eCH-0198 - Überblick relevanter Zertifikate Cloud-Nutzung

Name	Überblick relevanter Zertifikate Cloud-Nutzung
eCH-Nummer	eCH-0198
Kategorie	Hilfsmittel
Reifegrad	Definiert
Version	1.0
Status	**Genehmigt**
Genehmigt am	2016-06-01
Ausgabedatum	2016-06-15
Ersetzt Version	-
Voraussetzungen	-
Beilagen	-
Sprachen	Deutsch (Original), Französisch (Übersetzung)
Autoren	**Fachgruppe Cloud Computing** Reto Gutmann, ETH Zürich, rgutmann@ethz.ch Claudio Giovanoli, FHNW, claudio.giovanoli@fhnw.ch Pia Wittmann, ehemals CSC Switzerland GmbH Andreas Hänecke, CSC Switzerland GmbH, ahanecke@csc.com
Herausgeber / Vertrieb	Verein eCH, Mainaustrasse 30, Postfach, 8034 Zürich T 044 388 74 64, F 044 388 71 80 www.ech.ch / info@ech.ch

Zusammenfassung

Das vorliegende Hilfsmittel empfiehlt und beschreibt aktuelle und relevante Zertifikate für Cloud Computing-Anbieter in der Schweiz. Es soll den Endbenutzer bei der Wahl eines geeigneten Anbieters unterstützen. Das Hilfsmittel enthält eine Beilage 1, welche ein 10-Schritte Programm für die Evaluation der Cloud-Sicherheit und die dazugehörigen empfohlenen Zertifikate beschreibt.

Inhaltsverzeichnis

Hinweis

Aus Gründen der besseren Lesbarkeit und Verständlichkeit wird im vorliegenden Dokument bei der Bezeichnung von Personen ausschliesslich die maskuline Form verwendet. Diese Formulierung schliesst Frauen in ihrer jeweiligen Funktion ausdrücklich mit ein.

1 Einleitung

1.1 Status

Genehmigt: **Das Dokument wurde vom Expertenausschuss genehmigt. Es hat für das definierte Einsatzgebiet im festgelegten Gültigkeitsbereich normative Kraft.**

1.2 Anwendungsgebiet

Die Cloud-Zertifizierungen und die Prüfung von Cloud Services auf relevante Kriterien hinsichtlich des Datenschutzes, der Sicherheit und der zugesicherten Qualitätsmerkmale erlangen einen zunehmenden Stellenwert bei der Bewertung von vertrauenswürdigen Cloud-Services.

Momentan existieren auf nationaler und internationaler Ebene viele verschiedene Akteure im Normungs- und Standardisierungsumfeld von Cloud Computing. Altbewährte Standards decken die Anforderungen an das Cloud Computing nur teilweise ab und Standards mit explizitem Bezug zu Cloud Computing sind noch relativ neu und unbekannt und es ist offen, ob sie eine hohe Verbreitung und Akzeptanz erreichen werden.

Das vorliegende Hilfsmittel richtet sich an öffentliche aber auch private Organisationen, welche den Weg in die Cloud planen und Unterstützung bei der Wahl des geeigneten Cloud Computing-Anbieters suchen. Es beschreibt die Zertifikate, welche aus Sicht der Fachgruppe Cloud Computing in der Schweiz relevant sind, also in Fachkreisen etabliert und anerkannt sind wie die ISO Normen oder welche als zukünftig durchsetzungsfähig angesehen werden, wie das noch junge Euro Cloud Star Audit.

2 Empfohlene Zertifizierungen für Cloud Computing-Anbieter

Die nachfolgende Tabelle zeigt in summarischer Form auf, welche Zertifikate im Hilfsmittel aufgeführt sind und welchen Fokus die Zertifikate aufweisen.

Die Spalte Rechenzentrum weist Zertifikate aus, welche sich mehrheitlich auf die Erbringung von IT-Leistungen aus einem Rechenzentrum beziehen. Die IT-Leistungserbringung aus einem Rechenzentrum bildet die technologische und organisatorische Basis zur Erbringung von Cloud-Services.

Cloud Service Zertifikate integrieren in der Regel mehrere Bereiche aus Normen und Vorgaben aus dem Rechenzentrumsbereich und erweitern diese um die Cloud Spezifikas (z.B. Controls und Privacy).

Zertifikate und Normen	Kapitel	Rechenzentrum	Cloud Service
Europäische Zertifikate			
EuroCloud Star Audit ECSA	3.1	**x**	**x**
EuroCloud Star Audit Swiss	3.1	**x**	**x**
Trusted Cloud, TÜV Trust-IT	3.2	**x**	**x**
Internationale Zertifikate			
CSA Security, Trust & Assurance Registry (CSA STAR)	3.3	**x**	**x**
ISO-Normenreihe			
ISAE 3402	4.1	**x**	
ISO/IEC 20000	4.2	**x**	
ISO 27001, ISO 27002	4.3	**x**	
ISO 27017, ISO 27018:2014	4.4		**x**
Zertifikat für den Betrieb des Rechenzentrums			
Tier-IV-Zertifizierung	4.6	**x**	

3 Beschreibung der empfohlenen Zertifizierungen

3.1 Europäische Zertifikate: EuroCloud Star Audit (ECSA) und EuroCloud Star Audit Swiss

3.1.1 Beschreibung

EuroCloud Europe (ECE) verfolgt das Ziel die Akzeptanz für Cloud Services auf dem internationalen Markt zu schaffen sowie die kundenorientierte Bereitstellung dieser Dienste und deren Nachfrage zu unterstützen. ECE bietet das Zertifizierungssystem "EuroCloud Star Audit" (ECSA), um Vertrauen in Cloud Services durch Qualitätsbewertung sowohl auf der Kunden- als auch auf der Anwenderseite zu etablieren.

Das Zertifizierungsverfahren basiert auf einem europäischen Standard mit unterschiedlichen Modulen und einem landesspezifischen Self-Assessment oder Zertifizierung.

Die Zertifizierung ist spezifisch auf die Bereiche IaaS, PaaS und SaaS ausgelegt und hat definierte Aussagen zu Kontrollelementen, die abgestuft zu erfüllen sind, um als vertrauenswürdiger Cloud-Anbieter zertifiziert zu werden.

EuroCloud Swiss ist der schweizerische Fachverband für die Förderung des Cloud Computing in der Schweiz und der akkreditierte Landesvertreter von EuroCloud Star Audit.

Das Audit besteht aus verschiedenen Prüfungen, die ein Cloud- Anbieter durchlaufen muss. Anhand eines detaillierten Fragenkatalogs wird die Einhaltung von Sicherheitsrichtlinien bewertet. Das Zertifikat sieht maximal fünf Sterne vor. Wird die Höchstwertung erreicht, kann der Kunde von einem sehr vertrauenswürdigen Cloud-Anbieter ausgehen. Der Prüfkatalog des EuroCloud Star Audit SaaS wurde in enger Abstimmung verschiedenen Institutionen erarbeitet, darunter dem Deutschen Bundesamt für Sicherheit in der Informationstechnik (BSI), der ENISA / ETSI sowie der EU entwickelt.

Für die vorgenannten vertraglichen, technischen und organisatorischen Anforderungen hat EuroCloud ein spezielles Gütesiegel entworfen, dessen Nutzung voraussetzt, dass die für die Bereitstellung von Cloud-Services grundlegenden Anforderungen durch geschulte Auditoren geprüft und durch ein Zertifikat bestätigt werden. Für die Prüfanforderungen wurde in enger Abstimmung mit öffentlichen Institutionen, Forschungseinrichtungen, Cloud-Anbietern, Rechtsexperten und Wirtschaftsprüfungsgesellschaften ein Kriterienkatalog erstellt.

Konkret werden im EuroCloud Star Audit folgende Kategorien erfasst:

- Anbieterprofil
- Vertrag und Compliance
- Sicherheit
- Betrieb der Infrastruktur
- Betriebsprozesse
- Anwendung
- Implementierung

Durch ein Punktesystem und die Vorgabe von Mindestkriterien kann ein Anbieter verschiedene Gütestufen (ein bis fünf Sterne) erreichen.

Im Ergebnis werden je nach Umsetzungsgrad die drei folgenden Gütestufen vergeben:

- Trusted Cloud-Service – drei Sterne
- Trusted Cloud-Service Advanced – vier Sterne
- Trusted Cloud-Service Advanced HA (High Availability) – fünf Sterne

3.1.2 Empfehlung

Der weite Umfang der EuroCloud-Zertifizierung liefert einen grossen Beitrag zur Vertrauensbildung. Da die Zertifizierung noch jung ist, muss sich erst zeigen, ob sie von der Branche akzeptiert wird.

3.1.3 Nutzen

Insgesamt gesehen ist EuroCloud Star Audit ein gutes Instrument mit einem hohen Mass an Transparenz und Orientierung für den Anwender und hilft ihm bei der Wahl des Cloud-Anbieters. Anhand der Zertifizierungsstufen kann der Nutzer die Zuverlässigkeit und den Umgang mit seinen Nutzerdaten durch den jeweiligen Cloud-Anbieters ablesen.

3.2 Europäisches Zertifikat: TÜV Trust-IT: Trusted Cloud

3.2.1 Beschreibung

Das standardisierte Prüfverfahren „Trusted Cloud“ basiert auf Basis relevanter Normen und Standards und besteht aus einem siebenstufigen Verfahren.

Die relevanten Standards und Normen sind:

- COBIT
- ITIL
- ISO/IEC 27001
- IDW PS
- BDSG
- TKG

Das siebenstufige Verfahren unterteilt sich:

1. Scope-Definition
2. Dokumentenprüfung
3. Analyse Prozess, Organisation, Audit, Technische Analyse
4. Ergebnisbericht
5. Zertifizierung
6. Monitoring-Audit Jahr 1
7. Monitoring-Audit Jahr 2

Dabei erfolgt die Prüfung in den Kategorien:

- organisatorische und technische Sicherheit,
- Qualität des Service-Managements und
- Compliance.

Es existieren für jedes Themenfeld vier Trust-Level (Güteklassen). Die jeweiligen Trust-Levels werden nach verschiedenen Sicherheitsanforderungen mit entsprechenden Servicemodellen IaaS, PaaS und SaaS gekennzeichnet. Die unterschiedlichen Levels unterscheiden sich bzgl. des Datenschutzes. Die niedrigste Güteklasse, Basislevel 1, eignet sich

für die Speicherung und Verarbeitung unkritischer Daten, während der Trust-Level 4 höchste, deutsche Sicherheitsstandards erfüllt und der ständigen Kontrolle unterliegt.

Die erfolgreiche Zertifizierung wird mit einem Zertifikat, welches drei Jahre gültig ist, bescheinigt.

3.2.2 Empfehlung

Die Zertifizierung „Trusted Cloud“ von TÜV Trust-IT liefert für den Anwender ein standardisiertes Prüfverfahren auf Grundlage relevanter Normen und Standards. Auf diese Weise schafft die Zertifizierung Vertrauen in den jeweiligen Cloud-Anbieter.

3.2.3 Nutzen

Der Anwender kann anhand der Güteklassen den Umgang des Cloud-Anbieters mit Sicherheit der Nutzerdaten und die Qualität des Service-Managements ablesen.

3.3 Internationales Zertifikat: Cloud Security Alliance, Security, Trust & Assurance Registry (CSA STAR)

3.3.1 Beschreibung

Cloud Security Alliance (CSA) ist einer der bekanntesten Programme zur Prüfung der Cloud-Anbieter. Die CSA führt ein Register, in welchem alle Anbieter von Cloud-Servies aufgeführt sind. Durch das Register soll eine Vergleichbarkeit der Anbieter und deren Sicherheitsmassnahmen ermöglicht werden.

Die Prüfung wird anhand des hauseigenen Meta-Frameworks vorgenommen, welches die gängigen Standards, Regelungen und Best Practices beinhaltet.

Folgende Standards und Normen werden bei der Prüfung der CSA-Zertifizierung beachtet:

- ISO 27001/27002
- ISACA COBIT
- PCI
- NIST
- Jericho Forum
- NERC CIP

Es gibt drei verschiedene Levels, die die Beurteilung von Cloud-Anbietern erlauben:

- Level 1: CSA STAR Self-Assessment
- Level 2: STAR Certification; STAR Attestation; C-STAR Assessment
- Level 3: STAR Continuous

Zu Level 1: CSA STAR Self-Assessment

CSA STAR Self-Assessment ist allen Cloud-Anbietern frei zugänglich und erlaubt diesen die Durchführung der eigenen Bewertung nach CSA-Vordrucken.

Zu Level 2: STAR Certification; STAR Attestation; C-STAR Assessment[1]

CSA STAR Certification: Ist eine Prüfung des Cloud-Anbieters durch eine dritte Instanz. Dabei werden die Erfüllung der Anforderungen nach ISO/IEC 27001:2005 und CSA Cloud Controls Matrix bescheinigt. Mit CSA Cloud Controls Matrix wird weitere Service-Qualität abgefragt als es nach ISO/IEC 27001:2005 erfolgt.

Des Weiteren beruht STAR Certification auf weiteren internationalen Standards:

- ISO/IEC 17021:2011
- ISO/IEC 27006:2011
- ISO 19011

Die **STAR Attestation** ist als STAR Certification auf Level 2 zu sehen. Es bezieht sich vor allem auf die Kriterien der Cloud Controls Matrix. Insgesamt ist es eine vereinfachte Prüfung im Vergleich zu STAR Certification.

Zu Level 3: CSA STAR Continuous Monitoring

Dieser Level der Überprüfung eines Cloud-Anbieters erlaubt die Automatisierung der vorliegenden Sicherheitspraxis. Dabei werden die Sicherheitsinformationen permanent veröffentlicht und die Kunden und die Tool-Lieferanten können diese Informationen im jeweiligen Kontext abrufen.

3.3.2 Empfehlung

Es wird empfohlen Cloud Service Anbieter mit Level 2 auszuwählen, um die Gewissheit zu haben, dass die wichtigen Standards berücksichtigt wurden.

3.3.3 Nutzen

Der Anwender kann an der Abstufung der Zertifizierung herauslesen inwieweit Standards berücksichtigt worden sind und so den zuverlässigen Umgang mit den Daten in der Cloud ablesen. Zudem werden bei der Zertifizierung auch die internationalen Standards berücksichtigt, die Auskunft über Datensicherheit und die Service-Qualität geben.

[1] Diese Art der Überprüfung bezieht sich vor allem auf den chinesischen Markt und ist hier nicht relevant.

4 Die ISO-Normenreihe für Qualitätsmanagement-systeme

4.1 ISAE 3402

4.1.1 Beschreibung

ISAE 3402 ist ein international anerkannter Standard für interne Kontrollsysteme. Wer rechnungslegungsrelevante Geschäftsprozesse oder IT-Services zur Verfügung stellt, weist mit dem Standard nach, dass hinsichtlich der ausgelagerten Prozesse ein funktionierendes internes Kontrollsystem vorhanden ist.

4.1.2 Empfehlung

Unbedingt empfohlen für Anbieter von rechnungsrelevanten Geschäftsprozessen oder IT-Dienstleistungen.

4.2 ISO/IEC 20000

4.2.1 Beschreibung

Die ISO/IEC 20000 ist der Standard für IT-Service Management. Wer nach ISO 20000 zertifiziert ist, weist nach, dass er seine IT-Services prozessorientiert implementiert hat, dass sein Betrieb auf die Kundenbedürfnisse und das Qualitätsmanagement ausgerichtet ist, und dass seine IT-Organisation ständig verbessert wird. Die Zertifizierung ist während drei Jahren gültig.

4.2.2 Empfehlung

Die Norm schafft mit der starken Ausrichtung auf die Kundenbedürfnisse eine breite Vertrauensbasis.

4.3 ISO 27001 und ISO 27002

4.3.1 Beschreibung

Die ISO 27001 ist der Standard für das Informationssicherheitsmanagement und gilt als eines der vertrauenswürdigsten Zertifikate im IT-Sektor. Die ISO 27001 sieht die Implementierung eines Information Security Management Systems (ISMS) vor. Es umfasst alle Prozesse, Verfahren und Maßnahmen, die ein Unternehmen einsetzt, um ein vorgegebenes Sicherheitsniveau zu erreichen.

Wer nach ISO 27001 zertifiziert ist, weist nach, dass er über ein umfassendes und effektives Informationssicherheits-Managementsystem verfügt und in der Lage ist, mit Sicherheitsrisiken umzugehen.

4.3.2 Empfehlung

Die Fachgruppe Cloud Computing empfiehlt zudem zu kontrollieren, ob die jährlichen Audits und Re-Zertifizierungen durchgeführt werden.

4.3.3 Nutzen

Das durch einen externen und unabhängigen Prüfer ausgestellte Zertifikat bescheinigt dem Anbieter ein umfassendes und etabliertes Sicherheitsmanagement. Somit hat der Kunde Gewissheit, dass die Sicherheit im Rechenzentrum des Anbieters gewährleistet ist.

4.4 ISO 27017 und ISO 27018:2014

4.4.1 Beschreibung

Die beiden Normen ISO 27017 (Cloud Security) und ISO 27018 (Cloud Privacy) spezifizieren die ISO 27001 bezüglich der Sicherheit von Cloud-Leistungen. Die ISO 27017 weitet den Schutz der Informationen auch auf nicht private Benutzer aus und berücksichtigt so die Besonderheit beim Betrieb eines Cloud Service. Die ISO 27018 behandelt den Schutz der Privatsphäre der Benutzer über die Sicherstellung der PII (Personally Identifiable Information).

4.4.2 Empfehlung

Es ist zu beachten, dass sich diese Zertifizierung vor allem auf den Schutz der Privatdaten der Anwender konzentriert. Streng genommen kann keine Zertifizierung nach ISO 27018 vorgenommen werden, da es sich dabei um reine Umsetzungsempfehlungen handelt. Bei diesen ist nicht genau spezifiziert welche Anforderungen zur Erlangung des Zertifikats erfüllt sein müssen.

Die Zertifikate basieren auf der ISO 27001 Zertifizierung, bei welcher zusätzlich die Massnahmen aus der ISO 27018 berücksichtigt wurden.

4.5 Zertifikat für den Betrieb des Rechenzentrums: Tier-IV-Zertifizierung

4.5.1 Beschreibung

Eine Tier-IV Zertifizierung nach den Vorgaben von Uptime Institute ist auf eine fehlertolerante Infrastruktur ausgerichtet. Sie referenziert ausschliesslich die physikalische Topologie, welche für die Betriebsleistungen in einem Rechenzentrum Voraussetzung ist. So ist die Tier-IV Zertifizierung darauf ausgelegt, dass eine Verfügbarkeit der Grundinfrastruktur von 99,99% erreicht wird.

4.5.2 Empfehlung

In der Schweiz haben aktuell die Swisscom und BrainServe Ltd die Tier-IV-Zertifizierung erreicht und die Green Datacenter AG eine Tier III Zertifikation. Da die Tier-IV-Zertifizierung durch die Sicherstellung der physischen, informationstechnischen und organisatorischen Sicherheit sehr breit ist, stellt sie einen hohen Vertrauensnachweis dar. Die Tier-IV-Zertifizierung ist beim Bedarf nach einer sehr hohen Verfügbarkeit der Cloud-Lösung zu empfehlen.

5 Ergänzende Empfehlungen

Zertifikate und Normen sind ein nützliches Hilfsmittel bei der Evaluierung von Cloud Services. Sie beantworten aber nicht alle Fragen, die sich ein Anwender vor der Auswahl eines Cloud Anbieters allenfalls stellt. Der „Cloud Standards Customer Council“ hat eine Reihe von Fragen zusammengestellt, die sich ein Anwender vor der Wahl eines Cloud Anbieters stellen sollte. Die Fragen lauten vereinfacht (Quelle: siehe Link unter Anhang A):

F01: Hat der Cloud Leistungserbringer Prozesse definiert, welche die Governance, das Risikomanagement und die Compliance sicherstellen?

F02: Ist der Cloud Leistungserbringer offen für Audit von Drittparteien?

F03: Wie verwaltet der Cloud Leistungserbringer Personen, Rollen und Identitäten?

F04: Wie werden Daten und Informationen geschützt?

F05: Werden Datenschutzrichtlinien eingehalten?

F06: Wie werden die Anwendungen in der Cloud geschützt?

F07: Sind die Cloud Netzwerke und Verbindungen geschützt?

F08: Wie wird die Sicherheit der physischen Infrastruktur sichergestellt?

F09: Ist die Sicherheit in den Cloud Service Leistungen enthalten?

F10: Wie sind die Sicherheitsanforderungen beim Ausstieg aus der Cloud definiert?

Antworten auf diese Fragen können auf verschiedene Arten gefunden werden:

- Durch das Vorhandensein von Zertifikaten.
- Durch Konsultation der Webseite des potentiellen Anbieters.
- Durch direkte Anfrage beim Cloud Anbieter, wenn die Webseite keine Angaben zur Frage macht.

Der Zusammenhang zwischen einzelnen Fragen und Zertifikaten ist eher schwach. Datenschutz und Informationssicherheit ist ein Thema in allen aufgeführten Cloud Zertifikaten; allerdings geben die Zertifikate nicht spezifisch darüber Auskunft, ob ein zertifizierter Anbieter eine befriedigende Antwort auf jede diese Fragen hat. So gibt beispielsweise keines der aufgeführten Zertifikate Auskunft zur Frage F10. Zudem bleibt der Entscheid darüber, was eine befriedigende Antwort ist, in der Verantwortung des Anwenders.

Das Dokument „D4.1 - Cloud certification guidelines and recommendations“ des CloudWatch Gremiums (Quelle: siehe Link unter Anhang A) enthält eine umfangreiche Sammlung von Informationen zu Einsatz- und Eignungskriterien für Cloud Zertifikate. Soweit anwendbar sind Informationen aus dem genannten Dokument im vorliegenden Überblick enthalten.

In der folgenden Tabelle sind für die Cloud-spezifischen Zertifikate die wichtigsten Einsatzgebiete aufgeführt:

Zertifikate und Normen	Cloud-spezi-fisch	Service Qualität	Datensi-cherheit	Vertrau-lichkeit	Recht, Compli-ance
EuroCloud Star Audit ECSA	**X**	**X**	**X**	**X**	**X**
EuroCloud Star Audit Swiss	**X**	**X**	**X**	**X**	**X**
Trusted Cloud, TÜV Trust-IT	**X**	**X**	**X**	**X**	**X**
CSA Security, Trust & Assur-ance Registry (CSA STAR)	**X**	**X**	**X**	**X**	**(X)**
ISO 27017, ISO 27018:2014	**X**	**(X)**	**X**	**X**	**(X)**

6 Haftungsausschluss/Hinweise auf Rechte Dritter

eCH-Standards, welche der Verein **eCH** dem Benutzer zur unentgeltlichen Nutzung zur Verfügung stellen oder welche **eCH** referenzieren, haben nur den Status von Empfehlungen. Der Verein **eCH** haftet in keinem Fall für Entscheidungen oder Massnahmen, welche der Benutzer auf Grund dieser Dokumente trifft und / oder ergreift. Der Benutzer ist verpflichtet, die Dokumente vor deren Nutzung selbst zu überprüfen und sich gegebenenfalls beraten zu lassen. **eCH**-Standards können und sollen die technische, organisatorische oder juristische Beratung im konkreten Einzelfall nicht ersetzen.

In **eCH**-Standards referenzierte Dokumente, Verfahren, Methoden, Produkte und Standards sind unter Umständen markenrechtlich, urheberrechtlich oder patentrechtlich geschützt. Es liegt in der ausschliesslichen Verantwortlichkeit des Benutzers, sich die allenfalls erforderlichen Rechte bei den jeweils berechtigten Personen und/oder Organisationen zu beschaffen.

Obwohl der Verein **eCH** all seine Sorgfalt darauf verwendet, die **eCH**-Standards sorgfältig auszuarbeiten, kann keine Zusicherung oder Garantie auf Aktualität, Vollständigkeit, Richtigkeit bzw. Fehlerfreiheit der zur Verfügung gestellten Informationen und Dokumente gegeben werden. Der Inhalt von **eCH**-Standards kann jederzeit und ohne Ankündigung geändert werden.

Jede Haftung für Schäden, welche dem Benutzer aus dem Gebrauch der **eCH**-Standards entstehen ist, soweit gesetzlich zulässig, wegbedungen.

7 Urheberrechte

Wer **eCH**-Standards erarbeitet, behält das geistige Eigentum an diesen. Allerdings verpflichtet sich der Erarbeitende, sein betreffendes geistiges Eigentum oder seine Rechte an geistigem Eigentum anderer, sofern möglich, den jeweiligen Fachgruppen und dem Verein **eCH** kostenlos zur uneingeschränkten Nutzung und Weiterentwicklung im Rahmen des Vereinszweckes zur Verfügung zu stellen.

Die von den Fachgruppen erarbeiteten Standards können unter Nennung der jeweiligen Urheber von **eCH** unentgeltlich und uneingeschränkt genutzt, weiterverbreitet und weiterentwickelt werden.

eCH-Standards sind vollständig dokumentiert und frei von lizenz- und/oder patentrechtlichen Einschränkungen. Die dazugehörige Dokumentation kann unentgeltlich bezogen werden.

Diese Bestimmungen gelten ausschliesslich für die von **eCH** erarbeiteten Standards, nicht jedoch für Standards oder Produkte Dritter, auf welche in den **eCH**-Standards Bezug genommen wird. Die Standards enthalten die entsprechenden Hinweise auf die Rechte Dritter.

Anhang A – Referenzen & Bibliographie

Begriff	Beschreibung
BMWi Studie	Das Normungs- und Standardisierungsumfeld von Cloud Computing.Studie für das Bundesministerium für Wirtschaft und Technologie (BMWi). Eine Untersuchung aus europäischer und deutscher Sicht unter Einbeziehung des Technologieprogramms „Trusted Cloud“. Abschlussbericht Stand Februar 2012 http://www.bmwi.de/DE/Mediathek/publikationen,did=476730.html
CloudWatch	A European Cloud observatory supporting cloud policies, standards profiles & services; Herausgeber der Empfehlung “D4.1 – Cloud certification guidelines and recommendations” http://www.cloudwatchhub.eu/ http://cordis.europa.eu/docs/projects/cnect/4/610994/080/deliverables/001-D41Cloudcertificationguidelinesandrecommendationsrevisedversion.pdf
CSA STAR	CSA Security,Trust und Assurance Registry https://cloudsecurityalliance.org/star/
EuroCloud Star Audit ECSA	EuroCloud Star Audit Zertifizierung https://eurocloud-staraudit.eu/
EuroCloud Star Audit Swiss	EuroCloud Star Audit Zertifizierung für die Schweiz http://www.eurocloudswiss.ch/
ISAE 3402	International Standard on Assurance Engagements (ISAE) 3402 http://www.ifac.org/system/files/downloads/b014-2010-iaasb-handbook-isae-3402.pdf
ISO/IEC 20000	Information technology -- Service management -- Part 1: Service management system requirements http://www.iso.org/iso/catalogue_detail?csnumber=51986
ISO 27001	Information technology -- Security techniques -- Information security management systems – Requirements http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54534
ISO 27002	Information technology -- Security techniques -- Code of practice for information security controls http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54533
ISO 27017	Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud services http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=43757
ISO 27018	Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors http://www.iso.org/iso/catalogue_detail?csnumber=61498

Safe Harbor	European Commission's Directive on Data Protection http://www.export.gov/safeharbor/eu/eg_main_018493.asp
Security for Cloud Computing	Cloud Standards Customer Council: Security for Cloud Computing: 10 Steps to Ensure Success V2.0 http://www.cloud-council.org/Security_for_Cloud_Computing_Version_2.pdf
Studie „Cloud Labeling"	Im Rahmen der GovCloud.CH Umsetzung erstellte Studie der Firma CBusiness Services GmbH in Kooperation mit der Fachhochschule Nordwestschweiz (FHNW). Stand Oktober 2013 http://www.isb.admin.ch/themen/projekte_programme/01752/01801/index.html?lang=de
Tier-IV-Zertifizierung	TIA-942 (Telecommunications Infrastructure Standard for Data Centers), Klassifizierung des US-amerikanischen Uptime Instituts https://uptimeinstitute.com/
TÜV Trust-IT	Beschreibung zur der Zertifizierung: Trusted Cloud https://www.it-tuv.com/leistungen/cloud-security/trusted-cloud.html

Anhang B – Mitarbeit & Überprüfung

Name	Organisation/Firma
Reto Gutmann	ETH Zürich
Claudio Giovanoli	Fachhochschule Nordwestschweiz
Pia Wittmann	Ehemals CSC Switzerland GmbH
Andreas Hänecke	CSC Switzerland GmbH

Anhang C – Abkürzungen und Glossar

Begriff	Beschreibung
Label	Ein Label wird grundsätzlich einmal vergeben. Die Einhaltung der Anforderungen wird nicht wiederholend bewertet. Ein Label kann über verschiedene Aspekte, wie Herkunft, Zusammensetzung, Qualität, Produktionsbedingungen eines Produktes oder Dienstleistung vergeben werden. Die Erteilung eines Labels erfolgt über eine Organisation und nicht über eine eigentliche Prüfungsstelle. Im Vergleich zu einer Zertifizierung ist ein Label eine stark abgeschwächte Form und besonders auf Marketingzwecke ausgerichtet.
Norm	Eine Norm ist ein 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 die Tätigkeiten oder deren Ergebnisse festlegt, wobei ein optimaler Ordnungsgrad in einem gegebenen Zusammenhang angestrebt wird.
Safe Harbour	Safe Harbor ist eine Datenschutzvereinbarung zwischen der EU und den USA, die es europäischen Unternehmen ermöglicht, personenbezogene Daten legal in die USA zu übermitteln. Europäische Rechtsstandards werden von Unternehmen, die sich nach der Safe-Harbor-Regelung zertifizieren, voll akzeptiert und respektiert. Der Europäische Gerichtshof hat allerdings das Safe Harbor Abkommen am 6. Oktober 2015 für ungültig erklärt.
Standard	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.
Zertifikat	Ein Zertifikat wird von einer unabhängigen Stelle geprüft und vergeben. Es legt grundsätzlich die Qualitätsstandards für ein Produkt, System oder eine Dienstleistung fest und ist zeitlich beschränkt. Eine Überprüfung der Einhaltung dieser Standards findet regelmässig statt, wodurch die Erneuerung des Zertifikats gewährleistet werden kann. Die Zertifizierung ist dabei der Prozess, welcher durchlaufen werden muss, um an die Bescheinigung (das Zertifikat) zu gelangen.