2013

Eine Bestandsaufnahme von Standardisierungspotentialen und -lücken im Cloud Computing

Robin Fischer
Karlsruher Institut für Technologie (KIT), Karlsruhe, Germany, robin.fischer@kit.edu

Christian Janiesch
Karlsruher Institut für Technologie (KIT), Karlsruhe, Germany, christian.janiesch@kit.edu

Joachim Strach
Booz & Company, München, Germany, joachim.strach@booz.com

Nicolai Bieber
Booz & Company, München, Germany, nicolai.bieber@booz.com

Wolfgang Zink
Booz & Company, München, Germany, wolfgang.zink@booz.com

See next page for additional authors

Authors
Robin Fischer, Christian Janiesch, Joachim Strach, Nicolai Bieber, Wolfgang Zink, and Stefan Tai

Eine Bestandsaufnahme von Standardisierungspotentialen und -lücken im Cloud Computing

Robin Fischer[1], Christian Janiesch[1], Joachim Strach[2],
Nicolai Bieber[2], Wolfgang Zink[2], und Stefan Tai[1]

[1] Karlsruher Institut für Technologie (KIT), Karlsruhe, Germany
{robin.fischer,christian.janiesch,stefan.tai}@kit.edu
[2] Booz & Company, München, Germany
{joachim.strach,nicolai.bieber,wolfgang.zink}@booz.com

Abstract. Die Standardisierung im Cloud Computing ist erst im Entstehen begriffen. Sie gewinnt jedoch zunehmend an Eigendynamik. Bisherige Standardisierungsbemühungen stecken konzeptionell in den Kinderschuhen, da uneinheitliche Definitionen und fehlendes Orientierungswissen ein zielorientiertes Handeln behindern. Die vorliegende Arbeit schlägt deshalb eine konsistente Taxonomie für die strukturierte Betrachtung und begriffliche Eindeutigkeit bei der Beschreibung und Bewertung von Standards vor. Darauf aufbauend wird ein Vorgehensmodell zur Analyse der aktuellen Standardisierungslage vorgestellt. Dieses verwendet eine Standardisierungslandkarte, die das Forschungsfeld anhand der Dimensionen Herausforderungen und Ansatzpunkte aufspannt. Die vorgenommene Analyse erfasst gegenwärtige Standardisierungspotentiale und -lücken im Cloud Computing. Die abschließend vorgenommene Bewertung zeigt Handlungsoptionen künftiger Standardisierungsbemühungen auf.

Keywords: Cloud Computing, Standards, Übersicht, Potentiale, Lücken

1 Einleitung

Cloud Computing ermöglicht den bedarfsgerechten Bezug von Speicherkapazitäten, Rechenleistung und Anwendungen über das Internet. Der Einsatz von Cloud-Diensten ist dabei mit einer nutzungsbezogenen Abrechnung der verwendeten Ressourcen gekoppelt, so dass Investitionskosten reduziert werden können [1].

Anwender von Cloud Computing sehen sich bei der Auswahl und Bewertung von passenden Cloud-Diensten einer Reihe von Herausforderungen ausgesetzt (vgl. bspw. [2]). Das Fehlen einer einheitlichen Begriffswelt, die über die Unterteilung von Cloud Computing über Anwendungs-, Plattform- und Infrastruktur-Dienste hinausgeht, erschwert es Anwendern einzuschätzen, inwieweit ein Cloud-Dienst ihren Bedürfnissen gerecht wird [3]. Das liegt auch daran, dass es nur vereinzelt Standards gibt, die zentrale Aspekte des Cloud Computing, wie bspw. Protokolle und Schnittstellen, Service Level Agreements (SLA) oder rechtliche Vorgaben einheitlich regeln und damit für einen Vergleich herangezogen werden könnten. Dies hemmt die Akzeptanz von

11th International Conference on Wirtschaftsinformatik,
27th February – 01st March 2013, Leipzig, Germany

Cloud-Diensten bei potentiellen Anwendern, insbesondere im Mittelstand, und behindert die Entwicklung von interoperablen und offenen Cloud-Diensten.

Wir haben durch die Sichtung von etwa 160 potentiell für das Cloud Computing relevanten Standards sowie durch eingehende Betrachtung einer Auswahl davon eine Standardisierungslandkarte erstellt. Diese katalogisiert die nach unserer Erhebung relevantesten Standards. Die so nach einheitlichen Kriterien erstellte Übersicht für Standards im Cloud Computing, soll Anwender von Cloud-Diensten bei der Auswahl der für ihre Bewertung von Cloud-Diensten relevanten Standards leiten und damit einen standardisierten Vergleich von Cloud-Diensten ermöglichen. Wir haben darüber hinaus eine Potential- und Lückenanalyse durchgeführt, die anhand der entwickelten Standardisierungslandkarte weiteren Standardisierungsbedarf aufzeigt.

Im Folgenden erläutern wir kurz das der Arbeit zugrundeliegende Verständnis von Cloud Computing und Standards und gehen auf verwandte Untersuchungen ein. In Kapitel 3 erläutern wir ausführlich das Vorgehen bei der Erhebung der Standards, den Aufbau der Standardisierungslandkarte sowie das Vorgehen bei der Potential- und Lückenanalyse. Die überblicksartige Einordnung der Standards und eine zusammenfassende Diskussion der Potentiale und Lücken finden in Kapitel 4 statt. Kapitel 5 fasst die Ergebnisse zusammen und versucht Handlungsempfehlungen zu geben.[1]

2 Definitionen und verwandte Arbeiten

2.1 Cloud Computing

Das Zusammenspiel von Infrastrukturkomponenten (Server, Speicher, Netze, Middleware) und verfügbaren Diensten erscheint dem Anwender als *Wolke* möglicher Computer- und Kommunikationsanwendungen, wodurch der Begriff des Cloud Computing geprägt wurde. Cloud Computing bietet demnach die Möglichkeit, Speicherkapazitäten, Rechenleistung und Anwendungen nach kundenspezifischen Bedarfen als Dienst über das Internet zu beziehen. Die so ermöglichte bedarfsgerechte, skalierbare und flexible Nutzung von IT-Diensten wird unterstützt durch neuartige Geschäftsmodelle, bei denen die Abrechnung je nach Funktionsumfang, Nutzungsdauer und Anzahl der Nutzer erfolgt [1].

Als Servicemodelle werden Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) und Software-as-a-Service (SaaS) unterschieden (ausführliche Informationen dazu finden sich bspw. bei [1], [4]). Unter Betriebs-, Eigentums- und Organisationsaspekten können Private Clouds (für eine geschlossene Nutzergruppe) und Public Clouds (für eine große Anzahl verschiedener Nutzer) unterschieden werden. In

[1] Die Studie „Das Normierungs- und Standardisierungsumfeld von Cloud Computing“ wurde im Rahmen des Technologieprogramms Trusted Cloud des Bundesministeriums für Wirtschaft und Technologie (BMWi) durchgeführt und ist unter http://www.trusted-cloud.de/ abrufbar. Dieser Artikel derselben Autoren stellt eine aktualisierte Fassung dar, die das wissenschaftliche Vorgehen in den Vordergrund stellt. Bei der ausführlichen Studie liegt der Fokus mehr auf der Einzelbewertung von Standards und Standardisierungsinitiativen.

der Realität finden sich auch Nutzungskombinationen (Hybrid Clouds) von Private Clouds, Public Clouds und traditionellen on-premise IT-Umgebungen [4].

2.2 Standardbegriff

Die Anwendung von Standards ist freiwillig. In ihnen selbst liegt keine Verbindlichkeit. Eine Anwendungspflicht kann sich jedoch aufgrund von Gesetzen, Rechts- oder Verwaltungsvorschriften, Verträgen oder sonstigen Rechtsgründen ergeben. In der Praxis können Standards zudem durch weichere Steuerungsinstrumente bzw. ihre Bedeutung im Markt Verbindlichkeit entfalten. Wir betrachten im Folgenden nicht nur Standards im engeren Sinn, die durch ein Standardisierungsgremium verabschiedet werden [5], sondern auch Vorarbeiten, Vorgaben und Zertifizierungen.

Der Begriff Cloud-Standards steht dabei vereinfachend und als Sammelbegriff für Orientierungswissen, Spezifikationen, Standards im engeren Sinne, Normen, und rechtliche Vorgaben (Rechtsnormen). In engem Bezug zu Standards stehen (Referenz-)Implementierungen. Diese umfassen etablierte Cloud-Dienste, APIs, Testbeds oder Plugfests. Für Standards sind sie von vorbereitender oder ergänzender Natur, die die Praktikabilität im Einsatz zeigen oder andeuten. Referenzimplementierungen basieren in der Regel auf einer Spezifikation für einen Standard (auch Entwürfen hierfür) oder einem Standard.

Neben der Klassifizierung von Standards steht der Begriff der *Zertifizierung* in einem orthogonalen Zusammenhang: Anbieter und Anwender von Cloud-Diensten, können zur Bestätigung der Einhaltung bestimmter Kriterien, Standards oder rechtlichen Vorgaben *Zertifikate* erwerben. Die Aussagekraft von Zertifikaten wie auch die Nachvollziehbarkeit des Vorgangs der Zertifizierung steigt dabei mit dem Grad der Formalisierung und Verbindlichkeitswirkung.

2.3 Andere Arbeiten zu Cloud-Standards

Jeffery and Burkhard Neidecker-Lutz [6] beschreiben offene Herausforderungen sowie den gegenwärtigen State-of-the-Art im Cloud Computing. Dabei erfolgt auch eine Priorisierung von Handlungsfeldern zur Adressierung der Herausforderungen. Die Smart Cloud Study Group [7] beschreibt Herausforderungen und Potentiale des Cloud Computing im Allgemeinen.

Frameworks der European Network and Information Security Agency (ENISA) [8] sowie der Cloud Security Alliance (CSA) [9] fokussieren Sicherheitsaspekte im Cloud Computing. EuroCloud [10] bietet einen weiteren Überblick und Lösungsansätze. Weiterhin gibt die ENISA [11] einen Überblick über Erwartungen und Hindernisse des Cloud Computing speziell für den europäischen Mittelstand. In der Cloud Control Matrix (CCM) [12] werden für das Management von Cloud-Diensten relevante Herausforderungen (engl. *control areas*) identifiziert und Empfehlungen zur Ausübung der Steuerung (engl. *control specification*) dargestellt. Die CSA [13] nennt weitere Herausforderungen beim Management von Cloud-Diensten und setzt diese in Bezug zu Herausforderungen beim Management von IT-Systemen aus bspw. COBIT 4.1, ISO 27001 oder NIST SP800. Auch die Cloud Computing Use Case Discussion

Group [14] hat Anwendungsfälle für Cloud Computing erarbeitet. Einen weiteren kurzen Überblick von Standards gegliedert nach Forschungsfeldern (engl. *study areas*) verschafft [15].

Das National Institute of Standards and Technology (NIST) [16] analysiert die Standardisierungslandschaft im Cloud Computing und leitet Handlungsempfehlungen zur Standardentwicklung und -adaption ab. Zur Bewertung und Klassifizierung der Standards werden hier konkret auf die öffentliche Verwaltung der USA zugeschnittene Szenarien verwendet [17]. Die Internet Engineering Task Force (IETF) [18] gibt einen Überblick zu aktuellen Standardisierungsinitiativen und Standards. Eine Taxonomie wird dabei nicht verwandt. Das vom NIST initiierte Cloud Standards Wiki[2] listet existierende Cloud-Standards ohne diese zu klassifizieren. Das zur Erstellung der Liste verwendete methodische Vorgehen ist nicht dokumentiert. Das ITU Telecommunication Standardization Bureau [19] bietet eine Auflistung von Aktivitäten zur Cloud-Standardisierung. Auch hier wird keine Taxonomie zur Kategorisierung der gelisteten Standards verwendet.

3 Methodischer Teil

3.1 Auswahlverfahren der betrachteten Standards

Die Untersuchung der Standardisierung im Cloud Computing basiert auf einer umfassende Primär- und Sekundärrecherche der in Abschnitt 2.3 angeführten Arbeiten sowie Cloud-Standards entsprechend der obigen Definition. Ergänzend dazu wurden auch aktuelle Forschungsergebnisse gesichtet, insb. aus dem 7. Forschungsrahmenprogramm der EU, um ein umfassenderes Bild aktueller Entwicklungsströme zu bekommen. Die dieser Arbeit zu Grunde liegende Untersuchung war maßgeblich für das Standardverständnis des Technologieprogramms *Trusted-Cloud*[3], in dessen Rahmen sie durchgeführt wurde. Zwischenergebnisse der Studie wurden in Interviews mit Experten aus Trusted-Cloud-Projekten validiert und wurden durch die Analyse der durch Fragebögen in der Trusted-Cloud-Community erhobenen Daten substantiiert. Die Ergebnisse der Untersuchung wurden abschließend in Workshops zur Diskussion gestellt. Der Teilnehmerkreis umfasste dabei nationale Standardisierungsbeteiligte aus dem Trusted-Cloud-Programm.

Die Analyse begann mit einer breiten Sichtung möglicher Akteure, Initiativen und Standards im Cloud Computing. Der verfolgte Analyseansatz besteht aus vier Schritten: Fokus, Auswahl, Einzelbewertung und zusammenfassende Bewertung.

Zunächst fanden eine Festlegung des Fokus der Untersuchung und eine Eingrenzung der Rechercheergebnisse statt, die näher betrachtet werden. Wir unterscheiden Standards, die einen expliziten Bezug zum Cloud Computing haben, von Standards, die einen impliziten Bezug zu Cloud Computing haben, d. h. einen Geltungsbezug zu Basistechnologien oder zu Grundprinzipien des Cloud Computing. Vollständig außer-

[2] http://cloud-standards.org/
[3] http://www.trusted-cloud.de/

halb des Fokus dieser Untersuchung sind Standards, die weder einen expliziten noch impliziten Bezug zum Cloud Computing aufweisen. Weiterhin unterscheiden wir Standards, die nur für spezifische Branchen von Relevanz sind, sowie Standards, die ein branchenübergreifendes Wirkungsfeld haben. Der Fokus der Untersuchung liegt auf branchenübergreifenden Standards, die einen expliziten Bezug zu Cloud Computing besitzen. Insgesamt wurden so etwa 160 potentielle für das Cloud Computing relevante Standards identifiziert und klassifiziert.

Es folgte die Festlegung transparenter Kriterien zur weiteren Auswahl. Die betrachteten Standards sollten dabei ein möglichst großes inhaltliches Spektrum abdecken. Wo möglich, wurden möglichst umfangreiche Standards mit prototypischem Charakter von bekannten Standardisierungsorganisationen bevorzugt. Das Spektrum wurde durch die Herausforderungen und Ansatzpunkte gemäß der im folgenden Abschnitt definierten Taxonomie aufgespannt. In der Untersuchung wurde die Auswahl von Cloud-Standards so auf 21 zu bewertende Standards eingegrenzt (vgl. Tabelle 1).

Danach fand die Einzelbewertung der ausgewählten Standards unter Verwendung einheitlicher Bewertungskriterien statt. Wir untersuchten hierbei Reifegrad, Durchsetzungsfähigkeit und Partizipationsmöglichkeit. Die Einzelbewertung findet sich aus platzgründen nicht in dieser Publikation.

3.2 Erstellung einer Standardisierungslandkarte

Auswahl relevanter Herausforderungen der Standardisierung. Bei der Analyse der oben genannten Dokumente haben wir neun übergeordnete Herausforderungen bestimmt. Insbesondere aus der Sicht der Anbieter von Cloud-Diensten ist die Sicherstellung von Effizienz bei der Dienstbereitstellung von zentraler Bedeutung [6], [11], [14]. Überwiegend aus der Sicht von Cloud-Anwendern sind neben der Effektivität der Dienstnutzung und -steuerung übergreifende Anforderungen an Transparenz, Informationssicherheit und Datenschutz wichtig [6], [8-11], [14]. Letzterer wurde aufgrund seiner Bedeutung für rechtskonformes Cloud Computing in Deutschland und der vielfältigen Anforderungen jenseits der klassischen Informationssicherheit (z. B. Datensparsamkeit, Auskunftsrechte etc.) bewusst gesondert betrachtet. Darüber hinaus sind Interoperabilität sowie Portabilität von Daten und Diensten zwischen verschiedenen Cloud-Anbietern wichtige Themen [6-7], [11], [14].

Eine Sonderrolle kommt zwei aus übergeordneten Interessen getriebenen Herausforderungen zu: Sicherstellung eines funktionierenden Wettbewerbs [6-7], [11] und Sicherstellung von Compliance [6-7], [14]. Beide Herausforderungen stehen nicht auf derselben Ebene, wie die zuvor genannten. So fördert bspw. erhöhte Portabilität und Interoperabilität aber auch verbesserte Transparenz den Gedanken des funktionierenden Wettbewerbs. Datenschutz hingegen ist wiederum ein Teilbereich der Compliance. Eine tabellarische Übersicht der Herausforderungen findet sich in den Spaltenüberschriften der Standardisierungslandkarte in Tabelle 2.

Standards können die *Effizienz der Dienstbereitstellung* von Cloud-Diensten erhöhen. Hier können vier Bereiche unterschieden werden: Die *Nutzung von Entwicklungstools und -komponenten* hilft, aufwändige Eigenentwicklungen im Entwicklungsprozess zu vermeiden. Der *Aufbau skalierbarer Architekturen* stellt eine weitere

Herausforderung dar. Hier müssen insbesondere Eigenschaften wie Redundanz, Fehlertoleranz und Mehr-Mandantenfähigkeit berücksichtigt werden. Eine weitere Herausforderung beim effizienten Betrieb ist *Ressourcenmanagement und Flexibilität*. Dies bezieht sich zunächst auf technische Ressourcen wie Hardware und Software aber auch auf Personalressourcen im Sinne der Kapazitätsplanung und Standardisierung von Qualifikationsanforderungen. Gerade im Cloud-Kontext sind die Erwartungen an die *Verfügbarkeit der Dienste* sehr hoch. Sie hängen von diversen Einflussfaktoren ab (z. B. Rechenzentrumshardware, Netzverfügbarkeit, Anwenderverhalten).

Zur Erhöhung der *Effektivität der Dienstnutzung und -steuerung* werden Lösungen benötigt, die den Dienst an sich bereitstellen (z. B. HTML, Remote-Desktop Protokolle, Standards für Shell-Zugriffe, Internet-Standards). Da diese aber allgemein verfügbar und meist standardisiert sind, werden sie im Weiteren nicht separat betrachtet. Eine höhere Relevanz kommt den folgenden Herausforderungen zu: Vor der eigentlichen Nutzung von Cloud-Diensten sind etwaige Fragen zur *Vertragsgestaltung inkl. Haftungsfragen* zu klären. Während der Nutzung ist einer der Haupterfolgsfaktoren die Möglichkeit zur eigenständigen *Steuerung der Dienste durch den Anwender.* Im Falle von Problemen während der Nutzung sollte es standardisierte *Governance- und Eskalationsmechanismen* geben.

Die *Transparenz der Leistungserbringung und Abrechnung* vereinfacht die komplexe und oft eher anonyme Auftraggeber-Auftragnehmerbeziehung im Cloud Computing. Konkret bestehen die Anforderungen, dass die *Abrechnung inkl. Lizenzmanagement* transparent für den Anwender ist. Weiterhin sollte Transparenz bzgl. der Leistungsseite bestehen (z. B. durch SLA-Monitoring). Wir subsumieren solche Anforderungen im Bereich *Qualitätssicherung und Überwachung SLA.* Obwohl es dem Kerngedanken des Cloud Computing widerspricht, kann es aufgrund datenschutzrechtlicher und anderer Vorschriften in bestimmten Branchen von hoher Relevanz sein, Transparenz über *Art und Ort der Datenverarbeitung* zu erhalten.

Informationssicherheit wird oft als das Haupthindernis für eine schnelle Verbreitung von Cloud Computing angeführt. Die Verwaltung einer potenziellen Vielfalt von Identitäten sowie die Konfiguration eines effizienten *Identitäts- und Rechtemanagement* für Cloud-Dienste, insbesondere bei der Verwendung einer föderierten Cloud-Architektur, könnte durch einheitliche Standards ermöglicht werden. Im Cloud Computing werden Daten verschiedener Akteure verarbeitet. Daraus resultieren unterschiedliche Anforderungen in Bezug auf das benötigte Niveau an *Vertraulichkeit und Integrität*. Es gilt den gesamten Lebenszyklus von Daten zu betrachten. Dies beginnt bei der technischen Übermittlung und Speicherung und endet erst bei der endgültigen Löschung. Themenbereiche sind u. a. Verschlüsselung und Schlüsselmanagement, anonymisierte Datenverarbeitung etc. *Zugriffsschutz, Logging, Abwehr von Angriffen* ermöglicht eine sichere Trennung von Mandanten sowie Zugriffskontrolle, die sichere Identifizierung und Authentisierung umfasst. Die gezielte Autorisierung sowie zugehörige Protokollierungsmechanismen sind wesentliche Funktionen für funktionierende Informationssicherheit. Darüber hinaus sollten Standards einen Beitrag zum zuverlässigen Schutz vor Angriffen bereitstellen. Neben der rein technischen Erfüllung von Sicherheitsanforderungen sind *Nachweis und Zertifizierung* der IT-Sicherheit von ebenso großer Bedeutung.

Datenschutz als Schutz von personenbezogenen, personenbeziehbaren und sensiblen Daten vor Missbrauch, ist gerade in Deutschland eine der größten Herausforderungen im Kontext des Cloud Computing. Die Sicherstellung der Datenschutz-Compliance bspw. durch geeignete Anbieterauswahl, regelmäßige Kontrolle oder Einforderung einer transparenten Dokumentation stellt viele Unternehmen vor eine große Herausforderung.

Cloud-*Interoperabilität* wird aus drei Gesichtspunkten betrachtet: Unter *Migration in die bzw. aus der Cloud* werden Fähigkeiten benötigt, die es ermöglichen Infrastruktur-, Middleware- oder Anwendungskomponenten sowie vollständige Anwendungen und Daten in die Cloud zu verlagern oder aus der Cloud zu entfernen. *Integrationsfähigkeit in on-premise IT* erlaubt die Interoperabilität von on-premise Systemen und Cloud-Diensten in Form einer Hybrid Cloud. *Cloud-Föderation* umschließt die Fähigkeit Cloud-Dienste unterschiedlicher Ebenen und Anbieter verlässlich und oft ad-hoc miteinander verbinden zu können. Eine Grundlage hierfür können einheitliche oder kompatible Schnittstellen bilden, so dass keine individuelle Integration von Cloud-Diensten notwendig ist.

Zur Vermeidung von Lock-in Effekten ist die *Portabilität zwischen Anbietern* notwendig. So können Dienste und Daten unter Verwendung von einheitlichen Standards einfach und auf regulärer Basis zwischen Anbietern portiert werden. *Dienst-Portabilität* beschreibt Fähigkeiten zur Portierung von Cloud-Diensten. *Daten-Portabilität* beschreibt entsprechend Fähigkeiten zur Portierung von Daten in der Cloud. Standards könnten u. a. einheitliche Datenformate und Exit-Vereinbarungen z. B. mit Datenintegritätszusicherung und Kostenanzeige umfassen.

Aufgrund der Skaleneffekte seitens der Anbieter und potenzieller Lock-in-Effekte, besteht im Cloud Computing die Gefahr einer Beeinträchtigung des Wettbewerbs zwischen den Anbietern und die Herausbildung von marktbeherrschenden Akteuren. Gerade in Deutschland und Europa ist die *Sicherstellung eines funktionierenden Wettbewerbs* von zentraler Bedeutung, der auch die Teilhabe von mittelständischen Unternehmen gewährleistet.

Unter *Compliance mit geltender Rechtslage* wird die Einhaltung von Gesetzen und Richtlinien sowie freiwilliger Vereinbarungen verstanden. Dies ist insb. eine Herausforderung, da der Nutzer von Cloud-Diensten nur eine geringe Transparenz über die Regeleinhaltung des Anbieters hat. Besonders relevant ist dies in den Bereichen IT-Sicherheit, Datenschutz sowie im kommerziellen Bereich.

Auswahl von Ansatzpunkten der Standardisierung. Standards können über unterschiedliche Mittel eine Standardisierung herbeiführen (vgl. auch [7]). Es lassen sich im Cloud-Umfeld die drei grundlegenden Bereiche Technik, Management und Recht unterscheiden. Analog zur Vorgehensweise bei den Herausforderungen haben wir die Ansatzpunkte auf einer zweiten Ebene differenziert. Eine tabellarische Übersicht findet sich in den Zeilenüberschriften der Standardisierungslandkarte in Tabelle 2.

Der Bereich *Technik* umfasst technische Standards. Konkret beinhaltet dies folgende Aspekte: *Datei- und Austauschformate* zur Übermittlung und Speicherung von (teil-)strukturierten Daten. Dies können neben Dokumenten, Bildern oder Mediendateien auch Virtual Machine Images oder ganze Anwendungen sein. *Programmiermo-*

delle bilden die Grundlage für Erstellung und Ausführung von Quellcode. Über die Vorgabe von Programmierkonzepten und -abstraktionen werden die Bausteine von Programmiersprachen definiert. *Protokolle und Schnittstellen* beschreiben einen dynamischen Ablauf zum Austausch von Information zwischen zwei Komponenten, Anwendungen oder Akteuren. *Standardkomponenten und Referenzarchitekturen* erleichtern den Aufbau und die Verwendung von Cloud-Infrastrukturen und Cloud-Diensten. Durch standardisierte Designvorgaben wie bspw. Referenzarchitekturen können Best Practices auf eigene Cloud-Dienste übertragen werden. *Benchmarks und Tests* helfen die Leistungsfähigkeiten unterschiedlicher Cloud-Dienste, bspw. durch die Vorgabe von Lastprofilen und Kennzahlen, zu bemessen und zu beurteilen.

Der Bereich *Management* beinhaltet Standards, die die kommerzielle Abwicklung sowie das Management auf der Seite von Cloud-Anbietern und Cloud-Anwendern unterstützen. *Geschäftsmodelle* bilden die Grundlage für den wirtschaftlichen Betrieb von Cloud-Diensten. Im Bereich des Cloud Computing ist insbesondere der Bereich einer einheitlichen Leistungsbeschreibung für die Standardisierung relevant. *Service Level Agreements* (SLA) erhöhen die Effizienz in der Vertragsgestaltung und erlauben die Festlegung und Sicherstellung gezielter Anforderungen an den Dienste-Anbieter. SLAs können so signifikant zur Vertrauensbildung beitragen. *Vertragsbedingungen* umfassen Rahmenverträge, die durch SLAs ergänzt werden, Endbenutzer-Lizenzvereinbarungen oder Vertragsbausteine in unterschiedlichen Sprachen. *Managementmodelle und -prozesse* (z. B. im Sinne der im IT-Servicemanagement weit verbreiteten ITIL-Bibliotheken) können helfen einheitliches Vorgehen und Begrifflichkeiten sicherzustellen und Best Practice Prozesse zu fördern. *Controllingmodelle und -prozesse* können durch Vorgaben, bspw. zur Abrechnung und Rechnungslegung, oder dem Risikomanagement von bspw. IT-Systemen einheitliche Dokumente zur Dokumentation der Geschäftstätigkeit fördern. Dies kann ggfs. zur Vereinfachung von Zertifizierungen beitragen. *Leitfäden, Audit etc.* können sowohl potenziellen Anbietern als auch Nutzern von Cloud-Diensten hilfreich sein. Dies wird durch den Transport von Orientierungswissen, bspw. in Form von Best Practice, ermöglicht.

Regelungen und Vorschriften, die den geltenden Rechtsrahmen für die Akteure im Cloud Computing abstecken, können in drei Gruppen des Bereichs *Recht* unterschieden werden. *Rechtliche Vorgaben* stellen verbindliche Vorgaben, die auf entsprechenden Gesetzen, Richtlinien, Verordnungen o. ä. basieren. *Selbstverpflichtungen* fassen freiwillige Vereinbarungen und Kodizes zusammen, die z. B. von (Branchen-) Verbänden herausgegeben werden. *Unternehmensrichtlinien* stellen die schwächste Form von Regelungen und Vorschriften zum geltenden Rechtsrahmen dar. Unternehmensrichtlinien erlauben Unternehmen, sich bei der Geschäftstätigkeit bspw. strengeren Richtlinien zu unterwerfen als durch rechtliche Vorgaben gefordert.

3.3 Analyse von Standardisierungspotentialen und -lücken

In den vorherigen Schritten zur Bewertung des Portfolios von Cloud-Standards haben wir eine durch Herausforderungen und Ansatzpunkte aufgespannte Standardisierungslandkarte erstellt. Darin haben wir die Auswahl von 21 Standards eingeordnet. Die weitergehende Analyse und Bewertung dieser Ergebnisse erlaubt die Identifikation von Standardisierungslücken sowie die Ableitung von Handlungsempfehlungen für die Standardisierung.

Wir haben eine begleitende Potentialanalyse durchgeführt, die allgemeine Beiträge der Standardisierung identifiziert. Dabei wurde die Frage untersucht, inwieweit ein Ansatzpunkt (also beispielsweise ein Datei- und Austauschformat) einen Beitrag zur Lösung einer jeweiligen Herausforderung leisten kann. Die Bestimmung des allgemeinen Lösungsbeitrags wurde dabei auch durch Experten-Interviews sowie den Einsatz von Fragebögen unterstützt. Darin wurde allgemein erhoben, welche Relevanz eine Herausforderung für das Cloud Computing aufweist. Zusätzlich haben wir eine grundsätzliche Einschätzung des Beitrags der Ansatzpunkte zur Lösung der Herausforderung durch Standards erhoben. In beiden Fällen wurden Antwortmöglichkeiten auf einer Likert-Skala mit vier Ausprägungen erhoben:

- *Ja*: Der Ansatzpunkt hat augenscheinliches und umfangreiches Potential zur Lösung der Herausforderung.
- *Eher ja*: Der Ansatzpunkt hat grundsätzliches Potential zur Lösung der Herausforderung.
- *Eher Nein*: Der Ansatzpunkt hat geringes oder nicht direkt ersichtliches Potential zur Lösung der Herausforderung.
- *Nein*: Der Ansatzpunkt hat voraussichtlich kein Potential zur Lösung der Herausforderung.

Die Analyse von Standardisierungslücken verbindet die Potentialanalyse mit der vorgenommenen Bewertung existierender Standards. Dazu wurde eine Standardisierungslücke als vorhanden klassifiziert, wenn tendenziell Potential („eher ja“) zur Lösung einer Herausforderung im Cloud Computing durch einen Standard vorhanden ist, existierende Standards dieses aber noch nicht vollständig ausschöpfen. Weiterer Bedarf zur Standardisierung wurden als „erhöht“ oder „hoch“ klassifiziert werden, wenn Potential der Standardisierung offensichtlich („ja“) ist, existierende Standards dieses aber noch nicht vollständig bzw. unzureichend ausschöpfen. Neben der Bewertung des Lösungsbeitrags vorhandener Standards zur Adressierung der jeweiligen Herausforderung durch Standardisierung eines Ansatzpunktes, wurde auch eine Einschätzung der Dringlichkeit der Standardisierung für jede Herausforderung vorgenommen. Dies ermöglicht die Priorisierung von Handlungsempfehlung. Identifizierte Standardisierungsbedarfe der Kategorie „hoch“ zeichnen sich durch tendenziell kurzfristige Dringlichkeit aus. „Erhöhte“ Bedarfe und „vorhandene“ Lücken sind mittel- bis langfristig dringlich. Die Ergebnisse der Analyse und Einschätzung der Standardisierungslücken wurden ebenfalls in Experteninterviews und Workshops validiert.

4 Ergebnisse und Diskussion

4.1 Relevante Standardisierungsgremien und ihre Standards

Es existiert eine Vielzahl verschiedener Akteure im Normungs- und Standardisierungsumfeld von Cloud Computing. Der Auswahl liegt eine anfängliche Recherche von über 70 verschiedenen Institutionen zu Grunde. Der Fokus liegt auf Normungsorganisationen, Standardentwicklungsorganisationen, Interessensvereinigungen, sonstigen Konsortien oder öffentlichen Einrichtungen. Ihnen allen ist gemein, dass sie Gremien besitzen, die Standards oder Vorarbeiten mit implizitem oder explizitem Bezug zum Cloud Computing forcieren. Einzelne Forschungseinrichtungen oder privat-wirtschaftliche Unternehmen sind nicht im Fokus. Bei Letzteren bestehen keine regulären Mitwirkungsmöglichkeiten für Außenstehende.

In den USA nimmt NIST eine Vorreiterrolle bei der Cloud-Standardisierung ein. Einige internationale Standardisierungsgremien zeigen ebenfalls großes Engagement, während die überwiegende Mehrheit ihren Fokus nur langsam auf Standards für das Cloud Computing ausrichtet. Auf europäischer Ebene wird das ETSI eine koordinierende Rolle einnehmen. EuroCloud ist ein paneuropäischer Unternehmensverband der Anbieter von Cloud Computing mit großem Einfluss. In Deutschland unternehmen das DIN, der BITKOM und das BSI Schritte bei der Anforderungsdefinition.

Es wurden 21 Standards, Vorgaben, Zertifizierungen bzw. Vorarbeiten ausgewählt. Diese wurden im Detail untersucht, bewertet und von ähnlichen Standards abgegrenzt. Bei der Auswahl und Bewertung der 21 Cloud-Standards handelt es sich um eine Momentaufnahme von Mitte 2012 bei der wir insgesamt etwa 160 Standards in Betracht gezogen haben. Die 21 Cloud-Standards besitzen nach Möglichkeit Vorbildcharakter und decken die Bereiche Technik, Management und Recht ab. Kein branchenspezifischer Standard wurde als relevant genug erachtet, um in die engere Auswahl zu gelangen. Eine Übersicht der Standards ist in Tabelle 1 dargestellt.

Tabelle 1. 21 ausgewählte Cloud-Standards für Technik, Management und Recht

Standard	Initiator	Ähnliche
CCRA (Cloud Computing Reference Architecture): Referenzarchitektur für Cloud-Service-Angebote	TOG	Referenzarchitekturen der NIST oder des BSI
CDMI (Cloud Data Management Interface): API zum Zugriff auf Daten in IaaS, DaaS Szenarios	SNIA	XAM, iSCSI, NFS, WebDAV
CIMSVM (CIM System Virtualization Model): Objektmodel und Schnittstellen für Virtuelle Systeme & Komponenten	DMTF	TOSCA
Cloud Audit (Automated Audit, Assertion, Assessment, and Assurance API): API für automatisierte Auditierung	CSA	SCAP
CTP (Cloud Trust Protocol): Einheitliche Techniken und Nomenklatur zur Erhöhung der Transparenz	CSA	SCAP, OCRL
Hive (Apache Hive): Programmiermodell für Datenabfragen	Apache	JAQL, PIG
OCCI (Open Cloud Computing Interface): API zum Management von Clouds (insb. IaaS)	OGF	DeltaCloud, Libcloud, EC2, Eucalyptus, vCloud etc.
OpenStack (OpenStack Cloud Software): Rahmenwerk zum Aufbau von Cloud-Infrastrukturen	(Diverse)	OpenNebula, Nimbus (Schnittstellen: CMDI, OCCI, OVF)
OAuth (Web Authorization Protocol): Protokoll und Schnittstelle zum Identitätsmanagement	IETF	OpenID, WS-Federation, SAML
OVF (Open Virtualization Format): Dateiformat für Virtuelle Maschinen	DMTF, ANSI, ISO	AMI, EMI
SCAP (Security Content Automation Protocol): Protokoll und Schnittstelle zum Abruf von Sicherheitsinformationen	NIST	CloudAudit
TOSCA (Topology and Orchestration Specification for Cloud Applications): Beschreibungssprache für Cloud-Dienste	OASIS	CIMSVM, USDL, e3Value, SNN
USDL (Unified Service Description Language): Beschreibungssprache für virtuelle Dienstleistungen	W3C	OWL-S, WSMO, UDDI, WSDL, WADL, PAS1018
*WS-** (Web Service Standards): Spezifikationen, Standards und Normen für Web Services	OASIS, OGF, W3C	WSDL, WS-I, WS-Policy, WS-Security, WS-Agreement etc.
BSI-ESCC (Eckpunktepapier Sicherheitsempfehlungen für Cloud Computing Anbieter): Leitfaden	BSI	Andere Anforderungs-dokumente
EuroCloud-SA (EuroCloud Star Audit): Zertifikat für Anbieter von Cloud-Diensten	EuroCloud	EuroPriSe, TiC
GRC Stack (Governance, Risk Management and Compliance Stack): Rahmenwerk zu Risikobewertung von Anbietern	CSA	CloudAudit, CCM, CAIQ, CTP
NIST-UC (Cloud Computing Use Cases): Leitfaden für Cloud-Anwendungsfälle mit Fokus auf US-Behörden	NIST	Use Cases von OGF oder DMTF
SSAE-16 (Statement on Standards for Attestation Engagements No. 16): Zertifikat für Anbieter von Cloud-Diensten	AICPA	CobiT, BSI-100, ISAE 3402, ITIL, SAS 70, IDW PS 330/951/FAIT1
OCM (Open Cloud Manifesto): Selbstverpflichtung zu Offenheit für Cloud-Anbieter	(Diverse)	keine
95/46/EG (EU-Richtlinie 95/46/EG „Datenschutzrichtlinie“): Datenschutzvorgaben der EU	EU	BDSG, DSG der Länder, Safe Harbor

Die überwiegende Mehrheit der Standards hat internationale Relevanz. Einzelne weisen einen (leichten) europäischen bzw. nationalen Bezug auf (z. B. BSI-ESCC, USDL, NIST-UC, EuroCloud-SA, 95/46/EG). Die Bewertungsergebnisse für die Standards spiegeln den frühen Entwicklungsstand im Cloud Computing wider. Standards, die bereits vor dem Cloud Computing existierten, weisen eine tendenziell grö-

ßere Reife auf (z. B. SCAP, WS-*, OAuth, CIMSVM, SSAE-16) als solche, die aktuell explizit für das Cloud Computing erarbeitet werden. Die Durchsetzungsfähigkeit von Standards mit explizitem Bezug zum Cloud Computing erweist sich hingegen tendenziell höher, als bei solchen mit implizitem Bezug.

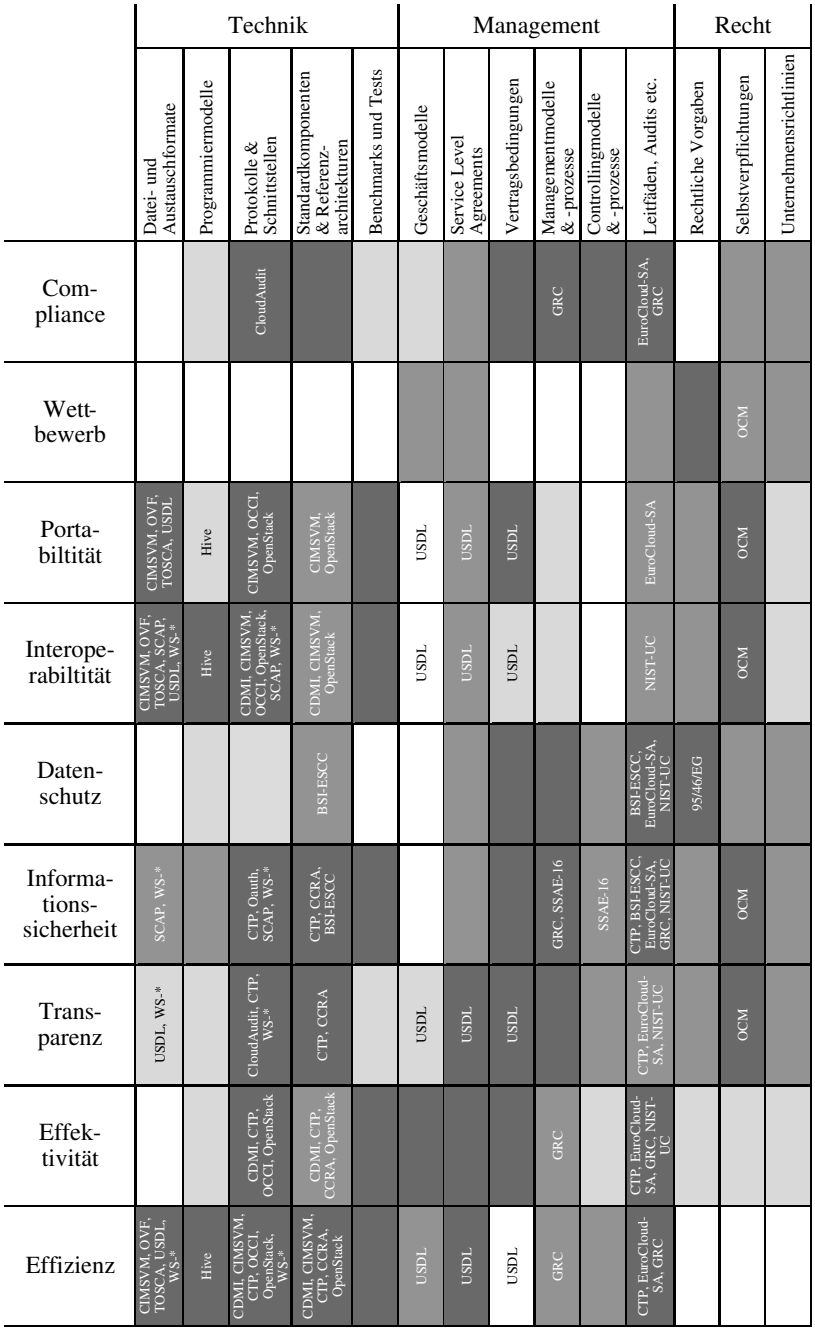
4.2 Diskussion der Ergebnisse

Tabelle 2 zeigt Standards sowie Standardisierungspotentiale und -lücken anhand einer Überlagerung in der Landkarte und fasst so die Ergebnisse der Studie zusammen.

Die Mehrzahl der Standards fokussiert die Herausforderungen Informationssicherheit, Effizienz, Interoperabilität oder Portabilität aus technischer Perspektive. Bedarf an technischen neuen oder umfänglicheren Standards besteht bspw. bei Standardkomponenten, Referenzarchitekturen, Benchmarks, Tests oder Protokollen und Schnittstellen. Im Bereich der Managementstandards finden sich nur wenige Standards. Es existieren keine oder nicht ausreichend umfassende Standards für Geschäftsmodelle, Dienstgütevereinbarungen, Managementmodelle sowie -prozesse sowie für das Controlling im Cloud Computing. Das Zusammenspiel des Rechtsrahmens und der Standardisierung im Cloud Computing ist vielschichtig und wird bislang überwiegend auf Herausforderungen im Bereich Datenschutz reduziert. Im Bereich der vertraglichen Regelungen fehlen unter anderem standardisierte, verbindliche unternehmensinterne Vorschriften (Binding Corporate Rules, BCR) für Cloud-Anbieter zum Datenschutz im Zuge einer Selbstregulierung. Auf europäischer und deutscher Ebene ist daher die Klärung des grundsätzlichen strategischen regulatorischen Vorgehens notwendig.

Die Potentialanalyse legt nahe, dass für jede der identifizierten Herausforderungen ein Lösungsansatz durch Standardisierung erfolgsversprechend erscheint. Dabei versprechen technische Ansatzpunkte insbesondere für Herausforderungen, die im Kern eher technischer Natur sind (wie bspw. Effizienz, Effektivität, Informationssicherheit aber auch Interoperabilität und Portabilität) eine Lösung. Im Bereich der Sicherstellung des funktionierenden Wettbewerbs, der Compliance sowie des Datenschutzes liefern technische Ansatzpunkte die geringsten Beiträge. Die Potentialanalyse zeigt weiter, dass die genannten, vermeintlich von technischer Natur stammenden Herausforderungen nur dann angemessen adressiert werden können, wenn auch Standardisierungspotentiale durch Ansatzpunkte auf Management- (Effizienz, Effektivität) und Rechtsebene (Interoperabilität, Portabilität) ausgereizt werden. Auch zeigt sich, dass der Bereich der Informationssicherheit sowie in Teilen auch Portabilität und Compliance nur durch auf Technik-, Management- und Rechtsebene aufeinander abgestimmte Standardisierungsbestrebungen gelöst werden können.

Tabelle 2. Landkarte der Standardisierung im Cloud Computing



Es lassen sich folgende Standardisierungsbedarfe hervorheben: Es fehlen Standardkomponenten und Referenzarchitekturen zur Leistungsüberwachung und Sicherstellung von Compliance. Existierende Standards greifen diesen Aspekt bislang nur unzureichend auf. Benchmarks & Tests sind nicht verfügbar. Insbesondere im Bereich der Effektivität der Dienstnutzung könnte durch Vergleichbarkeit mehr Vertrauen geschaffen werden. Protokolle & Schnittstellen zur Transparenzsteigerung durch automatisierten Informationsaustausch sind unzureichend ausgeprägt. Deutlich sind die Lücken bei standardisierten Vertragsbedingungen zur Gewährleistung der Informationssicherheit und Sicherstellung des Datenschutzes speziell für kleine und mittelständische Unternehmen. Darüber hinaus sehen wir weiteres Potential für umfassende und erprobte Datei- und Austauschformate zur Unterstützung von Interoperabilität von Cloud-Diensten sowie für standardisierte Protokolle & Schnittstellen zum Austausch im Sinne der Portabilität. Es finden sich noch keine ausreichenden, rechtlichen Vorgaben zur Sicherstellung des funktionierenden Cloud-Wettbewerbs.

5 Ausblick und Empfehlungen

Wir haben basierend auf einem Screening von etwa 160 Standards sowie über 70 Standardisierungsinitiativen im Cloud Computing 21 Cloud-Standards ausgewählt und in einer Standardisierungslandkarte dargestellt. Diese Übersicht haben wir überlagert mit den Ergebnissen einer Potentialanalyse. Die Ergebnisse haben z. T. deutlich Lücken aufgezeigt, aber auch Bereiche, für die bereits Standards existieren, welche die gestellten Anforderungen nur bedingt erfüllen oder nicht ausreichend erprobt sind.

Aus den Gesamtergebnissen der Untersuchung lassen sich damit einige Handlungsempfehlungen für die Standardisierung im Cloud Computing ableiten: Zunächst sollten offene Standardisierungslücken weiter priorisiert werden und insbesondere öffentliche Anforderungen klar formuliert werden. Bestehende Standards sollten kontinuierlich katalogisiert werden. Darüber hinaus sollte die Offenheit von Standards im Cloud Computing durch das Setzen von Anreizen gefördert werden. Auch sollten existierende Standards auf ihre tatsächliche Offenheit geprüft werden. Wichtig ist dabei Eckpunkte zu definieren, um Doppelarbeit zu vermeiden. Auch erscheint es sinnvoll, Standards für das Vertragswesen vom rechtlichen Rahmen abzugrenzen. Die Standardisierung sollte über nationale, europäische und internationale Verwaltungsebenen hinweg sowie unter Einbeziehung aller Akteure zentral koordiniert werden (z. B. als Standardisierungs-Roadmap). Der bestehende nationale wie europäische Rechtsrahmen sollte auf Angemessenheit und Implikationen für das Cloud Computing umfassend geprüft werden, um geeignete rechtliche Vorgaben abzuleiten. Staatliche Organisationen sollten dabei in fokussierter Weise und begrenztem Maße inhaltlich bei der Standardisierung mitwirken. Der Schwerpunkt liegt auf der Anforderungsdefinition. Die eigentliche Standardisierung ist Aufgabe der Wirtschaft unter Mitwirkung der Wissenschaft. Dabei sollte insbesondere die Rolle der Anwender von Cloud-Diensten mehr Wertschätzung erfahren.

Literatur

1. Baun, C., Kunze, M., Nimis, J., Tai, S.: Cloud Computing: Web-basierte dynamische IT-Services. 2. Auflage, Springer, Berlin (2011)
2. Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., Zaharia, M.: A View of Cloud Computing. Communications of the ACM 53, 50-58 (2010)
3. Marstona, S., Lia, Z., Bandyopadhyaya, S., Zhanga, J., Ghalsasi, A.: Cloud Computing: The Business Perspective. Decision Support Systems 51, 176-189 (2011)
4. National Institute of Standards and Technology (NIST): NIST SP 800-145, The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf
5. ISO/IEC: ISO/IEC Guide 2: Standardization and related activities: General vocabulary. ISO/IEC, Geneva (1996)
6. Jeffery, K., Neidecker-Lutz, B.: The Future of Cloud Computing: Opportunities for European Cloud Computing Beyond 2010. Report (2010)
7. Smart Cloud Study Group: Smart Cloud Strategy (2010), http://www.soumu.go.jp /main_sosiki/joho_tsusin/eng/councilreport/pdf/100517_1.pdf
8. European Network and Information Security Agency (ENISA): Cloud Computing Benefits, Risks and Recommendations for Information Security (2009)
9. Cloud Security Alliance (CSA): Security Guidance for Critical Areas of Focus in Cloud Computing V2.1, http://www.cloudsecurityalliance.org/guidance/csaguide.pdf (2009)
10. EuroCloud: Leitfaden: Recht, Datenschutz & Compliance, http://www.eurocloud.de /2010/12/02/eurocloud-leitfaden-recht-datenschutz-compliance/ (2010)
11. European Network and Information Security Agency (ENISA): An SME perspective on Cloud Computing: Survey (2009)
12. Cloud Security Alliance (CSA): Cloud Controls Matrix (CCM) Version 1.2, https://cloudsecurityalliance.org/research/ccm/#_overview (2011)
13. Cloud Security Alliance (CSA): Consensus Assessments Initiative Questionnaire v1.1, https://cloudsecurityalliance.org/wp-content/uploads/2011/03/CSA-CAI-Question-Set-v1-1_FINAL_v6.xlsx (2011)
14. Cloud Computing Use Case Discussion Group: Cloud Computing Use Cases. Version 4.0, http://cloudusecases.org/ (2010)
15. Sakai, H.: Standardization Activities for Cloud Computing. NTT Technical Review, https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201106gls.pdf (2011)
16. National Institute of Standards and Technology (NIST): NIST-SP 500-291, NIST Cloud Computing Standards Roadmap, http://www.nist.gov/customcf/get_pdf.cfm?pub_id= 909024 (2011)
17. National Institute of Standards and Technology (NIST): Cloud Computing Use Cases, http://www.nist.gov/itl/cloud/use-cases.cfm (2010)
18. Internet Engineering Task Force (IETF): Cloud SDO Activities Survey and Analysis. draft-khasnabish-cloud-sdo-survey-03.txt, https://rsync.tools.ietf.org/html/draft-khasnabish-cloud-sdo-survey-03 (2012)
19. ITU Telecommunication Standardization Bureau: Activities in Cloud Computing Standardization, Repository (Version 1.0, May 2010), http://www.itu.int/dms_pub/itu-t/oth/49/01/T49010000020002PDFE.pdf (2010)