Kompetenzzentrum
Öffentliche IT

KOMPETENZZENTRUM ÖFFENTLICHE INFORMATIONSTECHNOLOGIE

STANDARDISIERUNG FÜR DIE ÖFFENTLICHE IT

Dr. Michael Stemmer, Gabriele Goldacker

Fraunhofer FOKUS

IMPRESSUM

Autoren:
Dr. Michael Stemmer, Gabriele Goldacker

Gestaltung:
Reiko Kammer

Herausgeber:
Kompetenzzentrum Öffentliche IT
Fraunhofer-Institut für Offene Kommunikationssysteme FOKUS
Kaiserin-Augusta-Allee 31, 10589 Berlin
Telefon: +49-30-3463-7173
Telefax: +49-30-3463-99-7173
info@oeffentliche-it.de
www.oeffentliche-it.de
www.fokus.fraunhofer.de

1. Auflage Mai 2014

VORWORT

Standardisierung ist ein buntes Feld: Foren- und Branchenstandards, Industriestandards, Herstellerstandards, Anwenderstandards, staatliche Setzungen und zugleich die Einheitlichkeit und Widerspruchsfreiheit des Normenwerks und DIN, CEN, CENELEC, ETSI, ISO, IEC und ITU-T. Die Sprachverwirrung reicht noch weiter: offene Standards, proprietäre Standards oder auch freie Standards, Europäische und nationale Normen, technische Spezifikationen.

Normen und Standards spielen in der Informationstechnologie eine wichtige Rolle. Sie reduzieren punktuell Vielfalt, um sie an anderen Stellen zu ermöglichen, sie öffnen Märkte und tragen zum nahtlosen Zusammenspiel von Produkten und Diensten unterschiedlicher Anbieter bei. Sie können ein Mindestniveau an Qualität und Sicherheit gewährleisten und unterstützen oftmals die schnelle und weite Verbreitung von Innovationen.

Um diese Wirkungen zu entfalten ist Standardisierung fast immer auf Kompromisse angewiesen und bedarf entsprechend Zeit zur Aushandlung. Dies wird sich auch nicht ändern. Dafür ist das Thema politisch zu brisant und damit immer wieder im Zentrum der Aufmerksamkeit. Zudem geht es immer auch darum, bestimmte Technologien zu fördern, konkurrierende Unternehmen zu attackieren oder Wirtschaftspolitik zu betreiben.

Betrachtet man IT im öffentlichen Raum als eine übergreifende Gesamtinfrastruktur, wird sehr schnell deutlich, dass man über Domänen hinweg vor identischen Herausforderungen steht. Es geht um die Etablierung von einheitlichen Standards öffentlicher IT, wobei sich die Frage stellt, ob und inwieweit die derzeitige Entwicklung und Umsetzung von IT-Standards diesen Herausforderungen gerecht wird. Durch wen und auf welche Weise sollen Standards für die öffentliche IT entwickelt werden? Und wie sollen sie durchgesetzt werden? Gibt es alternative Lösungsansätze? Wodurch zeichnen sie sich aus und wie lassen sie sich nutzbar machen?

Mit dem vorliegenden Whitepaper wollen wir diese Fragen stellen und einen ersten Überblick über mögliche Antworten geben. So sehen wir dieses Dokument als Vorschlag für eine Art Verständnisnorm in der bunten Standardisierungswelt und damit als Auftakt für eine Diskussion über die Standardisierung im öffentlichen Raum und darüber hinaus. Ganz im Sinne dieser Zielsetzung konnten wir bereits im Vorfeld zahlreiche Gespräche und Interviews mit Expertinnen und Experten aus Wirtschaft, Forschung, öffentlicher Hand und Normungsorganisationen führen.

Wir wünschen Ihnen eine anregende Lektüre und freuen uns auf Ihre Rückmeldungen und eine fruchtbare Diskussion.

Jens Fromm

Leiter Kompetenzzentrum Öffentliche IT

DANKSAGUNG

Das Kompetenzzentrum ÖFIT des Fraunhofer FOKUS dankt den folgenden Behörden, Organisationen und Firmen für die hilfreichen Anregungen, Kommentare und Diskussionen: Bundesministerium des Innern (BMI), Koordinierungsstelle für IT-Standards (KoSIT), Bundesamt für Sicherheit in der Informationstechnik (BSI), Bundesministerium für Wirtschaft und Energie (BMWi), Bundesnetzagentur, Deutsches Institut für Normung (DIN), DATABUND e.V. Unser besonderer Dank gilt dem Referat IT 2 »IT-Steuerung Bund« des BMI sowie den folgenden Personen: Annette Dürkop, Volker Gebauer, Roman Grahle, Silke Hildebrandt, Tobias Kaufmann, Thomas Knebel, Annegret Kübler-Bork, Reiner Liebler, Tobias Mikolasch, Miriam Pfändler, Ulrich Schlobinski, Dr. Astrid Schumacher, Dr. Heike Stach, Frank Steimke, Mario Wendt.

Dieses Dokument gibt ausschließlich die Meinung der Autoren wieder und repräsentiert nicht notwendigerweise den Standpunkt der Kommentatoren.

UNTER ÖFFENTLICHER IT VERSTEHT MAN INFORMATIONSTECHNOLOGIEN, DIE IN EINEM ÖFFENTLICHEN RAUM DURCH DIE GESAMTGESELLSCHAFTLICHE RELEVANZ UNTER BESONDERER BERÜCKSICHTIGUNG DER STAATLICHEN VERANTWORTUNG STEHEN.

INHALTSVERZEICHNIS

1. EINFÜHRUNG

Die Festlegung und Etablierung von Standards spielt eine Schlüsselrolle für die öffentliche IT. Die verschiedenen Bestandteile öffentlicher IT-Infrastrukturen müssen untereinander und mit den von Bürgern, Unternehmen, Behörden und weiteren Institutionen eingesetzten Anwendungen, Systemen und Endgeräten zusammenarbeiten. Dies kann nur gelingen, wenn sie die erforderliche Funktionalität aufweisen, miteinander interoperabel sind und ein einheitliches Mindestniveau hinsichtlich Qualität und Sicherheit aufweisen. Hierzu müssen entsprechende Standards existieren. Für nicht-öffentliche IT-Lösungen, sei es beim einzelnen Bürger oder innerhalb von Unternehmen und Behörden, wäre es prinzipiell auch möglich, Schnittstellen, Qualität und Sicherheit individuell festzulegen. Der öffentliche Raum erfordert jedoch Standards, die auf einem möglichst breiten Konsens der beteiligten Interessensparteien beruhen, dem aktuellen Stand der Technik entsprechen und zeitnah an neue Erkenntnisse und Entwicklungen angepasst werden.

Wir erörtern zunächst grundlegende Begriffe sowie Zwecke und Probleme der Standardisierung allgemein. Danach gehen wir auf die Bedeutung der Standardisierung für die öffentliche IT ein und stellen ausgewählte Standards und typische Standardisierungsprozesse vor. Anschließend werden Herausforderungen bei der Standardisierung öffentlicher IT identifiziert und einige Lösungsansätze thesenartig skizziert.

1.1 GRUNDBEGRIFFE

Mit der fortschreitenden Digitalisierung gewinnen die zugrunde liegenden Informations- und Kommunikationstechnologien zunehmend an Bedeutung. Sie bilden mittlerweile – vergleichbar zu Verkehrs-, Energie- oder Sicherheitsinfrastrukturen – eine digitale Infrastruktur, die für das Funktionieren von Gesellschaft, Wirtschaft und Verwaltung nahezu unverzichtbar geworden ist. Vor diesem Hintergrund verstehen wir unter **Öffentlicher IT** »Informationstechnologien, die in einem öffentlichen Raum durch die gesamtgesellschaftliche Relevanz unter besonderer Berücksichtigung der staatlichen Verantwortung stehen«.[1] Der öffentliche Raum wird hierbei durch die ihn konstituierenden gesellschaftlichen Subsysteme aufgespannt, von denen wir hier insbesondere die Zivilgesellschaft (Bürgerinnen und Bürger), die Wirtschaft und die öffentliche Hand betrachten.

Beispiele öffentlicher IT sind das Internet, Online-Dienste, die den neuen Personalausweis nutzen, und Bürgerbeteiligungs-Plattformen. Die öffentliche Hand kann in Bezug auf öffentliche IT die Rolle des Regulierers, des Beschaffers, des Nutzers und des Dienstanbieters innehaben.

Öffentliche IT umfasst neben staatlicher IT[2], die Schnittstellen zum Bürger und zur Wirtschaft aufweist, auch zahlreiche weitere privatwirtschaftliche und gesellschaftliche Anwendungsbereiche moderner Informations- und Kommunikationstechnologie. Sie ist nicht auf E-Government beschränkt, sondern betrifft alle Lebens-, Wirtschafts-, Verwaltungs- und Politikbereiche, soweit sie sich in öffentlichen Räumen abspielen und durch IT unterstützt werden. In allen diesen Bereichen existieren vielfältige IT-Standards und Standardisierungsprozesse, die im Folgenden aus der Perspektive der öffentlichen IT betrachtet werden.

Unter einem **Standard** verstehen wir eine einheitliche und anerkannte Art und Weise etwas herzustellen oder durchzuführen.[3] Grundlage für einen Standard ist häufig eine **Technische Spezifikation**, deren Inhalt in Form eines Dokumentes festgehalten ist. Eine technische Spezifikation wird dann als Standard bezeichnet, wenn sie in Expertenkreisen hinreichend anerkannt ist und/oder in der Praxis hinreichend akzeptiert und genutzt wird. Im Zusammenhang mit öffentlicher IT sind vor allem Standards der Informations- und Kommunikationstechnologie (IT-Standards) relevant. Entsprechend ihrem Status sind verschiedene Arten von Standards zu unterscheiden, die zudem auf unterschiedliche Weise zustande kommen können.

---

[1] Jens Fromm, Petra Hoepner, Mike Weber, Christian Welzel: Öffentliche Informationstechnologie – Abgrenzung und Handlungsfelder. Whitepaper. Fraunhofer FOKUS. Berlin, Juni 2013.

[2] Unter staatlicher IT verstehen wir sowohl die öffentlichen als auch die nicht-öffentlichen Bestandteile von Informationstechnologien, die in Verantwortung der öffentlichen Hand betrieben werden. Dies umfasst IT auf allen staatlichen und überstaatlichen Ebenen, d. h. auf internationaler, europäischer, Bundes-, Landes- und kommunaler Ebene sowie im Rahmen von Bündnissen, wie z. B. der NATO.

[3] Die Bezeichnung »Standard« wird in der Literatur und im täglichen Gebrauch je nach Kontext mit unterschiedlichen Bedeutungen verwendet. Wir verwenden sie hier in einem allgemeinen Sinn als einheitlichen Oberbegriff. Unsere Definition lehnt sich an eine etwas ausführlichere Definition an, wie sie neben anderen Quelle beispielsweise auch in der Wikipedia zu finden ist: »Ein Standard ist eine vergleichsweise einheitliche oder vereinheitlichte, weithin anerkannte und meist angewandte (oder zumindest angestrebte) Art und Weise, etwas herzustellen oder durchzuführen, die sich gegenüber anderen Arten und Weisen durchgesetzt hat.« [Quelle: de.wikipedia.org/wiki/Standard]

Abbildung 1: Öffentlicher Raum und ihn konstituierende gesellschaftliche Subsysteme

Ein im Rahmen eines formalen Normungsverfahrens beschlossener Standard wird als **Norm** bezeichnet.[4] Die Entstehung einer Norm ist durch Offenheit, eine breite Einbeziehung möglichst aller relevanten Interessensparteien und ein mehrstufiges formales, konsensorientiertes Erstellungs- und Abstimmungsverfahren gekennzeichnet. Vor Verabschiedung einer Norm hat die Öffentlichkeit die Möglichkeit, Kommentare einzureichen. Die Beschlussfindung bei europäischen und internationalen Normen erfolgt auf der Basis (gewichteter oder ungewichteter) nationaler Stimmen. Im IT-Bereich existiert mit dem DIN[5] und der DKE[6] auf deutscher Ebene, mit CEN[7], CENELEC[8] und ETSI[9] auf europäischer Ebene und mit ISO[10], IEC[11] und ITU[12] auf internationaler Ebene ein System von staatlich bzw. überstaatlich autorisierten **Normungsorganisationen**, die diese Prozesse organisieren und moderieren.

Der sogenannte Neue Ansatz[13] der EU weist europäischen Normen eine besondere Bedeutung zu. In EU-Verordnungen und -Richtlinien sollen möglichst nur wesentliche funktionale, Qualitäts- und Sicherheitsanforderungen verbindlich gemacht werden. Die weitere Ausgestaltung erfolgt bevorzugt in europäischen Normen, deren Umsetzung jedoch nicht verbindlich ist. Jede Lösung, die die Anforderungen der Verordnung oder Richtlinie erfüllt, ist prinzipiell zulässig. Setzt andererseits eine Lösung alle relevanten Normen um, wird davon ausgegangen, dass sie der Verordnung bzw. der Richtlinie genügt (Konformitätsvermutung). Die entsprechenden Normen werden regelmäßig als Stand der Technik betrachtet. Damit erhalten diese Normen mittelbare Rechtswirkung.

Ein wesentlicher Anspruch der Normung ist es, für jeden Normungsgegenstand auf jeder Ebene (international, europäisch, national) nur jeweils eine geltende Norm zuzulassen, um widersprüchliche oder konkurrierende Regeln zu vermeiden. Die Länder der Europäischen Union sind als Mitglieder von CEN, CENELEC und ETSI zudem verpflichtet, nationale Normen zurückzuziehen, wenn für die fraglichen Normungsgegenstände entsprechende europäische Normen herausgegeben werden. Eine verpflichtende Übernahmeregelung zwischen internationalen und nationalen Normungsorganisationen existiert formell nicht. Jedoch wird über die Wiener Vereinbarung zwischen ISO und CEN,[14] sowie die Dresdener Vereinbarung zwischen IEC und CENELEC[15] der Prozess zwischen europäischer und internationaler Ebene geregelt, um Inkonsistenzen zwischen den Normenwerken zu vermeiden.

---

[4] In DIN EN 45020:2007-03 (Normung und damit zusammenhängende Tätigkeiten - Allgemeine Begriffe (ISO/IEC Guide 2:2004); Dreisprachige Fassung EN 45020:2006), Abschnitt 3.2 wird der Begriff der Norm wie folgt definiert: »Norm: Dokument, das mit Konsens erstellt und von einer anerkannten Institution angenommen wurde und das für die allgemeine und wiederkehrende Anwendung Regeln, Leitlinien oder Merkmale für Tätigkeiten oder deren Ergebnisse festlegt, wobei ein optimaler Ordnungsgrad in einem gegebenen Zusammenhang angestrebt wird. ANMERKUNG: Normen sollten auf den gesicherten Ergebnissen von Wissenschaft, Technik und Erfahrung basieren und auf die Förderung optimaler Vorteile für die Gesellschaft abzielen.«
Im englischen Sprachraum ist die Unterscheidung zwischen Standard und Norm hingegen nicht bekannt. Hier bezeichnet man beides mit »standard«, was insbesondere bei der Übersetzung ins Deutsche leider häufig zu Missverständnissen führt. Der ISO/IEC Guide 2:2004 definiert so beispielsweise den Norm-Begriff in Abschnitt 3.2 wie folgt: »standard: document, established by consensus and approved by a recognized body, that provides, for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context. Note 1 to entry: Standards should be based on the consolidated results of science, technology and experience, andaimed at the promotion of optimum community benefits.«
Diese Problematik sollte jedoch nicht dazu führen, dass man im Deutschen den Begriff des Standards auf die obige ISO/IEC-Guide-2-Definition für »standard« reduziert und damit außer Normen keine weiteren Standards mehr als solche akzeptiert. Um im Englischen Normen von weiteren Standards zu unterscheiden, spricht man auch von »de jure standard« und »formal standard« für Ersteres und von »de facto standard« und »informal standard« für Letzteres.

[5] Deutsches Institut für Normung

[6] Deutsche Kommission Elektrotechnik Elektronik Informationstechnologie im DIN und VDE

[7] European Committee for Standardization (Comité Européen de Normalisation)

[8] European Committee for Electrotechnical Standardization (Comité Européen de Normalisation Electrotechnique)

[9] European Telecommunications Standards Institute

[10] International Organization for Standardization

[11] International Electrotechnical Commission

[12] International Telecommunication Union

[13] Entschließung des Rates vom 7. Mai 1985 über eine neue Konzeption auf dem Gebiet der technischen Harmonisierung und der Normung (85/C 136/01)

[14] http://boss.cen.eu/ref/Vienna_Agreement.pdf

[15] http://www.iec.ch/about/globalreach/partners/regional/iec_cenelec_agreement.htm

UNTER EINEM STANDARD VERSTEHEN WIR EINE EINHEITLICHE UND ANERKANNTE ART UND WEISE ETWAS HERZUSTELLEN ODER DURCHZUFÜHREN.

Neben Normen gibt es weitere Standards, die durch die Initiative einzelner oder mehrerer Interessensparteien, durch gesellschaftliche oder wirtschaftliche Prozesse oder einfach durch gelebte Praxis zustande kommen. Man unterscheidet typischerweise:

- **Foren- und Branchenstandards**, die durch nicht staatlich autorisierte Standardisierungsgremien, wie z. B. IETF[16], W3C[17], OASIS[18] oder IEEE[19], analog zu Normen in einem weitgehend formalen und für die breite Beteiligung interessierter Parteien offenen Prozess entwickelt und vereinbart werden,
- **Industriestandards**, die von mehreren Anbietern gemeinsam festgelegt werden (z. B. Compact Disc, DVD, Blu-ray),
- **Herstellerstandards**, die von einem Anbieter allein gesetzt werden (z. B. Betriebssysteme, wie Microsoft Windows, Google Android oder Apple iOS),
- **Anwenderstandards**, die durch Organisationen festgelegt werden, die Informationstechnik anwenden (z. B. Unternehmensarchitekturen, Style Guides, Beschaffungsstandards und weitere Festlegungen, die im Rahmen der IT-Governance eines Unternehmens oder Konzerns getroffen werden) und
- **Staatliche und überstaatliche Standards**, deren Erstellung von der öffentlichen Hand initiiert und koordiniert wird (z. B. XÖV, SAGA) oder die durch Gesetze und Verordnungen geschaffen werden (z. B. durch das deutsche E-Government-Gesetz oder die Umsetzung der EU-Dienstleistungsrichtlinie).

Darüber hinaus erarbeiten viele Normungsorganisationen nicht nur Normen, sondern auch weitere technische Spezifikationen, die nicht den Status einer Norm erhalten, sich aber dennoch in der Praxis zu einem Standard entwickeln können. Der Unterschied zwischen Normen und diesen technischen Spezifikationen besteht dabei im Grad der Konsensfindung. Im Gegensatz zu Normen besteht bei technischen Spezifikationen nicht die Notwendigkeit des Vollkonsenses. Einige dieser technischen Spezifikationen sind bezüglich der Offenheit und Transparenz des Erarbeitungsprozesses daher eher als Industriestandards einzustufen (beispielsweise eine DIN SPEC oder eine ETSI Group Specification). Sie durchlaufen jedoch einen einheitlichen Prozess, welcher durch die Normungsorganisationen gewährleistet wird.

Man unterscheidet zudem zwischen offenen, proprietären und freien Standards. Als offene Standards werden häufig Standards bezeichnet, die in einem für alle interessierten Parteien offenen Prozess entstanden und öffentlich zugänglich sind[20] und zu fairen, angemessenen und diskriminierungsfreien Bedingungen[21] genutzt werden dürfen. Unter offene Standards fallen somit insbesondere Normen, aber auch viele Foren- und Branchenstandards. Hersteller- und Industriestandards bezeichnet man in Abgrenzung zu offenen Standards häufig auch als **proprietäre Standards**. Standards, die ohne Einschränkungen und kostenfrei genutzt werden können, werden auch als **freie Standards** bezeichnet.[22]

[16] Internet Engineering Task Force
[17] World Wide Web Consortium
[18] Organization for the Advancement of Structured Information Standards
[19] Institute of Electrical and Electronics Engineers
[20] Vgl. bspw. Anhang 2 zu der Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen »Interoperabilisierung europäischer öffentlicher Dienste« (KOM(2010) 744 der Europäischen Kommission), Dezember 2010.
[21] Man bezeichnet diese Kriterien auch als FRAND-Bedingungen: **F**air, **R**easonable **A**nd **N**on-**D**iscriminatory.
[22] In der Literatur und im allgemeinen Sprachgebrauch ist die Definition und Verwendung der Attribute »offen« und »frei« in Bezug auf Standards uneinheitlich. Zudem fehlt eine klare Abgrenzung zwischen beiden Attributen, sodass diese teils auch mehr oder weniger synonym verwendet werden. Wir verstehen im Folgenden »offen« im Sinne des Zugangs zu einem Standard. Dies umfasst einerseits die Mitwirkungsmöglichkeiten bei der Entstehung des Standards und andererseits die Zugänglichkeit seiner Spezifikation. »Frei« verstehen wir hingegen im Sinne der Nutzung eines Standards. Dies umfasst die Abwesenheit von Einschränkungen und/oder Kosten für die Nutzung und Anwendung des Standards. Eine Patent-behaftete Norm beispielsweise, die unter FRAND-Bedingungen genutzt werden kann, ist mit diesem Verständnis zwar ein offener, aber kein freier Standard.

EIN IM RAHMEN EINES FORMALEN NORMUNGSVERFAHRENS BESCHLOSSENER STANDARD WIRD ALS NORM BEZEICHNET.

1.2 ZWECK UND NUTZEN VON STANDARDS

Standards haben in erster Linie eine ordnende Funktion, welche sowohl Technologien als auch Märkte betrifft. Sie definieren einheitliche Begriffe, Regeln, Strukturen, Anforderungen oder Lösungen und reduzieren hiermit die Komplexität der prinzipiellen Möglichkeiten auf ausgewählte Varianten. Zusammen schaffen und gestalten die für einen bestimmen Bereich, wie z. B. die öffentliche IT, relevanten Standards einen gemeinsamen Rahmen, in dem sich die von den beteiligten Akteuren entwickelten und bereitgestellten Technologien, Produkte, Verfahren und Dienstleistungen bewegen.

Öffentliche IT, die weitgehend auf Normen und offenen Standards basiert (und dies auch vermittelt), hat größere Chancen auf Akzeptanz bei neu zu gewinnenden Nutzern in Wirtschaft und Verwaltung wie auch bei den Bürgern. Normen und offene Standards gelten allgemein als gute Basis für betriebssichere und gefahrenarme Produkte.

Normen und offene Standards vereinen das Wissen vielfältiger Experten, berücksichtigen ein breites Spektrum technischer und wirtschaftlicher Anforderungen und haben i. d. R. eine hohe Reife. Aus formaler Sicht repräsentieren sie zudem den jeweiligen Stand der Technik. Konforme Entwicklungen haben daher gute Chancen auf eine wirtschaftlich angemessene Nutzungsdauer.

Normen und offene Standards spezifizieren vornehmlich funktionale, qualitative und organisatorische Anforderungen und vermeiden Anforderungen, die nur von bestimmten Herstellern oder Anbietern erfüllt werden können. Dies sind Grundvoraussetzungen für Herstellervielfalt und wirtschaftlich-technischen Wettbewerb innerhalb des notwendigen gemeinsamen Rahmens.

Neben anderen Voraussetzungen kann öffentliche IT nur dann nachweisbar betriebssicher und frei von absehbaren Gefahren für ihre Nutzer sein, wenn für die Entwicklung, die Installation und den Betrieb klare, offen verfügbare und im Detail überprüfbare Regeln existieren.

Normen und offene Standards können überdies, beispielsweise im Rahmen einer Ausschreibung, als Referenzrahmen genutzt werden, um Missverständnisse zwischen Kunden, Anbietern und Herstellern zu vermeiden.

1.3 PROBLEME UND RISIKEN VON STANDARDS

Formalisierte Normungs- und Standardisierungsprozesse werden häufig als zu langsam empfunden. Dies gilt insbesondere dann, wenn eine einheitliche Lösung für ein gegebenes Problem dringend erforderlich ist und diese Lösung zudem offensichtlich erscheint. Ursache ist oft die Konsensfindung. Normen und Standards, die in derartigen Prozessen entstanden sind, entsprechen in Bereichen mit rasanter Entwicklung, wie der IT, manchmal schon bei Fertigstellung nicht mehr den Nutzerbedürfnissen oder dem inzwischen weiterentwickelten Stand der Technik.

Standards stellen häufig nur relativ schwache Kompromisse der an der Erarbeitung Beteiligten dar. Dies bedeutet im Einzelfall beispielsweise, dass nur Basisfunktionen standardisiert sind oder dass ein Standard mehrere Alternativen für eine Funktion zulässt. Im ersten Fall ist durch eine Realisierung des Standards auch nur Interoperabilität für die Basisfunktionen erzielbar. Der zweite Fall kann bedeuten, dass zur Sicherstellung von Interoperabilität alle Alternativen realisiert sein müssen, was hohe Kosten verursacht und zu großen und komplexen Realisierungen führt.

NORMEN UND OFFENE STANDARDS GELTEN ALLGEMEIN ALS GUTE BASIS FÜR BETRIEBSSICHERE UND GEFAHRENARME PRODUKTE.

Es ist auch zu beobachten, dass in Normungsorganisationen, wie dem ETSI und dem DIN, für bestimmte technische Probleme zwar ein Standard (z. B. ETSI Standard, DIN SPEC), aber keine formelle Norm erarbeitet wird, obwohl letzteres angemessen und möglich wäre. Auf diese Weise kommt man zwar häufig schneller zu einem Ergebnis als in einem konsensorientierten Normungsprozess, allerdings sind die Beteiligungsmöglichkeiten bei der Erarbeitung häufig eingeschränkt, es gibt keine Kommentierungsmöglichkeit für die Öffentlichkeit und/oder die Abstimmungsberechtigung oder Stimmgewichtung weicht ab.

Manche Standards sind zu komplex, weil z. B. Lösungen für in der Realität nicht relevante Teilprobleme eingearbeitet wurden.[23] Derartige Standards eignen sich dann auch nicht als Anforderungsreferenz bei Ausschreibungen oder müssen bedarfsgerecht profiliert[24] werden. Diese Profilierung erfordert Fachkenntnisse und kann aufwendig und daher kostspielig sein. Es ist zudem möglich, dass Realisierungen eines Standards, die auf unterschiedlichen Profilen basieren, nicht interoperabel sind.

Die Anwendung existierender Standards in deutlich anderen als den ursprünglichen Einsatzgebieten kann zu suboptimalen Lösungen führen. Die Existenz ziemlich, aber nicht genau passender Standards kann die Erstellung besser geeigneter Standards verhindern oder verzögern, weil beispielsweise zu lange auf dem existierenden Standard beharrt wird oder die originär zuständigen Bearbeiter des neuen Anwendungsbereichs über zu wenig Expertise verfügen, bei der Weiterentwicklung aber trotzdem mitentscheiden.

Der Einsatz von Standards in bisher ungeregelten Bereichen erfordert stets eine Anpassung der Produkte einiger Anbieter. Manchmal fehlt hier die Einsicht in die Sinnhaftigkeit des Einsatzes der Standards, wenn es bisher doch auch ohne diese funktioniert hat.

Eine einheitliche Standardisierung ist nicht in jedem Markt durch die relevanten Anbieter gewollt, z. B. weil jeder dieser Anbieter einen ausreichenden Marktanteil für sein Produkt sieht und den Marktzugang für Anbieter kompatibler Produkte nicht erleichtern will.

Normen und Standards können patentgeschützte Teile beinhalten, deren Nutzung eine Lizenzvereinbarung mit dem Patentinhaber erfordert und Lizenzgebühren nach sich ziehen kann. Gerade im Bereich der IT – wo beispielsweise beliebig häufig kopierbare Software betroffen ist – existieren in diesen Fällen bisher keine befriedigenden Lizenzmodelle. Zudem ist auch das Patentrecht international nicht einheitlich. Dies kann es erschweren, die Kosten für die Nutzung eines entsprechenden Produktes realistisch abzuschätzen.

Nicht-offene De-facto-Standards, die von einzelnen Herstellern mit großer Marktmacht gesetzt werden, behindern den Wettbewerb und können überhöhte Kosten verursachen.

»Standards haben in erster Linie eine ordnende Funktion, welche sowohl Technologien als auch Märkte betrifft.«

[23] Beispiel: ITU-T-Empfehlung X.500 im Vergleich zu IETF LDAP
[24] Bei einer Profilierung werden konkrete Realisierungs- und/oder Nutzungsalternativen für ein spezifisches Einsatzumfeld ausgewählt.

2. STANDARDS IN DER ÖFFENTLICHEN IT

Im Bereich der IT existieren bereits vielfältige Standards und Standardisierungsprozesse, die wir im Folgenden aus der Perspektive der öffentlichen IT betrachten.

2.1 ZIELE

Mit der Entwicklung und Etablierung von Standards für den Bereich der öffentlichen IT werden folgende Ziele verfolgt (die ebenso für andere Bereiche gelten):

Interoperabilität, Kompatibilität und Koexistenzfähigkeit

Die Vielzahl informationstechnischer Produkte, Dienste und Infrastrukturen im Bereich öffentlicher IT kann nur dort reibungslos zusammenwirken, wo dies durch gemeinsame Schnittstellen und Protokolle oder geeignete Adapter gewährleistet ist. Bedingt durch die anhaltend dynamische Entwicklung der Informationstechnik ist dies bislang jedoch immer nur in bestimmten Teilbereichen der Fall. So schaffen und kontrollieren Anbieter mit einer großen Marktmacht beispielsweise derzeit im Bereich der Smartphones weit verbreitete Plattformen (z. B. Apple iOS und Google Android). Innerhalb dieser wird ein hoher Grad an Interoperabilität und Kompatibilität gewährleistet, während der Austausch und das Zusammenwirken zwischen den unterschiedlichen Hersteller-Plattformen schwierig ist oder sogar gezielt unterbunden wird. Für den Bereich der öffentlichen IT ist hingegen ein hoher Grad an Interoperabilität und Kompatibilität anzustreben, ohne sich an einen bestimmten Anbieter und seine Plattform binden und somit andere Anbieter benachteiligen zu müssen. Voraussetzung hierfür ist eine möglichst weitgehende Nutzung von offenen und plattformübergreifenden Standards und Normen.

Interoperabilität und Kompatibilität beziehen sich vornehmlich auf die zur Erfüllung einer konkreten Aufgabe notwendigen Hard- und Softwarekomponenten. Daneben ist für öffentliche IT auch die Koexistenzfähigkeit zwischen diesen Komponenten und weiteren, für andere Zwecke auf demselben Gerät oder über dasselbe Kommunikationsmedium verwendeten Komponenten wesentlich.

Die Notwendigkeit von Interoperabilität, Kompatibilität und Koexistenzfähigkeit ist im öffentlichen Raum noch um ein Vielfaches größer als innerhalb von Verwaltungen oder Behörden, da auch die von den weiteren Beteiligten genutzten Produkte (z. B. verbreitete Betriebssysteme oder Anwenderprogramme) in die Betrachtung einbezogen werden müssen.

Qualität und Sicherheit

Die Verlässlichkeit, Vertrauenswürdigkeit und Sicherheit von Informationstechnik ist im öffentlichen Raum von besonderer Bedeutung. Standards helfen, Kriterien für diese und weitere Qualitätseigenschaften, wie z. B. Ergonomie und Barrierefreiheit, zu definieren und die Eigenschaften zu quantifizieren und vergleich- und überprüfbar zu machen. Durch die verbindliche Vorgabe von Normen und Mindeststandards und entsprechende Zulassungs-, Zertifizierungs- und Auswahlprozesse kann überdies ein festgelegtes Qualitäts- und Sicherheitsniveau sichergestellt werden.

Einheitlichkeit der Bedienung

IT-Produkte sollen möglichst leicht, intuitiv und komfortabel bedien- und konfigurierbar sein. Besonders wenn unterschiedliche Produkte für denselben Zweck genutzt werden, erleichtern einheitliche Bedienelemente, Bezeichnungen, Positionen auf dem Bildschirm und Abfrageabläufe die Bedienung erheblich. Gerade im Bereich der öffentlichen IT, wo vielfältige Endgeräte und Einsatzumgebungen berücksichtigt werden müssen, tragen Standards zur Vereinheitlichung bei, ohne vorteilhafte Gestaltungsalternativen zu verhindern.

GEEIGNETE STANDARDS FÖRDERN DIE WIEDERVERWENDBARKEIT VON HARD- UND SOFTWAREKOMPONENTEN UND ERMÖGLICHEN SO POSITIVE SKALENEFFEKTE.

Wirtschaftlichkeit, Zukunftsfähigkeit und Nachhaltigkeit

Mit der vereinheitlichenden Wirkung von Normen und offenen Standards auf öffentliche Informationstechnik sind auch wirtschaftliche Vorteile für Zivilgesellschaft, Wirtschaft und öffentliche Hand verbunden. So kann beispielsweise der Wettbewerb zwischen den Anbietern gestärkt und eine zu starke Bindung an einen oder mehrere Anbieter reduziert werden.[25] Geeignete Standards fördern die Wiederverwendbarkeit von Hard- und Softwarekomponenten und ermöglichen so positive Skaleneffekte. Auch kann eine gesicherte Funktion entsprechend festgelegter Qualitäts- und Sicherheitsstandards Ausfälle, Schäden und Folgeschäden und die damit verbundenen Kosten verhindern helfen. Breit akzeptierte oder verbindliche Standards, die nicht von den unternehmerischen Entscheidungen einzelner Anbieter abhängen, unterstützen auch die langfristige Stabilität und Entwicklungsfähigkeit von IT-Infrastrukturen und leisten somit einen wesentlichen Beitrag zur Zukunftsfähigkeit und Nachhaltigkeit öffentlicher IT.

Transparenz und Nachvollziehbarkeit

Eine wesentliche Anforderung an Strukturen und Lösungen im öffentlichen Raum ist deren Transparenz und Nachvollziehbarkeit. Normen und offene Standards unterstützen dies, indem sie wesentliche Eigenschaften öffentlicher IT nicht nur fest-, sondern auch offenlegen.

Partizipation der Stakeholder

Offene Normungs- und Standardisierungsgremien ermöglichen die Beteiligung aller interessierten Kreise an der Entwicklung der Strukturen und Eigenschaften öffentlicher IT und damit deren Mitwirkung an der Gestaltung des öffentlichen Raumes. Dies betrifft sowohl Akteure der Wirtschaft und der öffentlichen Hand als auch der Zivilgesellschaft. Die öffentliche Hand kann sich dabei direkt an der Standardisierung beteiligen, aber auch durch die Vorgabe von Anforderungen den Standardisierungsprozess lenken.

Innovationsfähigkeit und Flexibilität

Standards, die notwendige Eigenschaften und Fähigkeiten öffentlicher IT klar festlegen, schaffen damit gleichzeitig einen sicheren Rahmen für wettbewerbliche Differenzierung, beispielsweise durch zusätzliche Funktionen, erhöhte Bedienfreundlichkeit oder effiziente Realisierung. Normen und Standards sollten überdies, soweit möglich, keine konkreten Realisierungen vorgeben, damit flexibel auf technische und wirtschaftliche Rahmenbedingungen und auf Nutzererwartungen reagiert werden kann.

Rechtssicherheit bei der Formulierung von Ausschreibungen und Verträgen

Ausschreibungen und Verträge der öffentlichen Hand, die sich in ihren technischen Anforderungen auf Normen und offene Standards beziehen, erhöhen die Sicherheit, dass ein gemeinsames Verständnis bzgl. der erwarteten Leistung zwischen den

»Die Verlässlichkeit, Vertrauenswürdigkeit und Sicherheit von Informationstechnik ist im öffentlichen Raum von besonderer Bedeutung.«

[25] Vgl. Communication from the Commission to the European parliament, the Council, the European economic and social Committee and the Committee of the Regions: Against lock-in: building open ICT systems by making better use of standards in public procurement (COM(2013) 455 der Europäischen Kommission)., Juni 2013.

EINE WESENTLICHE ANFORDERUNG AN STRUKTUREN UND LÖSUNGEN IM ÖFFENTLICHEN RAUM IST DEREN TRANSPARENZ UND NACHVOLLZIEHBARKEIT.

Parteien besteht. Die EU hat in der Vergaberichtlinie 2004/18/EG[26] eine Hierarchie der derart referenzierbaren Normen und Standards festgelegt, die in die VOL/A[27] und in die VOF[28] übernommen wurden.[29]

2.2 DIE ROLLE DER ÖFFENTLICHEN HAND

Die öffentliche Hand tritt im Kontext öffentlicher IT in verschiedenen Rollen auf:

- **Regulierer/Gesetzgeber**: Die öffentliche Hand wirkt durch regulative und/oder legislative Maßnahmen darauf hin, dass unerwünschte Effekte öffentlicher IT unterbleiben oder gemildert werden. Solche Effekte sind beispielsweise unangemessene Preise für die Nutzung oligarchisch betriebener Dienste/Komponenten, Benachteiligung (kleinerer) Wettbewerber, Benachteiligung von Bevölkerungsgruppen oder geografischen Regionen, Missachtung von Umwelt- oder Arbeitsschutz.
- **Beschaffer**: Die öffentliche Verwaltung kauft, mietet oder least IT-Leistungen – wie z. B. Hard- und/oder Software, IT-Dienstleistungen, Netzanschlüsse, Speicherplatz, Datenzugänge, Verarbeitungskapazität, Zugänge zu Software – oder beauftragt entsprechende Entwicklungen für den Eigenbedarf.
- **Nutzer**: Die öffentliche Verwaltung benutzt Anwendungen der öffentlichen IT.
- **Anbieter/Betreiber**: Die öffentliche Verwaltung stellt Dienste und/oder Infrastrukturkomponenten (Server, Teilnetze, …) für die öffentliche Nutzung zur Verfügung. Neben der Verantwortung für die technische Betriebsfähigkeit und die angemessene Leistungsfähigkeit dieser Dienste und Komponenten besteht auch eine Verantwortung der öffentlichen Verwaltung für Aspekte wie Zugangs- und Nutzungsgerechtigkeit, Schutz des Nutzers gegen Angriffe unter Nutzung der Dienste bzw. Komponenten etc.

Als großer Beschaffer, Nutzer und Anbieter öffentlicher IT haben Bund, Länder und Kommunen eine relevante Marktmacht, um von den Herstellern zu erreichen, dass diese Lösungen bereitstellen, die auf Normen oder offenen Standards basieren. Dazu ist ein koordiniertes Vorgehen aller föderalen Ebenen von Vorteil, wenn nicht sogar erforderlich.

Möchte die öffentliche Hand Lösungen, die auf Normen oder offenen Standards basieren, gegen etablierte De-facto-Herstellerstandards durchsetzen, ist häufig ein zunächst höherer Finanzierungsaufwand erforderlich. Die neuen Lösungen müssen realisiert werden, und Hersteller sind i. d. R. nicht von vornherein überzeugt, dass sich eine von der öffentlichen Hand forcierte Lösung am Markt durchsetzen wird. Bei entsprechenden Rahmenbedingungen kann es allerdings sinnvoll sein, auch als öffentliche Hand für bestimmte Zwecke auf De-facto-Standards bzw. proprietäre Lösungen zu setzen.

Die öffentliche Hand muss auch bei der Durchsetzung von Lösungen, die auf Normen und Standards basieren, sorgfältig darauf achten, die weiteren Beteiligten im öffentlichen Raum – Wirtschaft und Bürger – nicht über Gebühr zu belasten, beispielsweise indem diese neue Produkte oder zusätzliche Komponenten beschaffen müssen oder einen hohen Anpassungsaufwand haben.

[26] Richtlinie 2004/18/EG des Europäischen Parlaments und des Rates vom 31. März 2004 über die Koordinierung der Verfahren zur Vergabe öffentlicher Bauaufträge, Lieferaufträge und Dienstleistungsaufträge
[27] Vergabe- und Vertragsordnung für Leistungen (VOL) Teil A Allgemeine Bestimmungen für die Vergabe von Leistungen (VOL/A)
[28] Vergabeordnung für freiberufliche Dienstleistungen – VOF –
[29] Wegen der großen Vielfalt relevanter IT-Spezifikationen, die nicht den Status einer Norm haben, hat die Europäische Kommission zudem die Europäische Multi-Stakeholder-Plattform (MSP) für die IT-Normung errichtet. Eine wesentliche Aufgabe dieses Gremiums ist, derartige IT-Spezifikationen zu identifizieren, die eine große wirtschaftliche Relevanz besitzen und für die keine vergleichbare, geeignete Norm existiert. Erfüllt eine Spezifikation darüber hinaus bestimmte formale Anforderungen – offener, konsensorientierter Erstellungsprozess, öffentliche Verfügbarkeit, FRAND-Lizenzbedingungen und weitere – kann sie für die bevorzugte Referenzierung in Ausschreibungen der öffentlichen Hand zugelassen werden.

ES EXISTIERT EINE VIELZAHL VON GREMIEN, IN DENEN IT-NORMEN UND OFFENE IT-STANDARDS ERARBEITET WERDEN.

2.3 EXISTIERENDE STANDARDS

Es existiert eine Vielzahl von Gremien, in denen IT-Normen und offene IT-Standards erarbeitet werden. Hinzu kommen unzählige De-facto-Standards, die durch IT-Anbieter, IT-Anwender und staatliche Stellen gesetzt werden. Da IT immer mehr und in immer stärkerem Maße unsere Lebens- und Arbeitswelt durchdringt, sind zudem viele Branchen und Anwendungsbereiche, wie z. B. Gesundheitswesen, öffentliche Sicherheit, Energienetze, Automobilwirtschaft, Logistik und Verwaltung, von IT und dabei nicht nur von generellen, sondern auch von branchenspezifischen IT-Standards betroffen.

Im Folgenden betrachten wir die Situation der für den öffentlichen Raum relevanten IT- Standards am Beispiel der staatlichen und staatlich koordinierten Erarbeitung von Standards für die öffentliche Verwaltung näher.

Ein wesentlicher Bereich sind IT-Standards für den Datenaustausch in der öffentlichen Verwaltung. Hierzu wurden und werden die auf XML-basierenden **XÖV-Standards** entwickelt. Beispiele sind XMeld für das Meldewesen, XPersonenstand und XAusländer, also Fachstandards für die Innenverwaltung, sowie XWaffe für das nationale Waffenregister. Als Datenaustauschstandards innerhalb der öffentlichen Verwaltung haben die XÖV-Standards eine hohe Bedeutung für die staatliche IT, darüber hinaus durch ihre Bezüge zu Bürgern und Wirtschaft aber auch für die öffentliche IT.

Ebenfalls zu nennen ist der Metastandard **SAGA**[30], dessen Aufgaben wie folgt definiert sind: »SAGA ist eine Zusammenstellung von Referenzen auf Spezifikationen und Methoden für Software-Systeme der öffentlichen Verwaltung. Durch Beschluss des IT-Rats ist die Anwendung von SAGA 5 für die Bundesverwaltung bei der Auswahl ihrer Informationstechnologien verbindlich.«[31] SAGA legt mit abgestuften Verbindlichkeitsgraden konkrete Normen und Standards für die verschiedenen Funktionsbereiche eines IT-Systems fest. Hiermit ist es eine Übersicht und Auswahl der als relevant erachteten IT-Standards für die öffentliche Verwaltung. Obwohl sich SAGA vornehmlich an staatliche Stellen richtet, ist es auch für die öffentliche IT generell von Interesse. Neben verwaltungsinterner Interoperabilität wird auch Interoperabilität mit Dritten geschaffen, die Lösungen auf Basis derselben Standards einsetzen.

2.4 STANDARDISIERUNGS-PROZESSE

Für die Standardisierung öffentlicher IT stehen insbesondere folgende Prozesse zur Verfügung:

- Aktive Mitarbeit in Normungsgremien und mandatierte Normung
- Aktive Mitarbeit in Standardisierungsforen und -konsortien
- Staatliche und staatlich koordinierte Erarbeitung von Standards
- Empfehlung existierender Normen und Standards
- Staatliche Verbindlichmachung existierender Normen und Standards
- Direkte staatliche Standardsetzung durch Gesetze und Verordnungen
- Erarbeitung proprietärer Standards durch Industriegruppierungen oder einzelne Hersteller

»Die öffentliche Hand, Unternehmen, Verbände und akademische Einrichtungen haben die Möglichkeit, aktiv an der Normungsarbeit von DIN und DKE teilzunehmen.«

[30] SAGA ist mittlerweile ein Eigenname. Es stand ursprünglich für »Standards und Architekturen für E-Government-Anwendungen«.
[31] http://www.cio.bund.de/DE/Architekturen-und-Standards/SAGA/saga_node.html

Aktive Mitarbeit in Normungsgremien und mandatierte Normung

Die öffentliche Hand, Unternehmen, Verbände und akademische Einrichtungen haben die Möglichkeit, aktiv an der Normungsarbeit von DIN und DKE teilzunehmen. Begründete nationale Normungsanträge kann prinzipiell jeder bei DIN und DKE stellen. Die Bundesregierung hat Anspruch auf bevorzugte Bearbeitung von Normungsgegenständen, die im öffentlichen Interesse sind.

Das DIN klärt, ob Bedarf an den beantragten Normungsprojekten besteht und ob die Normung auf nationaler, europäischer oder internationaler Ebene erfolgen soll. Für die Annahme eines Normungsprojektes sind außerdem ausreichend Mittel (durch Zahlungen der interessierten Mitglieder) erforderlich.[32] Die breite Mitgliederstruktur des DIN bietet eine gute Grundlage, nationale Normungsprojekte mit einer breiten Mischung von Experten aus den betroffenen Bereichen besetzen zu können. Die Öffentlichkeit kann sich über geplante Normungsprojekte informieren und dazu Stellung nehmen.

Ein nationales Normungsprojekt erstellt zunächst einen Normentwurf. Für einen inhaltlich hochwertigen Entwurf und einen zügigen Entwurfsprozess ist die aktive Mitarbeit entsprechender Experten unverzichtbar. Wenn im zuständigen Arbeitskreis über die Veröffentlichung des Entwurfs Konsens erreicht ist, wird er zur öffentlichen Kommentierung bereitgestellt. Die Verabschiedung einer deutschen Norm erfolgt nach angemessener Bearbeitung aller Kommentare (ggf. durch ein Schlichtungs- oder Schiedsverfahren) und einem Konsens über den endgültigen Text.

Soll die **Normung auf europäischer oder internationaler** Ebene erfolgen, so stellt das DIN einen Normungsantrag bei der zuständigen europäischen oder internationalen Normungsorganisation. Die Erarbeitung und Verabschiedung der Norm findet ähnlich der nationalen Normung statt. Die einzelnen Entwurfsstufen und Abstimmungsmodalitäten sind im Detail anders. Auf europäischer und internationaler Ebene ist für die Veröffentlichung einer Norm i. d. R. kein vollständiger Konsens, sondern bereits eine qualifizierte (teils auch gewichtete) Mehrheit der nationalen Stimmen ausreichend. Die Experten für die Normungsprojekte bei CEN, CENELEC, ISO und IEC müssen vom DIN bzw. der DKE akkreditiert werden. Diese delegierten Experten vertreten dann die Position ihres jeweiligen Landes in der europäischen bzw. internationalen Normungsarbeit. Entscheidungen über die Delegation werden in den jeweiligen nationalen Normungsgremien getroffen.

Sieht die öffentliche Hand **EU-weiten Normungsbedarf** für einen Bereich, kann sie darauf hinwirken, dass die EU einen entsprechenden Auftrag (ein Mandat) an eine oder mehrere europäische Normungsorganisationen (CEN, CENELEC und ETSI) erteilt.[33] Nach Annahme des Mandates erfolgt die nationale Zuarbeit über die zuständigen Gremien der nationalen Normungsorganisationen. Verabschiedet wird eine auf diesem Weg entstandene, harmonisierte Norm auf dem üblichen Weg für europäische Normen. Für die Bearbeitung der Mandate können auf allen beteiligten Ebenen EU-Zuschüsse gewährt werden.

»Die Bundesregierung hat Anspruch auf bevorzugte Bearbeitung von Normungsgegenständen, die im öffentlichen Interesse sind.«

[32] Die öffentliche Hand sowie Universitäten, nicht jedoch außeruniversitäre Forschungseinrichtungen, sind von der Zahlung befreit.

[33] Bisher wurden Mandate vornehmlich erteilt, wenn Gesundheitsschutz, Umweltschutz oder Energieverbrauch, physische Interoperabilität oder Koexistenz (z. B. Frequenznutzung) oder transnationale Wirtschaftsprozesse (z. B. Rechnungsstellung, Maut) betroffen waren. Auch in den Bereichen elektronische Signatur, E-Health, intelligente Transportsysteme und Smart Metering/Smart Grid wurden bereits Mandate erteilt.

DEUTSCHE BEHÖRDEN BETREIBEN AUCH STANDARDISIERUNG IN EIGENREGIE.

Aktive Mitarbeit in Standardisierungsforen und -konsortien

Standardisierungsforen und -konsortien haben sehr unterschiedliche Mitgliedschafts-, Beteiligungs- und Abstimmungsmodelle. In der Regel ist jedoch eine aktive, kontinuierliche Beteiligung natürlicher Personen am Standardisierungsprozess erforderlich, um bei Abstimmungen berücksichtigt zu werden. Auch für die Foren und Konsortien gilt, dass ein hochwertiger Standard nur durch die Mitarbeit entsprechender Experten erzielbar ist.

Staatliche und staatlich koordinierte Erarbeitung von Standards

Deutsche Behörden betreiben auch Standardisierung in Eigenregie.

Hier ist zunächst der **IT-Planungsrat**[34] zu nennen, der mit der IT-Koordinierung von Bund und Ländern beauftragt ist und in diesem Rahmen u. a. die Aufgabe hat, Bedarfe für einheitliche Standards von Bund und Ländern festzulegen und fachunabhängige und fachübergreifende IT-Interoperabilitäts- und -Sicherheitsstandards verbindlich vorzugeben. Die rechtliche Grundlage hierfür bildet der IT-Staatsvertrag zwischen Bund und Ländern.[35]

Die Koordinierungsstelle für IT-Standards (**KoSIT**)[36] unterstützt den IT-Planungsrat hierbei. Zu ihren Aufgaben gehört u. a. die Koordinierung der Entwicklung und Nutzung von IT-Standards für den Datenaustausch in der öffentlichen Verwaltung. Konkret wird durch die KoSIT die Erstellung von auf XML basierenden Datenaustauschstandards (**XÖV**-Standards) koordiniert.

Für den Bereich der Innenverwaltung ist von der Innenministerkonferenz die **»Projektgruppe Standard«** eingerichtet worden, die die Aufgabe hat, »die Interoperabilität im Bereich des elektronischen Datenaustauschs der Innenverwaltung (Meldewesen, Personenstandswesen und Ausländerwesen) sicherzustellen«.[37] Diese hat ebenfalls die KoSIT mit der entsprechenden Koordination beauftragt. Die KoSIT kann in ähnlicher Weise auch von anderen Bund-Länder-Gremien beauftragt werden.

Die Standards werden von Vertretern der öffentlichen Hand, teilweise auch unter Beteiligung von z. B. Fachverfahrensherstellern, erarbeitet. Wenn sie aus einem gemeinsamen Bedarf resultieren, können sie abschließend wiederum vom IT-Planungsrat für Bund und Länder verbindlich gemacht werden. Diese staatlichen Standards sind vorrangig für den Gebrauch in und insbesondere zwischen Verwaltungen ausgelegt und geeignet.

Ein weiterer Bereich der staatlichen bzw. staatlich koordinierten Standardisierung ist die Erstellung von (sicherheitstechnischen) Mindeststandards, IT-Grundschutz-Standards und Technischen Richtlinien durch das Bundesamt für Sicherheit in der Informationstechnik (BSI). Während die Mindeststandards vornehmlich für den Einsatz durch Bundesbehörden entwickelt werden, sind die IT-Grundschutz-Standards und die Technischen Richtlinien sowohl auf Behörden als auch auf Unternehmen hin ausgerichtet. Die BSI-Dokumente können durch Gesetze, Verordnungen und Verwaltungsvorschriften (in deren jeweiligem Geltungsbereich) verbindlich gemacht werden.

»Standardisierungsforen und -konsortien haben sehr unterschiedliche Mitgliedschafts-, Beteiligungs- und Abstimmungsmodelle.«

[34] http://www.it-planungsrat.de/DE/Home/home_node.html
[35] http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/it_planungsrat_1.html
[36] http://www.it-planungsrat.de/DE/Organisation/KoSIT/KoSIT_node.html
[37] http://www1.osci.de/detail.php?gsid=bremen76.c.6618.de

DIE ÖFFENTLICHE HAND KANN MITTELS VERSCHIEDENER MECHANISMEN DIE ANWENDUNG EXISTIERENDER NORMEN UND STANDARDS VERBINDLICH VORGEBEN.

Empfehlung existierender Normen und Standards

Die öffentliche Hand, Verbände, Nutzergruppen und andere (bis hin zu einzelnen Unternehmen) können die Verwendung konkreter Normen und Standards für ihren unmittelbaren Zuständigkeitsbereich, aber auch für die darüber hinausgehende Zusammenarbeit empfehlen. Damit lässt sich naturgemäß nur ein Regelungsbedarf befriedigen, für den bereits geeignete Normen oder Standards vorhanden sind. Durch eine solche Empfehlung ist aufgrund der fehlenden Verbindlichkeit jedoch in der Praxis noch keine Interoperabilität sichergestellt.

Staatliche Verbindlichmachung existierender Normen und Standards

Die öffentliche Hand kann mittels verschiedener Mechanismen die Anwendung existierender Normen und Standards verbindlich vorgeben. Dies kann durch Verweisung in Gesetzen und Verordnungen, für die Verwaltungen von Bund und Ländern darüber hinaus durch Beschluss des IT-Planungsrats und für den Bereich der Bundesverwaltung auch durch Beschluss des IT-Rats erfolgen.

Durch einen Gesetzes- oder Verordnungsverweis erlangt eine Technische Richtlinie des Bundesamtes für Sicherheit in der Informationstechnik (BSI) oder ein von diesem erstelltes Schutzprofil nach den Common Criteria (ISO/IEC 15408) unmittelbare Verbindlichkeit für den Geltungsbereich des Gesetzes oder der Verordnung.[38]

Direkte staatliche Standardsetzung durch Gesetze und Verordnungen

Indem in Gesetzen und Verordnungen direkt (ohne Verweis auf entsprechende Normen oder existierende Standards) konkrete Anforderungen an Produkte und Dienstleistungen festgesetzt werden, werden implizit Standards – z. B. bezüglich der Leistung, Qualität oder Sicherheit von Produkten – formuliert.

Erarbeitung proprietärer Standards durch Industriegruppierungen oder einzelne Hersteller

Unabhängig von der öffentlichen Hand können auch proprietäre Industrie- und Herstellerstandards entstehen, die für den Bereich der öffentlichen IT relevant sind. Die zugehörigen Standardisierungsprozesse und entstehenden Standards sind hier stark von den jeweiligen Akteuren abhängig, von ihren Interessen geprägt und nur begrenzt bis gar nicht durch die öffentliche Hand zu beeinflussen.

»Unabhängig von der öffentlichen Hand können auch proprietäre Industrie- und Herstellerstandards entstehen, die für den Bereich der öffentlichen IT relevant sind.«

[38] Beispiele: Smart Meter (Energiewirtschaftsgesetz), Gesundheitskarte, Heilberufsausweise (Sozialgesetzbuch), digitale Signatur, digitaler Fahrtenschreiber, neuer Personalausweis, De-Mail.

3. HERAUSFORDERUNGEN

Vor dem Hintergrund des im vorangehenden Kapitel geschilderten Status und der zukünftigen Entwicklung von öffentlicher IT und ihrer Standardisierung ergeben sich eine Reihe wichtiger Herausforderungen, die im Folgenden beschrieben werden.

Bedeutungszuwachs öffentlicher IT

Mit der umfassenden Digitalisierung von Gesellschaft, Wirtschaft, Verwaltung und Politik hat die Informationstechnik einen Stellenwert erreicht, der sie zu einem entscheidenden Faktor für das Funktionieren des öffentlichen Raums macht. Öffentliche IT gewinnt daher zunehmend an Bedeutung, der durch eine adäquate Standardisierung Rechnung getragen werden muss.

Fachliche Breite

Öffentliche IT erschöpft sich nicht im E-Government, sondern reicht weit darüber hinaus. Auch in den Bereichen Gesundheitswesen, Energieversorgung und vielen weiteren stellt IT einen zentralen Baustein für die Kommunikation zwischen den Akteuren der Wirtschaft, der Zivilgesellschaft und der öffentlichen Hand dar. Für all diese Bereiche bedarf es geeigneter und aufeinander abgestimmter fachunabhängiger, fachspezifischer und fachübergreifender IT-Standards.

Komplexität und Dynamik der Technologie

Systeme der Informations- und Kommunikationstechnologie gehören zu den komplexesten Systemen unserer Zeit. Sie unterliegen zusammen mit ihren Technologien und Paradigmen zudem einer intensiven Entwicklungs- und Änderungsdynamik. Auch für den Teilbereich der öffentlichen IT stellen diese Rahmenbedingungen die Standardisierung vor besondere Herausforderungen.

Langwierigkeit von Standardisierungsprozessen

Ein generelles Problem von Standardisierungsprozessen ist deren Dauer von der Entstehung eines Bedarfs über die Initiierung eines Normungs- bzw. Standardisierungsvorhabens bis zur Veröffentlichung und ggf. Verbindlichmachung eines Standards. Bei internationalen Normen sind 3 - 5 Jahre von der Initiierung bis zur Veröffentlichung durchaus keine Ausnahme[39], auch wenn mittlerweile kürzere Fristen angestrebt werden. Die Zeit bis zur Umsetzung im und für den öffentlichen Raum kommt noch hinzu. Im schnelllebigen IT-Bereich besteht damit die Gefahr, dass Standards nicht zur Verfügung stehen, wenn sie gebraucht werden, und von der technologischen Entwicklung bereits überholt sind, wenn sie erscheinen.

Berücksichtigung der Stakeholder

Mit ihrer fachlichen Breite und der Komplexität der ihr zugrunde liegenden Technologien verfügt öffentliche IT über eine umfangreiche und vielschichtige Stakeholder-Struktur. Diese gilt es in angemessener Weise bei Standardisierungsprozessen – sowohl auf der nationalen als auch auf der europäischen und

»Mit ihrer fachlichen Breite und der Komplexität der ihr zugrunde liegenden Technologien verfügt öffentliche IT über eine umfangreiche und vielschichtige Stakeholder-Struktur.

[39] Zur Normung im Bereich Cloud Computing wurde beispielsweise auf ISO/IEC-Ebene im Jahr 2009 das Sektorkommitee SC38 (Distributed Application Platforms and Services) und hierin die Arbeitsgruppe WG3 (Cloud Computing) gegründet. Aktuell (März 2014) liegen mit ISO/IEC DIS 17788 und ISO/IEC DIS 17789 die ersten Normentwürfe zum Cloud Computing als internationale Normentwürfe vor. Mit der Veröffentlichung als internationale Normen ist im weiteren Verlauf des Jahres 2014 zu rechnen.

NORMEN UND STANDARDS BIETEN EIN HOHES MASS AN INVESTITIONSSICHERHEIT, WENN UND SOLANGE SIE FÜR DAS EINSATZUMFELD ANGEMESSEN SIND.

der internationalen Ebene – zu berücksichtigen und in diese einzubeziehen. Dies kann durch die Offenheit der Verfahren alleine nicht immer gewährleistet werden: Unterschiedliche Organisierbarkeit von Interessen, politische Priorisierungen und Verfügbarkeit von Ressourcen können beispielsweise einer angemessenen Beteiligung entgegenstehen. Insbesondere die Interessen der Allgemeinheit und der Verbraucher sind aus diesen Gründen bislang eher unterrepräsentiert.

Balance zwischen Dauerhaftigkeit und Flexibilität

Normen und Standards bieten ein hohes Maß an Investitionssicherheit, wenn und solange sie für das Einsatzumfeld angemessen sind. Das sehr dynamische Einsatzumfeld IT kann häufige Anpassungen erforderlich machen, wenn nicht die Normen und Standards von vornherein eine große und vorausschauende Flexibilität besitzen, was jedoch wiederum zu einer hohen Komplexität führen kann.

Grenzen der Standardisierungsnotwendigkeit

Normung, Standardisierung und insbesondere die Verbindlichmachung von Normen und Standards muss sich auf den notwendigen Umfang beschränken. Speziell eine Überregulierung wirkt innovationshemmend und verursacht vermeidbare Kosten, wenn sachlich unnötige Anforderungen erfüllt werden müssen.

Überblick über Standards und Standardisierungsvorhaben

Die Vielfalt der Standards und Standardisierungsgremien mit faktischer IT-Relevanz und die enge Verzahnung zahlreicher Komponenten miteinander erschweren die Identifikation der für einen gegebenen Bedarf bereits existierenden Standards und Standardisierungsvorhaben.

Überblick über in Gesetzen und Verordnungen referenzierte Standards

Wenn Standards geändert werden müssen, auf die in Gesetzen oder Verordnungen verwiesen wird, sind die daraus resultierenden Folgen schwer abschätzbar, weil kein systematischer Vorwärtsbezug zwischen den Standards und den betroffenen Gesetzen und Verordnungen existiert. Die Verantwortung, Gesetze und Verordnungen mit den referenzierten Standards in Einklang zu halten, liegt in der Regel bei der Legislative. Der explizite Bezug auf eine bestimmte Version eines Standards löst dieses Problem. Verweisen jedoch unterschiedliche Gesetze oder Verordnungen auf unterschiedliche Versionen eines Standards, kann dies neue Probleme verursachen.

4. LÖSUNGSANSÄTZE

Im Folgenden werden abschließend und thesenartig einige Lösungsansätze skizziert, mit denen den identifizierten Herausforderungen der Standardisierung öffentlicher IT begegnet werden kann.

Systematisierung der Standardisierungsprozesse der öffentlichen Hand

Die Standardisierungsprozesse der öffentlichen Hand im Bereich IT sind historisch und föderal bedingt unterschiedlich organisiert.[40] Wegen der föderalen Struktur der öffentlichen Verwaltung sind staatliche IT-Standards zudem i. d. R. nur jeweils für bestimmte Teilbereiche der öffentlichen Hand und des öffentlichen Raums verbindlich. Wegen der gestiegenen und weiter steigenden Bedeutung öffentlicher IT bietet es sich an, diese Prozesse stärker zu systematisieren und geeignet zu institutionalisieren.

Erhöhung der Transparenz und stärkere Einbeziehung der Stakeholder

Staatlich und staatlich koordiniert erarbeitete IT-Standards sind bisher eher auf verwaltungsinterne Anforderungen zugeschnitten als auf die weitergehenden Anforderungen des öffentlichen Raums, welcher Wirtschaft, Bürger und Zivilgesellschaft mit einbezieht. Daher sollten die Transparenz dieser Standardisierungsprozesse erhöht und die verschiedenen Stakeholder-Gruppen öffentlicher IT stärker mit einbezogen werden. Dies gilt insbesondere für technische Experten hinsichtlich der Umsetzung der Standards.

Verbesserte und breitere Nutzung der Normungsorganisationen

Im Sinne einer Systematisierung und Institutionalisierung sollte auch überlegt werden, ob und falls ja welche (Teile von) IT-Standards der öffentlichen Hand evtl. besser in den Normungsorganisationen auf deutscher, europäischer oder internationaler Ebene (DIN/DKE, CEN/CENELEC/ETSI, ISO/IEC/ITU) mit ihren bewährten Strukturen und Prozessen aufgehoben sein könnten. Die öffentliche Hand könnte in diesen Fällen durch eine aktive Mitwirkung in den jeweils zuständigen Normungsgremien ihre Sicht und Interessen als Stakeholder einbringen. So entwickelte und fortgeschriebene Normen könnten dann gegebenenfalls für bestimmte Verantwortungsbereiche der öffentlichen Hand verbindlich umgesetzt werden. Die Einbeziehung der Stakeholder würde bei diesem Vorgehen durch die entsprechenden Mechanismen der Normungsorganisationen gewährleistet.

Stärkere Orientierung auf europäische und internationale Standards

Der öffentliche Raum macht nicht an nationalen Grenzen halt. Die bestehenden IT-Standards der öffentlichen Hand sollten daher dahingehend überprüft werden, ob es vergleichbare Standards oder Standardisierungsvorhaben auf europäischer und internationaler Ebene gibt und welche Möglichkeiten zur Vereinheitlichung ggf. bestehen. Zudem sollte geprüft werden, ob und wie bestehende deutsche IT-Standards der öffentlichen Hand (oder geeignete Teile solcher Standards) zu europäischen oder internationalen Standards weiterentwickelt werden können.

Stärkung offener und freier Standards

Nicht jeder IT-Standard mit Relevanz für den öffentlichen Raum kann und sollte durch die nationalen, europäischen und internationalen Normungsorganisationen oder durch die öffentliche Hand selbst entwickelt werden. Oftmals führen De-facto-Standards von Herstellern, Industriekonsortien oder nicht-staatlichen Standardisierungsorganisationen schneller und flexibler

[40] Beispiele für unterschiedlich organisierte staatliche Standardisierungsaktivitäten sind SAGA, XÖV sowie Technische Richtlinien und Mindeststandards des BSI.

zur Durchsetzung neuer Technologien am Markt, als es mit dem konsensorientierten und tendenziell langwierigeren Prozess einer formalen Normung möglich ist. Da proprietäre Standards allerdings Wettbewerbsbeschränkungen mit sich bringen können, sollten insbesondere die Erstellung, Fortschreibung und Nutzung offener und freier Standards gefördert werden. Hierzu können beispielsweise offene und freie Standards bei der Beschaffung durch die öffentliche Hand gegenüber proprietären Standards bevorzugt werden. Auch kann die öffentliche Hand bei der Entwicklung und Fortschreibung offener und freier Standards eine aktive Rolle einnehmen.

Orientierung auf funktionale Standards

Um technologische Innovationen und Weiterentwicklungen des Marktes im Bereich öffentlicher IT nicht durch zu restriktive Festlegungen zu behindern, sollten, wo dies sinnvoll und möglich ist, Standards, die einheitliche Anforderungen festlegen, gegenüber Standards, die bestimmte Lösungen zur Erfüllung der Anforderungen festschreiben, bevorzugt werden.

Übertragen auf öffentliche IT bedeutet dies, dass es in der Regel ausreicht, funktionale und organisatorische Komponenten eines IT-Systems zu identifizieren und deren jeweilige Schnittstellen zu anderen Komponenten und geeignete Qualitäts- und Sicherheitsanforderungen festzulegen. Die konkrete interne Umsetzung der Funktionen einer Komponente kann hingegen dem Hersteller überlassen werden.

Agile Fortschreibung

Öffentliche IT befindet sich – wie Informationstechnologie generell – in einem besonders dynamischen Prozess ständiger Innovationen und Weiterentwicklungen. Daher ist es wichtig, die für den öffentlichen Raum relevanten IT-Standards kontinuierlich zu überprüfen und bei Bedarf zeitnah anzupassen. Dazu gehört auch, dass – wo dies erforderlich wird – neue Standardisierungsvorhaben kurzfristig initiiert und umgesetzt und nicht mehr benötigte Standards zeitnah identifiziert und zurückgezogen werden können und dass verbindliche Vorgaben von IT-Standards durch die öffentliche Hand in regelmäßigen Abständen auf Notwendigkeit und Alternativen hin überprüft werden.

Die agile Fortschreibung muss allerdings so erfolgen, dass dadurch die Standardisierungsziele Wirtschaftlichkeit, Zukunftsfähigkeit und Nachhaltigkeit nicht beeinträchtigt werden. Sorgfältig geplante und abgestimmte Fortschreibungszyklen müssen eine angemessene Balance zwischen Fortschreibungsbedarf einerseits und Dauerhaftigkeit von Standards und den darauf beruhenden Produkten andererseits gewährleisten.

Entwicklung einer Standardisierungsstrategie für öffentliche IT

Auf Basis des Vorhandenen und mit Blick auf die aktuellen und zukünftigen Herausforderungen sollte durch die öffentliche Hand unter Einbeziehung der verschiedenen Stakeholder-Gruppen eine systematische Strategie für die Standardisierung öffentlicher IT entwickelt werden. Hierbei sollten insbesondere die Ziele bestimmt, Kriterien für die Bewertung der Ergebnisse erarbeitet und geeignete Prozesse und Strukturen festgelegt werden.

GEFÖRDERT VOM

Bundesministerium
des Innern

KONTAKT

Jens Fromm
Leiter Kompetenzzentrum Öffentliche IT (ÖFIT)
Tel.: +49 30 3463-7173
Fax: +49 30 3463-99-7173
info@oeffentliche-it.de

Fraunhofer-Institut für
Offene Kommunikationssysteme FOKUS
Kaiserin-Augusta-Allee 31
10589 Berlin

www.fokus.fraunhofer.de
www.oeffentliche-it.de

kre | 1405 (Fotos: Steffen Konegen)