der TU Berlin war durch zwei Zielsetzungen gekennzeichnet. Zunächst war der Bedarf an Normen und Standards in den Verbundprojekten zu ermitteln, die vom Bundesministerium für Bildung und Forschung (BMBF) im Themenfeld „Schutz von Verkehrsinfrastrukturen“ in der ersten Programmphase (2007 – 2011) des deutschen Sicherheitsforschungsprogramms gefördert wurden. Durch Erstellung eines Normungshandbuchs sollte ferner die weitgehend eigenständige Entwicklung von Normungs- und Standardisierungsvorhaben in weiteren Themenfeldern des Sicherheitsforschungsprogramms und auch in darüber hinausgehenden Forschungsprojekten initiiert und unterstützt werden. Neben grundlegenden Hilfestellungen zur Umsetzung von Normungs- und Standardisierungsvorhaben waren dabei insbesondere die Möglichkeiten der entwicklungsbegleitenden Erstellung von DIN Spezifikationen (DIN SPECs) zu erörtern und Spezifika der Sicherheitsforschung zu berücksichtigen.

1.2 Voraussetzungen, unter denen das Vorhaben durchgeführt wurde

Der Name InfraNorm stand für ein Querschnittsprojekt im Themenfeld „Schutz von Verkehrsinfrastrukturen“ des Programms „Forschung für die zivile Sicherheit“ der Bundesregierung. Das Projekt wurde von der Entwicklungsbegleitenden Normung (EBN) des DIN e.V. und dem Fachgebiet Innovationsökonomie der Technischen Universität Berlin durchgeführt. Es kooperierte mit den zehn BMBF-geförderten Verbundprojekten AISIS, SKRIBT, ORGAMIR, SinoVE Management, VeRSiert, Critical Parts, VESPER, V-SICMA, FluSs und SiVe.

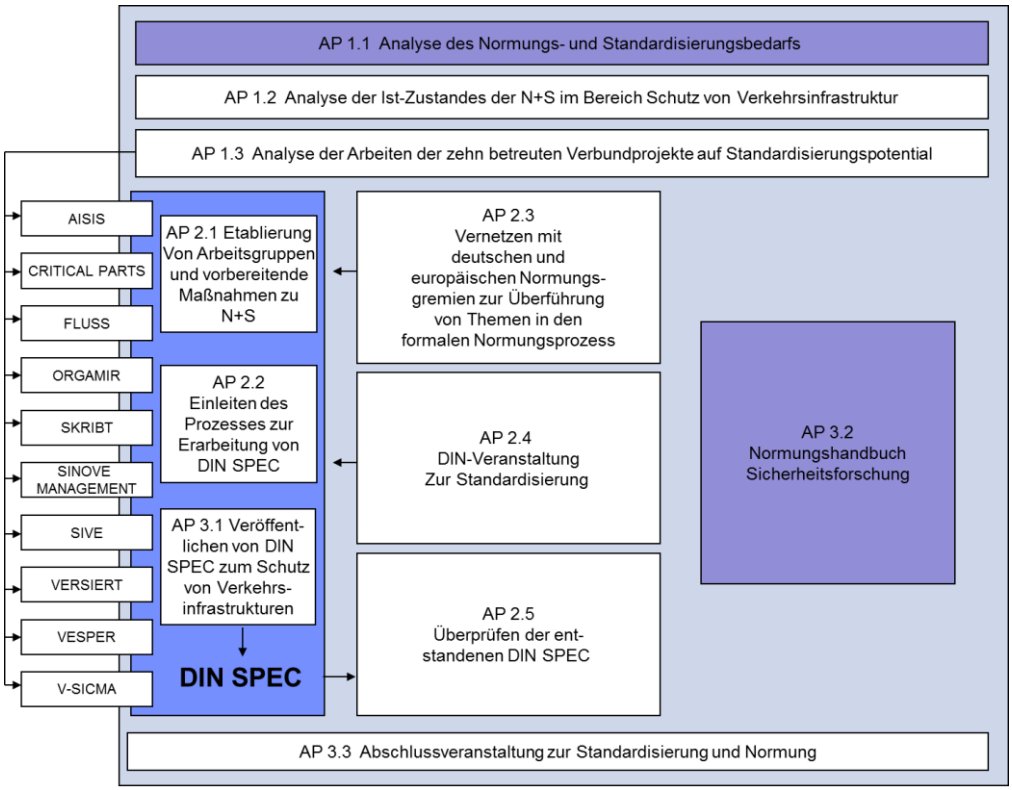
Da der Normungsbedarf im Themenfeld „Schutz von Verkehrsinfrastrukturen“ erst aufgrund von Zwischenergebnissen der weiteren Projekte dieses Bereichs ermittelt wurde, hatte InfraNorm im Vergleich zu diesen anderen Verbundprojekten eine zeitlich versetzte Laufzeit. Aus Sicht der Partnerprojekte konnte die Zusammenarbeit deshalb nicht im Voraus geplant werden. Innerhalb der jeweiligen Projekte waren daher durch Umplanungen geeignete Rahmenbedingungen für die Zusammenarbeit zu schaffen und Ressourcen bereitzustellen.

Die Ermittlung des Bedarfs an Normen und Standards erforderte die Mitwirkung von Teilnehmern der Verbundprojekte und externer Experten. Die Erstellung von Fallstudien für das Normungshandbuch war von der Bereitschaft des DIN und der Partner abhängig, TU-Forscher als Gast in die relevanten Normungs- bzw. Standardisierungsgremien aufzunehmen. Für weitere Fallstudien war die Interviewbereitschaft externer Experten erforderlich. Die angestrebte Mitwirkung geeigneter Ansprechpartner sowie die Aufnahme in verschiedene Normungs-/Standardisierungsarbeitsgruppen im Gaststatus konnten erfolgreich initiiert werden.

1.3 Planung und Ablauf des Vorhabens

Einführung

Für die Durchführung des Projektes wurden an der TU Berlin zwei Arbeitspakete vorgesehen. Das Arbeitspaket 1.1 Analyse des Normungs- und Standardisierungsbedarfs war in sechs Mannmonaten zu erbringen und im Projektmonat 15 abzuschließen. Arbeitspaket 3.2. hatte die Erstellung des Normungshandbuchs für die Sicherheitsforschung zum Inhalt. Für das Arbeitspaket, welches im 36. Projektmonat abzuschließen war, wurden 18 Mannmonate vorgesehen. Die Einbindung der beiden Arbeitspakete in das Gesamtprojekt wird in der folgenden Abbildung gezeigt.



Darst. 1: Ablaufschema des Projekts InfraNorm

Umsetzung von AP 1.1 Analyse des Normungs- und Standardisierungsbedarfs

Im Rahmen von AP 1.1 wurden drei Studien erstellt:

- Ergebnisse der ersten Befragung zum Normungs- und Standardisierungsbedarf für den Schutz von Verkehrsinfrastrukturen, Stand: 30. Juli 2010 (19 Seiten), Empfänger: 24 InfraNorm-Partner, 15 externe Experten
- Ergebnisse der zweiten Befragung zum Normungs- und Standardisierungsbedarf für den Schutz von Verkehrsinfrastrukturen, Stand: 15. September 2010 (20 Seiten), Empfänger: 24 InfraNorm-Partner, ausgewählte externe Experten
- Standards und Normen in den relevanten Themenfeldern des Projekts InfraNorm. Vorstudie, Stand: 6. Oktober 2010 (55 Seiten), Empfänger: 24 InfraNorm-Partner, 12 externe Experten

Die Studien basierten auf fünf Elementen:

- selbst entwickelte Interviewleitfäden und Fragebögen,
- Interviews mit InfraNorm-Partnern und externen Experten,
- Befragungsauswertungen und Interpretationen,
- Analysen relevanter Normen und Standards sowie
- Analysen relevanter Arbeitsgruppenaktivitäten in Normungs- und Standardisierungsorganisationen.

Zum Clustern der Normungs- und Standardisierungshinweise wurde die Software ATLAS.ti verwendet.

Umsetzung von AP 3.2 Normungshandbuch Sicherheitsforschung

Das Arbeitspaket hatte insbesondere drei Ergebnisse:

- Studie „Bedeutung von Sicherheitsnormen, -standards und -spezifikationen“ (45 Seiten, im Januar 2012 an die 468 Mitglieder der Innovationsplattform versendet)
- Studie Sicherheitsethik, Privacy und Normung (39 Seiten) sowie
- Normungshandbuch für die Teilnehmer des deutschen Sicherheitsforschungsprogramms

Über diese Beiträge hinausgehend wurden die Ergebnisse beider Arbeitspakete in zahlreichen nationalen und internationalen Fachartikeln und -konferenzen vorgestellt.

1.4 Wissenschaftlicher und technischer Stand, an den angeknüpft wurde

Stand der Wissenschaft und Technik

Viele innovationsökonomische Fragestellungen basieren auf einer langen Forschungstradition. So wurde beispielsweise Schumpeters innovationsökonomische Theorie bereits Mitte des 20. Jahrhundert veröffentlicht. Die angewandte Standardisierungsforschung im Kontext von Forschung und Innovation konnte bei Projektbeginn erst auf eine rund zehnjährige Tradition zurückblicken. Im Jahr 2009 wurde das Normungspolitische Konzept der Bundesregierung veröffentlicht. Eine konkrete Untersuchung zum Normungspotenzial von Sicherheitstechnologien und -dienstleistungen wurde jedoch noch nicht durchgeführt. Einige entsprechende Normungsgremien hatten sich zwar bereits konstituiert, doch ihre Arbeiten befanden sich noch im Anfangsstadium. Bedeutend waren dabei u.a. die folgenden Gremien:

- ISO/TC 223 Societal security (Sicherheit und Schutz des Gemeinwesens) sowie der deutsche Spiegelausschuss im deutschen Normenausschuss Feuerwehrwesen (FNFW)
- CEN/BT/WG 161 CEN BT/WG 161 'Protection and Security of the Citizen' sowie der deutsche Spiegelausschuss im Normenausschuss Feuerwehrwesen (FNFW)
- CEN/TC 391 'Security of the Citizen' (Sicherheit der Bürger) sowie der deutsche Spiegelausschuss im Normenausschuss Feuerwehrwesen (FNFW)

- CEN/TC 379 ‚Supply Chain Security' (Sicherheit von Lieferketten) sowie der deutsche Spiegelausschuss im Normenausschuss Feuerwehrwesen (FNFW)
- CEN/BT/WG 160 ‚Risk Assessment' (‚Risiko-Einschätzung und -Bewertung') sowie der deutsche Spiegelausschuss Sicherheitstechnische Grundsätze (NASG)

Konkret wurde der für InfraNorm relevante Stand der Forschung einerseits durch die Sicherheitsforschung und andererseits durch die Normungsforschung geprägt. Die vom Bundesministerium für Wirtschaft und Technologie (BMWi) bei der VDI/VDE Innovation + Technik GmbH in Auftrag gegebene Studie "Marktpotenzial von Sicherheitstechnologien und Sicherheitsdienstleistungen in Deutschland und Europa" kam dabei 2009 zu dem Ergebnis, dass die deutschen Unternehmen zur Erschließung ihres Potenzials eine Reihe von Maßnahmen benötigen. Die Normung wurde dabei als wesentliches Element herausgestellt.

Im Rahmen der Normungsforschung wurde auf europäischer Ebene die Studie „Standards in the Service Sector – An Explorative Study" (Blind, 20031) im Auftrag der Europäischen Kommission durchgeführt. Erstmals erfolgten dort Untersuchungen zu Standardisierungspotenzialen im Dienstleistungssektor. Mit dem Projekt „Dienstleistungsstandards für globale Märkte" wurde durch das BMBF von Februar 2000 bis Juni 2004 eine erste Initiative gefördert, die das Ziel hatte, Standardisierungspotenziale in der allgemeinen deutschen Dienstleistungswirtschaft zu erheben. Beide Projekte kamen zu dem Schluss, dass – auch aufgrund der großen Potenziale, die durch eine Standardisierung erschlossen werden können – der Zeitpunkt günstig sei, um die Standardisierung im Dienstleistungssektor voranzutreiben2.

Das Projekt COPRAS war eine unterstützende Maßnahme des 6. Europäischen Forschungsrahmenprogramms. Es zielte darauf ab, Transferleistungen zwischen IKT-Forschungsprojekten und IKT-Standardisierung zu verbessern. Dazu beabsichtigte es, Forschungsinstitute darin zu unterstützen, die relevanten Normungsorganisationen zu finden und Forschungsergebnisse in den Normungsprozess einzuspeisen. Für InfraNorm wurde u.a. die Broschüre COPRAS (2006)[3] verwendet. Das 2004 - 2006 durchgeführte EU-Projekt INTEREST hatte eine ähnliche Ausrichtung. Auf einigen Ergebnissen dieses Vorhabens konnte InfraNorm ebenfalls aufbauen.

Eine Reihe von Aspekten wurde in keinem der genannten Projekte thematisiert. Dabei handelt es sich insbesondere um:

- Die Aufarbeitung des aktuellen deutschen, europäischen und internationalen rechtlichen Kontexts der Sicherheitsstandardisierung
- Die systematische projektübergreifende Ermittlung von Standardisierungsbedarfen, -potentialen und -synergien
- Einen Wegweiser über derzeitige nationale, europäische und internationale Normungsinstrumente im Forschungskontext, z.B.
    - im Hinblick auf die FuE-Förderung und
    - den Umgang mit geistigen Eigentumsrechten

[1] http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.199.7671&rep=rep1&type=pdf

[2] Für InfraNorm attraktiv, wurde in diesem Bereich im Frühjahr 2010 ein security-bezogenes Standardisierungsprojekt begonnen. Dieses derzeit noch nicht abgeschlossene Vorhaben konnte durch die TU Berlin begleitet werden. Nach dem erwarteten Abschluss jenes Projekts im Sommer 2014 kann die entsprechende Fallstudie fertig gestellt werden.

[3] http://www.w3.org/2004/copras/docu/D26.pdf

- Maßnahmen zur Standardisierung deutscher FuE-Ergebnisse der Sicherheitsforschung zur Standortförderung
- Die Nutzung deutscher Normungsinstrumente für Forschungskontexte, vor allem von DIN SPECs
- Die Erarbeitung von Lösungen für Spezifika von Sicherheitslösungen im gesellschaftlichen Kontext.

Zusammengefasst war das vorliegende Teilvorhaben in seiner spezifischen Form bislang noch nicht Gegenstand anderweitiger Forschungen/ Entwicklungen/ Untersuchungen oder Patente.

Verwendete Fachliteratur, benutzte Informations- und Dokumentationsdienste

Da im Rahmen von InfraNorm ein Handbuch erstellt wurde, kam vielfältige Fachliteratur zum Einsatz. Die wichtigsten Werke sind dabei:

Bahke, T. (2002). Normen und Wettbewerb. Berlin 2002.

Bekkers, R. (2001). The development of European mobile telecommunications standards: An assessment of the success of GSM, TETRA, ERMES and UMTS (doctoral dissertation). Eindhoven University of Technology, The Netherlands.

Bekkers, R. (2011). Review of the literature. In: Blind, K. et al. (2011). Report of the Study on the Interplay between Standards and Intellectual Property Rights (IPRs). Berlin, Utrecht, Paris, Geneva, Oslo 2011, 17-28.

Bekkers, R., West, J. (2009). The Limits to IPR Standardization Policies as Evidenced by Strategic Patenting in UMTS. Telecommunications Policy 33 (2009) 80–97.

Best, K. (2007). Reducing the Cost of Standards Activities. http://support.kavi.com/documentation/white_papers/reducing_costs.pdf, Abruf am 14.04.2011.

Blarkom, G. W., Borking, John, J., Olk., J.G. (2003). Handbook of Privacy and Privacy-Enhancing Technologies - PISA Privacy Incorporating Software Agent. The Hague, 2003. Onlineversion: http://www.cbpweb.nl/downloads_technologie/pisa_handboek.pdf, Abruf am 13.03.2012.

Blind, K. (2008). Standardization and Standards in Security Research and Emerging Security Markets. Fraunhofer Symposium 'Future Security', 3rd Security Research Conference Karlsruhe, 10th - 11th September 2008, 63-72.

Blind, K. (2009). Standardisation: a catalyst for innovation. http://publishing.eur.nl/ir/repub/asset/17558/EIA-2009-039-LIS.pdf, Abruf am 25.10.2011.

Blind, K. (2010). Patentierung und Standardisierung - Komplementäre Strategien für Forschungseinrichtungen. PTB-Mitteilungen 120 (2010), Heft 4, 304-307. http://www.ptb.de/s/c/XCA5tN34/patentDB_Dokumente/A330.pdf, Abruf am 13.01.2013.

Blind, K., Bekkers, R., Dietrich, Y., Iversen, E., Köhler, F., Müller, B., Pohlmann, T., Smeets, S., Verweijen, J. (2011). Report of the Study on the Interplay between Standards and Intellectual Property Rights (IPRs). Berlin, Utrecht, Paris, Geneva, Oslo 2011.

Blind, K., Bierhals, R., Thumm, N., Hossain, K., Sillwood, J. Iversen, E., van Reekum, R., Rixius, B. (2002). Study on the Interaction between Standardisation and Intellectual Property Rights. EC Contract No G6MA-CT-2000-02001.

Blind, K., Gauch, S. (2007a). Probleme und Lösungsansätze. Warum Forscher wenig normen. In: Wissenschaftsmanagement, Special 2/2007, 14-15.

Blind, K., Gauch, S. (2007b). Forscher profitieren von Normung. Normen sollten parallel zu den Forschungsprozessen erarbeitet werden. In: Wissenschaftsmanagement, Special 2/2007, 16-17.

Blind, K., Gauch, S. (2009). Research and Standardisation in Nanotechnology: Evidence from Germany. In: Journal of Technology Transfer 34 (3), June 2009, 320-342.

Blind K, Iversen, E. (2004). The Interrelationship between IPR and Standardisation: Patterns and Policies. Presented at the EURAS Conference: Paris, 2004.

Blind, K., Jungmittag, A., Mangelsdorf, A. (2011). The Economic Benefits of Standardization. An update of the study carried out by DIN in 2000. http://www.din.de/sixcms_upload/media/2896/DIN_GNN_2011_engl_akt_neu.pdf, Abruf am 10.05.2013.

Blind, K., Nowak, B. (2008). Weiterführung der Untersuchung der Zusammenhänge von nationalen Normungstätigkeiten und dem wirtschaftlichen Erfolg von klein- und mittelständischen Unternehmen (KMUs) in der Luft- und Raumfahrindustrie, Projekt im Auftrag des Normenausschuss Luft- und Raumfahrt des DIN e.V. Berlin: DIN. http://www.nl.din.de/sixcms_upload/media/2566/INS_225_Endbericht_Deutsch.pdf, Abruf am 03.06.2010.

BMI [Hrsg.] (2005). Schutz Kritischer Infrastrukturen – Basisschutzkonzept. Empfehlungen für Unternehmen. Berlin 2005.

BMI (2009). Gesetz über Personalausweise und den elektronischen Identitätsnachweis sowie zur Änderung weiterer Vorschriften. http://www.bmi.bund.de/cae/servlet/contentblob/607490/publicationFile/35245/eperso.pdf, Abruf am 12.04.2012.

BMJ (2009). Bundesdatenschutzgesetz. (BDSG). http://bundesrecht.juris.de/bundesrecht/bdsg_1990/gesamt.pdf, Abruf am 27.08.2010.

Brim, S. (2004). Guidelines for Working Groups on Intellectual Property Issues. http://www.ietf.org/rfc/rfc3669.txt, Abruf am 12.11.2010 .

Cavoukian, A. (2011a). Privacy by Design. The 7 Foundational Principles. http://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples.pdf, Abruf am 20.03.2012.

Cavoukian, A. (2011b). Privacy by Design. Die 7 Grundprinzipien. http://privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples-german.pdf, Abruf am 20.03.2012.

CEN (2005). CWA 15263 “Analysis of Privacy Protection Technologies, Privacy- Enhancing Technologies (PET), Privacy Management Systems (PMS) and Identity Management systems (IMS), the Drivers thereof and the need for standardization”. http://www.cen.eu/cen/Sectors/Sectors/ISSS/CEN%20Workshop%20Agreements/Pages/DPPCWA.aspx, Abruf am 05.03.2012.

CEN (2010a). Guidance - Characteristics of the CEN/CENELEC Workshop Agreement and CEN/CENELEC Workshop guidelines. http://www.cen.eu/boss/supporting/guidance%20documents/gd052%20-%20cwa%20and%20cen%20workshop%20guidelines/Pages/default.aspx, Abruf am 12.11.2012.

CEN (2010b). CWA 16113:2010 “Personal Data Protection Good Practices”. http://www.cen.eu/cen/Sectors/Sectors/ISSS/CEN%20Workshop%20Agreements/Pages/DPPCWA.aspx, Abruf am 05.03.2012.

CEN/CENELEC (2010). CEN/CENELEC Guide 8. CEN-CENELEC Guidelines for Implementation of the Common IPR Policy (Patents and other statutory intellectual property rights based on inventions). Ed. 2. ftp://ftp.cenorm.be/BOSS/Reference_Documents/Guides/CEN_CLC/CEN_CLC_8.pdf, Abruf am 31.01.2011.

CEN/CENELEC (2012a). Guidance - Characteristics of the CEN/CENELEC Workshop Agreement and CEN/CENELEC Workshop guidelines. http://www.cen.eu/boss/supporting/

guidance%20documents/gd052%20-%20cwa%20and%20cen%20workshop%20guidelines/Pages/default.aspx, Abruf am 05.01.2013.

CEN/CENELEC (2012b). CEN-CENELEC Position Paper on Horizon 2020. http://www.cencenelec.eu/News/Policy_Opinions/PolicyOpinions/PPhorizon2020.pdf, Abruf am 26.06.2012.

CEN/CENELEC (o.D.). Linking research and standardization. Integrating standards in your research project: a pocket guide for project proposers. ftp://ftp.cencenelec.eu//Publications/Brochures/LinkingResearch.pdf, Abruf am 25.10.2011.

CEN-CENELEC STAIR (2011). The Operationalisation of the Integrated Approach: Submission of STAIR to the Consultation of the Green Paper "From Challenges to Opportunities: Towards a Common Strategic Framework for EU Research and Innovation funding". http://ec.europa.eu/research/horizon2020/pdf/contributions/post/european_organi-sations/ -cenelec_stair_joint_strategic_working_group.pdf, Abruf am 21.05.2012.

CoE [Council of Europe] (1981). Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten. Strasbourg, 28.I.1981. Zusatzprotokoll. Amtliche Übersetzung Deutschlands. http://conventions.coe.int/treaty/ger/treaties/html/108.htm, Abruf am 29.03.2012.

CoE [Council of Europe] (2010). Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Council of Europe Convention 108. http://conventions.coe.int/treaty/ger/treaties/html/108.htm, Abruf am 10.09.2010.

COPRAS (2006). Brochures. http://www.w3.org/2004/copras/docu/D26.pdf, Abruf am 11.11.2010.

de Brentani, U. (1991). Success Factors in Developing New Business Services. European Journal of Marketing, 25(2), 33 – 59.

de Vries, H. J. (1999). Standards for the Nation. Analysis of National Standardization Organisations. Bosten u.a. 1999.

Dejure (2012). Europäische Menschenrechtskonvention. http://dejure.org/gesetze/MRK/8.html, Abruf am 27.03.2012.

Die Bundesregierung (2009). Normungspolitisches Konzept der Bundesregierung. http://www.bmwi.de/BMWi/Redaktion/PDF/M-O/normungspolitisches-konzept-der-bundesregierung,property=pdf,bereich=bmwi,sprache=de,rwb=true.pdf, Abruf am 13.12.2011.

DIN (1994a). DIN 820 Teil 1 "Normungsarbeit – Grundsätze". Berlin 1994.

DIN (1994b). DIN 820 Teil 3 "Normungsarbeit – Begriffe". Berlin 1994.

DIN (2000). Economic Benefits of Standardization: Summary of Results. http://www.din.de/sixcms_upload/media/2896/economic_benefits_standardization.pdf, Abruf am 04.03.2010.

Dolmans, M. (2002). Standards for Standards. Paper for American Bar Association, Section of Antitrust law, Spring meeting 2002, Session on Trade Associations, Washington DC, April 26, 2002, and for the Joint Department of Justice Antitrust Division/Federal Trade EC Commission hearings on Competition and Intellectual Property Law and Policy in the Knowledge-Based Economy, Session on Comparative Law Topics: Licensing of Intellectual Property in Other Jurisdictions, Washington DC, May 22. http://www.ftc.gov/opp/intellect/020522dolmans.pdf, Abruf am 07.04.2011.

ECORYS (2009). Study on Competitiveness of the EU Security Industry. http://ec.europa.eu/enterprise/policies/security/files/study_on_the_competitiveness_of_the_eu_security_industry_en.pdf, Abruf am 25.04.2012.

Egyedi, T.M. (2007). Experts on causes of incompatibility between standard-compliant products. In: Doumeingts, G., J. P. Mueller, G. Morel, Vallespir, B. [Hrsg.] (2007). Enterprise

Interoperability. Berlin, Heidelberg, New York, 553-563.
Egyedi, T.M., Dahanayake, A. (2003). Difficulties Implementing Standards. In: Egyedi, T.M., Krechmer, K., & K. Jakobs (Eds.), Proceedings of the 3rd IEEE Conference on Standardization and Innovation in Information Technology, SIIT 2003, October 22-24 2003, Delft, the Netherlands, 75-84.
Ehmann, E. [Hrsg.] (2012). Lexikon für das IT-Recht. Die 140 wichtigsten Praxisthemen. Heidelberg, München, Landsberg, Frechen, Hamburg 2012.
Eisenhardt, K. M. (1989). Building Theories from Case Study Research. In: Academy of Management Review, 14(4), 532–550.
EPO (2012). Espacenet. http://documents.epo.org/projects/babylon/eponet.nsf/ 0/ 4E8744EB66E8F944C12577D600598EEF/$File/espacenet_brochure_en.pdf, Abruf am 07.02.2012.
Epstein, R. J., Marcus, A. J. (2003). Economic Analysis of the Reasonable Royalty: Simplification and Extension of the Georgia-Pacific Factors. Journal of the Patent & Trademark Office Society. Juli 2003.
ESRIF (2009). Final Report December 2009. http://ec.europa.eu/enterprise/policies/ security/files/esrif_final_report_en.pdf, Abruf am 01.04.2010.
ETSI (2010). Ex ante disclosures of licensing terms. http://www.etsi.org/WebSite/AboutETSI/ IPRsInETSI/Ex-ante.aspx, Abruf am 11.02.2011.
ETSI (2011). ETSI TR 187 020 V1.1.1 (2011-05). Technical Report Radio Frequency Identification (RFID); Coordinated ESO response to Phase 1 of EU Mandate M436. http://www.etsi.org/deliver/etsi_tr/187000_187099/187020/01.01.01_60/tr_187020v010101p.pdf, Abruf am 10.04.2012.
ETSI (2012). Making better standards: Practical ways to success. http://portal.etsi.org/mbs, Abruf am 20.08.2012.
EUR-Lex (2007). Verordnung (EG) Nr. 1321/2007 der Kommission vom 12. November 2007 zur Festlegung von Durchführungsbestimmungen für die Zusammenführung der gemäß der Richtlinie 2003/42/EG des Europäischen Parlaments und des Rates ausgetauschten Informationen über Ereignisse in der Zivilluftfahrt in einem Zentralspeicher http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:294:0003:0004: DE:PDF, Abruf am 13.02.2012.
EUR-Lex (2010a). Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:DE:HTML, Abruf am 16.05.2011.
EUR-Lex (2010b). Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:DE:HTML, Abruf am 16.05.2011.
EUR-Lex (2010c). Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks. http://eur-lex.europa.eu/Notice.do? mode=dbl&lng1=de,de&lang=&lng2=bg,cs,da,de,el,en,es,et,fi,fr,hu,it,lt,lv,mt,nl,pl,pt,ro,sk,sl,sv,&val=425159:cs&page=&hwords=null, Abruf am 16.05.2011.
EUR-Lex (2010d). Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation

in criminal matters. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do? uri=OJ:L:2008: 350:0060:01:DE:HTML, Abruf am 16.05.2011.

EUR-Lex (2010e). Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A Digital Agenda for Europe /* COM/2010/0245 f/2 */. http://eur-lex.europa.eu/ LexUriServ/LexUriServ.do?uri=COM:2010:0245:REV1:DE:HTML, Abruf am 16.05.2011.

EUR-Lex (2010f). Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr. Amtsblatt Nr. L 281 vom 23/11/1995 S. 0031 - 0050 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:DE:HTML, Abruf am 19.03.2012.

EUR-Lex (2010g). Richtlinie 2010/40/EU des europäischen Parlaments und des Rates vom 7. Juli 2010 zum Rahmen für die Einführung intelligenter Verkehrssysteme im Straßenverkehr und für deren Schnittstellen zu anderen Verkehrsträgern. http://eur-lex.europa.eu/ LexUriServ/LexUriServ.do?uri=OJ:L:2010:207:0001:0013:DE:PDF, Abruf am 05.04.2012.

EUR-Lex (2011). Strategic vision for European Standards, COM(2011)311. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0311:FIN:EN:PDF, Abruf am 22.08.2012.

EUR-Lex (2012). Mitteilung der Kommission an das Europäische Parlament und den Rat über die Verbesserung des Datenschutzes durch Technologien zum Schutz der Privatsphäre /* KOM/2007/0228 endg. */, Europäische Union, http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=de&type_doc=COMfinal&an_doc=2007&nu_doc=228, Abruf am 21.03.2012.

Europa (2010b). Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). http://europa.eu/legislation_summaries/information_society/l24120_de.htm, Abruf am 16.05.2011.

European Council (2010). The Stockholm Programme - An Open and Secure Europe Serving and Protecting Citizens. http://eur-lex.europa.eu/LexUriServ/ LexUriServ.do?uri=OJ: C:2010:115:0001:0038:en:PDF, Abruf am 01.11.2011.

Europäische Kommission (1992). Communication from the Commission "Intellectual Property Rights and Standardisation", COM (92) 445 final, Brussels 1992.

Europäische Kommission (2006). Grünbuch über Detektionstechnologien und ihre Anwendung durch Strafverfolgungs-, Zoll- und andere Sicherheitsbehörden. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52006DC0474:DE:NOT, Abruf am 13.08.2012.

Europäische Kommission (2007). Communication From the Commission to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs). http://eur-lex.europa.eu/LexUriServ/site/en/com/2007/ com2007_.pdf, Abruf am 26.01.2012.

Europäische Kommission (2008). Towards an increased contribution from standardisation to innovation in Europe. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do? uri=COM:2008: 0133:FIN:en:PDF, Abruf am 20.08.2012.

Europäische Kommission (2011). Programming Mandate Addressed to CEN, CENELEC and ETSI to Establish Security Standards. ftp://ftp.cen.eu/CEN/Sectors/List/Securityand Defence/SecurityoftheCitizen/M_487.pdf, Abruf am 01.02.2012.

Europäische Kommission (2012). COM(2012) 11 final. Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf, Abruf am 01.11.2012.

Europäische Union (2008). Richtlinie 2008/114/EG des Rates vom 8. Dezember 2008 über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern. Amtsblatt der Europäischen Union. Nr. L 345, 75-82.

Folmer, E. (2012). Quality of Semantic Standards. Enschede, NL 2012.

Fomin, V., Keil, T., Lyytinen, K. (2003). Theorizing about Standardization: Integrating Fragments of Process Theory in Light of Telecommunication Standardization Wars. Sprouts: Working Papers on Information Environments, Systems and Organizations, 3(1), 29-60.

Fräßdorf, H. (2008). Rechtsfragen des Zusammentreffens gewerblicher Schutzrechte, technischer Standards und technischer Standardisierung - Dissertation, Universität Hamburg, 2008.

Gauch, S. (2006). Towards a theoretical assessment of the link between research and standardisation, Proceedings of the 11th EURAS Workshop on Standardisation.

Grindley, P. (1995). Standards, Strategy and Policy. New York, NY 1995.

Hatto, P. (2010). Standards and Standardization Handbook. http://ec.europa.eu/research/industrial_technologies/pdf/handbook-standardisation_en.pdf, Abruf am 21.04.2011.

Hatto, P. (2013). Standards and Standardisation. A practical guide for researchers. European Union 2013.

Hofstede, G. (1991). Cultures and Organizations – Software of the Mind. Intercultural Cooperation and its importance for survival. McGraw-Hill 1991.

Hofstede, G. (2001). Lokales Denken, globales Management. Interkulturelle Zusammenarbeit und globales Management. 2. Aufl., München 2001.

Hofstede, G. (2003). Geert Hofstede™ Cultural Dimensions. http://www.geert-hofstede.com/hofstede_dimensions.php, Abruf am 12.12.2012.

Hommels, A., Egyedi, T.M. (2010). Beyond the 'Point of No Return': Constructing Irreversibility in Decision Making on the Tetra Standard in Dutch Emergency Communication. International Journal of IT Standards & Standardization Research, 8/1, 28-48.

ICO (2006). Data Protection Technical Guidance Note: Privacy enhancing technologies (PETs). http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/privacy_enhancing_technologies.pdf, Abruf am 02.02.2012.

ICO (2010). Privacy Impact Assessment Handbook 2.0. http://www.ico.gov.uk/upload/ documents/ pia_handbook_html_v2/, Abruf am 02.02.2012.

INTEREST (2006). INTEREST. Integrating Research and Standardisation. A Guide to Standardisation for R&D Organisations and Researchers. http://www-i4.informatik.rwth-aachen.de/Interest/Manual_R%26D.pdf, Abruf am 18.04.2011.

ISO (2011). ISO deliverables. http://www.iso.org/iso/standards_development/processes_and_procedures/deliverables.htm, Abruf am 17.11.2011.

ISO (2012). Standard Development Process. http://www.iso.org/iso/standards_development/processes_and_procedures/deliverables/deliverables_schema-2.htm, Abruf am 21.05.2012.

ISO/IEC (2009a). ISO/IEC Directives, Part 1. Procedures for the technical work. http://www.iec.ch/members_experts/refdocs/iec/Directives-Part1-Ed7.pdf, Abruf am 31.01.2011.

ISO/IEC (2009b). ISO/IEC Guide 2 "Standardization and related activities - General vocabulary". http://www.iec.ch/members_experts/refdocs/iec/Directives-Part1-Ed7.pdf, Abruf am 31.01.2011.

ITU (2012). Privacy in Cloud Computing. ITU-T Technology Watch Report March 2012.

Lin, C.-Y. (2006). Öffentliche Videoüberwachung in den USA, Großbritannien und Deutschland – Ein Drei-Länder-Vergleich. Dissertation an der Universität Göttingen. http://webdoc.sub.gwdg.de/diss/2006/lin/lin.pdf, Abruf am 06.08.2012.

Löwer, U. M. (2006). Interorganisational standards. Heidelberg [u.a.], 2006.

Madrid Resolution (2009). International Standards on the Protection of Personal Data and Privacy, International Conference of Data Protection and Privacy Commissioners. 5 November 2009. www.privacyconference2009.org/dpas_space/space_reserved/documentos_adoptados/common/2009_Madrid/estandares_resolucion_madrid_en.pdf, Abruf am 26.04.2013.

Morikawa, M., Morrison, J. (2006). Who Develops ISO Standards? A Survey of Participation in ISO's International Standards Development Processes. http://www.pacinst.org/reports/iso_participation/ iso_participation_study.pdf, Abruf am 05.01.2012.

Nagenborg, M. (2011). Körperscanner. In: Maring, M. (Hrsg.). Fallstudien zur Ethik in Wissenschaft, Wirtschaft, Technik und Gesellschaft. Schriftenreihe des Zentrums für Technik- und Wirtschaftsethik am Karlsruher Institut für Technologie, Band 4. Karlsruhe 2011. 236-242. http://digbib.ubka.uni-karlsruhe.de/volltexte/1000021177, Abruf am 07.08.2012.

OECD (2002). Kurzfassung OECD-Richtlinien über Datenschutz und grenzüberschreitende Ströme personenbezogener Daten. http://www.oecd.org/dataoecd/16/7/15589558.pdf, Abruf am 21.03.2012.

OECD (2010). OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. http://www.oecd.org/dataoecd/16/7/15589558.pdf, Abruf am 16.05.2011.

Olabarria Uzquiano, M. (2011). Working together in the CEN-CENELEC system. Präsentation am 08.04.2011 in Berlin.

Perinorm DIN, RUB (2008). http://www.ub.ruhr-uni-bochum.de/imperia/md/content/benutzung/db-infos/perinorm.pdf, Abruf am 21.04.2011.

Piersall, C. (2003). ISO/TC8 - Ships & Marine Technology" Time to Market" (The ISO/TC8 Case Study) to Second ISO Conference for Technical Committee and Subcommittee Chairs. Präsentation, Genf, 2003.

PRISE (2008a). Deliverable 3.2 - Legal Evaluation Report. http://prise.oeaw.ac.at/docs/PRISE_D3.2_Legal_Evaluation_Report.pdf, Abruf am 15.02.2012.

PRISE (2008b). Deliverable 6.2 - Criteria for privacy enhancing security technologies. http://prise.oeaw.ac.at/docs/PRISE_D_6.2_Criteria_for_privacy_enhancing_security_technologies.pdf, Abruf am 15.02.2012.

PRISE (2008c). Deliverable - 3.3 Proposal Report. Privacy enhancing shaping of security research and technology – A participatory approach to develop acceptable and accepted principles for European Security Industries and Policies. http://www.prise.oeaw.ac.at/docs/PRISE_D3.3_Proposal_Report.pdf, Abruf am 30.07.2012.

Privacyrights (2010a). Fair Information Principles (U.S. Dept. of Health, Education and Welfare, 1973). http://www.privacyrights.org/ar/fairinfo.htm, Abruf am 16.05.2011.

Privacyrights (2010b). Fair Information Practices (U.S. Dept. of Health, Education and Welfare, 1973). In: Smith, R. E. (1993). The Law of Privacy Explained by Robert Ellis Smith, Privacy Journal, 1993, 50-51. http://www.privacyrights.org/ar/fairinfo.htm#1, Abruf am 16.05.2011.

Rannenberg, K. (2011). Standardisation in electronic identity management. The Future of European Electronic Identity Management. Digital Enlightenment Foundation. http://www.digitalenlightenment.org/upload/pdf/K_Rannenberg_Standards-Paris. SC27WG5.pdf. Paris, 31.10.2011.

Riefler, B. (2008). The Composition of Working Groups in Industry-Specific Standardization Organizations. http://www.ivr.uni-stuttgart.de/mikro/RePEc/stt/download_dpaper/ composition_of_working_groups.pdf, Abruf am 14.04.2011.

Rost, M. (2009). Die „Neuen Datenschutz-Schutzziele. Because: code is not law. Berlin, 6.11.2009. https://www.datenschutzzentrum.de/vortraege/20091106-rost-datenschutz-schutzziele.pdf, Abruf am 21.02.2012.

Rost, M. (2010). Die Neuen Schutzziele. Beherrschbare, faire und vertrauenswürdige IT-Infrastrukturen. https://www.datenschutzzentrum.de/vortraege/20101026-rost-schutz ziele.pdf, Abruf am 14.03.2012.

Rost, M., Pfitzmann, A. (2009). Datenschutz-Schutzziele – revisited. Datenschutz-Schutzziele – revisited, in: DuD - Datenschutz und Datensicherheit, 33. Jahrgang, Heft 6, Juli 2009: 353-358. http://www.springerlink.com/content/c31u58k320074028/, Abruf am 12.03.2012.

Sack, D. K. (2007). Corporate Security – Standort-Security, Stuttgart/Berlin.

Sáez, A. C., Urech, A., Pereira, J. (2009). Current status of Security in Mass Transport. DEMASST Deliverable 3.1: Current status of security in mass transport. November 2009.

Schmid, V. (2010). German Privacy and IT-Security Law (Its Law) as a Contribution to the European Area of Freedom, Security and Justice? Paper presented at the 5th Security Research Conference. Berlin 2010.

Schmidt, S., Werle, R. (1998). Coordinating Technology: Studies in the International Standardization of Telecommunications. Cambridge, MA, London 1998.

Shapiro, C. (2001). Navigating the Patent Thicket: Cross Licenses, Patent Pools, and Standard Setting. Innovation Policy and the Economy, Vol. 1, 119-150.

Sherif, M. H. (2001). Contribution Towards A Theory Of Standardization In Telecommunications. Paper presented at the 1st IEEE Conference on Standardisation and Innovation in Information Technology, Aachen 1999. www-i4.informatik.rwth-aachen.de/~jakobs/ sit99/proceedings/ Sherif.doc, Abruf am 26.06.2010.

Sherif, M. H., Jakobs, K., Egyedi, T. M. (2007). Standards of quality and quality of standards for Telecommunications and Information Technologies. In: Hörlesberger, M. Elnawawi, M. Khalil, T. (Eds.). Challenges in the Management of New Technologies. Singapore 2007, 427-447.

Solove, D. (2002). Conceptualizing Privacy. California Law Review, 90, 1087. Onlineversion: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=313103, Abruf am 13.03.2012.

Swann, G. P. (2000). The Economics of standardization. Final Report for Standards and Technical Regulations Directorate Department of Trade and Industry. Manchester Business School. University of Manchester Manchester 2000.

Tassey, G. (1982). The Role of Government in Supporting Measurement Standards for High-Technology Industries, Research Policy, 11, 311-320.

Tassey, G. (2000). Standardization in Technology-Based Markets. Research Policy, 29 (4-5), 587-602.

Thoma, K. (2010). Positionspapier des wissenschaftlichen Programmausschusses zum nationalen Sicherheitsforschungsprogramm. http://www.bmbf.de/pubRD/WPA_Positions papier_2010.pdf, Abruf am 14.11.2010.

UDHR (1948). Universal Declaration of Human Rights, Abruf über http://www.udhr.org/UDHR/ART29.HTM am 27.03.2012.

Updegrove, A. (2007a). Chapter 2: Participating In Standard Setting Organizations: Value Propositions, Roles And Strategies. http://www.consortiuminfo.org/ essentialguide/ participating1.php, Abruf am 23.05.2011.
Updegrove, A. (2007b). Chapter 3: Getting the Most from Your Membership. Essential Guide to Standards. http://www.consortiuminfo.org/essentialguide/participating2.php, Abruf am 14.04.2011.
Varian, H. R. (1996). Economic Aspects of Personal Privacy, University of California at Berkeley. http://www.sims.berkeley.edu/~hal/Papers/privacy/, Abruf am 20.02.2012.
VDI/VDE/IT (2009). Marktpotenzial von Sicherheitstechnologien und Sicherheitsdienstleistungen. Thema: Der Markt für Sicherheitstechnologien in Deutschland und Europa - Wachstumsperspektiven und Marktchancen für deutsche Unternehmen. Schlussbericht. http://www.vdivde-it.de/Images/publikationen/dokumente/Schlussbericht_druck3.pdf, Abruf am 03.02.2011.
W3C (2002). Current Patent Practice. W3C Note 24 January 2002. http://www.w3.org/TR/2002/NOTE-patent-practice-20020124, Abruf am 11.04.2011.
W3C (2004). W3C Patent Policy. http://www.w3.org/Consortium/Patent-Policy-20040205/#def-essential-definition, Abruf am 01.10.2012.
Wakke, P., Blind, K. (2012). The Impact of Participation within Formal Standardization on Firm Performance. SSRN: http://ssrn.com/abstract=2045529 und http://dx.doi.org/ 10.2139/ssrn.2045529, Abruf am 03.12.2012.
Warren, S. L., Brandeis, L. D. (1890). The Right to Privacy. Harvard Law Review Vol. IV, No. 5. http://www.estig.ipbeja.pt/~ac_direito/privacy.pdf, Abruf am 20.02.2012.
Wehnert, J. (2006). Ready – Set – Slow: A View from Inside a CEN Working Group. In: Jakobs, K. (Ed.). Advanced topics in information technology standards and standardization research, Vol. 1, 138-149.
Wilkins, L., Christians, C. G. (2008). The handbook of mass media ethics. New York, 2009.
Württemberger, T. (2012). Rechtswissenschaftliche Begleitforschung zur intelligenten Videoüberwachung. BMBF-Innovationsforum „Zivile Sicherheit“. http://www.bmbf.de/ pubRD/B1-I_Wuerttemberger_Redemanuskript.pdf, Abruf am 27.08.2012.
Yin, R. K. (2003). Case study research, design and methods, 3. Aufl., Newbury Park 2003.

Als elektronisches Medium wurde vor allem die Datenbank Perinorm International genutzt. Sie beinhaltet in über einer Million Datensätzen die europa- und weltweit wichtigsten Fakten über Normen, technische Regelwerke und Rechtsvorschriften. Perinorm International umfasst Datenbanken aus 24 Ländern (Stand: Mai 2011) sowie die Daten der europäischen und internationalen Normeninstitute CEN, CENELEC, ETSI, ISO, IEC und ITU.

1.5 Zusammenarbeit mit anderen Stellen

Die Durchführung des Vorhabens war durch vielfältige Kooperationen gekennzeichnet. Die wichtigste Zusammenarbeit im Rahmen von InfraNorm betraf die gemeinsame Projektumsetzung mit dem Projektkoordinator DIN e.V. Die Ermittlung des Bedarfs an Normen und Standards basierte auf dem Austausch mit 24 Teilnehmern der zehn Verbundprojekte und 15 externen Experten. Eine weitere, für den Projekterfolg sehr wertvolle, Zusammenarbeit erfolgte mit der VDI Technologiezentrum GmbH. Um den normungsbezogenen Informationsbedarf von InfraNorms Zielgruppe zu erheben, versendete das VDI Technologiezentrum zwei

an der TU Berlin erarbeitete Fragebögen an rund 500 Sicherheitsforscher. Die auf dieser Grundlage gewonnenen Informationen waren für das Normungshandbuch von hohem Wert.

Für das Normungshandbuch wurden zudem fünf Fallstudien über Standardisierungsmaßnahmen erstellt, die im Rahmen von InfraNorm durchgeführt wurden. Neben der Kooperation mit dem DIN erfolgte dabei in alphabetischer Reihenfolge eine Zusammenarbeit mit den folgenden Institutionen:

- BAM Bundesanstalt für Materialforschung und -prüfung
- Bergische Universität Wuppertal
- C.I.K., Universität Paderborn
- CAD-Zeichenbüro Rogsch, Neustadt
- EBS Business School
- Fraport AG
- Fraunhofer-Institut IFF
- Fraunhofer-Institut FKIE
- IABG mbH
- IST GmbH, Frankfurt
- Landespolizeiamt Dezernat 43, Behörde für Hafenanlagensicherheit Schleswig Holstein
- Lübecker Hafengesellschaft mbH
- PSI AG
- Reederei Scandlines Deutschland GmbH
- TraffGo HT GmbH
- TSB Innovationsagentur Berlin GmbH
- Vomatec International GmbH

Für eigene weitere Fallstudien erfolgte eine Zusammenarbeit mit:

- dem Koordinator des Standardisierungsprojekts PreparedNet,
- den Koordinatoren der Standardisierungsprojekte Smart-CM und SCUTUM (aus den USA und Italien) und
- Ansprechpartnern aus einem IEC- und einem CEN-Projekt.

Des Weiteren wurde eine gemeinsame Fallstudie mit zwei holländischen Forscherinnen erstellt:

- Tineke M. Egyedi, Delft University of Technology, Department of Infrastructures und
- Anique Hommels, Maastricht University, Department of Technology and Society Studies.

In der Studie wird in besonderer Weise dargelegt, wie nationale Interessen in der europäischen Sicherheitsstandardisierung erfolgreich verfolgt werden können. Neben dem Kapitelbeitrag im Normungshandbuch wird der Artikel im September 2013 auch auf der Konferenz SIIT 2013 präsentiert. Für weiterführende Arbeiten wurde eine Zusammenarbeit mit dem Normenausschuss NA 159-01-16 GA Gemeinschaftsarbeitsausschuss NADL/DKE „Dienstleistungen für Sicherheitsanlagen“ aufgebaut. Bei der Vermittlung von Fallstudien waren vor allem Herr Stephan Krebs vom DIN und Herr Henryk Sieradzki von der DKE behilflich.

2 Eingehende Darstellungen

2.1 Verwendung der Zuwendung und erzielte Ergebnisse im Einzelnen, mit Gegenüberstellung der vorgegebenen Ziele

AP 1.1 Analyse des Normungs- und Standardisierungsbedarfs

Aufgabenbeschreibung

Entsprechend der nachstehenden Tabelle war in AP 1.1 der Normungs- und Standardisierungsbedarf in den vom BMBF geförderten Verbundprojekten im Bereich „Schutz von Verkehrsinfrastrukturen“ zu identifizieren und zu konkretisieren. Hierzu waren auf Basis eines selbst entwickelten Leitfadens Interviews in den einzelnen Verbundprojekten durchzuführen. Neben den Verbundpartnern sollten auch externe Experten befragt werden. Die Erhebung war in Form einer zweistufigen, schriftlichen Befragung vorzunehmen.

Geplante Bearbeitungszeit	**M 1 – M 15**	**Gesamtpersonalaufwand**	**6 PM**
Ziel des Arbeitspaketes	Ermittlung des Bedarfs an Normen / Standards als Grundlage für den weiteren Abgleich mit existierendem Normenbestand und Ableitung von konkreten Normungsinitiativen		
Voraussetzung (Input & Herkunft)	Eigenentwickelter Interviewleitfaden und Fragebogen, Beteiligung der Verbundprojekte und externer Experten		
Ergebnisse (Output)	Normungsbedarf im Bereich Schutz von Verkehrsinfrastrukturen		

Darst. 2: Übersicht des Arbeitsplans für AP 1.1

In einer ersten Befragungsrunde war der Normungsbedarf der Ansprechpartner der Verbundprojekte und der externen Experten anhand „offener Fragen“ zu erheben. Die Antworten waren im Anschluss auszuwerten und zu aggregieren. Die Ergebnisse waren in einer zweiten geschlossenen Befragungsrunde zu konkretisieren, hinsichtlich ihrer zeitlichen Priorität zu bewerten und anschließend zu konsolidieren.

Umsetzung

Die zweistufige Befragung wurde plangemäß durchgeführt. Wichtig war es dabei zu Beginn des Vorhabens InfraNorm bekannt zu machen. Das Projekt wurde daher u.a. bei Besuchen der folgenden Institutionen vorgestellt:

- C.I.K., Universität Paderborn (Projekt OrGaMIR)
- Deutsches Zentrum für Luft- und Raumfahrt e. V. (DLR) (Projekt Critical Parts)
- DB Kommunikationstechnik GmbH (Projekt SinoVE Management)
- EADS Innovation Works Germany (Projekt SiVe)
- European Center for Aviation Development – ECAD (Projekt FluSs)

- Fraunhofer EMI (Projekte AISIS, SKRIBT, FluSs)
- Fraunhofer FKIE (Projekt Vesper)
- Hamburg Consult (Projekt V-SICMA)

Die wichtigsten inhaltlichen Ergebnisse aus AP 1.1 umfassen:

- 246 Normungshinweise von 39 Interviewpartnern in 40 Themenfeldern in der ersten Befragungsrunde zum Normungs- und Standardisierungsbedarf für den Schutz von Verkehrsinfrastrukturen (vgl. Darst. 3)
- Übersicht bereits existierender Standards und Normen in den ermittelten Themenfeldern
- Auswahl von zehn ersten Normungsthemen für InfraNorm durch 30 Interviewpartner in der zweiten Befragungsrunde.

Die parallele Untersuchung existierender Standards und Normen in den identifizierten Themenfeldern basierte auf:

- Analysen in der Datenbank Perionorm,
- Ermittlung der Aktivitäten nationaler, Europäischer und internationaler Normungsorganisationen und Gremien sowie
- Hinweisen der Interviewpartner der ersten Befragungsrunde zum Normungs- und Standardisierungsbedarf für den Schutz von Verkehrsinfrastrukturen.

Ausgehend von der Übersicht in Darst. 3 führten die Arbeiten zu den folgenden Ergebnissen[4]:

- In Bezug auf Themenfeld 1 - Informations- und Kommunikationssysteme erörterten die Gesprächspartner einen vielfältigen Bedarf an Kompatibilitäts- und Schnittstellenstandards für Behörden und Organisationen mit Sicherheitsaufgaben (BOS) einerseits und Infrastrukturbetreiber andererseits. Derzeit kann ihrem Bedarf durch vorhandene Standards nicht entsprochen werden.
- Während für die IT-Sicherheit ein großes Spektrum von Normen und Standards verfügbar ist, existiert ein Mangel an Prüf- und Qualitätsstandards für „security"-spezifische Informationssysteme. Im Bereich „1.5 Standards für die IT-Sicherheit und die Systemprüfung" zeigt sich insbesondere hinsichtlich der Prüfszenarien für „Systems of Systems" für die Sicherheit von Verkehrsinfrastrukturen ein ungedeckter Bedarf.
- Gewünschten Qualitäts- und Sicherheitsstandards zur Konstruktion und -ausstattung von Flughäfen (2.4) kann derzeit nicht entsprochen werden. Dies betrifft beispielsweise den Wunsch nach geeigneten Regelwerken für Sensortunnel.
- Für das Thema „3.1 Sensorqualität und -klassifikation" auf dem Gebiet „3. Sensorik und Detektion" sind nahezu keine Normen und Standards verfügbar. Die existierenden Teststandards für Sensoren und Sensorsysteme (3.2) beziehen sich vorrangig auf Detektoren für radioaktive und nukleare Gefahrenstoffe. In einigen Bereichen existieren alternative Regelungen, z.B. für das Testen von Detektionssystemen für Flughäfen.

[4] Der in den Stichpunkten verwendete Begriff „Standards" schließt auch Normen und Spezifikationen ein.

1. Informations- und Kommunikationssysteme

1.1 Kompatibilitäts- und Schnittstellenstandards zur Vernetzung der an der Sicherheit von Verkehrsinfrastrukturen beteiligten Akteure
1.2 Kompatibilitäts- und Schnittstellenstandards für die interne Arbeit der BOS[5]
1.3 Kompatibilitäts- und Schnittstellenstandards für die interne Arbeit der Infrastrukturbetreiber
1.4 Standards für SCADA[6]-Systeme
1.5 Standards für die IT-Sicherheit und die Systemprüfung
1.6 Sonstiges

2. Physikalische Sicherheit und Schutzsysteme

2.1 Baustoffe
2.2 Allgemeine Qualitäts- und Sicherheitsstandards zur Bauwerkskonstruktion und -ausstattung
2.3 Qualitäts- und Sicherheitsstandards zur Konstruktion und -ausstattung von Bahnhöfen
2.4 Qualitäts- und Sicherheitsstandards zur Konstruktion und -ausstattung von Flughäfen
2.5 Bauwerkskonstruktion und -ausstattung für Tunnel
2.6 Bauwerkskonstruktion und -ausstattung für Brücken

3. Sensorik und Detektion

3.1 Sensorqualität und -klassifikation
3.2 Teststandards für Sensoren und Sensorsysteme
3.3 Sensordatenaufnahme und -auswertung
3.4 Sensorschnittstellen und -datenübertragung
3.5 Sonstiges

4. Sicherheitskommunikation

4.1 Verkehrsträgerübergreifende Themen der Sicherheitskommunikation
4.2 Sicherheitskommunikation im schienengebundenen Verkehr

5. Simulation und Modellierung

5.1 Modellierungsgrundlagen
5.2 Simulationsgrundlagen
5.3 Standards zum Vergleich und zur Zertifizierung von Methoden und Tools
5.4 Kompatibilität und Schnittstellen für Modellierungs- und Simulationswerkzeuge
5.5 Spezialthemen der Simulation und Modellierung im Bereich Tunnelsicherheit

6. Überwachungssysteme, insbesondere zur Videoüberwachung

6.1 Standards für die Endgeräte
6.2 Informationsextraktion
6.3 Systemkompatibilität und Schnittstellen
6.4 Standards zur Berücksichtigung von Datenschutz/Privacy
6.5 Qualitäts- und Teststandards

7. Zutritts- und Lenkungssysteme für Personen und Fahrzeuge

7.1 Zutrittssysteme
7.2 Fluchtwege

Darst. 3: Normungs- und Standardisierungsbedarfsthemen im Projekt InfraNorm[7]

[5] Behörden und Organisationen mit Sicherheitsaufgaben
[6] SCADA steht für „supervisory control and data acquisition“
[7] Der Begriff „Standards“ schließt in der Tabelle auch Normen und Spezifikationen ein.

- Für die Themen im Bereich „3.3 Sensordatenaufnahme und -auswertung“ bieten derzeitige Normen und Standards kaum Anhaltspunkte.
- Für den Bereich „3.4 Sensorschnittstellen und -datenübertragung“ werden Lösungsgrundlagen z.B. durch die Standards RDF und XML, durch die SensorML, die TransducerML sowie die Standards IEEE 1451 und IEEE 8002.15.4 geboten.
- Analog den Ergebnissen zum Thema 2.4 ist derzeit kein Standard für Belastungsgrenzwerte zum Gesundheitsschutz beim Einsatz von Sensortunneln (Thema „3.5 Sonstiges“) verfügbar.
- Für das Themenfeld „4. Sicherheitskommunikation“ können die beschriebenen Kommunikationsstandards im Bereich 1 eine Lösungsgrundlage bieten.
- Im Bereich „5. Simulation und Modellierung“ wurde von mehreren Interviewpartnern der Bedarf an geeigneten, standardisierten Szenarien bzw. standardisierten Vorgaben zur Entwicklung von Szenarien erörtert. Die Szenarien werden als Basis der Simulations- und Modellierungsarbeiten benötigt. Auf Grundlage von Normen oder Standards soll ein geeignetes Qualitätsniveau sichergestellt werden.
- Konkret in Bezug auf den Bereich „5.1 Modellierungsgrundlagen“ besteht beispielsweise Bedarf nach einem standardisierten Leitfaden zur konzeptuellen Modellierung.
- Im Bereich „5.2 Simulationsgrundlagen“ fehlen vorrangig Parameter, insbesondere zur Simulation menschlichen Verhaltens sowie Simulationsparameter für Gehgeschwindigkeiten.
- Im Hinblick auf das Themenfeld „5.3 Standards zum Vergleich und zur Zertifizierung von Methoden und Tools“ fehlen z.B. grundlegende, methodenbezogene Standards für die Modellierung menschlichen Verhaltens.
- Für den Standardisierungsbedarf der Interviewpartner im Bereich „5.4 Kompatibilität und Schnittstellen für Modellierungs- und Simulationswerkzeuge“ ist das derzeitige Angebot nicht befriedigend. Der Entwicklungsbedarf für Standards in diesem Bereich wird durch internationale Studien bestätigt.
- Hinsichtlich der Spezialthemen der Simulation und Modellierung im Bereich Tunnelsicherheit (5.5) stehen ebenso wie bei den Themen 2.5 und 2.6 bisher vorrangig Safety-Aspekte im Mittelpunkt. Die derzeitigen Regelwerke bieten dabei Ausbaupotential.
- Für das Themenfeld „6. Überwachungssysteme, insbesondere zur Videoüberwachung“ wurde durch die Interviewpartner ein vielschichtiger Standardisierungsbedarf dargestellt. Im Bereich „6.1 Standards für die Endgeräte“ erscheint insbesondere der Standardisierungsbedarf für Security-Anforderungen an die Endgeräte in Sicherheitssystemen sowie zur Erzeugung einer Wahrscheinlichkeitsangabe für detektierte Gefahren ungedeckt.
- Dem Bedarf an Standards im Themenbereich „6.2 Informationsextraktion“ kann derzeit nicht in befriedigender Weise entsprochen werden. Das Fehlen geeigneter Darstellungsparameter stellt dabei eine besondere Einflussgröße dar.
- Zur Berücksichtigung von Datenschutz und Privacy beim Einsatz von Überwachungssystemen in Verkehrsinfrastrukturen (Bereich 6.4) fehlen Standards sowohl national als auch international, z.B. für die Thematik „Privacy by Design“ und für „Privacy Enhancing Technologies“. Erste Arbeitsgruppen, die dies berücksichtigen, sind die ISO JTC 1/SC 27/WG 5 Identity management and privacy technologies, welche vom DIN NA 043 Normungsausschuss Informationstechnik und Anwendung gespiegelt wird, sowie ETSI „RFID Security and Privacy by design“.

- Den gewünschten Standards im Bereich „6.5 Qualitäts- und Teststandards“ kann derzeit nicht entsprochen werden. Die Entwicklung und Anwendung des zuvor vorgeschlagenen Teststandards im Bereich Datenschutz macht dabei existierende Standards der Kategorie 6.4 erforderlich.
- Im Bereich „7. Zutritts- und Lenkungssysteme für Personen und Fahrzeuge“ steht dem geäußerten Standardisierungsbedarf im Bereich „7.1 Zutritt“ einem Experten zufolge ausschließlich die allgemeine europäische EN 50 133-Reihe Access Control Systems / Alarmanlagen – Zutrittskontrollanlagen für Sicherungsanwendungen gegenüber.
- Gewünscht werden darüber hinaus u.a. differenzierte Standards zum Gebäudezutritt in Abhängigkeit von Gebäudeteil-Gefährdungsklassen. Dies setzt eine standardbasierte Definition entsprechender Gefährdungsklassen voraus.
- Für „7.2 Fluchtwege“ erscheint insbesondere der Bedarf an Kompatibilitätsstandards zwischen Überwachungs-, Brandmelde- und Fluchtwegeinformationssystemen ungedeckt.
- Für die „security“-bezogene Bauwerksklassifikation (8.2) stehen derzeit keine Standards zur Verfügung.
- Für Klassifikationen von Bedrohungslagen im schienengebundenen Verkehr (8.3) zeigt sich derzeit ein ähnliches Bild, allerdings wurde durch Interviewpartner auf eine mögliche Standardisierbarkeit von Ergebnissen der geförderten Projekte im Themenfeld „Schutz von Verkehrsinfrastrukturen“ verwiesen.

Aufgrund der Ergebnisse der zweiten Befragungsrunde, an der sich 30 Interviewpartner beteiligten, wurden unter Hinzuziehung der Ergebnisse der Normenrecherche die in Darst. 4 gezeigten prioritären Bearbeitungsthemen identifiziert.

Ausgewählte Standardisierungsthemen von InfraNorm
Kompatibilitäts- und Schnittstellenstandards zur Vernetzung der an der Sicherheit von Verkehrsinfrastrukturen beteiligten Akteure
Verkehrsträgerübergreifende Themen der Sicherheitskommunikation
Modellierungsgrundlagen
Simulationsgrundlagen
Klassifikation allgemeiner Bedrohungslagen von Verkehrsinfrastrukturen
Qualitäts- und Sicherheitsstandards zur Bauwerkskonstruktion und -ausstattung allgemein sowie speziell für Bahnhöfe
Sensorschnittstellen und -datenübertragung
Standards zum Vergleich und zur Zertifizierung von Methoden und Tools
Kompatibilität und Schnittstellen für Modellierungs- und Simulationswerkzeuge

Darst. 4: Ausgewählte Standardisierungsthemen von InfraNorm

Die Ergebnisse wurden dem Projektpartner DIN sowie den Teilnehmern der beteiligten Verbundprojekte zur Verfügung gestellt. Ziel war die Gründung von Arbeitsgruppen und die Entwicklung entsprechender Spezifikationen. Es konnten fünf Spezifikationen entwickelt werden:

- DIN SPEC 91284 Grundlagen mikroskopischer Entfluchtungsanalysen
- DIN SPEC 91287 Datenaustausch zwischen Informationssystemen in der zivilen Gefahrenabwehr
- DIN SPEC 91293 Security-Modellierungstechnik (SMT) zur gefahrenstufenabhängigen Darstellung und Analyse sicherheitsrelevanter Informationen
- DIN SPEC 91296 Klassifizierung von Gefährdungen für Bauwerke infolge von Terrorismus
- DIN SPEC 91282 Terminologie für das Sicherheitsmanagement von Verkehrsinfrastrukturen

Wie in der folgenden Abbildung zu sehen, wurden alle erarbeiteten Spezifikationen in den ermittelten Themenfeldern erstellt, wobei eine Spezifikation sogar zwei Gebiete adressiert.

Umsetzung der ausgewählten Standardisierungsthemen von InfraNorm	
Thema	**Umsetzung**
Kompatibilitäts- und Schnittstellenstandards zur Vernetzung der an der Sicherheit von Verkehrsinfrastrukturen beteiligten Akteure	DIN SPEC 91287 Datenaustausch zwischen Informationssystemen in der zivilen Gefahrenabwehr
Verkehrsträgerübergreifende Themen der Sicherheitskommunikation	DIN SPEC 91282 Terminologie für das Sicherheitsmanagement von Verkehrsinfrastrukturen
Modellierungsgrundlagen	DIN SPEC 91293 Security-Modellierungstechnik (SMT) zur gefahrenstufenabhängigen Darstellung und Analyse sicherheitsrelevanter Informationen
Simulationsgrundlagen	DIN SPEC 91284 Grundlagen mikroskopischer Entfluchtungsanalysen (addressiert auch den Bereich Modellierungsgrundlagen)
Klassifikation allgemeiner Bedrohungslagen von Verkehrsinfrastrukturen	DIN SPEC 91296 Klassifizierung von Gefährdungen für Bauwerke infolge von Terrorismus

Darst. 5: Umsetzung der ausgewählten Standardisierungsthemen von InfraNorm

Die verbleibenden Themen bieten Grundlagen für weitere Standardisierungsaktivitäten.

AP 3.2 Normungshandbuch Sicherheitsforschung

Aufgabenbeschreibung

Um Akteuren in den weiteren Themenbereichen des Sicherheitsforschungsprogramms den Transfer ihrer Forschungsergebnisse zu erleichtern, sollte ein Handbuch entwickelt werden. Die Merkmale des Arbeitspakets werden in der folgenden Tabelle skizziert.

Geplante Bearbeitungszeit	M 25 – M 36	Gesamtpersonalaufwand	18 PM
Ziel des Arbeitspaketes	Unterstützung der Entwicklung von Normen und Standards in weiteren Themenfeldern des Sicherheitsforschungsprogramms		
Voraussetzung (Input & Herkunft)	Interviewleitfäden, Fragebögen des AP 1.1 Primärstudien, Zugang zu Datenbanken		
Ergebnisse (Output)	Handbuch inklusive Empfehlungen zur Sicherstellung von Vertraulichkeit		

Darst. 6: Übersicht des Arbeitsplans für AP 3.2

Die vorgesehenen Inhalte umfassten u.a. die Vorstellung von Methodiken zur Bedarfsanalyse und für Recherchen in Normen-Datenbanken. Ferner war die entwicklungsbegleitende Normung des DIN vorzustellen und ein strukturiertes Vorgehen der Einbindung von Forschungsprojekten aufzuzeigen. Für die Erarbeitung von Hinweisen zur Vermeidung von Informationsproliferation und einem Missbrauch von Informationen wurden Interviews in den Verbundprojekten sowie mit externen Experten vorgesehen. Als Grundlage hierfür war ein Leitfaden zu entwickeln. Die Ergebnisse waren in einem zweistufigen Verfahren zu konsolidieren. Weiterhin waren Sekundärauswertungen von Dokumenten durchzuführen.

Ergebnisse

Die wichtigsten Ergebnisse umfassten drei Dokumente:

- eine Studie zu security-bezogenen Normen, Spezifikationen und Standards
- eine Studie Sicherheitsethik, Privacy und Normung sowie
- das Normungshandbuch für die Teilnehmer des deutschen Sicherheitsforschungsprogramms

Studie zu security-bezogenen Normen, Spezifikationen und Standards

Zur Konkretisierung der von der Zielgruppe benötigten Inhalte des Normungshandbuchs leistete die im Frühjahr 2011 unter den Teilnehmern des deutschen Sicherheitsforschungsprogramms durchgeführte Umfrage zu security-bezogenen Normen, Spezifikationen und Standards einen wertvollen Beitrag. Für die Durchführung der Studie diente ein Fragebogen mit 14 Fragen in acht Themenbereichen.

Ein spezielles Anliegen der Umfrage bestand darin, wahrgenommene Risiken bei der security-spezifischen Normung und Standardisierung aufzudecken. Daher wurden die Teilnehmer gebeten, ihre Risikowahrnehmung darzustellen. Es wurden sieben Themenfelder identifiziert, vgl. Darst. 7.

Missbrauch	Föderalismus	**Fehlentwicklungen**
--	**Pseudosicherheit**	--
Ethische Fragen	Leitmarktrisiken	**Allgemeine Risiken**

Darst. 7: Identifizierte Risikofelder der Teilnehmer der Studie zu security-bezogenen Normen, Spezifikationen und Standards

Missbrauchsgefahren beziehen sich insbesondere auf die Veröffentlichung sensibler Informationen und eine Nutzung mit unlauteren Absichten. Das **Föderalismusproblem** besteht vor allem in dem Risiko, dass die Entwicklung gemeinsamer Standards durch länderspezifische Unterschiede behindert wird. **Fehlentwicklungen** beziehen Teilnehmer z.B. auf technische Regeln minderer Qualität, die zu einer mangelnden Anwendbarkeit führen. Der Begriff **Pseudosicherheit** thematisiert die Gefahr, den Beitrag einer erarbeiteten Norm oder eines Standards falsch einzuschätzen und Restrisiken unzweckmäßig zu berücksichtigen. **Ethische Risiken** beziehen sich in besonderer Weise auf den Einsatz von Überwachungstechnologien und den Umgang mit personenspezifischen Daten. **Leitmarktbezogen** wurde der fehlende Einfluss Deutschlands im internationalen Normungskontext auf Grund der Dominanz Großbritanniens und der USA „zugunsten der jeweils eigenen nationalen Industrie“ erörtert. **Allgemeine Risiken** sehen mehrere Teilnehmer in einer Verhinderung von Innovationen. Ihre Aussagen implizieren eine geringe Bekanntheit der kurzfristig entwickelbaren DIN SPECs im Sicherheitsforschungsprogramm. Darüber hinaus erscheinen Einsatzmöglichkeiten von Normen und Spezifikationen zur Innovationsförderung tendenziell unbekannt.

In einer weiteren Frage wurden Konflikte in der Normung und Standardisierung thematisiert. Anhand der Darstellung der typischen fünf Phasen eines Normungsprozesses wurden die Teilnehmer gebeten, eine Rangfolge der Phasen entsprechend ihren beigemessenen Konfliktpotentialen zu bilden. Die relevanten und betrachteten Phasen der Normung und Standardisierung umfassen die Initiierung des Vorhabens (Phase 1), die Entwicklung (Phase 2), die Veröffentlichung einer Norm (Phase 3), die Anwendung (Phase 4) sowie die Überarbeitung (Phase 5).

Im Ergebnis wird der Phase 2, und damit der „Entwicklung“ das größte Konfliktpotential beigemessen. Es folgen die „Initiierung des Vorhabens“ (Phase 1), die Phase „Überarbeitung“ (5) sowie die „Anwendung“ (Phase 4). Die Phase der „Veröffentlichung“ (3) wird mit dem geringsten Konfliktpotential verbunden. In bisherigen Forschungsarbeiten wird bei der Betrachtung von Normungs- und Standardisierungskonflikten bereits ein initiiertes Projekt vorausgesetzt. Die Befragungsergebnisse erweitern hier den Fokus und decken zusätzliche Probleme auf, die für die grundsätzliche Durchführung von Normungs- und Standardisierungsprojekten kritisch sind.

Ausgehend von den zuvor dargestellten Ergebnissen thematisierte eine weitere Frage Konfliktrisiken in der Phase mit dem größten Konfliktpotential. Aus den Aussagen wurden entsprechend Darst. 8 acht Konfliktgruppen abgeleitet.

Unwissenheit über bestehende Normen	Identifikation gemeinsamer Mehrwerte	**Interessenkonflikte/ Konsensfindung**
Organisatorische Probleme und Verzögerungen	**Intellectual Property Rights**	Spezialaspekte im internationalen Kontext
Widerstände der Anwender/Akzeptanzprobleme	Spezifische Standardisierungsaspekte beim Schutz vor CBRNE[8]	--

Darst. 8: Wahrgenommene Konfliktrisiken

Die **Identifikation gemeinsamer Mehrwerte** stellt eine zentrale Voraussetzung für gemeinsame Normungs- und Standardisierungsaktivitäten dar. Ein Teilnehmer der Umfrage wies dabei darauf hin, dass ein gemeinsamer Entschluss zur Durchführung eines entsprechenden Vorhabens nur erfolge, wenn „alle Initiatoren mehr gewinnen, als sie verlieren".

Als **organisatorische Probleme** wurden vor allem zwei Aspekte identifiziert: Zuständigkeiten und Kompetenzfragen sowie „Langwierigkeiten" auf Grund einer zu großen Anzahl von Stakeholdern. Die **Unwissenheit über bestehende Normen** birgt weitere Konfliktpotentiale. Deutlich wird die fehlende Kenntnis über die Datenbank Perinorm. Dies kann gleichzeitig dazu führen, dass der Entwicklung von Normen und Standards ein höherer Aufwand beigemessen wird, als sie tatsächlich auslöst.

Ein Sechstel der Teilnehmer maß der **Konsensfindung** das größte Konfliktpotential bei. Als Einflussgrößen wurden dabei divergierende Ziele sowie Interessenkonflikte wirtschaftlicher und politischer Art genannt, vor allem wenn die Teilnehmer im Wettbewerb stehen. Die Phase 2 ist dabei aus Teilnehmersicht durch besondere Herausforderungen gekennzeichnet.

Als **Spezialaspekte der internationalen Normung und Standardisierung** wurden kulturelle und wirtschaftliche Aspekte beschrieben. Die kulturellen Problemfelder umfassen dabei die Bereiche „Sprache", „Formulierungen", „Inhalte" und „Interessen". Als wirtschaftliches Problem wurde insbesondere die rasche Etablierung von de facto Standards durch ausländische Firmen beschrieben.

Konfliktpotential in Bezug auf **geistige Eigentumsrechte** basiert vor allem auf der Offenlegung von Know How, das nicht genügend geschützt ist.

Widerstände der Anwender bzw. Akzeptanzprobleme gehen u.a. auf eine ungeeignete Kosten-Nutzen-Relation und auf nachträgliche Änderungen zurück. Des Weiteren sind sie insbesondere darauf zurückzuführen, dass eine entwickelte Norm als unzweckmäßig angesehen wird.

Konflikte in Bezug auf Normungs- und Standardisierungsmaßnahmen im Bereich CBRNE äußern sich der Befragung folgend insbesondere durch ungeklärte Zuständigkeiten

[8] Chemische, biologische, radioaktive, nukleare und explosive Gefahren

verschiedenster Behörden, die einer Normung entgegenstehen. In Darst. 9 werden die wahrgenommenen Konflikte in den einzelnen Phasen wiedergegeben.

Aggregierte phasenspezifische Konfliktpotentiale
Phase 1
Identifikation gemeinsamer Mehrwerte
Unwissenheit über existierende Normen und Standards
Spezialaspekte im internationalen Kontext
Phase 2
Interessenkonflikte und Konsensfindung
Intellectual Property Rights
Spezialaspekte im internationalen Kontext
Phase 3
Akzeptanz/Widerstände der Anwender
Phase 4
Akzeptanz/Widerstände der Anwender
Spezielle Rahmenbedingungen bei CBRNE
Phase 5
Organisatorische Probleme und Verzögerungen
Interessenkonflikte und Konsensfindung
Akzeptanz/Widerstände der Anwender

Darst. 9: Aggregierte phasenspezifische Konfliktrisiken in Normungs- und Standardisierungsprozessen

Für die Erstellung des Normungshandbuchs wurden aus der Befragung umfangreiche Anforderungen abgeleitet:

- Ein Großteil der involvierten Personen ist ihren statistischen Angaben zufolge a) in **öffentlichen Forschungseinrichtungen oder Hochschulen** oder b) **in kleinen und mittelgroßen Unternehmen (KMU)** tätig. Für beide Zielgruppen sollten neben allgemeinen Hinweisen **spezifische Empfehlungen** entwickelt werden.
- Die Ergebnisse zu Frage 1 wiesen auf die besondere Bedeutung von **security-bezogenen Schnittstellenstandards und Terminologien** hin. Dies sollte durch zwei entsprechende **Fallstudien** sowie einen Strategiekatalog für die Entwicklung von Schnittstellen berücksichtigt werden.
- Frage 2 zeigte u.a. die **Bedeutung von security-bezogenen Patenten**. Der Normungskontext setzt hier spezielle Rahmenbedingungen, die in dem Handbuch aufgegriffen werden sollten.
- Die Ergebnisse zu den Fragen 3 bis 6 verdeutlichen den **allgemeinen Bedarf** für das Normungshandbuch, da die Mehrheit der Teilnehmer kaum über eigene Erfahrungen verfügt. Die geplanten Hilfestellungen umfassten daher z.B. die Erörterung der Arbeit und der Dokumentenarten wichtiger Normungsorganisationen sowie Empfehlungen zur Durchführung von Normenrecherchen.
- Frage 7 reflektierte die Normungsmotive der Teilnehmer. Das Handbuch sollte Hinweise für eine erfolgreiche Umsetzung ausgewählter Motive geben.

- In Frage 8 wurde insbesondere der **Zeit- und Kostenaufwand** als Normungsbarriere identifiziert. Lösungsmöglichkeiten sollten u.a. auf Grundlage von Fallstudien aufgezeigt werden.
- Bei der Beantwortung von Frage 9 wurden spezielle **ethische und privacy-bezogene Probleme** erörtert. Im Handbuch wurden hierfür zwei spezielle Kapitel vorgesehen.
- Laut Frage 10 und 11 bergen die Phasen der **Initiierung, der Entwicklung und der Überarbeitung** der geschaffenen Regelwerke die größten Konfliktpotentiale. Auf Grundlage von Fallstudien sollten spezielle Empfehlungen für diese Phasen erarbeitet werden.
- Vielfältige Konfliktrisiken wurden anhand der Befragung aufgezeigt. Zur Erörterung von Lösungen im Normungshandbuch wurden vor allem die folgenden Probleme ausgewählt: organisatorische Probleme durch geeignete Gremienbildung, Ermittlung bestehender Normen durch Normrecherchen, Verhandlungsstrategien, Intellectual Property Rights sowie Steigerung der Akzeptanz der erarbeiteten Regelwerke.

Die Ergebnisse der Studie wurden unter der Überschrift „Bedeutung von Sicherheitsnormen, -standards und -spezifikationen“ dokumentiert und im Januar 2012 an die 468 Mitglieder der Innovationsplattform versendet.

Studie Sicherheitsethik, Privacy und Normung

In der zuvor genannten Studie „Bedeutung von Sicherheitsnormen, -standards und -spezifikationen“ wurden ausgewählte ethik- und datenschutzbezogene Aspekte angesprochen. Sie bildeten eine wichtige Grundlage für die vertiefenden Analysen im Bereich Sicherheitsethik, Privacy und Normung.

Unterstützt durch die VDI Technologiezentrum GmbH wurde es möglich, auf Basis einer schriftlichen Befragung bei gleichem Aufwand wesentlich mehr Informationen zu erheben als ursprünglich auf Grundlage von Interviews vorgesehen war. Dadurch konnten die vielfältigen Interrelationen zwischen Sicherheitslösungen, Ethik, Privacy und Normung detailliert betrachtet werden. Zur Konkretisierung der Fragestellung diente ein zehn Fragen umfassender Fragebogen mit acht Themenbereichen (vgl. Darst. 10).

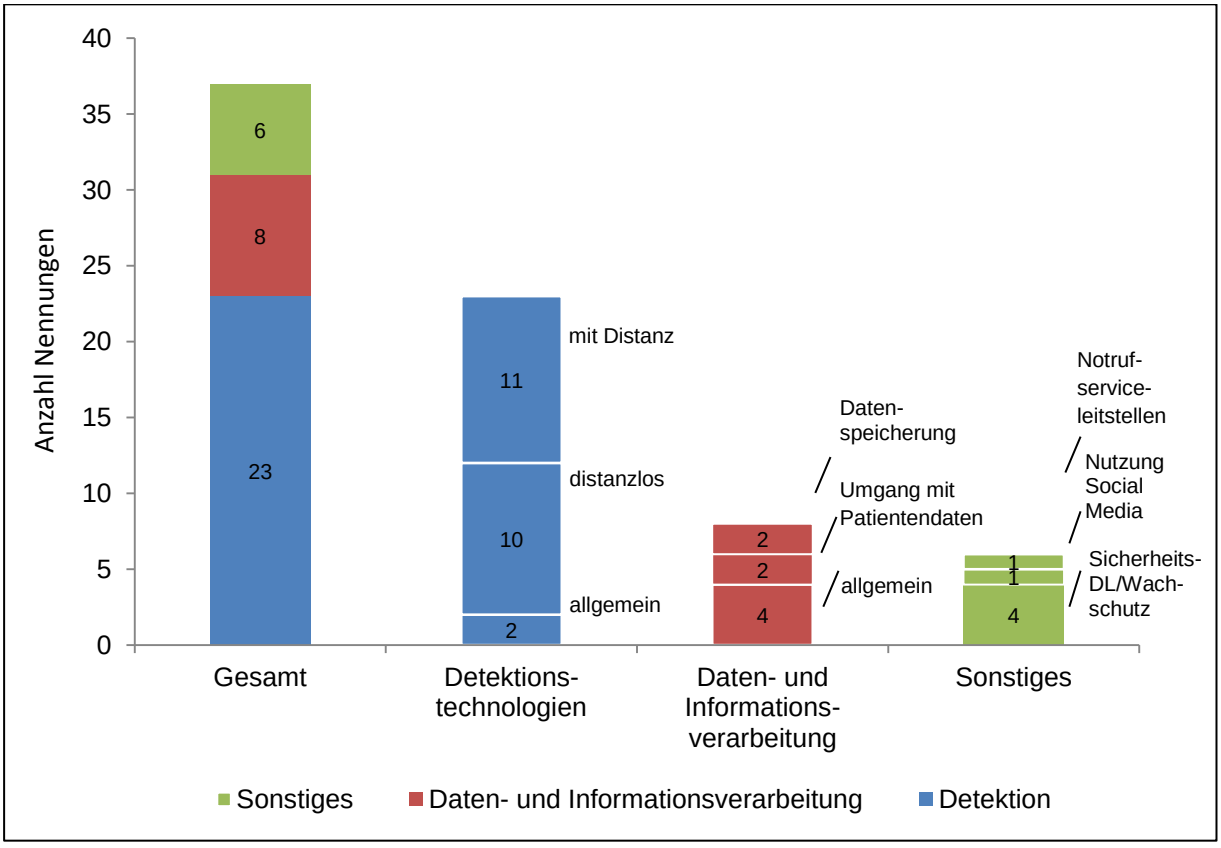
Die Ergebnisse zeigten, dass rund die Hälfte der Teilnehmer Risiken bei der Entwicklung von Normen und Standards für security-bezogene Produkte und Dienstleistungen sieht. Die wahrgenommenen Risiken wurden im Detail erfasst.

Eine weitere Frage beschäftigte sich damit, inwiefern den Teilnehmern bereits bestehende Normen, Standards oder sonstige Regelwerke zur Berücksichtigung ethik- und privacy-spezifischer Aspekte bei der Entwicklung bzw. Anwendung von Security-Produkten und Dienstleistungen bekannt sind. Es wurde deutlich, dass hier ein großer Informationsbedarf besteht, der im Normungshandbuch aufzugreifen war.

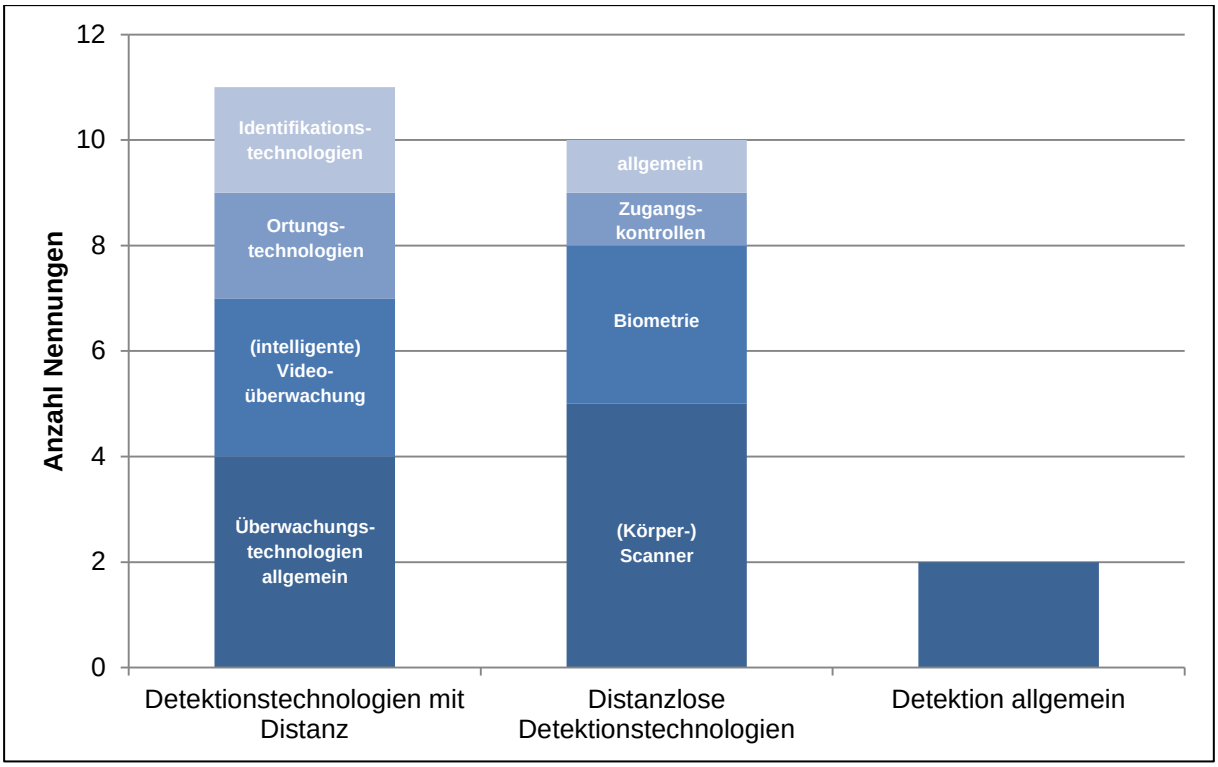
Themen der Umfrage
Stellenwert security-bezogener Normen und Standards
Wahrnehmung ethik- oder privacy-spezifischer Risiken für verschiedene Arten von Normen und Standards
Kenntnis über bestehende Normen und Standards zur Berücksichtigung ethik- und privacy-relevanter Aspekte
Security-bezogene Technologien, Produkte und Dienstleistungen mit besonderen ethik- und privacy-spezifischen Risiken
Risikopotential der identifizierten Technologien
Ethik- und privacy-spezifische Risiken ausgewählter Technologien, Produkte und Dienstleistungen
Weiterer Normungs- und Standardisierungsbedarf zur Berücksichtigung ethik- und privacy-spezifischer Aspekte
Weitere Technologien, Produkte und Dienstleistungen mit besonderem Normungs- und Standardisierungsbedarf

Darst. 10: Themenbereiche der Umfrage „Sicherheitsethik, Privacy und Normung“

Nachdem die Teilnehmer in Frage 2 ethik- und privacy-spezifische Risiken von security-Normen und Standards benannten, befasste sich Frage 5 mit Technologien, Produkten und Dienstleistungen, welche durch entsprechende Risiken gekennzeichnet sind. Die Ergebnisse werden in der folgenden Darstellung gezeigt. Dabei wurden spezielle Themencluster identifiziert: **Detektionstechnologien mit** und **ohne Körperkontakt, Daten- bzw. Informationsverarbeitung** sowie **Sonstiges** (sonstige Technologien und Dienstleistungen).



Darst. 11: Technologien, Dienstleistungen, Produkte mit ethik- und privacy-spezifischem Risikopotential



Darst. 12: Stellenwert des ethik- und privacy-spezifischen Risikopotentials verschiedener Detektionstechnologien und -dienstleistungen

Im Hinblick auf **Detektionstechnologien** sind distanzlose Technologien und solche mit Körperkontakt gleichermaßen durch ethik- und privacy-spezifische Risiken gekennzeichnet. Gemäß Darst. 1 stellen (Körper-)Scanner die mit Abstand am häufigsten genannten Security-Lösungen dar.

Als **Technologien mit Distanz** wurden insbesondere Überwachungstechnologien wie Videoüberwachung, die automatisierte Erkennung von Verhaltensmustern, Ortungstechnologien und Identifikationstechnologien wie z.B. die Kfz-Kennzeichenerkennung, genannt.

Zu den **distanzlosen Detektionstechnologien** zählen neben (Körper-)Scannern vor allem biometrische Technologien und Lösungen, aber auch Zugangskontrollen und Geräte mit Körperkontakt im Allgemeinen.

Entsprechend der folgenden Darstellung wurden im Zusammenhang mit den identifizierten Technologien, Dienstleistungen und Produkten drei konkrete Gruppen von ethik- und privacy-spezifischen Risiken identifiziert. Insgesamt wurde den Risiken **einer missbräuchlichen Verwendung personenbezogener Daten** die stärkste Bedeutung beigemessen.

Im Folgenden wurden die Teilnehmer gebeten, weitere ethik- und privacy-spezifische Risiken zu benennen, die bei anderen Technologien auftreten können.

Potentielle ethik- und privacy-spezifische Risiken	
Freiheitseinschränkung durch Sicherheitsziele	
Inhalte	Technologien
- Eingriff in Privatsphäre allgemein - Personenidentifikation - Fehlende Legitimation - Fehlende Zustimmung - Fehlende Verhältnismäßigkeit	- Personen-/Video-Tracking - Data Mining/Datenanalyse, -profiling - Identifikationstechnologien
Diskriminierung	Missbräuchliche Verwendung personenbezogener Daten
- Diskriminierung allgemein - Bewegungsbezogenes Profiling - Data Mining/ Datenanalyse, -profiling	- Missbrauch allgemein - Fehlende Vertraulichkeit - Voyeurismus

Darst. 13: Übersicht über potentielle ethik- und privacy-spezifische Risiken

Allgemein wurde ein Bedarf nach mehr Kontrollen und Transparenz von Datenschutzpraktiken zum Ausdruck gebracht. Neben den bereits erörterten Risiken wie Missbrauch und Diskriminierung wurden **Datensicherheit, Function Creep und Fehlidentifikation** genannt. Der Begriff Function Creep beschreibt dabei eine schleichende Erweiterung der Datennutzung über die Zwecke der ursprünglichen Bestimmung hinaus.

Erneut wurde das **Video-Tracking** als Gebiet mit besonderen ethik- und privacy-spezifischen Risiken identifiziert. Das Risiko der **Fehlidentifikation** wurde insbesondere mit diesem Technologiegebiet verbunden. Teilnehmer, die sich bei der Beantwortung dieser Frage auf Körperscanner bezogen, erwähnten vordergründig die Gefahr der **Preisgabe intimer Details.**

In einer weiteren Frage wurden die Teilnehmer gebeten, Normungs- und Standardisierungsempfehlungen zur besseren Berücksichtigung ethik- und privacy-spezifischer Aspekte bei der Entwicklung und Anwendung von security-bezogenen Produkten und Dienstleistungen zu geben. Ein Teilnehmer kommentierte dies stellvertretend für mehrere andere, ähnlich gelagerte Statements mit den Worten: „Der Bedarf ist hoch!“

Bedarf bestehe u.a. beim Einsatz intelligenter Videoüberwachung bzw. bezüglich des Video-Trackings, wobei besondere Rahmenbedingungen kennzeichnend sind. So formulierte ein weiterer Teilnehmer:

> *„Bezüglich intelligenter Videoüberwachung (sind) (...) zuerst parlamentsgesetzliche Rechtsgrundlagen zu schaffen.“*

Ergänzend wurden Wünsche nach proaktiven Bürgerinformationen über Überwachungs- und Datenerhebungsmaßnahmen zum Ausdruck gebracht.

Empfohlen wurde ferner die Zertifizierung von ethisch unbedenklicher Sicherheitstechnologie sowie eine spezielle Kennzeichnung bzw. ein Gütesiegel für ethisch unbedenkliche security-bezogene Produkte und Dienstleistungen.

In der abschließenden Frage wurden die Teilnehmer gebeten, weitere Technologien, Produkte oder Dienstleistungen anzugeben, für die ein besonderer Normungs- und Standardisierungsbedarf zur Reduzierung ethik- und privacy-spezifischer Risiken besteht. Es wurden sechs Bereiche identifiziert: Datenspeicherung, Videoüberwachung, Biometrie, (Online-) Sensorik, Sicherheitsdienstleistungen/Wachschutz und Zutrittskontrollen.

Auf Grundlage der Umfrage wurden insbesondere drei Implikationen für das Normungshandbuch abgeleitet.

- Von mehreren Teilnehmern wurde auf Missbrauchsrisiken von Sicherheitslösungen verwiesen. Zur Vermeidung ist insbesondere die Brücksichtigung eines europäischen Dokuments von Bedeutung, auf das im Normungshandbuch hinzuweisen war. In der COM(2011) 311 werden dabei klare Vorgaben definiert, für einige spezielle Detektionsaspekte keine frei verfügbaren Normen und Standards zu entwickeln: „Standards for certain security applications, such as scanners at airports or banknoteprinting presses, should only be made available to entities which have the required security clearances“ (EUR-Lex, 2011:12).
- Die Teilnehmer wurden nach bestehenden Regelwerken in den Bereichen Ethik und Privacy befragt. Lediglich zwei Personen konnten formelle Normen oder Standards benennen. Gleichzeitig wurde in Frage 9 mehrfach der Hinweis gegeben, bestehende Normen und Standards zu berücksichtigen. Im Normungshandbuch wurde daher eine ausführliche Darstellung bestehender Normen und Standards erforderlich, welche ethik- und privacy-relevante Aspekte im Bereich security-relevanter Technologien und Dienstleistungen adressieren.
- Ein hohes Potential an ethik- und privacy-spezifischen Risiken wurde von den Teilnehmern insbesondere bei Detektionstechnologien gesehen, vor allem zur Detektion mit Distanz. Neben der allgemeinen Überwachung nimmt die intelligente Videoüberwachung hier einen besonderen Stellenwert ein. Im Bereich der distanzlosen Detektion wurden Scannertechnologien am häufigsten genannt. Bei der Entwicklung von Normen und Standards auf diesen Gebieten erfordern ethik- und privacy-spezifische Aspekte daher eine besondere Aufmerksamkeit.

Normungshandbuch

Aufbauend auf den zuvor dargestellten Vorarbeiten ist das Normungshandbuch in elf Kapitel gegliedert. Nach dem einführenden Kapitel stellt **Kapitel 2** den Forschungskontext dar.

Kapitel 3 bietet eine Einführung in die Normung und Standardisierung. Dabei werden die Merkmale von Normen und Spezifikationen sowie ihre grundsätzliche Erarbeitung auf nationaler, europäischer und internationaler Ebene dargestellt.

In **Kapitel 4** wird die Relevanz der Normung für die Sicherheitsforschung aufgezeigt. Dabei werden sowohl industriepolitische Ziele erläutert als auch die vielfältigen Vorteile beschrieben, welche durch die Beteiligung an Normungs- und Standardisierungsprozessen erzielt werden können.

Kapitel 5 dient der Beschreibung allgemeiner Strategien für die sicherheitsbezogene Normung und Standardisierung. Dabei werden Empfehlungen zur Integration von Normungsaktivitäten in die Forschung sowie geeignete Umsetzungshilfsmittel dargestellt.

Die rechtlichen Rahmenbedingungen der security-bezogenen Normung und Standardisierung bilden den Inhalt von **Kapitel 6**. Im Mittelpunkt stehen dabei Regelungen in den Bereichen Datenschutz und Privacy sowie ihre Anwendung im Security-Kontext.

Kapitel 7 gibt ausführliche Informationen zur Integration ethischer Aspekte in die sicherheitsbezogene Normung und Standardisierung. Ausgewählte Normen und Spezifikationen in den Bereichen Privacy, Datenschutz und Datensicherheit werden erörtert. Darüber hinaus wird eine detaillierte Betrachtung der Themen Privacy Impact Assessments, Privacy by Design und Privacy Enhancing Technologies vorgenommen.

Kapitel 8 erörtert die Rahmenbedingungen zum Umgang mit geistigen Eigentumsrechten in der Normung bzw. Standardisierung. Dabei stehen patentbezogene Themen im Mittelpunkt. Relevante Regelungen von Normungsorganisationen, wie z.B. das FRAND[9]-Prinzip, werden ausführlich erläutert.

Zur Verdeutlichung der Chancen der Normung und Standardisierung, Vertiefung der Umsetzungsprozesse und Ermittlung von Erfolgsfaktoren werden in **Kapitel 9** und **10** zehn Normungs- und Standardisierungsvorhaben anhand von Fallstudien dargestellt.

Kapitel 11 dient der Zusammenfassung und Darstellung von Empfehlungen für die relevanten Adressatenkreise im Sicherheitsforschungsprogramm.

Konkret werden die Hinweise im letzten Kapitel des Handbuchs Bezug nehmend auf die sechs allgemeinen Normungs- und Standardisierungsphasen Vorbereitung, Initiierung, Entwicklung, Veröffentlichung, Anwendung und Überarbeitung dargestellt.

Eine **grundlegende Empfehlung** für die Programmteilnehmer betrifft die strategische Verankerung der Normungs- und Standardisierungsaktivitäten. In vielen forschenden Organisationen stehen für Patentierungsfragen zentrale Ansprechpartner zur Verfügung. Um geeignete Rahmenbedingungen für Normungs- und Standardisierungsprojekte zu entwickeln, ist es hilfreich, auch mit der diesbezüglichen Unterstützung spezielle Ansprechpartner zu betrauen und die Normungs- und Standardisierungsaktivitäten organisationsweit transparent zu machen.

Für die **Vorbereitung** spezieller FuE-basierter Normungs- oder Standardisierungsvorhaben ist es wichtig, die Aktivitäten frühzeitig in der FuE-Projektplanung zu berücksichtigen. Im Rahmen vieler öffentlicher Förderprogramme sind Normungs- und Standardisierungsaktivitäten zum FuE-Ergebnistransfer förderbar. Daher ist bereits bei der Antragstellung eine Planung der entsprechenden Maßnahmen empfehlenswert. Die Maßnahmen können z.B. in Arbeitspakete zur Verbreitung der Projektergebnisse integriert werden.

Gemessen am Zeitplan der relevanten FuE-Projekte bietet eine frühzeitige **Initiierung** der Normungs- bzw. Standardisierungsvorhaben häufig Vorteile. Sie betreffen insbesondere die

[9] fair, reasonable and nondiscriminatory (terms)

Nutzung möglicher Synergien mit den entsprechenden Vorhaben. Denkbar sind dabei z.B. kombinierte Bedarfsanalysen bei der Zielgruppe, um sowohl Informationen zur Gestaltung der Forschungsvorhaben als auch über erforderliche Inhalte der geplanten Regelwerke zu gewinnen. Erfahrungen des Projekts InfraNorm zeigten nicht nur in diesem Kontext die Bedeutung, eine grundsätzliche Normungs- bzw. Standardisierungsbereitschaft in den Konsortialverträgen von FuE-Projektkonsortien zu fixieren.

Die gezielte Wahl von Projektpartnern mit einer guten Marktpositionierung kann die spätere Verbreitung der Regelwerke enorm begünstigen. Im Bereich der zivilen Sicherheit stellen öffentliche Beschaffer eine wichtige Gruppe von Nachfragern für Produkte und Dienstleistungen dar. Daher hat ihr Einbezug in Normungs- und Standardisierungsprozesse eine besondere Bedeutung.

Blind (2009) zeigte, dass Normen und Standards die Entwicklung von Leitmärkten fördern können. Gleichzeitig ist es wichtig, eine Anwendbarkeit der Regelwerke in bedeutenden Zukunftsmärkten sicherzustellen und in Europäischen und internationalen Standardisierungsprojekten gezielt Teilnehmer aus diesen Regionen einzubeziehen. Darst. 14 fasst die Empfehlungen für die Vorbereitung und Initiierung zusammen.

Vorbereitung von Normungs- und Standardisierungsvorhaben
• Normungs- und Standardisierungsaktivitäten organisationsintern zentral durch Bestimmung von Kontaktpersonen unterstützen • Normungs- und Standardisierungsaktivitäten organisationsintern zentral erfassen • Bei Planung von (Förder-)Projekten Ressourcen für entsprechende Aktivitäten berücksichtigen
Initiierung von Normungs- und Standardisierungsvorhaben
• Frühzeitig entsprechende Aktivitäten initiieren • In Verbundprojekten schon bei der Antragstellung sowie später im Konsortialvertrag Normungsbereitschaft fixieren • Vorbereitende Aktivitäten für die Normung und Standardisierung mit anderen Aufgaben der relevanten FuE-Projekte verbinden • Innovationsplattformen zur Ankündigung der Vorhaben und Partnergewinnung nutzen • Passende weitere Partner in Hinblick auf Erfahrung und Verbreitungsmöglichkeiten einbeziehen • Öffentliche Beschaffer einbeziehen • Ressourcen geeignet bereitstellen • Normrecherchen durchführen • Stand der Konsortialstandards in einschlägigen Datenbanken ermitteln

Darst. 14: Empfehlungen für Teilnehmer des Forschungsprogramms für die Vorbereitung und Initiierung von Normungs- und Standardisierungsvorhaben

In der **Entwicklungsphase** sind Synergien nutzbar, um Normungs- und Standardisierungsmaßnahmen mit anderen Aufgaben der relevanten FuE-Projekte zu verbinden und die spätere Entwicklung des Regelwerks effizient zu gestalten. Synergien können beispielsweise erzielt werden, indem Projekt- und Standardisierungsmeetings miteinander verbunden werden, sodass der Reiseaufwand für das relevante Standardisierungsvorhaben möglichst gering ist.

Bei Normen und Standards im Security-Kontext ist es besonders wichtig, eine Übereinstimmung mit relevanten privacy-spezifischen Regelwerken sicherzustellen. Bei Bedarf sind in die Normungs- oder Standardisierungsaktivitäten Rechtsexperten und Vertreter der von der

Technologieanwendung Betroffenen zur Berücksichtigung von Privacy-Aspekten einzubeziehen. Dies kann auch zur späteren Akzeptanzsteigerung der Regelwerke sowie der entsprechenden technischen Lösungen einen wertvollen Beitrag leisten. In diesem Zusammenhang ist es ebenfalls bedeutsam, mögliche regelwerksbezogene Verwundbarkeitspotentiale der relevanten Systeme zu prüfen[10] und geeignete Schutzmaßnahmen zu implementieren. Sicherheitskritische Aspekte sind auszusparen.

Aus Kosten- und Effizienzgründen ist es sinnvoll, wenn möglich, eine zusätzliche Nutzung der Normen oder Standards im Nicht-Gefahrenfall zu ermöglichen. Internationalisierungsoptionen sind auf geeignete Weise sicherzustellen. In Darst. 15 werden die Empfehlungen für die Entwicklungsphase zusammengefasst.

Entwicklung von Normungs- und Standardisierungsvorhaben
• Normungs- und Standardisierungsmaßnahmen mit FuE-Aufgaben verbinden • Mögliche Konfliktpotentiale gemeinsam identifizieren, mit besonderem Augenmerk verfolgen • Ausreichend Zeit zur Definition des Gültigkeitsbereichs der Regelwerke einplanen • Aufgaben geeignet teilen • Wo möglich, Telefonkonferenzen und elektronische Medien nutzen • Übereinstimmung mit relevanten privacy-spezifischen Regelwerken sicherstellen • Bei Bedarf Rechtsexperten und Vertreter der von der Technologieanwendung Betroffenen zur Berücksichtigung von privacy-Aspekten einbeziehen • Mögliche regelwerksbezogene Verwundbarkeitspotentiale der relevanten Systeme prüfen und geeignete Schutzmaßnahmen implementieren, sicherheitskritische Aspekte aussparen • Wenn möglich, zusätzliche Nutzung im Nicht-Gefahrenfall ermöglichen • Internationalisierungsmöglichkeiten schaffen • Ansprechpartner für künftige Aktivitäten benennen

Darst. 15: Empfehlungen für Teilnehmer des Forschungsprogramms – Phase Entwicklung

Insofern ein Gremienmitglied nur befristet in der Forschungseinrichtung tätig ist, sind Ansprechpartner für künftige Aktivitäten zu benennen.

In der **Veröffentlichungsphase** hat die Einleitung geeigneter Marketingmaßnahmen besondere Bedeutung. Dabei erweisen sich vor allem die folgenden Aktivitäten als erfolgversprechend[11]:

- Entwicklung von Referenzimplementierungen/Pre-Implementierungen
- Entwicklung von Referenzumgebungen/Einbau in Demonstratoren
- Angebot von Interoperabilitätsworkshops (z.B. Plug-Tests)
- Organisation eines Dialogs zwischen Standardentwicklern und Implementierern
- Angebot von Fachartikeln und -vorträgen
- Käuflicher Erwerb der DIN SPEC zur Weitergabe an Multiplikatoren oder Pilotanwender in der Zielgruppe.

[10] Entsprechend dem Mandat M/487 ist die Entwicklung von Methoden für Security Vulnerability Assessments vorgesehen, welche derartige Verwundbarkeitsanalysen erleichtern können.
[11] Neben den Erkenntnissen aus InfraNorm basieren einige der folgenden Empfehlungen auf Folmer (2012:250).

Durch eine Verbindung mit Aktivitäten zur Verbreitung von FuE-Ergebnissen lassen sich im Hinblick auf die Diffusion des entwickelten Regelwerks wirkungsvolle Synergien erzeugen. Die Integration der entwickelten Standards/Normen in künftige FuE-Projekte bietet ebenfalls Erfolgspotentiale, sowohl zur Verbreitung der Regelwerke als auch zu ihrer Weiterentwicklung.

Für die **Anwendungs- und Überarbeitungsphase** ist es wichtig, die Weiterentwicklung des Regelwerks geeignet vorzubereiten, indem Änderungsbedarfe zweckmäßig gesammelt werden und Ressourcen für die beabsichtigten Maßnahmen bereitgestellt werden. In mehreren betrachteten InfraNorm-Projekten wurde beschlossen, ein Monitoring der Reaktionen auf die erarbeiteten Spezifikationen vorzunehmen. Darst. 16 fasst die Empfehlungen für die Veröffentlichungs-, Anwendungs- und Überarbeitungsphase zusammen.

Veröffentlichung der Ergebnisse aus Normungs- und Standardisierungsvorhaben
• Geeignete Marketingmaßnahmen einleiten • Synergien zwischen Aktivitäten zur Verwertung relevanter FuE-Ergebnisse und von Maßnahmen zur Förderung der Diffusion der neuen Regelwerke identifizieren • Synergien zwischen Aktivitäten zur Förderung der Diffusion der neuen Regelwerke und neuen FuE-Projekten in Bezug auf den Einsatz der Regelwerke identifizieren
Anwendung der Ergebnisse aus Normungs- und Standardisierungsvorhaben
• Geeignetes Monitoring implementieren • Änderungsbedarf bei allen Partnern sammeln
Überarbeitung der Ergebnisse aus Normungs- und Standardisierungsvorhaben
• Comittment für die geplanten Änderungen bei den Partnern erwirken • Ressourcen sichern

Darst. 16: Empfehlungen für Teilnehmer des Forschungsprogramms – Phase Veröffentlichung, Anwendung und Überarbeitung

Ergänzende Empfehlungen betreffen die Entwicklung neuer Privacy-Normen und Standards. Entsprechend Kap. 6 und 7 des Handbuchs kann sich die Einhaltung von ethik- und privacy-bezogenen Regelwerken für die Entwickler von Sicherheitstechnologien hinsichtlich der Vermarktungschancen als signifikant erweisen. Vergleiche zwischen der InfraNorm-Studie „Sicherheitsethik, Privacy und Normung“ und dem aktuellen Stand der Normung und Standardisierung zeigten, dass Fragestellungen neuer technischer Lösungen durch bisherige Privacy-Regelwerke oft nur bedingt abgebildet werden. Auf dieser Grundlage bietet die Entwicklung ergänzender privacy-bezogener Normen und Spezifikationen in Kombination mit einer geeigneten Umsetzung Potentiale, die Akzeptanz neuer technischer Lösungen zu steigern. Chancen und Möglichkeiten zur Entwicklung derartiger Regelwerke sollten daher frühzeitig geprüft werden.

Zur Verdeutlichung einer Konformität sowohl mit diesen als auch mit bestehenden privacy-bezogenen Regelwerken bietet die Entwicklung von Privacy-Zertifikaten in Verbindung mit einer Nutzung derartiger Zertifizierungsprozesse Erfolgspotentiale. Darüber hinaus ist im Hinblick auf die Akzeptanz neuer security-bezogener Lösungen eine geeignete Information der Bevölkerung über relevante Technologie- und Einsatzmerkmale bedeutsam.

Normungs- und Standardisierungsprojekte im Sicherheitsforschungsprogramm werden durch den Bezug zu gemeinsamen FuE-Projekten häufig durch kleine, in ihren Interessen relativ

homogene Arbeitsgruppen erstellt. Wichtig ist es dabei, die Interessen der breiten Öffentlichkeit auf geeignete Weise zu berücksichtigen. Den Beispielen einiger begleiteter Vorhaben entsprechend bieten Workshops und Umfragen im Rahmen der relevanten FuE-Projekte hierfür gute Möglichkeiten und können gleichzeitig spezielle Synergien zwischen Forschung und Standardisierung schaffen.

Neben den zuvor ausführlich dargestellten Ergebnissen wurden vielfältige weitere Publikationen erstellt. Eine detaillierte Beschreibung bietet Kap. 2.6.

2.2 Darstellung der wichtigsten Positionen des zahlenmäßigen Nachweises

Wichtige Positionen des Nachweises betreffen die Personalkosten und die Reisekosten. Auf Grundlage der detaillierten Vorstudien und des ermittelten Informationsbedarfs der Zielgruppe wurde ein umfangreicherer Arbeitsaufwand erforderlich als bei Antragstellung abgeschätzt werden konnte. Der Kostenaufwand pro Mannmonat war jedoch geringer als geplant, so dass das Projekt im Rahmen des geplanten Budgets umgesetzt werden konnte. Zudem brauchte die Position „Dienstreisen ins außereuropäische Ausland“ nicht ausgeschöpft zu werden. Kosten konnten gespart werden, da ausländische Ansprechpartner in telefonische Interviews einwilligten und Informationen über weitere internationale Projekte durch deutsche Teilnehmer bereitgestellt werden konnten.

2.3 Darstellung der Notwendigkeit und Angemessenheit der geleisteten Arbeit

Die Bedeutung von Sicherheitsstandards ist auf deutscher und internationaler Ebene gestiegen. Dies belegen insbesondere folgende Aspekte:

- Das Europäische Normungsinstitut CEN hat das Thema „Schutz und die Sicherheit der Bürger“ zu einem seiner künftigen Schwerpunktfelder erklärt (CEN Annual Report, 2009).
- Ende 2010 wurde die Koordinierungsstelle Sicherheitswirtschaft im DIN eingerichtet.
- Anfang Januar 2011 wurde der Workshops "Zertifizierung von Sicherheitstechnologien und -dienstleistungen" im DIN durchgeführt. Die intensive Beteiligung an der Veranstaltung verdeutlicht das große Interesse der Öffentlichkeit an dieser Thematik.
- Bei dem Workshop hob MinDirig. Dr. Rainer Jäkel „die hohe Bedeutung, die die Bundesregierung dem Thema zivile Sicherheitstechnologien und -dienstleistungen als Zukunftsmarkt beimisst, hervor. Damit das Potenzial dieses Zukunftsmarkts sich voll entwickeln könne, werden europa- und weltweit akzeptierte Normen und Spezifikationen benötigt“ (DIN Mitteilungen, Februar 2011, S.3).

Die Wichtigkeit deutscher Normungsaktivitäten bei der Entwicklung eines europäischen Marktes für Sicherheitsprodukte wird in einem Positionspapier von Thoma (2010) wie folgt beschrieben:

> „Mit der Entstehung eines neuen Marktes ergibt sich die Frage nach den Strategien und Vorgehensweisen zur Entwicklung dieses Marktes und zur Positionie-

rung nationaler und europäischer Industrien. Einen wesentlichen Beitrag können dazu Normungs- und Standardisierungsprozesse liefern, deutsche Akteure sollten auf laufende und zukünftige europäische und internationale aktiv Einfluss nehmen. Gegenwärtig ist der Markt der öffentlichen Sicherheit stark fragmentiert und wird erschwert durch zeit- und kostenaufwändige nationale Zertifizierungen."[12]

Weitere Arbeiten, die den Bedarf für Sicherheitsstandards in Europa von externer Seite bestätigt sind, z.B.:

- ESRIF (2009). Final Report December 2009. http://ec.europa.eu/enterprise/policies/security/files/esrif_final_report_en.pdf.
- CREATIF (2009). D.2.x.3: Standards and methods available for testing CBRNE detection systems. http://www.creatif-network.eu/resources.html.
- ECORYS (2009). Study on Competitiveness of the EU Security Industry. http://ec.europa.eu/enterprise/policies/security/files/study_on_the_competitiveness_of_the_eu_security_industry_en.pdf.
- DIESIS (2010). DIESIS. Design of an Interoperable European federated Simulation network for critical InfraStructures. D3.3 Standard for Interoperable Critical Infrastructure Simulation.
- Sáez, A. C., Urech, A., Pereira, J. (2009). Current status of Security in Mass Transport. DEMASST Deliverable 3.1: Current status of security in mass transport, November 2009.
- Security Standardisation Programming-Mandate M/487.

Das europäische Security Standardisation Programming-Mandate M/487 der Europäischen Kommission wurde als Reaktion auf den großen europaweiten Standardisierungsbedarf auf diesem Gebiet verfasst und im Sommer 2011 verabschiedet. Durch das Mandat fordert die Kommission Europäische Standardisierungsorganisationen auf, Standards zur Unterstützung europäischer Policies und Gesetzgebungen zu entwickeln und zu adoptieren. Die Arbeit im Rahmen des Mandates umfasst vier Forschungsgebiete, zu denen auch der Bereich "Security of Infrastructures and Utilities" zählt. Entsprechend dem bereits veröffentlichen ersten der beiden M/487-Reports ist in den folgenden Jahren mit einer Intensivierung der europäischen Normungsaktivitäten im Sicherheitsbereich zu rechnen. Derzeit werden entsprechende Roadmaps erstellt.

Die Stärkung der Position deutscher Akteure und der Ausbau der Normungskompetenzen erhalten durch das Mandat zusätzliche Bedeutung. Mit dem Normungsinstitut NEN, das maßgeblich mit der Durchführung der Mandatsaufgaben betraut wurde, konnte eine Forschungskooperation aufgebaut werden (vgl. Kap. 2.4). Darüber hinaus werden Normen und Standards auch im Rahmen des Europäischen Rahmenprogramms Horizon 2020 im Vergleich zu bisherigen Forschungsprogrammen eine größere Rolle spielen.

Der Bedarf für die durchgeführten Arbeiten wurde u.a. durch die Vorstudien zum Normungshandbuch verdeutlicht. Deutsche Sicherheitsforscher haben i.d.R. wenige Kenntnisse über Sicherheitsnormen und vor allem DIN SPECs sind häufig unbekannt.

[12] Thoma, K. (2010). Positionspapier des wissenschaftlichen Programmausschusses zum nationalen Sicherheitsforschungsprogramm. http://www.bmbf.de/pub/WPA_Positionspapier_ 2010.pdf, Abruf am 25.01.2011, S.9.

Das Projekt wurde rationell durchgeführt. Effizienz konnte z.B. durch die attraktive Zusammenarbeit mit Mitarbeitern der VDI Technologiezentrum GmbH, welche die Innovationsplattformen betreuten, erreicht werden. Für eine weitere Fallstudie wurden anstelle eigener Feldforschungen Vorarbeiten Holländischer Forscher genutzt. Konsequent wurde im Hinblick auf kostenintensive Auslandsreisen gespart. Auf dieser Grundlage konnte das Projekt günstiger abgeschlossen werden als geplant.

2.4 Darstellung des voraussichtlichen Nutzens, insbesondere der Verwertbarkeit des Ergebnisses im Sinne des fortgeschriebenen Verwertungsplans

Das Normungshandbuch für Sicherheitsforscher bezweckt mit dem Ziel der Standortförderung vorrangig einen Nutzen für deutsche, in der Sicherheitsforschung tätige Organisationen im Rahmen ihrer Verwertungsaktivitäten auf nationaler, europäischer und internationaler Ebene. Das Handbuch wird allen Teilnehmern des Sicherheitsforschungsprogramms zur Verfügung gestellt. Effekte werden insbesondere innerhalb des Rahmenprogramms "Forschung für die zivile Sicherheit 2012-2017“ erwartet. In eines dieser Vorhaben, in das Projekt ENSURE (Laufzeit: 8/2013 bis 7/2016), ist das Fachgebiet Innovationsökonomie selbst einbezogen und wird Arbeiten zur Förderung des FuE-Ergebnistransfers mittels Normung und Standardisierung erbringen. Weitere Anfragen zur Nutzung des Handbuchs von potentiellen Interessenten existieren, z.B. von der DKE, vom ZVEI sowie von mehreren europäischen Normungsexperten.

In Kap. 2.1 wurde beschrieben, dass auf Grundlage der Emittlung des Normungs- bzw. Standardisierungsbedarfs in Arbeitspaket 1.1 fünf DIN-Spezifikationen entwickelt wurden, die den beteiligten Akteuren und den Partnern ihrer Verbundprojekte zugutekommen. Ein Beispiel hierzu gibt Engelt/Hasenfuß (2013)[13]. An der Erstellung der DIN SPECs waren 20 Organisationen beteiligt. Die Wirkung auf die von ihnen repräsentierten Verbundprojekte ist jedoch wesentlich größer.

Neben den bereits umgesetzten DIN Spezifikationen wurden Themen für weitere Standardisierungsvorhaben definiert, die zum Transfer von FuE-Ergebnissen der Sicherheitsforschung weitere Unterstützung bieten können. In besonderer Weise wurden Themen für Datenschutz- und Privacy-Standards ermittelt, die das Potential haben, die Akzeptanz verschiedener, konkret beschriebener neuer Sicherheitslösungen zu erhöhen.

Ein wichtiger Verwertungsbereich betrifft Publikationen und Fachvorträge. Mit Unterstützung der VDI Technologiezentrum GmbH konnte die Vorstudie des Normungshandbuchs „Bedeutung von Sicherheitsnormen, -standards und -spezifikationen“ an rund 500 deutsche Sicherheitsforscher versendet werden. Zwei Artikel zu InfraNorm-Studien wurde in den DIN-Mitteilungen mit einer Auflage von 3.528 Exemplaren publiziert. Die Ergebnisse wurden darüber dem nationalen Convenor der ISO TC 223 WG 3 Emergency Management im Rahmen von Kooperationsgesprächen vorgestellt sowie dem nationalen Convenor für die CLC/TC 79 Alarm systems und die IEC/TC 79 Alarm and electronic security sytems zwecks Kooperati-

[13] Engelt, A., Hasenfuß, P. (2012). Standardisierung als Instrument zur nachhaltigen Verwertung innovativer Produkte und Dienstleistungen. Entwicklungsbegleitende Normung (EBN) im DIN. Erfahrungsbericht über die Erstellung einer DIN-Spezifikation im Sicherheitsforschungsprogramm. DIN Mitteilungen (2012/6), 20-21.

onsanbahnung zur Verfügung gestellt. Die Koordinierungsstelle Sicherheitswirtschaft im DIN erhielt die Studie ebenfalls. Eine ausführliche Übersicht über bisherige Publikationen bietet Kap. 2.6. Es bestehen Überlegungen, ausgewählte Fallstudien des Handbuchs in einem englischsprachigen Werk zu publizieren.

Das Konsortium des oben erwähnten Vorhabens ENSURE erkannte die Bedeutung von Normungs- und Standardisierungsmaßnahmen für den langfristigen Erfolg und die Verwertung von Projektergebnissen. Im Rahmen des Vorhabens soll durch die TU Berlin ein Standardisierungskonzept entwickelt werden. Über die sicherheitsbezogene Standardisierung hinaus konnte sich das Fachgebiet Innovationsökonomie durch InfraNorm sowohl als kompetenter Partner in der Sicherheitsforschung als auch vertiefend in der grundlegenden Standardisierungsforschung positionieren. Im Sicherheitsforschungsprojekt ENSURE ist es neben den standardisierungsbezogenen Aktivitäten mit der Bearbeitung weiterer, innovationsökonomischer Fragestellungen von Schutzsystemen betraut. Es ist zudem in das FP7-Projekt CeRtIfication of Security Products (CRISP) einbezogen, welches durch die niederländische Normungsorganisation NEN koordiniert wird. Das Fachgebiet Innovationsökonomie der TU Berlin wird dabei u.a. das Arbeitspaket „Review of standards, certification and accreditation for security products“ leiten (geplante Laufzeit: 12/2013 bis 11/2016).

Zunehmend wird die Forscherin, die an der TU Berlin maßgeblich mit der Durchführung von InfraNorm betraut war, aufgrund des Vorhabens auch in anderen Kontexten als Standardisierungsexpertin eingeladen, z.B.:

- Workshop zur Priorisierung von Untersuchungsfeldern im Sicherheitsbereich im Rahmen der Studie „Erarbeitung eines Leitfadens zur Begutachtung und Bewertung von Sicherheitslösungen“ am 29. Februar 2012 in Berlin im Rahmen der „Initiative Innovation mit Normen und Standards“ des BMWi
- Young DKE Workshop am 15. Mai 2013, Einladung durch die DKE
- Workshop "Innovationspotenziale der Normung" am 05. Juli 2013 in Leipzig, Einladung durch das MOSZ

Ein weiterer Verwertungsbereich betrifft die Lehre und die Betreuung von Studierenden. Im Rahmen des Vorhabens konnte bereits eine Studienarbeit zum Thema „Probleme und Schutzmechanismen in unterschiedlichen Schutzbereichen von Wirtschaftssystemen - Ein strukturierter Vergleich der drei Aktionsgebiete Normung, Patentierung und Schutz vor Produktpiraterie“ vergeben und mitterweile abgeschlossen werden. Von Seiten Berliner Sicherheitsforscher bestehen zudem Überlegungen unter Beteiligung des Fachgebiets Innovationsökonomie einen Security-Studiengang einzurichten.

2.5 Darstellung des während der Durchführung des Vorhabens dem Zuwendungsempfänger bekannt gewordenen Fortschritts auf dem Vorhabensgebiet bei anderen Stellen

Fortschritt in der Praxis

Ermittlung des Normungs- und Standardisierungsbedarfs

In Arbeitspaket 1.1 wurden von der TU Berlin prioritäre Themen für Standardisierungsvorhaben erarbeitet. In Kap.2.1 wurde gezeigt, dass auf diesen Gebieten im Rahmen von InfraNorm fünf Standardisierungsprojekte durchgeführt wurden. Zu Beginn der Vorhaben wurde vom DIN e.V. eine vertiefende Prüfung auf bereits existierende Normen auf den jeweiligen Gebieten durchgeführt. Das Ergebnis zeigte, dass die Themen nicht durch existierende Normen abgedeckt wurden.

Normungshandbuch

Im Sommer 2011 wurde, wie beschrieben, das europäische Security Standardisation Programming-Mandate M/487 verabschiedet. Die Stärkung der Position deutscher Akteure und der Ausbau der Normungskompetenzen erhielt durch das Mandat zusätzliche Bedeutung.

Derzeit befindet sich die EU-Datenschutz-Grundverordnung in der Entwicklung. Der aktuelle Stand ist in der COM(2012) 11 als Proposal dokumentiert. Durch den geplanten Ersatz nationaler Datenschutzregelungen wird mit ihrer Einführung eine größere Vereinheitlichung des Datenschutzes innerhalb der EU beabsichtigt. Art. 23 der Grundverordnung (Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen) wird die Grundsätze des „Privacy by design[14] bzw. Privacy by default“ definieren (vgl. Europäische Kommission, 2012). Dennoch ist die Verordnung technikneutral formuliert. Die Fertigstellung der Verordnung ist bis Ende 2013 vorgesehen. Es ist davon auszugehen, dass das Dokument ebenso wie die von ihm abgelöste Richtlinie 95/46 EG die Grundlage für neue Normen und Standards bilden wird, insbesondere aufgrund seiner technikneutralen Ausrichtung. Daher haben Hinweise zur erfolgreichen Normung und Standardisierung besondere Bedeutung.

Fortschritt in der Forschung

Von dem britischen Forscher Peter Hatto wurde im Frühjahr 2013 der Guide “Standards and Standardisation. A practical guide for researchers” herausgebracht. Auf ausgewählte Aspekte des Guides wird im Normungshandbuch verwiesen. Die wichtigsten Aspekte des Handbuchs werden von Hatto jedoch nicht tangiert. Sie betreffen insbesondere:

- Die Erstellung von DIN SPECs
- Privacy und ethische Aspekte in der Security-Standardisierung
- Fallstudien zur Security-Standardisierung
- Die spezielle Nutzung der Normung und Standardisierung zur Realisierung nationaler Vorteile.

[14] In Kap. 7 wird eine detaillierte Betrachtung des Privacy-by-Design-Konzepts vorgenommen.

Die Zielgruppe Hattos besteht vor allem aus Teilnehmern multinationaler europäischer FuE-Projekte. Daher wird die Verwirklichung nationaler Vorteile, wie sie z.B. anhand nationaler Strategien in der Fallstudie „TETRA“ im Normungshandbuch erörtert wird, in Hattos Guide nicht thematisiert.

Im Rahmen der Ergebnisverwertung von InfraNorm besuchte die für das Teilprojekt „Normungshandbuch“ verantwortliche Forscherin im April 2013 die internationale ITU-Konferenz in Japan. Dort definierte Prof. van de Kaa den Bereich ethische Aspekte und Privacy als neue Lücke in der Standardisierungsforschung. Er selbst erforscht vor allem de facto-Standards und nahm die Forschungsarbeiten der TU Berlin mit großem Interesse zur Kenntnis, da vergleichbare Fortschritte nicht an anderen Stellen existieren.

Im Rahmen von InfraNorms Ergebnisverwertung besuchte die Forscherin zudem im Juni 2013 die 17. EURAS Annual Standardisation Conference – Boosting European Competitiveness. Auf der EURAS kommen jährlich die wichtigsten europäischen Standardisierungsforscher zusammen. Zunehmend zählt die Konferenz auch außereuropäische Teilnehmer. Weder die Präsentationsinhalte der Konferenzteilnehmer noch der dortige Forschungsdialog zeigten Inhalte auf, die mit den Ergebnissen des Projekts InfraNorm an der TU Berlin vergleichbar sind.

2.6 Erfolgte oder geplante Veröffentlichungen des Ergebnisses nach Nr. 6.

Bisherige Veröffentlichungen neben den Projektstudien und dem Normungshandbuch umfassen:

Wurster, S., Egyedi, T., Hommels, A. (2013). „The Development of the Public Safety Standard TETRA: Lessons and Recommendations for Research Managers and Strategists in the Security Industry“. Proceedings of the „8th International Conference on Standardization and Innovation in Information Technology“ (IEEE-SIIT 2013) (Forthcoming).

Wurster, S. (2013). „Ethical and Privacy-Specific Risks – Flaws of Critical Infrastructure Protection and Solutions Offered by Standardisation”. Proceedings of the 18th EURAS Annual Standardization Conference - Standards and Innovation-, 413-427.

Wurster, S. (2013). “Security Technologies for the Protection of Critical Infrastructures – Ethical Risks and Solutions offered by Standardization”. In: International Telecommunication Union: Proceedings of the 2013 ITU Kaleidoscope Academic Conference Buildung Sustainable Communities, Kyoto, Japan, 22-24 April 2013, 21-30.

Wurster, S. (2013). „Security-Technologien zum Schutz kritischer Infrastrukturen – ethische Risiken und Lösungen mittels Normung und Standardisierung“. DIN Mitteilungen 2013/3, 58.

Wurster, S. (2013). "Development of a Specification for Data Interchange Between Information Systems in Civil Hazard Prevention. Identification of Success Factors, Challenges and Solutions Based on Case Study Research". The International Journal of IT Standards and Standardization Research (IJITSR), 11(1), 46-66, January-June 2013.

Wurster, S. (2013). “Development of a Specification for Computer Based Microscopic Evacuation Analyses and Simulations. Identification of Success Factors Based on Case Study Research”. GSTF Journal on Computing (JoC) Vol 2 (4), 7-14.

Siegel, N., Wurster, S. (2012). "Standards for the Protection of Transport Infrastructures". In: Aschenbruck, N., Martini, P., Meier, M., Tölle, J. [Hrsg.] (2012). Communication in Computer and Information Science 318. Future Security. 7th Security Research Conference, Future Security 2012, Bonn, September 2012, Proceedings. Heidelberg, Dordrecht, London, New York, Springer, 21-24.

Wurster, S. (2012). Example of Good Practice in R&D Stage Standardization in Germany: Development of a Specification for Data Interchange Between Information Systems in Civil Hazard Prevention. 3rd Annual International Conference on Infocomm Technologies in Competitive Strategies (ICT 2012) and Advances in Distributed and Parallel Computing (ADPC 2012), 7-14.

Wurster, S. (2012). "Development of a Specification for Data Interchange Between Information Systems in Civil Hazard Prevention. Identification of Success Factors, Challenges and Solutions Based on Case Study Research and Participant Observation". Proceedings of the 17th EURAS Annual Standardization Conference - Standards and Innovation-, 397-416.

Wurster, S. (2012). "Bedeutung von Sicherheitsnormen, -standards und -spezifikationen. Ergebnisse einer Studie in der deutschen Sicherheitsforschung". DIN Mitteilungen 2012/6, 23-27.

Wurster, S. (2012). "Example of Good Practice in Linking Research and Standardization in Germany: Development of a Specification for Data Interchange in Civil Hazard Prevention". KSA, Seoul, South Korea, May 29th, 2012.

Wurster, S. (2012). "Transfer of Security Research Results Through Standardization - Case Studies From the Project InfraNorm". 7th Future Security Conference, Bonn, September 4th - 6th, 2012.

Wurster, S. (2011). "InfraNorm - Norms and Standards for the Protection of Transportation Infrastructure". Proceedings of the Annual International Conference on Innovation and Entrepreneurship, 19-24.

Weitere Veröffentlichungen sind in Proceedings künftiger EURAS-, SIIT- und/oder ITU-Konferenzen vorgesehen. Zusätzliche Publikationen im IJITSR-Journal sind ebenfalls möglich.

Anlage: Berichtsblätter in deutscher und englischer Sprache

Berichtsblatt 1

1. ISBN oder ISSN ---	2. Berichtsart (Schlussbericht oder Veröffentlichung) Schlussbericht
3. Titel Schlussbericht des Projekts InfraNorm - Normungs- und Standardisierungspotenzial im Bereich des Schutzes von Verkehrsinfrastrukturen, Teilvorhaben: Normungshandbuch	
4. Autor(en) [Name(n), Vorname(n)] Wurster, Simone	5. Abschlussdatum des Vorhabens 28.02.2013
	6. Veröffentlichungsdatum August 2013
	7. Form der Publikation Schlussbericht (Print- u. Online-Version)
8. Durchführende Institution(en) (Name, Adresse) Technische Universität Berlin Institut für Technologie und Management FG Innovationsökonomie - VWS 2 Müller-Breslau-Straße 15 10623 Berlin	9. Ber. Nr. Durchführende Institution
	10. Förderkennzeichen 13N10915
	11. Seitenzahl 43
12. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	13. Literaturangaben 146
	14. Tabellen 16 Darstellungen
	15. Abbildungen Siehe „Tabellen“
16. Zusätzliche Angaben	
17. Vorgelegt bei (Titel, Ort, Datum) Abteilung EINS – Sicherheitsforschung, Projektträger des BMBF, VDI Technologiezentrum GmbH VDI-Platz 1, 40468 Düsseldorf, Technische Informationsbibliothek, Deutsche Forschungsberichte, Welfengarten 1B, 30167 Hannover, jeweils August 2013	
18. Kurzfassung Der Schlussbericht hat folgende Inhalte: 1. Einführende Aspekte in kurzer Darstellung • Aufgabenstellung • Voraussetzungen, unter denen das Vorhaben durchgeführt wurde • Planung und Ablauf des Vorhabens • Wissenschaftlicher und technischer Stand, an den angeknüpft wurde • Zusammenarbeit mit anderen Stellen 2. Eingehende Darstellungen • Verwendung der Zuwendung und erzielte Ergebnisse im Einzelnen • Darstellung der wichtigsten Positionen des zahlenmäßigen Nachweises • Darstellung der Notwendigkeit und Angemessenheit der geleisteten Arbeit • Darstellung des voraussichtlichen Nutzens, insbesondere der Verwertbarkeit des Ergebnisses im Sinne des fortgeschriebenen Verwertungsplans • Darstellung des während der Durchführung des Vorhabens dem Zuwendungsempfänger bekannt gewordenen Fortschritts auf dem Vorhabensgebiet bei anderen Stellen • Erfolgte oder geplante Veröffentlichungen des Ergebnisses nach Nr. 6.	
19. Schlagwörter Normung, Standardisierung, zivile Sicherheit, zivile Sicherheitsforschung, Privacy	
20. Verlag ---	21. Preis ---

Document Control Sheet 1

1. ISBN or ISSN ---	2. type of document (e.g. report, publication) Final report
3. title Schlussbericht des Projekts InfraNorm - Normungs- und Standardisierungspotenzial im Bereich des Schutzes von Verkehrsinfrastrukturen, Teilvorhaben: Normungshandbuch	
4. author(s) (family name, first name(s)) Wurster, Simone	5. end of project 28 February 2013
	6. publication date August 2013
	7. form of publication Print version and online version
8. performing organization(s) (name, address) Technische Universität Berlin Institut für Technologie und Management FG Innovationsökonomie - VWS 2 Müller-Breslau-Straße 15 10623 Berlin	9. originator's report no. Final report
	10. reference no. 13N10915
	11. no. of pages 43
12. sponsoring agency (name, address) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	13. no. of references 146
	14. no. of tables 16 tables and figures
	15. no. of figures See 14.
16. supplementary notes	
17. presented at (title, place, date) Abteilung EINS – Sicherheitsforschung, Projektträger des BMBF, VDI Technologiezentrum GmbH VDI-Platz 1, 40468 Düsseldorf, Technische Informationsbibliothek, Deutsche Forschungsberichte, Welfengarten 1B, 30167 Hannover, August 2013	
18. abstract The final report has the following content: 1. Short introduction • Project goals • Prerequisites of the project • Planning and timing of the project • Scientific and technical state on which the project was built • Co-operation with other organizations 2. Detailed description • Use of grants and results in detail • Description of major items of the budget • Description of the necessity and appropriateness of the activities • Presentation of anticipated benefits, including the use of the results (exploitation plan) • Progress in the project area in other organizations • Publication of the results	
19. keywords Standardization, civil security, civil security research, privacy	
20. publisher ---	21. price ---

Berichtsblatt 2

1. ISBN oder ISSN NN	2. Berichtsart (Schlussbericht oder Veröffentlichung) Veröffentlichung
3. Titel Normungshandbuch für die Teilnehmer des deutschen Forschungsrahmenprogramms „Forschung für die zivile Sicherheit“	
4. Autor(en) [Name(n), Vorname(n)] Wurster, Simone	5. Abschlussdatum des Vorhabens 28.02.2013
	6. Veröffentlichungsdatum tba
	7. Form der Publikation Buch
8. Durchführende Institution(en) (Name, Adresse) Technische Universität Berlin Institut für Technologie und Management FG Innovationsökonomie - VWS 2 Müller-Breslau-Straße 15 10623 Berlin	9. Ber. Nr. Durchführende Institution
	10. Förderkennzeichen 13N10915
	11. Seitenzahl 254
12. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	13. Literaturangaben 219
	14. Tabellen 80 Darstellungen
	15. Abbildungen Siehe „Tabellen“
16. Zusätzliche Angaben	
17. Vorgelegt bei (Titel, Ort, Datum) Abteilung EINS – Sicherheitsforschung, Projektträger des BMBF, VDI Technologiezentrum GmbH VDI-Platz 1, 40468 Düsseldorf	

18. Kurzfassung

Das Normungshandbuch ist in elf Kapitel gegliedert. Nach dem einführenden Kapitel stellt **Kapitel 2** den Forschungskontext dar. **Kapitel 3** bietet eine Einführung in die Normung und Standardisierung. Dabei werden die Merkmale von Normen und Spezifikationen sowie ihre grundsätzliche Erarbeitung auf nationaler, europäischer und internationaler Ebene dargestellt. In **Kapitel 4** werden die Relevanz der Normung für die Sicherheitsforschung sowie ihre Vorteile aufgezeigt. **Kapitel 5** dient der Beschreibung allgemeiner Strategien für die sicherheitsbezogene Normung und Standardisierung. Dabei werden Empfehlungen zur Integration von Normungsaktivitäten in die Forschung sowie geeignete Umsetzungshilfsmittel dargestellt. Die rechtlichen Rahmenbedingungen der security-bezogenen Normung und Standardisierung bilden den Inhalt von **Kapitel 6**. Im Mittelpunkt stehen dabei Regelungen in den Bereichen Datenschutz und Privacy sowie ihre Anwendung im Security-Kontext. **Kapitel 7** gibt ausführliche Informationen zur Integration ethischer Aspekte in die sicherheitsbezogene Normung und Standardisierung. Ausgewählte Normen und Spezifikationen in den Bereichen Privacy, Datenschutz und Datensicherheit werden erörtert. Darüber hinaus wird eine detaillierte Betrachtung der Themen Privacy Impact Assessments, Privacy by Design und Privacy Enhancing Technologies vorgenommen. **Kapitel 8** beschreibt die Rahmenbedingungen zum Umgang mit geistigen Eigentumsrechten in der Normung bzw. Standardisierung. Es werden sowohl eigene Eigentumsrechte der betreffenden Akteure der Sicherheitsforschung als auch fremde Eigentumsrechte thematisiert. Dabei stehen patentbezogene Themen im Mittelpunkt. Relevante Regelungen von Normungsorganisationen, wie z.B. das FRAND-Prinzip, werden ausführlich erläutert. Zur Verdeutlichung der Chancen der Normung und Standardisierung, Vertiefung der Umsetzungsprozesse und Ermittlung von Erfolgsfaktoren werden in **Kapitel 9** und **10** zehn Normungs- und Standardisierungsvorhaben anhand von Fallstudien dargestellt. **Kapitel 11** dient der Zusammenfassung und Darstellung von Empfehlungen für die relevanten Adressatenkreise der Normung und Standardisierung im Sicherheitsforschungsprogramm.

19. Schlagwörter
Normung, Standardisierung, zivile Sicherheit, zivile Sicherheitsforschung, Privacy

20. Verlag NN, wahrscheinlich Beuth Verlag	21. Preis NN

Document Control Sheet 2

1. ISBN or ISSN ---	2. type of document (e.g. report, publication) Publication
3. title Standardization Manual for the Participants of the German Framework Programme "Research for Civil Security"	
4. author(s) (family name, first name(s)) Wurster, Simone	5. end of project 28 February 2013
	6. publication date tba
	7. form of publication book
8. performing organization(s) (name, address) Technische Universität Berlin Institut für Technologie und Management FG Innovationsökonomie - VWS 2 Müller-Breslau-Straße 15 10623 Berlin	9. originator's report no.
	10. reference no. 13N10915
	11. no. of pages 254
12. sponsoring agency (name, address) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	13. no. of references 219
	14. no. of tables 80 tables and figures
	15. no. of figures See 14.
16. supplementary notes	
17. presented at (title, place, date) Abteilung EINS – Sicherheitsforschung, Projektträger des BMBF, VDI Technologiezentrum GmbH VDI-Platz 1, 40468 Düsseldorf	

18. abstract

The Standardization Manual consists of eleven chapters. Chapter 1 gives an introductory summary. Chapter 2 describes the research context. Chapter 3 provides an introduction to standardization. The characteristics of standards and specifications as well as their development at national, European and international level are represented. Chapter 4 shows the relevance of standards for security research and its benefits. Chapter 5 describes general strategies for security-related standardization. Recommendations for the integration of standardization activities in research and appropriate methodologies are presented. The legal framework of security-related standardization is the foundation of Chapter 6. The focus is on regulations in the areas of data protection and privacy as well as their application in the security context. Chapter 7 provides detailed information on integrating ethical aspects into security-related standardization. Selected standards and specifications in the areas of privacy, data protection and data security are discussed. In addition, a detailed description of the issues privacy impact assessments, privacy by design and privacy enhancing technologies is given. Chapter 8 discusses the framework for dealing with intellectual property rights in standardization. Issues of the researchers' own and third-party intellectual property rights are discussed. The main focus is on patent-related issues. Relevant rules of standards organizations, such as the FRAND principle are explained in detail. Chapters 9 and 10 present ten standardization projects through case studies to illustrate the opportunities of standardization, to deepen the implementation processes and to identify success factors. Finally, chapter 11 provides a summary and recommendations for the relevant target audiences in the German security research program.

19. keywords Standardization, civil security, security research, privacy	
20. publisher NN, probably Beuth Verlag	21. price NN

Berichtsblatt 3

1. ISBN oder ISSN NN	2. Berichtsart (Schlussbericht oder Veröffentlichung) Veröffentlichung
3. Titel The Development of the Public Safety Standard TETRA: Lessons and Recommendations for Research Managers and Strategists in the Security Industry	
4. Autor(en) [Name(n), Vorname(n)] Wurster, Simone, Egyedi, Tineke M. Hommels, Anique	5. Abschlussdatum des Vorhabens 28.02.2013
	6. Veröffentlichungsdatum 24.09.2013
	7. Form der Publikation Konferenz-Proceedings
8. Durchführende Institution(en) (Name, Adresse) Technische Universität Berlin Institut für Technologie und Management FG Innovationsökonomie - VWS 2 Müller-Breslau-Straße 15, 10623 Berlin, Department of Infrastructures/ TPM Faculty Delft University of Technology Delft, the Netherlands, Faculty of Arts and Social Sciences Department of Technology and Society studies Maastricht University Maastricht, the Netherlands	9. Ber. Nr. Durchführende Institution
	10. Förderkennzeichen 13N10915
	11. Seitenzahl 12
12. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	13. Literaturangaben 38
	14. Tabellen 4
	15. Abbildungen 1
16. Zusätzliche Angaben	
17. Vorgelegt bei (Titel, Ort, Datum) The 8th International Conference on Standardization and Innovation in Information Technology (IEEE-SIIT 2013)	
18. Kurzfassung Der Artikel beschreibt die Entwicklung des europäischen Public-Safety-Standards TETRA und bezweckt die Ableitung von Empfehlungen für Forschungsmanager, die an nationalen zivilen Sicherheitsforschungsprogrammen teilnehmen und Normen oder Standards für ihre security-spezifischen FuE-Ergebnisse entwickeln wollen. Die Forscher Weiss und Sirbu ermittelten, dass die politischen Fähigkeiten der Sponsoren einer Technologie für die Annahme dieser Technologie in der Standardisierung nicht signifikant sind. Die Fallstudie gibt ein Gegenbeispiel. TETRAs Etablierung wurde von herausragenden Persönlichkeiten mit besonderen Fähigkeiten und Strategien geprägt. Die Studie zeigt die Bedeutung von politischen Fähigkeiten, die Relevanz unterschiedlicher Lobbyarbeit und von Verhandlungsaktivitäten zur Beeinflussung der Standardisierung. Spezifische nationale Allianzstrategien sowie Lobbyarbeit auf europäischer Ebene waren für TETRAs Standardisierung entscheidend. Angesichts der multinationalen Dimensionen vieler Fragen der Sicherheit enthält der Artikel ferner Anregungen, die für duale national-europäische Standardisierungsstrategien benötigt werden, z.B. im Rahmen des Europäischen Security Standardization-Mandates M/487. Das Beispiel TETRA zeigt, wie eine solche mehrebenenorientierte Standardisierungsstrategie erfolgreich verfolgt werden kann.	
19. Schlagwörter Standardisierungsmaßnahmen in Europa, Security-Standards, Sicherheitstechnologien, Europäisches Mandate M/487, mehrebenenorientierte Standardisierungsstrategien	
20. Verlag NN	21. Preis ---

Document Control Sheet 3

1. ISBN or ISSN NN	2. type of document (e.g. report, publication) publication
3. title The Development of the Public Safety Standard TETRA: Lessons and Recommendations for Research Managers and Strategists in the Security Industry	
4. author(s) (family name, first name(s)) Wurster, Simone, Egyedi, Tineke M. Egyedi Hommels, Anique	5. end of project 28 February 2013
	6. publication date 24 September 2013
	7. form of publication Conference proceedings, forthcoming
8. performing organization(s) (name, address) Technische Universität Berlin Institut für Technologie und Management FG Innovationsökonomie - VWS 2 Müller-Breslau-Straße 15, 10623 Berlin, Department of Infrastructures/ TPM Faculty Delft University of Technology Delft, the Netherlands, Faculty of Arts and Social Sciences Department of Technology and Society studies Maastricht University Maastricht, the Netherlands	9. originator's report no.
	10. reference no. 13N10915
	11. no. of pages 12
12. sponsoring agency (name, address) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	13. no. of references 38
	14. no. of tables 4
	15. no. of figures 1
16. supplementary notes	
17. presented at (title, place, date) The 8th International Conference on Standardization and Innovation in Information Technology (IEEE-SIIT 2013)	
18. abstract In this article we describe the European standardisation of Terrestrial Trunked Radio (TETRA) and try to draw lessons for European research managers who participate in national civil security research programmes and wish to develop standards related to their security-specific R&D results. This study challenges the findings from Weiss and Sirbu (1990), which suggest that the political skills of the sponsors of a technology are not significant for its adoption in a standardisation process. TETRA's establishment was shaped by specific people, specific skills and specific strategies. Our study shows the importance of political skills, as well as the relevance of multiple lobbying and negotiation activities in influencing the standardisation process. Specific national strategies in forging alliances, as well as lobbying on the European level were crucial, and their realisation offers lessons to learn from. Moreover, given the indisputable multinational dimension in many security issues, our article contains suggestions regarding dual national-European level standardisation strategies needed, for instance, in the context of the European security standardisation Mandate M/487. The TETRA case illustrates how to pursue such a dual level standardisation strategy successfully.	
19. keywords European standardisation, security standards, security technologies, European Mandate M/487, dual level standardisation strategy	
20. publisher NN	21. price ---

Berichtsblatt 4

1. ISBN oder ISSN ISBN: 978-3-86130-655-9	2. Berichtsart (Schlussbericht oder Veröffentlichung) Veröffentlichung
3. Titel Ethical and Privacy-Specific Risks – Flaws of Critical Infrastructure Protection and Solutions Offered by Standardisation	
4. Autor(en) [Name(n), Vorname(n)] Wurster, Simone	5. Abschlussdatum des Vorhabens 28.02.2013
	6. Veröffentlichungsdatum 24.06.2013
	7. Form der Publikation Konferenz-Proceedings
8. Durchführende Institution(en) (Name, Adresse) Technische Universität Berlin Institut für Technologie und Management FG Innovationsökonomie - VWS 2 Müller-Breslau-Straße 15 10623 Berlin	9. Ber. Nr. Durchführende Institution
	10. Förderkennzeichen 13N10915
	11. Seitenzahl 15
12. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	13. Literaturangaben 27
	14. Tabellen 4
	15. Abbildungen 3
16. Zusätzliche Angaben	
17. Vorgelegt bei (Titel, Ort, Datum) Proceedings of the 18th EURAS Conference - Standards and Innovation-, Brüssel, 413-427.	

18. Kurzfassung

Namhafte Wissenschaftler zeigen den Beitrag von Standards zur Akzeptanzsteigerung innovativer Lösungen und zur Beschleunigung der Diffusion von Innovationen. Der vorliegende Artikel befasst sich mit dieser Thematik im Bereich der zivilen Sicherheit. Die globale Intensität und Häufigkeit von kriminellen und terroristischen Vorfällen zeigt die Verwundbarkeit demokratischer Gesellschaften und die Notwendigkeit kritische Infrastrukturen (KIs) zu schützen. Viele technologische Sicherheitslösungen zum Schutz der KI befinden sich in laufenden Sicherheitsforschungsprojekten in der Entwicklung oder sind bereits verfügbar. Allerdings können diese Lösungen ethische und datenschutzbezogene Risiken und damit gleichzeitig Hemmnisse für die Adoption dieser Systeme bergen. Spezielle Datenschutzstandards können demgegenüber Lösungen bieten. Die Forscher Fens und van de Kaa schlugen Anfang 2013 vor, einen Paradigmenwechsel in standardisierungsbezogenen Strategien und Forschungsarbeiten vorzunehmen und die Berücksichtigung von ethischen Aspekten als zusätzlichen Erfolgsfaktor zu erklären. Der vorliegende Artikel geht noch einen Schritt weiter. Er konzentriert sich auf spezifische ethikbezogene und Datenschutz-Standards und führt Privacy als neue Dimension des Zusammenspiels zwischen Standards und Innovation im Bereich der zivilen Sicherheit ein. Bisher werden Privacy-Fragen ziviler Sicherheitstechnologien und der KI-Schutz kaum durch die Standardisierungsforschung abgedeckt. Daher basiert der Artikel auf fünf Forschungszielen:

1. Aufzeigen, welche Security-Lösungen besondere ethische oder privacy-bezogene Risiken bergen
2. Aufzeigen eines Rankings anhand ihrer Risikopotenziale
3. Aufzeigen spezifischer ethischer und privacy-bezogener Risiken
4. Anzeigen von Normungsbedarfen
5. Ableitung von Implikationen für die Normungsforschung.

Die Ergebnisse werden auf Grundlage einer Umfrage unter deutschen Sicherheitsexperten erarbeitet. Der Artikel schließt mit Empfehlungen für neue Privacy- und Datenschutzstandards, die dazu beitragen können, die Akzeptanz für ausgewählte neue Security-Lösungen zu erhöhen sowie mit Anwendungen für drei Propositionen, die von dem Forscher van de Kaa formuliert wurden.

19. Schlagwörter Privacy, Standards, Security-Technologien, öffentliche Sicherheit, kritische Infrastrukturen	
20. Verlag Verlagshaus Mainz GmbH Aachen	21. Preis ---

Document Control Sheet 4

1. ISBN or ISSN ISBN: 978-3-86130-655-9	2. type of document (e.g. report, publication) publication
3. title Ethical and Privacy-Specific Risks – Flaws of Critical Infrastructure Protection and Solutions Offered by Standardisation	
4. author(s) (family name, first name(s)) Wurster, Simone	5. end of project 28 February 2013
	6. publication date 24.06.2013
	7. form of publication Conference proceedings
8. performing organization(s) (name, address) Technische Universität Berlin Institut für Technologie und Management FG Innovationsökonomie - VWS 2 Müller-Breslau-Straße 15 10623 Berlin	9. originator's report no.
	10. reference no. 13N10915
	11. no. of pages 15
12. sponsoring agency (name, address) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	13. no. of references 27
	14. no. of tables 4
	15. no. of figures 3
16. supplementary notes	
17. presented at (title, place, date) Proceedings of the 18th EURAS Conference - Standards and Innovation-, Brussels, 413-427.	

18. abstract

Well-known scholars show the contribution of standards to raise the acceptance of innovative solutions and to accelerate the diffusion of innovations. This paper deals with the topic in the civil security field. The global intensity and frequency of criminal and terrorist incidents show the vulnerability of democratic societies and the need for protecting so-called critical infrastructures (CIs) in particular. Many technological security solutions to protect CIs are being developed or are already available. However, these solutions may bear ethical and privacy-related risks which can impede their acceptance. Specific privacy standards may offer solutions. The Dutch researchers Fens and van de Kaa proposed a paradigm shift in standardization strategies and research and the use of ethical aspects as an additional factor to explain standardization success. This paper goes one step further. It focuses on specific ethical and privacy standards and introduces privacy as a new dimension of the interplay between standards and innovation in the civil security field. So far, privacy issues of civil security technologies and CI protection are barely covered by standardization research. Therefore, this paper has five research objectives:

1. Showing, what security-related technology solutions bear special ethical or privacy-specific risks
2. Showing a ranking of their risk potential
3. Showing specific ethical and privacy risks
4. Showing needs for standards
5. Linking the findings with the state of the art in research and deriving implications for research.

In order to integrate ethical aspects in standardization research, van de Kaa (2013) introduced the value sensitive design concept. This paper identifies security technologies as a specific application field of this concept and privacy issues as specific aspects of value sensitive design. Based on a survey among German security researchers, it deals with the topic from mainly German and European perspectives. It finishes by giving recommendations for new privacy standards which may help to raise acceptance for several new security solutions and by showing applications of three propositions which the researcher van de Kaa has formulated.

19. keywords
Privacy, standards, security technology, public security, critical infrastructures

20. publisher Verlagshaus Mainz GmbH Aachen	21. price ---

Berichtsblatt 5

1. ISBN oder ISSN ---	2. Berichtsart (Schlussbericht oder Veröffentlichung) Veröffentlichung
3. Titel Security Technologies for the Protection of Critical Infrastructures – Ethical Risks and Solutions offered by Standardization	
4. Autor(en) [Name(n), Vorname(n)] Wurster, Simone	5. Abschlussdatum des Vorhabens 28.02.2013
	6. Veröffentlichungsdatum 24.04.2013
	7. Form der Publikation Buchkapitel
8. Durchführende Institution(en) (Name, Adresse) Technische Universität Berlin Institut für Technologie und Management FG Innovationsökonomie - VWS 2 Müller-Breslau-Straße 15 10623 Berlin	9. Ber. Nr. Durchführende Institution
	10. Förderkennzeichen 13N10915
	11. Seitenzahl 10
12. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	13. Literaturangaben 21
	14. Tabellen 2
	15. Abbildungen 3
16. Zusätzliche Angaben	
17. Vorgelegt bei (Titel, Ort, Datum) International Telecommunication Union: Proceedings of the 2013 ITU Kaleidoscope Academic Conference Building Sustainable Communities, Kyoto, Japan, 22. - 24. April 2013	
18. Kurzfassung Der Mehrwert von Normen und Standards wird in zahlreichen wissenschaftlichen Artikeln angezeigt. Mehrere aktuelle Studien heben dabei konkret den Bedarf nach security-bezogenen Normen und Standards hervor. Security-Produkte und Dienstleistungen können Ethik- und Datenschutz-Risiken bergen, welche die Akzeptanz neuer Security-Lösungen behindern können. Spezielle Standards können helfen, diese Probleme zu überwinden, aber Fragen der Privatsphäre von Sicherheitstechnologien werden derzeit nicht in der Standardisierungsforschung thematisiert. Der vorliegende Artikel befasst sich mit dem Thema aus hauptsächlich deutschen und europäischen Perspektiven. Basierend auf einer Umfrage im deutschen Sicherheitsforschungsprogramm, gibt er einen Überblick über Security-Technologien, die spezifischen Risiken tragen und zeigt die Bedeutung der Risiken auf. Drei technologiebezogenen Kategorien wurden dabei identifiziert: Detektion mit Distanz, distanzlose Detektion und Datenverarbeitung. Relevante Risiken wurden beschrieben und diskutiert. Lösungen mittels Normung und Standardisierung wurden aufgezeigt. Der Artikel endet mit Empfehlungen für neue Privacy-Normen und Standards.	
19. Schlagwörter Privacy, Standards, öffentliche Sicherheit, kritische Infrastrukturen, Überwachungstechnologien, Datenverarbeitung	
20. Verlag ---	21. Preis ---

Document Control Sheet 5

1. ISBN or ISSN ---	2. type of document (e.g. report, publication) publication
3. title Security Technologies for the Protection of Critical Infrastructures – Ethical Risks and Solutions offered by Standardization	
4. author(s) (family name, first name(s)) Wurster, Simone	5. end of project 28 February 2013
	6. publication date April 2013
	7. form of publication Book chapter
8. performing organization(s) (name, address) Technische Universität Berlin Institut für Technologie und Management FG Innovationsökonomie - VWS 2 Müller-Breslau-Straße 15 10623 Berlin	9. originator's report no.
	10. reference no. 13N10915
	11. no. of pages 10
12. sponsoring agency (name, address) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	13. no. of references 21
	14. no. of tables 2
	15. no. of figures 3
16. supplementary notes	
17. presented at (title, place, date) International Telecommunication Union: Proceedings of the 2013 ITU Kaleidoscope Academic Conference Building Sustainable Communities, Kyoto, Japan, 22 - 24 April 2013	
18. abstract The added value of standards is shown in numerous research articles. Several recent studies also highlight the need for security standards. Security products and services may bear ethical and privacy-related risks which can impede acceptance of new security solutions. Specific privacy standards may help to overcome such problems, but privacy issues of security technologies are not covered by standardization research so far. This paper deals with the topic from mainly German and European perspectives. Based on a survey in the German security research program, it gives an overview of security technologies, the specific risks they bear and their importance. Three technology-related categories were identified: surveillance solutions for detection from distance, solutions for obtrusive detection and data processing. Relevant risks were described and discussed. Solutions based on standardization were shown. The paper finishes by giving recommendations for new privacy standards.	
19. keywords Privacy, standards, public security, critical infrastructures, surveillance technologies, data processing	
20. publisher ---	21. price ---

Berichtsblatt 6

1. ISBN oder ISSN ISSN 0722-2912	2. Berichtsart (Schlussbericht oder Veröffentlichung) Veröffentlichung
3. Titel Security-Technologien zum Schutz kritischer Infrastrukturen – ethische Risiken und Lösungen mittels Normung und Standardisierung	
4. Autor(en) [Name(n), Vorname(n)] Wurster, Simone	5. Abschlussdatum des Vorhabens 28.02.2013
	6. Veröffentlichungsdatum März 2013
	7. Form der Publikation Artikel in Fachzeitschrift
8. Durchführende Institution(en) (Name, Adresse) Technische Universität Berlin Institut für Technologie und Management FG Innovationsökonomie - VWS 2 Müller-Breslau-Straße 15 10623 Berlin	9. Ber. Nr. Durchführende Institution
	10. Förderkennzeichen 13N10915
	11. Seitenzahl 1
12. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	13. Literaturangaben 7
	14. Tabellen 0
	15. Abbildungen 0
16. Zusätzliche Angaben	
17. Vorgelegt bei (Titel, Ort, Datum) DIN Mitteilungen, Berlin, 2013/3	

18. Kurzfassung

Die weltweite Intensität und Häufigkeit von Sicherheitsbedrohungen seit der Jahrtausendwende zeigen die Verletzlichkeit demokratischer Gesellschaften und den Schutzbedarf kritischer Infrastrukturen. Privacy-Aspekte können die Akzeptanz neuer Sicherheitslösungen erschweren. Dem gegenüber bieten spezielle privacy-bezogene Normen und Standards Chancen zur Überwindung derartiger Probleme. Hierbei existieren mehrere Lücken. Im Projekt InfraNorm ist die Entwicklung eines Normungshandbuchs für alle Teilnehmer des deutschen Sicherheitsforschungsprogramms vorgesehen. Zur Vertiefung ethischer und privacy-bezogener Aspekte wurde eine Vorstudie erstellt. Im Ergebnis wurden drei Sicherheitsgebiete mit ethischen Problemen ermittelt: Detektion mit Distanz, distanzlose Detektion und Datenverarbeitung. Konkret waren drei konkrete Gruppen ethischer Risiken relevant: Freiheitseinschränkung durch Sicherheitsziele, Missbrauch und Diskriminierung. Auf dieser Grundlage zeigte sich ein Normungs- und Standardisierungsbedarf in den Bereichen Datenspeicherung, Videoüberwachung, Biometrie, Zugangskontrollen, Sensorik sowie Sicherheitsdienstleistungen. Dem geäußerten Bedarf wurden existierende Normen, Standards und weitere relevante Dokumente gegenübergestellt. Auf dieser Basis verblieben fünf Themen, die konkret einen Normungs- oder Standardisierungsbedarf implizieren:

- Zu speichernde Daten für Sicherheitszwecke und Speicherperioden
- Konkrete Definition von Speicherperioden für Videodaten
- Datenmatching im Kontext der öffentlichen Sicherheit
- Nutzung biometrischer Daten im Kontext der zivilen Sicherheit, v.a. im Bereich Datenmatching
- Ethische Aspekte beim Einsatz von Security-Sensorik.

Normungsarbeiten der interessierten Kreise zu diesen Themen könnte die stärkere Akzeptanz der betreffenden Security-Technologien fördern.

19. Schlagwörter
Privacy, Standards, öffentliche Sicherheit, Überwachungstechnologien, Datenverarbeitung

20. Verlag Beuth Verlag	21. Preis 42,-- €

Document Control Sheet 6

1. ISBN or ISSN ISSN 0722-2912	2. type of document (e.g. report, publication) publication
3. title Security Technologies for the Protection of Critical Infrastructures – Ethical Risks and Solutions offered by Standardization	
4. author(s) (family name, first name(s)) Wurster, Simone	5. end of project 28 February 2013
	6. publication date March 2012
	7. form of publication Journal article
8. performing organization(s) (name, address) Technische Universität Berlin Institut für Technologie und Management FG Innovationsökonomie - VWS 2 Müller-Breslau-Straße 15 10623 Berlin	9. originator's report no.
	10. reference no. 13N10915
	11. no. of pages 1
12. sponsoring agency (name, address) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	13. no. of references 7
	14. no. of tables 0
	15. no. of figures 0
16. supplementary notes	
17. presented at (title, place, date) DIN Mitteilungen, Berlin, 2013/3	

18. abstract

The global intensity and frequency of criminal and terrorist attacks since the turn of the century has shown the vulnerability of democratic societies and the need for protecting so-called critical infrastructures in particular. Security products and services may bear ethical and privacy-related risks which can impede acceptance of new security solutions. Specific privacy standards may help to overcome such problems, but privacy issues of security technologies are not covered by standardization research so far. The project InfraNorm aims to develop a standardization manual for the participants of the German Framework Programme "Research for Civil Security". In order to gain a deeper insight into ethical and privacy-related problems of security technologies and to identify possible solutions, a study among German security researchers was done. Three technology-related areas with ethical risks were identified: surveillance solutions for detection from distance, solutions for obtrusive detection and data processing. Furthermore, specific ethical and privacy risks were analyzed. Three groups of problems became apparent: restrictions to freedom, abuse and discrimination. Furthermore, the questionnaire addressed specific technologies, products and solutions and related standardization needs to reduce ethical risks. Based on the answers, six technology fields were identified: security services, data storage, video surveillance, biometrics, access control and sensors. Database and document analyses were done to compare the needs with existing standards and other relevant documents. In summary, five new working items for new standards were suggested:

- General definition of the kind of data stored for security reasons and of specific storage periods when there is no specific suspicion
- Matching of data
- Use of biometric data in the context of public security
- Ethical standards for sensors
- General requirements for the processing of video data, the storage period and the deletion when there is no specific suspicion.

Volunteers are needed to start new standardization projects in order to realize these goals.

19. keywords

Privacy, standards, public security, critical infrastructures, surveillance technologies, data processing

20. publisher Beuth Verlag	21. price € 42,--

Berichtsblatt 7

1. ISBN oder ISSN ISSN: 1539-3062	2. Berichtsart (Schlussbericht oder Veröffentlichung) Veröffentlichung
3. Titel Development of a Specification for Data Interchange Between Information Systems in Civil Hazard Prevention. Identification of Success Factors, Challenges and Solutions Based on Case Study Research	
4. Autor(en) [Name(n), Vorname(n)] Wurster, Simone	5. Abschlussdatum des Vorhabens 28.02.2013
	6. Veröffentlichungsdatum Mai 2013
	7. Form der Publikation Artikel in Fachzeitschrift
8. Durchführende Institution(en) (Name, Adresse) Technische Universität Berlin Institut für Technologie und Management FG Innovationsökonomie - VWS 2 Müller-Breslau-Straße 15 10623 Berlin	9. Ber. Nr. Durchführende Institution
	10. Förderkennzeichen 13N10915
	11. Seitenzahl 21
12. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	13. Literaturangaben 53
	14. Tabellen 2
	15. Abbildungen 1
16. Zusätzliche Angaben	
17. Vorgelegt bei (Titel, Ort, Datum) The International Journal of IT Standards and Standardization Research (IJITSR), 11(1), Mai 2013	
18. Kurzfassung Normen und Standards zur Erhöhung der öffentlichen Sicherheit fehlen für viele technische Aspekte, Kommunikationsprotokolle sowie für das Sicherheitsmanagement. Dabei existieren mehrere Forschungslücken, insbesondere in Bezug auf die FuE-basierte Normung und Standardisierung. Der Stand der Forschung bietet ein Framework zur Untersuchung von Projektmanagementaspekten, die zu einer erfolgreichen IKT-Standardisierung führen. Seine Eignung für die FuE-basierte Standardisierung im Security-Kontext wurde geprüft und erwies sich vor allem durch eine aktuelle Umfrage des Projekts InfraNorm im deutschen Sicherheitsforschungsprogramm als gegeben. Das Projekt zielt darauf ab, die Entwicklung von Normen und Spezifikationen für den Schutz von Verkehrsinfrastrukturen einzuleiten. Dieser Artikel gibt einen Einblick in die Entwicklung einer solchen auf FuE-Ergebnissen basierenden Spezifikation. Neben der Darstellung praktischer Beispiele für die Betrachtungsdimensionen des analysierten Frameworks schlägt der Artikel eine Erweiterung der Dimensionen vor. Standardisierungsherausforderungen und Lösungen werden ebenfalls vorgestellt. Am Ende des Artikels werden die wesentlichen Aspekte umrissen, die die Adoption der Spezifikation beeinflussen können. Dabei wird ein kurzer Überblick über die aktuellen Ergebnisse gegeben. Anwendungsgebiete der Ergebnisse umfassen insbesondere so genannte Fast-Track-Verfahren der Standardisierung, Standardisierungsprozesse, deren Ergebnisimplementierung auf freiwilliger Basis erfolgt, die Standardisierung von FuE-Ergebnissen und Standardisierungsprojekte, die in kleinen Gruppen durchgeführt werden.	
19. Schlagwörter DIN SPECs / DIN Specifications, InfraNorm, Public Security, R&D Stage Security Standardisation, Standardisation	
20. Verlag IGI Global	21. Preis 37,50 $

Document Control Sheet 7

1. ISBN or ISSN ISSN: 1539-3062	2. type of document (e.g. report, publication) publication
3. title Development of a Specification for Data Interchange Between Information Systems in Civil Hazard Prevention. Identification of Success Factors, Challenges and Solutions Based on Case Study Research	
4. author(s) (family name, first name(s)) Wurster, Simone	5. end of project 28 February 2013
	6. publication date May 2013
	7. form of publication Journal article
8. performing organization(s) (name, address) Technische Universität Berlin Institut für Technologie und Management FG Innovationsökonomie - VWS 2 Müller-Breslau-Straße 15 10623 Berlin	9. originator's report no.
	10. reference no. 13N10915
	11. no. of pages 21
12. sponsoring agency (name, address) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	13. no. of references 53
	14. no. of tables 2
	15. no. of figures 1
16. supplementary notes	
17. presented at (title, place, date) The International Journal of IT Standards and Standardization Research (IJITSR), 11(1), May 2013	
18. abstract Standards and specifications for public security are missing in many technical aspects as well as the areas of communication protocols and security management. Several research gaps related to these fields exist, particularly regarding R&D stage standardisation. The state of the art in research offers a framework to investigate project management aspects leading to successful ICT standardisation. Its applicability for R&D stage security standardisation was examined and mainly proved by a recent InfraNorm survey in the German security research program. The German project InfraNorm aims at initiating the development of standards and specifications for the protection of transportation infrastructure. This article gives insight into the development of such a specification based on R&D results. Besides providing practical examples for activities related to the standardization framework, the article suggests its extension. Standardisation challenges and solutions are also unveiled. The article finishes by outlining key aspects which may influence the adoption of the specification and by giving a short overview of current results. Application fields of the findings include, in particular, fast track standardisation procedures with voluntary implementation of the results, standardisations of R&D results and standardisation projects from small groups.	
19. keywords DIN SPECs / DIN Specifications, InfraNorm, Public Security, R&D Stage Security Standardisation, Standardisation	
20. publisher IGI Global	21. price $ 37,50

Berichtsblatt 8

1. ISBN oder ISSN ISSN: 2251-3043, E-periodical: 2010-2283	2. Berichtsart (Schlussbericht oder Veröffentlichung) Veröffentlichung
3. Titel Development of a Specification for Computer-Based Microscopic Evacuation Analyses and Simulations - Identification of Success Factors Based on Case Study Research	
4. Autor(en) [Name(n), Vorname(n)] Wurster, Simone	5. Abschlussdatum des Vorhabens 28.02.2013
	6. Veröffentlichungsdatum Frühjahr 2013
	7. Form der Publikation Artikel in Fachzeitschrift
8. Durchführende Institution(en) (Name, Adresse) Technische Universität Berlin Institut für Technologie und Management FG Innovationsökonomie - VWS 2 Müller-Breslau-Straße 15 10623 Berlin	9. Ber. Nr. Durchführende Institution
	10. Förderkennzeichen 13N10915
	11. Seitenzahl 8
12. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	13. Literaturangaben 41
	14. Tabellen 2
	15. Abbildungen 0
16. Zusätzliche Angaben	
17. Vorgelegt bei (Titel, Ort, Datum) GSTF Journal on Computing (JoC) Vol 2 No 4	
18. Kurzfassung Die öffentliche Sicherheit wird ständig mit neuen Bedrohungen konfrontiert. Spezielle Standards fehlen für viele technische Aspekte und auch im Bereich des Sicherheitsmanagements. Es existieren mehrere Forschungslücken, insbesondere in Bezug auf Standardisierungsprozesse in FuE-Phasen von Technologien. Das deutsche Projekt InfraNorm bezweckt die Initiierung der Entwicklung von Sicherheitsnormen und -spezifikationen. Basierend auf Fallstudien und der Verwendung von Methoden der teilnehmenden Beobachtung, gibt dieses Papier einen Einblick in die forschungsbegleitende Entwicklung einer solchen Spezifikation im Bereich Security-Simulationen und Modellierungen und zeigt die Ausprägung neuer Erfolgsfaktoren. Die Identifikation der Erfolgsfaktoren basierte auf einer vorgelagerten Umfrage unter Sicherheitsexperten. Anwendungsgebiete der Ergebnisse umfassen insbesondere so genannte Fast-Track-Verfahren der Standardisierung, Standardisierungsprozesse, deren Ergebnisimplementierung auf freiwilliger Basis erfolgt, die Standardisierung von FuE-Ergebnissen und Standardisierungsprojekte, die in kleinen Gruppen durchgeführt werden.	
19. Schlagwörter Spezifikationen, Standards, zivile Sicherheit, Fallstudien, Simulation, Modellierung	
20. Verlag ---	21. Preis ---

Document Control Sheet 8

1. ISBN or ISSN Print ISSN: 2251-3043, E-periodical: 2010-2283	2. type of document (e.g. report, publication) publication
3. title Development of a Specification for Computer-Based Microscopic Evacuation Analyses and Simulations - Identification of Success Factors Based on Case Study Research	
4. author(s) (family name, first name(s)) Wurster, Simone	5. end of project 28 February 2013
	6. publication date Spring 2013
	7. form of publication Journal article
8. performing organization(s) (name, address) Technische Universität Berlin Institut für Technologie und Management FG Innovationsökonomie - VWS 2 Müller-Breslau-Straße 15 10623 Berlin	9. originator's report no.
	10. reference no. 13N10915
	11. no. of pages 8
12. sponsoring agency (name, address) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	13. no. of references 41
	14. no. of tables 2
	15. no. of figures 0
16. supplementary notes -	
17. presented at (title, place, date) GSTF Journal on Computing (JoC) Vol 2 No 4	
18. abstract Public security is constantly tested by new threats. Standards for public security are missing in many technical aspects as well as the area of security management. Several research gaps related to these fields exist, particularly regarding R&D stage standardization. The German project InfraNorm aims to initiate the development of security standards and specifications. By using case study and participant observation methodologies, this paper gives insight into the development of such a specification for simulation and modeling based on R&D stage standardization and unveils new success factors. The identification of success factors is based on a preliminary survey among security researchers which determined potential problems they should solve. Application fields of the findings include, in particular, fast track standardization procedures with voluntary implementation of the results, standardizations of R&D results and standardization projects from small groups.	
19. keywords specifications, standards, civil security, case studies, simulation, modeling	
20. publisher ---	21. price ---

Berichtsblatt 9

1. ISBN oder ISSN ISSN 1865-0929 ISBN 978-3-642-33160-2 e-ISSN 1865-937 e-ISBN 978-3-642-33161-9	2. Berichtsart (Schlussbericht oder Veröffentlichung) Veröffentlichung
3. Titel Standards for the Protection of Transport Infrastructures	
4. Autor(en) [Name(n), Vorname(n)] Siegel, Norbert Wurster, Simone	5. Abschlussdatum des Vorhabens 28.02.2013 6. Veröffentlichungsdatum 4. September 2012 7. Form der Publikation Konferenz-Proceedings
8. Durchführende Institution(en) (Name, Adresse) DIN Deutsches Institut für Normung e. V. Am DIN-Platz Burggrafenstraße 6 10787 Berlin Technische Universität Berlin Institut für Technologie und Management FG Innovationsökonomie - VWS 2 Müller-Breslau-Straße 15 10623 Berlin	9. Ber. Nr. Durchführende Institution 10. Förderkennzeichen 13N10915 11. Seitenzahl 4
12. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	13. Literaturangaben 1 14. Tabellen 0 15. Abbildungen 0
16. Zusätzliche Angaben	
17. Vorgelegt bei (Titel, Ort, Datum) In: Aschenbruck, N., Martini, P., Meier, M., Tölle, J. [Hrsg.] (2012). Communication in Computer and Information Science 318. Future Security. 7th Security Research Conference, Future Security 2012, Bonn, September 2012, Proceedings. Heidelberg, Dordrecht, London, New York, Springer, 21-24.	
18. Kurzfassung Standards und Spezifikationen sind wichtige Instrumente für die Erschließung neuer Märkte. Ferner unterstützt die Standardisierung in einem frühen Stadium die Entwicklung von neuen Produkten und Dienstleistungen, weil sie die Kommunikation zwischen den verschiedenen Entwicklern durch Bereitstellung standardisierter Schnittstellen oder einheitlichen Terminologien verbessert. Das gemeinsame Projekt INFRANORM des Deutschen Instituts für Normung (DIN) und der Technischen Universität Berlin (TU Berlin) hilft bei der Entwicklung von Standards für den Schutz von Verkehrsinfrastrukturen, einem Bereich, in dem Normen und Spezifikationen derzeit fehlen. Mehrere DIN Spezifikationen zu diesem Thema sind ausgearbeitet und publiziert oder stehen kurz vor der Veröffentlichung. Der Artikel gibt hierzu einen Überblick.	
19. Schlagwörter Standardisierung, DIN Spezifikationen, Verkehrsinfrastrukturen	
20. Verlag Springer	21. Preis 85,60 € / 67,82 €

Document Control Sheet 9

1. ISBN or ISSN ISSN 1865-0929 ISBN 978-3-642-33160-2 e-ISSN 1865-937 e-ISBN 978-3-642-33161-9	2. type of document (e.g. report, publication) publication
3. title Standards for the Protection of Transport Infrastructures	
4. author(s) (family name, first name(s)) Siegel, Norbert Wurster, Simone	5. end of project 28 February 2013
	6. publication date 4 September 2012
	7. form of publication Conference proceedings
8. performing organization(s) (name, address) DIN Deutsches Institut für Normung e. V. Am DIN-Platz Burggrafenstraße 6 10787 Berlin Technische Universität Berlin Institut für Technologie und Management FG Innovationsökonomie - VWS 2 Müller-Breslau-Straße 15 10623 Berlin	9. originator's report no.
	10. reference no. 13N10915
	11. no. of pages 4
12. sponsoring agency (name, address) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	13. no. of references 1
	14. no. of tables 0
	15. no. of figures 0
16. supplementary notes	
17. presented at (title, place, date) In: Aschenbruck, N., Martini, P., Meier, M., Tölle, J. [Hrsg.] (2012). Communication in Computer and Information Science 318. Future Security. 7th Security Research Conference, Future Security 2012, Bonn, September 2012, Proceedings. Heidelberg, Dordrecht, London, New York, Springer, 21-24.	
18. abstract Standards and specifications are important instruments for opening up new markets. Furthermore, standardization at an early R&D stage supports the development of new products and services because it improves the communication between the various developers by providing standardized interfaces or unified terminologies. The joint project "INFRANORM" of DIN, the German Institute for Standardization and the Berlin University of Technology (TU Berlin) helps to initiate standardization projects for the protection of transport infrastructures, an area in which standards and specifications are currently lacking. Several security-related DIN Specifications (DIN SPECs) were developed or will be published soon. The article provides an overview.	
19. keywords Standardization, DIN Specifications, transport infrastructures	
20. publisher Springer	21. price € 85,60 / 67,82

Berichtsblatt 10

1. ISBN oder ISSN ISSN: 2251-2136	2. Berichtsart (Schlussbericht oder Veröffentlichung) Veröffentlichung
3. Titel Example of Good Practice in R&D Stage Standardization in Germany: Development of a Specification for Data Interchange Between Information Systems in Civil Hazard Prevention	
4. Autor(en) [Name(n), Vorname(n)] Wurster, Simone	5. Abschlussdatum des Vorhabens 28.02.2013
	6. Veröffentlichungsdatum September 2012
	7. Form der Publikation Konferenz-Proceedings
8. Durchführende Institution(en) (Name, Adresse) Technische Universität Berlin Institut für Technologie und Management FG Innovationsökonomie - VWS 2 Müller-Breslau-Straße 15 10623 Berlin	9. Ber. Nr. Durchführende Institution
	10. Förderkennzeichen 13N10915
	11. Seitenzahl 8
12. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	13. Literaturangaben 37
	14. Tabellen 3
	15. Abbildungen 0
16. Zusätzliche Angaben	
17. Vorgelegt bei (Titel, Ort, Datum) 3rd Annual International Conference on Infocomm Technologies in Competitive Strategies (ICT 2012) and Advances in Distributed and Parallel Computing (ADPC 2012), 7-14.	
18. Kurzfassung Standards und Spezifikationen für die öffentliche Sicherheit fehlen in vielen technischen Bereichen, für Kommunikationsprotokolle sowie für das Sicherheitsmanagement. Das deutsche Projekt InfraNorm zielt darauf ab, die Entwicklung von Normen und Spezifikationen für den Schutz von Verkehrsinfrastrukturen einzuleiten. Dieser Beitrag gibt einen Einblick in die Entwicklung einer solchen Spezifikation und zeigt neue Erfolgsfaktoren.	
19. Schlagwörter Spezifikationen, Standards, zivile Sicherheit, Datenaustausch	
20. Verlag Global Science and Technology Forum (GSTF)	21. Preis ---

Document Control Sheet 10

1. ISBN or ISSN ISSN: 2251-2136	2. type of document (e.g. report, publication) publication
3. title Example of Good Practice in R&D Stage Standardization in Germany: Development of a Specification for Data Interchange Between Information Systems in Civil Hazard Prevention	
4. author(s) (family name, first name(s)) Wurster, Simone	5. end of project 28 February 2013
	6. publication date September 2012
	7. form of publication Conference proceedings
8. performing organization(s) (name, address) Technische Universität Berlin Institut für Technologie und Management FG Innovationsökonomie - VWS 2 Müller-Breslau-Straße 15 10623 Berlin	9. originator's report no.
	10. reference no. 13N10915
	11. no. of pages 8
12. sponsoring agency (name, address) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	13. no. of references 37
	14. no. of tables 3
	15. no. of figures 0
16. supplementary notes	
17. presented at (title, place, date) 3rd Annual International Conference on Infocomm Technologies in Competitive Strategies (ICT 2012) and Advances in Distributed and Parallel Computing (ADPC 2012), 7-14.	
18. abstract Standards and specifications for public security are missing in many technical aspects as well as the areas of communication protocols and security management. The German project InfraNorm aims at initiating the development of standards and specifications for the protection of transportation infrastructure. This paper gives insight into the development of such a specification and unveils new success factors.	
19. keywords specifications, standards, civil security, data interchange	
20. publisher Global Science and Technology Forum (GSTF)	21. price ---

Berichtsblatt 11

1. ISBN oder ISSN ISBN 978-3-86130-337-4	2. Berichtsart (Schlussbericht oder Veröffentlichung) Veröffentlichung
3. Titel Development of a Specification for Data Interchange Between Information Systems in Civil Hazard Prevention. Identification of Success Factors, Challenges and Solutions Based on Case Study Research and Participant Observation	
4. Autor(en) [Name(n), Vorname(n)] Wurster, Simone	5. Abschlussdatum des Vorhabens 28.02.2013
	6. Veröffentlichungsdatum Juni 212
	7. Form der Publikation Konferenz-Proceedings
8. Durchführende Institution(en) (Name, Adresse) Technische Universität Berlin Institut für Technologie und Management FG Innovationsökonomie - VWS 2 Müller-Breslau-Straße 15 10623 Berlin	9. Ber. Nr. Durchführende Institution
	10. Förderkennzeichen 13N10915
	11. Seitenzahl 20
12. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	13. Literaturangaben 66
	14. Tabellen 4
	15. Abbildungen 0
16. Zusätzliche Angaben	
17. Vorgelegt bei (Titel, Ort, Datum) Proceedings of the 17th EURAS Annual Standardization Conference - Standards and Innovation-, 397-416, Kosice 2012.	
18. Kurzfassung Innovationen für den Schutz kritischer Infrastrukturen sind von großer Bedeutung. Standards und Spezifikationen fehlen jedoch in vielen Bereichen. Das Ziel des Projekts InfraNorm ist es, die Entwicklung von Standards und Spezifikationen für den Schutz von Verkehrsinfrastrukturen zu initiieren. Dieser Beitrag gibt einen Einblick in die Entwicklung einer solchen Spezifikation und zeigt neue Erfolgsfaktoren, Herausforderungen und Lösungen. Darüber hinaus erörtert er wichtige Aspekte, die die Adoption der Spezifikation beeinflussen können.	
19. Schlagwörter Spezifikationen, Standards, zivile Sicherheit, Datenaustausch	
20. Verlag Verlagshaus Mainz GmbH Aachen	21. Preis ---

Document Control Sheet 11

1. ISBN or ISSN ISBN 978-3-86130-337-4	2. type of document (e.g. report, publication) publication
3. title Development of a Specification for Data Interchange Between Information Systems in Civil Hazard Prevention. Identification of Success Factors, Challenges and Solutions Based on Case Study Research and Participant Observation	
4. author(s) (family name, first name(s)) Wurster, Simone	5. end of project 28 February 2013
	6. publication date June 212
	7. form of publication Conference proceedings
8. performing organization(s) (name, address) Technische Universität Berlin Institut für Technologie und Management FG Innovationsökonomie - VWS 2 Müller-Breslau-Straße 15 10623 Berlin	9. originator's report no.
	10. reference no. 13N10915
	11. no. of pages 20
12. sponsoring agency (name, address) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	13. no. of references 66
	14. no. of tables 4
	15. no. of figures 0
16. supplementary notes	
17. presented at (title, place, date) Proceedings of the 17th EURAS Annual Standardization Conference - Standards and Innovation-, 397-416, Kosice 2012.	
18. abstract Innovations for the protection of critical infrastructure are of great importance. Standards and specifications are missing in technical aspects and the areas of communication protocols and security management. The goal of the project InfraNorm is to initiate the development of standards and specifications for the protection of transportation infrastructure. This paper gives insight into the development of such a specification and unveils new success factors, challenges and solutions. It also outlines key aspects, which may influence the adoption of the specification.	
19. keywords specifications, standards, civil security, data interchange	
20. publisher Verlagshaus Mainz GmbH Aachen	21. price ---

Berichtsblatt 12

1. ISBN oder ISSN ISSN 0722-2912	2. Berichtsart (Schlussbericht oder Veröffentlichung) Veröffentlichung
3. Titel Bedeutung von Sicherheitsnormen, -standards und -spezifikationen. Ergebnisse einer Studie in der deutschen Sicherheitsforschung	
4. Autor(en) [Name(n), Vorname(n)] Wurster, Simone	5. Abschlussdatum des Vorhabens 28.02.2013
	6. Veröffentlichungsdatum Juni 2012
	7. Form der Publikation Beitrag in Fachzeitschrift
8. Durchführende Institution(en) (Name, Adresse) Technische Universität Berlin Institut für Technologie und Management FG Innovationsökonomie - VWS 2 Müller-Breslau-Straße 15 10623 Berlin	9. Ber. Nr. Durchführende Institution
	10. Förderkennzeichen 13N10915
	11. Seitenzahl 5
12. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	13. Literaturangaben 2
	14. Tabellen 0
	15. Abbildungen 5
16. Zusätzliche Angaben	
17. Vorgelegt bei (Titel, Ort, Datum) DIN Mitteilungen, Berlin, Juni 2012	

18. Kurzfassung

Der vorliegende Artikel basiert auf einer Umfrage im deutschen Sicherheitsforschungsprogramm. Ihr Ziel bestand darin, anhand von 14 Fragen Informationen für die Erstellung des Normungshandbuchs im Projekt InfraNorm zu gewinnen.

Die Umfrage zeigte, dass bisher nur wenige Schnittstellen zwischen den FuE-Aktivitäten im Sicherheitsforschungsprogramm und der deutschen, europäischen und internationalen Normung existieren. Um eine stärkere Interrelation zu ermöglichen, werden spezielle Normungs- und Standardisierungsthemen im Handbuch aufgegriffen.

Bei der Beantwortung der weiteren Fragen wurde u.a. die Bedeutung ethischer Aspekte bei der Entwicklung von Sicherheitsnormen, -spezifikationen und -standards erörtert. Zudem wurden Konfliktrisiken bei der Normung und Standardisierung aufgezeigt. Als besonders bedeutsam wurden dabei die Themen Identifikation gemeinsamer Mehrwerte, Konsensfindung, Intellectual Property Rights, organisatorische Probleme und Verzögerungen, Spezialthemen im internationalen Kontext sowie Widerstände der Anwender/Akzeptanzprobleme erachtet. Als bisher erlebte Konflikte wurden insbesondere zeitliche Probleme erörtert. Anhand der letzten Frage wurden sechs Vorschläge zur Reduktion von Konfliktrisiken in Normungs- und Standardisierungsprozessen abgeleitet: schnellere Verfahren, geeignetes Projektmanagement, breite Beteiligung, Leitmarktorientierung, Förderung internationaler Vorhaben und Schlichtungsmechanismen. Am Ende der Studie wird dargestellt, wie die Implikationen im Normungshandbuch umgesetzt werden sollen.

19. Schlagwörter Standards, Security-Technologien, öffentliche Sicherheit, kritische Infrastrukturen	
20. Verlag Beuth Verlag	21. Preis 42,-- €

Document Control Sheet 12

1. ISBN or ISSN ISSN 0722-2912	2. type of document (e.g. report, publication) publication
3. title Bedeutung von Sicherheitsnormen, -standards und -spezifikationen. Ergebnisse einer Studie in der deutschen Sicherheitsforschung	
4. author(s) (family name, first name(s)) Wurster, Simone	5. end of project 28 February 2013
	6. publication date June 212
	7. form of publication Technical article
8. performing organization(s) (name, address) Technische Universität Berlin Institut für Technologie und Management FG Innovationsökonomie - VWS 2 Müller-Breslau-Straße 15 10623 Berlin	9. originator's report no.
	10. reference no. 13N10915
	11. no. of pages
12. sponsoring agency (name, address) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	13. no. of references 2
	14. no. of tables 0
	15. no. of figures 5
16. supplementary notes	
17. presented at (title, place, date) DIN Mitteilungen, Berlin, June 2012	
18. abstract This article presents the results of a study in the German security research program. Its goal was to obtain information for the preparation of a standards manual in the project InfraNorm. Among other topics, the importance of ethical aspects in the development of security standards was discussed by the participants. Furthermore, risks of conflict in the standardization process were identified. The identification of common benefits, consensus building, Intellectual Property Rights, organizational problems and delays, special topics in the international context as well as resistors and problems to achieve acceptance were significant. Several proposals for reducing the risks of conflict in standardization processes were derived. At the end the study shows how the implications are to be implemented in the standardization manual.	
19. keywords Standards, security technology, public security, critical infrastructures	
20. publisher Beuth Verlag	21. price € 42,--

Berichtsblatt 13

1. ISBN oder ISSN ---	2. Berichtsart (Schlussbericht oder Veröffentlichung) Veröffentlichung
3. Titel Bedeutung von Sicherheitsnormen, -standards und -spezifikationen	
4. Autor(en) [Name(n), Vorname(n)] Wurster, Simone	5. Abschlussdatum des Vorhabens 28.02.2013
	6. Veröffentlichungsdatum Januar 2012
	7. Form der Publikation Report
8. Durchführende Institution(en) (Name, Adresse) Technische Universität Berlin Institut für Technologie und Management FG Innovationsökonomie - VWS 2 Müller-Breslau-Straße 15 10623 Berlin	9. Ber. Nr. Durchführende Institution
	10. Förderkennzeichen 13N10915
	11. Seitenzahl 45
12. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	13. Literaturangaben 14
	14. Tabellen 25 Tabellen und Abbildungen
	15. Abbildungen Siehe 14.
16. Zusätzliche Angaben	
17. Vorgelegt bei (Titel, Ort, Datum) Abteilung EINS – Sicherheitsforschung, Projektträger des BMBF, VDI Technologiezentrum GmbH VDI-Platz 1, 40468 Düsseldorf	

18. Kurzfassung

Das Projekt InfraNorm befasst sich mit dem Bedarf an Security-Normen und Standards. Ein spezielles Arbeitspaket bezweckt die Entwicklung eines Normungshandbuchs für Sicherheitsforscher. Im Frühjahr 2011 wurde eine Umfrage zu security-bezogenen Normen, Spezifikationen und Standards unter deutschen Sicherheitsforschern durchgeführt. Als Grundlage der Studie diente ein Fragebogen mit 14 Fragen in acht Themenbereichen.

Ein spezielles Anliegen der Umfrage bestand darin, wahrgenommene Risiken bei der security-spezifischen Normung und Standardisierung aufzudecken. Daher wurden die Teilnehmer gebeten, ihre Risikowahrnehmung darzustellen. Es wurden sieben Themenfelder identifiziert: Missbrauch, Föderalismus, Fehlentwicklungen, Pseudosicherheit, Ethische Fragen, Leitmarktrisiken sowie Allgemeine Risiken. In einer weiteren Frage wurden Konflikte in der Normung und Standardisierung thematisiert. Ausgehend von den typischen Phasen von Normungs- und Standardisierungsprozessen wird der Phase 2, und damit der „Entwicklung“ das größte Konfliktpotential beigemessen. Es folgen die „Initiierung des Vorhabens“ (Phase 1), die Phase „Überarbeitung“ (5) sowie die „Anwendung“ (Phase 4). Die Phase der „Veröffentlichung“ (3) wird mit dem geringsten Konfliktpotential verbunden. In bisherigen Forschungsarbeiten wird bei der Betrachtung von Normungs- und Standardisierungskonflikten bereits ein initiiertes Projekt vorausgesetzt. Die Befragungsergebnisse erweitern hier den Fokus und decken zusätzliche Probleme auf, die für die grundsätzliche Durchführung von Normungs- und Standardisierungsprojekten kritisch sind. Ausgehend von den zuvor dargestellten Ergebnissen thematisierte eine weitere Frage Konfliktrisiken in der Phase mit dem größten Konfliktpotential. Aus den Aussagen wurden acht Konfliktgruppen abgeleitet. Unwissenheit über bestehende Normen, Identifikation gemeinsamer Mehrwerte, Interessenkonflikte/Konsensfindung, Organisatorische Probleme und Verzögerungen, Intellectual Property Rights, Spezialaspekte im internationalen Kontext, Widerstände der Anwender/Akzeptanzprobleme und spezifische Standardisierungsaspekte beim Schutz vor CBRNE.

Für die Erstellung des Normungshandbuchs wurden aus der Befragung umfangreiche Anforderungen abgeleitet:

- Ein Großteil der involvierten Personen ist ihren statistischen Angaben zufolge a) in **öffentlichen Forschungseinrichtungen oder Hochschulen** oder b) **in kleinen und mittelgroßen Unternehmen (KMU)** tätig. Für beide Zielgruppen sollten neben allgemeinen Hinweisen **spezifische Empfehlungen** entwickelt werden.
- Die Ergebnisse zu Frage 1 wiesen auf die besondere Bedeutung von **security-bezogenen Schnittstellenstandards und Terminologien** hin. Dies sollte durch zwei entsprechende **Fallstudien** sowie einen Strategiekatalog für die Entwicklung von Schnittstellen berücksichtigt werden.
- Frage 2 zeigte u.a. die **Bedeutung von security-bezogenen Patenten**, Schutzmarken und Copyrights. Der Normungskontext setzt hier spezielle Rahmenbedingungen, die in dem Handbuch aufgegriffen werden sollten.
- Die Ergebnisse zu den Fragen 3 bis 6 verdeutlichen den **allgemeinen Bedarf** für das Normungshandbuch, da die Mehrheit der Teilnehmer kaum über eigene Erfahrungen verfügt. Die geplanten Hilfestellungen umfassten daher z.B. die Erörterung der Arbeit und der Dokumentenarten wichtiger Normungsorganisationen sowie Empfehlungen zur Durchführung von Normenrecherchen.
- Frage 7 reflektierte die Normungsmotive der Teilnehmer. Das Handbuch sollte Hinweise für eine erfolgreiche Umsetzung ausgewählter Motive geben.
- In Frage 8 wurde insbesondere der **Zeit- und Kostenaufwand** als Normungsbarriere identifiziert. Lösungsmöglichkeiten sollten u.a. auf Grundlage von Fallstudien aufgezeigt werden.
- Bei der Beantwortung von Frage 9 wurden spezielle **ethische und privacy-bezogene Probleme** erörtert. Im Handbuch wurden hierfür zwei spezielle Kapitel vorgesehen.
- Laut Frage 10 und 11 bergen die Phasen der **Initiierung, der Entwicklung und der Überarbeitung** der geschaffenen Regelwerke die größten Konfliktpotentiale. Auf Grundlage von Fallstudien sollten spezielle Empfehlungen für diese Phasen erarbeitet werden.
- Vielfältige Konfliktrisiken wurden anhand der letzten Gruppe von Fragen aufgezeigt. Zur Erörterung von Lösungen im Normungshandbuch wurden vor allem die folgenden Probleme ausgewählt: organisatorische Probleme durch geeignete Gremienbildung, Ermittlung bestehender Normen durch Normrecherchen, Verhandlungsstrategien, Intellectual Property Rights sowie Steigerung der Akzeptanz der erarbeiteten Regelwerke.

19. Schlagwörter
Standards, Security-Technologien, öffentliche Sicherheit, kritische Infrastrukturen

20. Verlag	21. Preis
---	---

Document Control Sheet 13

1. ISBN or ISSN ---	2. type of document (e.g. report, publication) publication
3. title Bedeutung von Sicherheitsnormen, -standards und -spezifikationen	
4. author(s) (family name, first name(s)) Wurster, Simone	5. end of project 28 February 2013
	6. publication date January 2012
	7. form of publication report
8. performing organization(s) (name, address) Technische Universität Berlin Institut für Technologie und Management FG Innovationsökonomie - VWS 2 Müller-Breslau-Straße 15 10623 Berlin	9. originator's report no.
	10. reference no. 13N10915
	11. no. of pages 45
12. sponsoring agency (name, address) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	13. no. of references 14
	14. no. of tables 25 tables and figures
	15. no. of figures See 14.
16. supplementary notes	
17. presented at (title, place, date) Abteilung EINS – Sicherheitsforschung, Projektträger des Bundesministeriums für Bildung und Forschung VDI Technologiezentrum GmbH, VDI-Platz 1, 40468 Düsseldorf	

18. abstract

The project InfraNorm addresses the need for security-related standards. A specific work package aims to develop a standardization manual for the participants of the German framework programme "Research for Civil Security". To determine the standardization-related prerequisites of the security researchers, but also perceived risks, they were asked to participate in a survey. For this purpose, a questionnaire with 14 questions in eight topic areas was used.

In summary, the survey unveiled that there are few interfaces between research and standardization in the security research program so far. The results related to question 1 show the importance of security-related interface standards and terminologies. Therefore, it is suggested to give specific advice for the development of such security standards. The results of question 2 show the importance of security-related patents, trademarks and copyrights. The standardization context sets specific conditions and requires recommendations. Participants were also asked about their opinion, what barriers prevent participation in the security-related standards from their point of view. They were asked to rate the importance of eleven barriers. The three most significant barriers include the use of other forms of exploitation of R&D results, the time required and the necessary costs.

Of particular interest was the aim to reveal perceived risks in security-related standardization. Therefore, the participants were asked to give a risk assessment which led to the identification of several topic areas like danger of abuse, federalism, pseudo security and ethical issues. In particular, the importance of ethical aspects in the development of security standards was discussed. Therefore specific recommendations to address these issues are important.

Risks of conflict in the standardization processes were analyzed in detail. Based on the typical stages of standardization processes, phase 2 (development) was ranked first, hence viewed to bear the biggest potential for conflict, followed by “initiation of the project” (phase 1), “revision” (phase 5), as well as “utilization” (phase 4). The stage “release” (phase 3) is associated with the least conflict potential. Solutions for the initiation of standardization projects and the development of standards are therefore important but recommendations are also required for the subsequent phases. Furthermore, specific risks of conflict in the standardization process were identified. The identification of common advantages, consensus building, Intellectual Property Rights, organizational problems and delays, special topics in the international context as well as resistors and problems to achieve acceptance were considered particularly significant. Therefore, it is important to offer solutions.

Based on the survey, specific recommendations were derived.

19. keywords
Standards, security technology, public security, critical infrastructures

20. publisher	21. price

Berichtsblatt 14

1. ISBN oder ISSN ---	2. Berichtsart (Schlussbericht oder Veröffentlichung) Veröffentlichung
3. Titel Transfer of Security Research Results Through Standardization - Case Studies From the Project InfraNorm	
4. Autor(en) [Name(n), Vorname(n)] Wurster, Simone	5. Abschlussdatum des Vorhabens 28.02.2013
	6. Veröffentlichungsdatum 04.09.2012
	7. Form der Publikation Poster
8. Durchführende Institution(en) (Name, Adresse) Technische Universität Berlin Institut für Technologie und Management FG Innovationsökonomie - VWS 2 Müller-Breslau-Straße 15 10623 Berlin	9. Ber. Nr. Durchführende Institution
	10. Förderkennzeichen 13N10915
	11. Seitenzahl 1
12. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	13. Literaturangaben 8
	14. Tabellen 2
	15. Abbildungen 1
16. Zusätzliche Angaben	
17. Vorgelegt bei (Titel, Ort, Datum) 7. Future Security Conference, Bonn, 4.-6. September 2012	

18. Kurzfassung

Im vorliegenden Beitrag werden auf Grundlage von zwei Fallstudien Normungsempfehlungen für Sicherheitsforscher erarbeitet.

Fallstudie 1 – Profil

- Art der Spezifikation: DIN SPEC für ein Datenaustauschformat
- Teilnehmer: 2 Universitätsforscher, 4 Unternehmensvertreter
- Dauer: 6 Monate

Fallbeispiel 2 – Profil

- Art der Spezifikation: DIN SPEC für Security- und Safety-Simulationen
- Teilnehmer: 4 Personen aus 4 Organisationen: 3 KMU-Vertreter, 1 Universitätsforscher
- Dauer: 6 Monate

Empfehlungen

- Planen Sie Maßnahmen der FuE-Phasen-Standardisierung zusammen mit dem betreffenden Projekt zur Sicherstellung der Verfügbarkeit von Ressourcen
- Verbinden Sie Aktivitäten zur Vorbereitung der Standardisierung mit anderen Aufgaben der relevanten Projekte
- Identifizieren Sie Synergien zwischen Aktivitäten zur Verwertung der relevanten FuE-Ergebnisse und von Aktivitäten, um die Verbreitung neu erarbeiteter Spezifikationen zu fördern
- Identifizierung Sie Synergien zwischen Aktivitäten zur Verbreitung neuer Spezifikationen und der Planung neuer FuE-Vorhaben in Bezug auf den Einsatz der neuen Spezifikationen
- Stellen Sie die Weiterentwicklung Ihrer erarbeiteten Spezifikation sicher
- Entwickeln Sie Beziehungen zu öffentlichen Auftraggebern um sie für den Einsatz der Sicherheitsstandards zu gewinnen
- Haben Sie acht auf eine geeignete Formulierung von security-bezogenen Spezifikationen um Mißbrauchsrisiken vorzubeugen

19. Schlagwörter
Standards, Security-Standardisierung, Sicherheitsforschung, DIN SPECs

20. Verlag ---	21. Preis ---

Document Control Sheet 14

1. ISBN or ISSN ---	2. type of document (e.g. report, publication) publication
3. title Transfer of Security Research Results Through Standardization - Case Studies From the Project InfraNorm	
4. author(s) (family name, first name(s)) Wurster, Simone	5. end of project 28 February 2013
	6. publication date 4 September 2012
	7. form of publication poster
8. performing organization(s) (name, address) Technische Universität Berlin Institut für Technologie und Management FG Innovationsökonomie - VWS 2 Müller-Breslau-Straße 15 10623 Berlin	9. originator's report no.
	10. reference no. 13N10915
	11. no. of pages 1
12. sponsoring agency (name, address) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	13. no. of references 8
	14. no. of tables 2
	15. no. of figures 1
16. supplementary notes	
17. presented at (title, place, date) 7th Future Security Conference, Bonn, September 4th - 6th, 2012	

18. abstract

Based on two case studies, advice for security research managers is derived:

Profile of case 1

- Type of standard: DIN SPEC on data exchange format
- Participants: 2 university employees, 4 company representatives
- Duration: 6 months

Profile of case 2

- Type of standard: DIN SPEC on security and safety simulations
- Participants: 4 people from 4 organizations: 3 SME representatives, 1 university employee
- Duration: 6 months

Advice

- Plan R&D stage standardization together with the relevant project to ensure availability of resources
- Link activities to prepare for standardization with other tasks of relevant R&D projects
- Identify synergies between activities intended to exploit relevant R&D results and activities to promote the diffusion of a new specification
- Identify synergies between activities to promote the diffusion of a new specification and future R&D projects regarding the utilization of the specification
- Pay attention to the further development of a specification
- Establish appropriate relationships to public procurers
- Ensure usability of standards and specifications in both exceptional and regular situations, if possible
- Implement appropriate strategies to avoid use of a security-related specification or standard other than its intended purposes

19. keywords

Standards, security standardization, civil security research, DIN SPECs

20. publisher ---	21. price ---

Berichtsblatt 15

1. ISBN oder ISSN ISBN: 978-981-08-9493-1	2. Berichtsart (Schlussbericht oder Veröffentlichung) Veröffentlichung
3. Titel INFRANORM - Norms and Standards for the Protection of Transportation Infrastructure	
4. Autor(en) [Name(n), Vorname(n)] Wurster, Simone	5. Abschlussdatum des Vorhabens 28.02.2013
	6. Veröffentlichungsdatum Juli 2011
	7. Form der Publikation Konferenz-Proceedings
8. Durchführende Institution(en) (Name, Adresse) Technische Universität Berlin Institut für Technologie und Management FG Innovationsökonomie - VWS 2 Müller-Breslau-Straße 15 10623 Berlin	9. Ber. Nr. Durchführende Institution
	10. Förderkennzeichen 13N10915
	11. Seitenzahl 5
12. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	13. Literaturangaben 52
	14. Tabellen 4
	15. Abbildungen 3
16. Zusätzliche Angaben	
17. Vorgelegt bei (Titel, Ort, Datum) Proceedings of the Annual International Conference on Innovation and Entrepreneurship, 19-24.	
18. Kurzfassung Innovationen für den Schutz von Verkehrsinfrastrukturen sind von großer Bedeutung. Normen und Standards fehlen in Bezug auf technische Aspekte, Kommunikationsprotokolle sowie für das Sicherheitsmanagement. INFRANORM ist ein gemeinsames Projekt zwischen dem Deutschen Institut für Normung (DIN) und der Technischen Universität Berlin und wird vom Bundesministerium für Bildung und Forschung finanziert. Sein Ziel ist es, die Entwicklung von Normen und Standards für den Schutz der Verkehrsinfrastruktur zu initiieren. Ein spezielles Arbeitspaket zielt auf die Entwicklung eines Normungshandbuchs. Es basiert auf Fallstudien, Interviews sowie auf einer Umfrage unter den Teilnehmern der deutschen Sicherheitsforschungsprogramms. Das Handbuch soll Erfolgsfaktoren und Problemmuster in der Entwicklung von Security-Normen und -Standards zeigen, um Handlungsanweisungen und Empfehlungen für die künftige Normungsarbeit zu geben. In diesem Artikel wird eine Fallstudie des Normungshandbuchs vorgestellt.	
19. Schlagwörter Normen, Spezifikationen, zivile Sicherheit, Fallstudien	
20. Verlag Global Science and Technology Forum (GSTF)	21. Preis ---

Document Control Sheet 15

1. ISBN or ISSN ISBN: 978-981-08-9493-1	2. type of document (e.g. report, publication) publication
3. title INFRANORM - Norms and Standards for the Protection of Transportation Infrastructure	
4. author(s) (family name, first name(s)) Wurster, Simone	5. end of project 28 February 2013
	6. publication date July 2011
	7. form of publication Conference proceedings
8. performing organization(s) (name, address) Technische Universität Berlin Institut für Technologie und Management FG Innovationsökonomie - VWS 2 Müller-Breslau-Straße 15 10623 Berlin	9. originator's report no.
	10. reference no. 13N10915
	11. no. of pages 5
12. sponsoring agency (name, address) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	13. no. of references 52
	14. no. of tables 4
	15. no. of figures 3
16. supplementary notes	
17. presented at (title, place, date) Proceedings of the Annual International Conference on Innovation and Entrepreneurship, 19-24.	
18. abstract Innovations for the protection of transportation facilities are of great importance. Norms and standards are missing in technical aspects and the areas of communication protocols and security management. INFRANORM is a joint project between the German Institute for Standardization (DIN) and the Berlin University of Technology and is funded by the German Federal Ministry of Education and Research. Its goal is to initiate the development of norms and standards for the protection of transportation infrastructure. A specific work package aims at developing a standardization manual. It is based on case studies, interviews of participants as well as a survey among the participants of the German security research program. The standardization manual is intended to show success factors and problem patterns in the development of security standards, to provide action guidelines and to offer recommendations for future standardization activities. This article presents one case study of the standardization manual.	
19. keywords specifications, standards, civil security, case studies	
20. publisher Global Science and Technology Forum (GSTF)	21. price ---