eCH-0198 - Vue d'ensemble des certificats pertinents pour l'utilisation du Cloud

Titre	Vue d'ensemble des certificats pertinents pour l'utilisation du Cloud
Code	eCH-0198
Type	Document auxiliaire
Stade	Défini
Version	1.0
Statut	**Approuvé**
Approuvé le	2016-06-01
Date de publication	2016-07-25
Remplace	-
Langues	-
Annexes	-
Langues	Allemand (original), français (traduction)
Auteur(s)	**Groupe spécialisé Cloud Computing** Reto Gutmann, ETH Zürich, rgutmann@ethz.ch Claudio Giovanoli, FHNW, claudio.giovanoli@fhnw.ch Pia Wittmann, anciennement CSC Switzerland GmbH Andreas Hänecke, CSC Switzerland GmbH, ahanecke@csc.com
Editeur / distributeur	Association eCH, Mainaustrasse 30, case postale, 8034 Zurich T 044 388 74 64, F 044 388 71 80 www.ech.ch / info@ech.ch

Condensé

Le présent document auxiliaire recommande et décrit les certificats actuels et pertinents pour les prestataires Cloud Computing en Suisse. Elle doit faciliter la tâche à l'utilisateur final lors de la sélection d'un prestataire approprié. Le document auxiliaire contient une annexe 1, qui décrit un programme en 10 étapes pour l'évaluation de la sécurité du Cloud et les certificats recommandés correspondants.

Sommaire

Indication

La forme épicène sera évitée lorsque cela est possible. Le nom commun sera utilisé si besoin afin de simplifier la forme, ce qui implicitement couvre l'autre genre.

1 Introduction

1.1 Statut

Approuvé: **le document a été approuvé par le Comité des experts et a force normative pour le domaine d'application défini dans la sphère de validité stipulée**.

1.2 Champ d'application

Les certifications Cloud et la vérification de la conformité des services Cloud avec les critères pertinents relatifs à la protection des données, à la sécurité et aux caractéristiques de qualité garanties prennent une place de plus en plus importante dans l'évaluation de la fiabilité services Cloud.

À l'heure actuelle, il existe, au niveau national et international, de nombreux acteurs distincts dans le domaine de la normalisation et de la standardisation du Cloud Computing. Les normes, qui ont fait leurs preuves par le passé, ne couvrent qu'en partie les exigences imposées au Cloud Computing et les normes se référant explicitement au Cloud Computing sont encore relativement nouvelles et méconnues. Reste à savoir dans quelle mesure elles seront diffusées et acceptées.

Le présent document auxiliaire s'adresse aux organisations aussi bien publiques que privées, qui prévoient de passer au Cloud et cherchent une assistance dans leur choix d'un prestataire Cloud Computing approprié. Il décrit les certificats qui, du point de vue du groupe spécialisé Cloud Computing, sont pertinents en Suisse, ce qui signifie qu'ils sont établis et reconnus dans les milieux spécialisés au même titre que les normes ISO ou qui seront considérés comme applicables à l'avenir, comme l'Euro Cloud Star Audit, qui est encore tout récent.

2 Certifications recommandées pour les prestataires Cloud Computing

Le tableau suivant présente sous forme sommaire les certificats répertoriés dans le document auxiliaire et la priorité attribué à chacun certificat.

La colonne Centre de données présente les certificats, qui se réfèrent principalement à la prestation de services IT depuis un centre de données. La prestation de services IT depuis un centre de données constitue, en termes de technologie comme d'organisation, la base de la prestation de services Cloud.

Les certificats de service Cloud incluent en règle générale plusieurs parties de normes et de directives tirées du domaine des centres informatiques et les complètent par des éléments propres au Cloud (ex. Controls & Privacy).

Certificats et normes	Chapitre	Centre de données	Service Cloud
Certificats européens			
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**
Certificats internationaux			
CSA Security, Trust & Assurance Registry (CSA STAR)	3.3	**x**	**X**
Série de normes ISO			
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**
Certificat pour l'exploitation du centre de données			
Certification Tier IV	4.6	**x**	

3 Description des certifications recommandées

3.1 Certificats européens: EuroCloud Star Audit (ECSA) et EuroCloud Star Audit Swiss

3.1.1 Description

EuroCloud Europe (ECE) a pour vocation de faire accepter les services Cloud sur le marché international ainsi que de favoriser la mise à disposition, axée sur le client, de ces services et de leur demande. ECE propose le système de certification «EuroCloud Star Audit» (ECSA), afin d'établir la confiance dans les services Cloud par une évaluation de la qualité tant du côté du client que de l'utilisateur.

La procédure de certification repose sur une norme européenne regroupant différents modules et une auto-évaluation (Self-Assessment) ou une certification propre à chaque pays.

La certification est conçue de manière spécifique pour les domaines IaaS, PaaS et SaaS et dispose d'affirmations définies pour les éléments de contrôle, qui doivent être remplis progressivement afin d'obtenir la certification de prestataire Cloud digne de confiance.

EuroCloud Swiss est l'association suisse de promotion du Cloud Computing en Suisse et le représentant national agréé d'EuroCloud Star Audit.

L'audit comporte différents contrôles auxquels doit se soumettre un prestataire Cloud. Un catalogue de questions détaillées sert à évaluer le respect des directives de sécurité. Le certificat prévoit un maximum de cinq étoiles. Une fois la valeur maximale atteinte, le client peut supposer que le prestataire Cloud est tout à fait digne de confiance. Le catalogue de contrôle de l'EuroCloud Star Audit SaaS a été élaboré en étroite collaboration avec différentes institutions, dont le Deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI – office fédéral allemand de la sécurité dans les techniques d'information), l'ENISA / l'ETSI ainsi que l'UE.

EuroCloud a conçu un label de qualité spécial pour les exigences contractuelles, techniques et organisationnelles susmentionnées, dont l'utilisation présuppose que les exigences fondamentales relatives à la fourniture de services Cloud ont bien été contrôlées par des auditeurs formés et confirmés par un certificat. Un catalogue de critères a été élaboré pour les exigences de contrôle, en étroite concertation avec des institutions publiques, des établissements de recherche, des prestataires Cloud, des experts en droit et des sociétés d'audit.

L'EuroCloud Star Audit traite des catégories suivantes de manière concrète:

- Profil du prestataire
- Contrat et Compliance
- Sécurité
- Exploitation de l'infrastructure
- Processus d'exploitation
- Utilisation
- Mise en œuvre

Un système de points et la prescription de critères minimaux permettent à un prestataire d'atteindre différents niveaux de qualité (d'une à cinq étoiles).

En terme de résultat, les trois niveaux de qualité suivants sont accessibles en fonction de degré de mise en œuvre:

- Trusted Cloud-Service – trois étoiles
- Trusted Cloud-Service Advanced – quatre étoiles
- Trusted Cloud-Service Advanced HA (High Availability) – cinq étoiles

3.1.2 Recommandation

Le vaste périmètre de la certification EuroCloud contribue grandement à établir la confiance. La certification étant encore récente, il reste encore à voir si elle sera adoptée par la filière.

3.1.3 Intérêts

De manière générale, l'EuroCloud Star Audit est un bon instrument avec un haut degré de transparence et d'orientation pour l'utilisateur, qui l'aide dans son choix d'un prestataire Cloud. Des niveaux de certification, l'utilisateur peut déduire la fiabilité et la gestion des données d'utilisateur pratiquée par le prestataire Cloud.

3.2 Certificat européen: TÜV Trust-IT: Trusted Cloud

3.2.1 Description

La procédure de contrôle standardisée «Trusted Cloud» repose sur les normes et standards pertinents et se compose d'une procédure à sept niveaux.

Les normes et standards pertinents sont:

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

La procédure à 7 niveaux se décompose comme suit:

1. Définition du périmètre
2. Contrôle des documents
3. Analyse processus, organisation, audit, analyse technique
4. Compte-rendu des résultats
5. Certification
6. Monitoring Audit 1ère année
7. Monitoring Audit 2ème année

Sont alors contrôlées les catégories suivantes:

- Sécurité organisationnelle et technique,
- Qualité de la gestion de service et
- Compliance.

Il existe, pour chacun des domaines thématiques, quatre Trust Level (niveaux de qualité). Ces différents Trust Levels sont identifiés selon les critères d'exigence avec les modèles de service correspondants IaaS, PaaS et SaaS. Ces Levels se distinguent en termes de protec-

tion des données. Le plus faible niveau de qualité, le niveau de base 1, convient à l'enregistrement et au traitement de données non critiques, tandis que le Trust Level 4 remplit les normes de sécurité allemandes maximales et est soumis à un contrôle permanent.

Un certificat d'une durée de validité de trois ans confirme que la certification a bien été effectuée avec succès.

3.2.2 Recommandation

La certification «Trusted Cloud» de TÜV Trust-IT offre à l'utilisateur un procédé de contrôle standardisé sur la base des normes et standards pertinents. De cette façon, la certification donne confiance concernant le prestataire Cloud concerné.

3.2.3 Intérêts

L'utilisateur peut à partir des niveaux de qualité déduire la façon dont le prestataire Cloud gère la sécurité des données de l'utilisateur et la qualité de la gestion du service.

3.3 Certificat international: Cloud Security Alliance, Security, Trust & Assurance Registry (CSA STAR)

3.3.1 Description

Cloud Security Alliance (CSA) est l'un des programmes les plus connus de contrôle des prestataires Cloud. La CSA tient un registre répertoriant tous les prestataire de services Cloud. Ce registre doit permettre de comparer les prestataires et les mesures qu'ils prennent en matière de sécurité.

Le contrôle est effectué sur la base du Meta-Framework développé par l'organisme, qui contient les normes, règles et Best Practices courantes.

Les normes et standards suivants sont respectés lors de l'examen de la certification CSA:

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

Il existe trois niveaux ou *levels* différents permettant l'évaluation des prestataires Cloud:

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

Concernant le Level 1: CSA STAR Self-Assessment

Le CSA STAR Self-Assessment est librement accessible à tous les prestataires Cloud et leur permettent de procéder à leur propre évaluation au moyen des imprimés de la CSA.

Concernant le Level 2: STAR Certification; STAR Attestation; C-STAR Assessment[1]
CSA STAR Certification: il s'agit d'un contrôle du prestataire Cloud par une instance tiers. Cette opération confirme que les exigences selon ISO/IEC 27001:2005 et CSA Cloud Controls Matrix sont bien respectées. Le CSA Cloud Controls Matrix sert à s'informer de la qualité du service comme cela est fait selon l'ISO/IEC 27001:2005.

En outre, STAR Certification repose sur d'autres normes internationales:

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

La **STAR Attestation** doit être considérée comme la STAR Certification de Level 2. Elle se rapporte avant tout aux critères de la Cloud Controls Matrix. Il s'agit globalement d'un contrôle simplifié comparé à la STAR Certification.

Concernant le Level 3: CSA STAR Continuous Monitoring
Ce niveau de vérification d'un prestataire Cloud permet l'automatisation des pratiques actuelles en matière de sécurité. Les informations de sécurité sont publiées en permanence et les clients et les fournisseurs d'outils peuvent consulter ces informations dans le contexte correspondant.

3.3.2 Recommandation

Il est recommandé d'opter pour un prestataire de Cloud Services de niveau 2 afin d'avoir la certitude que les standards importants sont bien pris en compte.

3.3.3 Intérêts

L'utilisateur peut déduire de la classification de la certification dans quelle mesure les standards sont pris en compte et la fiabilité de la gestion des données dans le Cloud. En outre, la certification tient également compte des normes internationales, qui fournissent des renseignements concernant la sécurité des données et la qualité du service.

[1] Ce type de contrôle se rapporte avant tout au marché chinois et n'est donc pas pertinent dans le présent contexte.

4 Série de normes ISO pour les systèmes de gestion de la qualité

4.1 ISAE 3402

4.1.1 Description

L'ISAE 3402 est une norme internationalement reconnue pour les systèmes de contrôle interne. Quiconque fournit des services IT ou des processus d'affaires pertinents pour la facturation, atteste par cette norme qu'il dispose bien d'un système de contrôle interne performant concernant les processus externalisés.

4.1.2 Recommandation

Recommandée de manière impérative pour les prestataires de processus d'affaires ou de services IT pertinents pour la facturation.

4.2 ISO/IEC 20000

4.2.1 Description

La norme ISO/IEC 20000 est la norme pour la gestion des services IT. Quiconque est certifié selon la norme ISO 20000 atteste par cette norme qu'il propos bien des services IT axés sur les processus, que son exploitation est orientée sur les besoins du client et que la gestion de la qualité, et qu'il améliore en continu son organisation IT. La certification est valable pendant trois ans.

4.2.2 Recommandation

La norme établit une vaste base de confiance avec une orientation marquée sur les besoins des clients.

4.3 ISO 27001 et ISO 27002

4.3.1 Description

L'ISO 27001 est la norme pour la sécurité de la gestion des informations et est considérée comme l'un des certificats les plus fiables du secteur IT. L'ISO 27001 prévoit la mis en œuvre d'un Information Security Management System (ISMS). Elle couvre tous les processus, procédures et mesures, qu'une entreprise met en œuvre en vue de garantir un niveau de sécurité prescrit.

Quiconque est certifié selon l'ISO 27001 atteste du fait qu'il dispose bien d'un système efficace et complet de sécurité de gestion des informations et est en position d'appréhender les risques de sécurité.

4.3.2 Recommandation

Le groupe spécialisé Cloud Computing recommande en outre de contrôler si les audits et re-certifications annuels sont bien effectués.

4.3.3 Intérêts

Le certificat délivré par un examinateur externe et indépendant la gestion de la sécurité complète et établie du prestataire. Le client a ainsi la certitude que la sécurité est garantie dans le centre de données du prestataire.

4.4 ISO 27017 et ISO 27018:2014

4.4.1 Description

Les deux normes ISO 27017 (Cloud Security) et ISO 27018 (Cloud Privacy) spécifient l'ISO 27001 concernant la sécurité des prestations Cloud. L'ISO 27017 étend la protection des informations également aux utilisateurs non particuliers et tient ainsi compte des spécificités de l'exploitation d'un service Cloud. L'ISO 27018 traite de la protection de la sphère privée des utilisateurs par la sécurité des PII (Personally Identifiable Information).

4.4.2 Recommandation

Il est à noter que cette certification se concentre avant tout sur la protection des données privées des utilisateurs. Stricto sensu, il ne peut être procédé à aucune certification selon la norme ISO 27018, car il s'agit simplement de recommandations de mise en œuvre. Celles-ci ne spécifient pas précisément quelles exigences doivent être remplies pour obtenir le certificat.

Les certificats reposent sur la certification ISO 2700, qui tient compte également des mesures de la norme ISO 27018.

4.5 Certificat pour l'exploitation du centre de données: certification Tier IV

4.5.1 Description

Une certification Tier IV selon les directives de l'Uptime Institute est orientée sur une infrastructure tolérant les erreurs. Elle référence exclusivement la topologie physique, qui est une condition sine qua non pour les prestations d'exploitation dans un centre de données. La certification Tier IV est conçue pour offrir une disponibilité de l'infrastructure de base de 99,99%.

4.5.2 Recommandation

En Suisse, Swisscom et BrainServe Ltd ont actuellement obtenu la certification Tier IV et Green Datacenter AG une certification Tier III. La certification Tier IV étant très vaste du fait de la garantie de la sécurité physique, informative et organisationnelle, elle constitue un justificatif de confiance de haut niveau. La certification Tier IV doit être recommandée en cas de besoins d'une solution Cloud extrêmement disponible.

5 Recommandations complémentaires

Les certificats et normes constituent un outil utile d'évaluation des services Cloud. Ils ne répondent toutefois pas à toutes les questions, qu'un utilisateur peut se poser avant de choisir un prestataire Cloud. Le «Cloud Standards Customer Council» a compilé une série de questions, qu'un utilisateur devrait se poser avant de choisir un prestataire Cloud. Ci-après, les questions en version simplifiée (source: voir lien en annexe A):

F01: Le prestataire de services Cloud a-t-il défini des processus, qui garantissent la gouvernance, la gestion des risques et la compliance?

F02: Le prestataire de services Cloud est-il ouvert aux audits par des parties tiers ?

F03: Comment le prestataire de services Cloud gère-t-il les personnes, les rôles et les identités?

F04: Comment les données et informations sont-elles protégées?

F05: Les directives en matière de protection des données sont-elles respectées?

F06: Comment les applications sont-elles protégées dans le Cloud?

F07: Les réseaux et connexions Cloud sont-elles protégées?

F08: Comment la sécurité de l'infrastructure physique est-elle garantie?

F09: La sécurité est-elle comprise dans les prestations du Cloud Service?

F10: Comment les exigences de sécurité sont-elles définies lorsque l'on quitte le Cloud?

Il existe plusieurs moyens de trouver des réponses à ces questions:

- Par la présence de certificats.
- En consultant le site Web du prestataire potentiel.
- En s'adressant directement au prestataire Cloud, à défaut d'information relative à la question sur le site Web.

Le lien entre les différentes questions et les certificats est relativement ténu. La protection des données et la sécurité des informations sont un enjeu pour tous les certificats Cloud répertoriés; toutefois, les certificats ne précisent pas de manière spécifique si un prestataire certifié offre bien une réponse satisfaisante à chacune de ces questions. Ainsi, aucun des certificats répertoriés n'apporte de réponse à la question F10. En outre, il appartient à l'utilisateur de décider si une réponse est satisfaisante ou non.

Le document «D4.1 - Cloud certification guidelines and recommendations» de l'organisme CloudWatch (source: voir le lien en annexe A) comprend un recueil détaillé d'informations sur les critères d'utilisation et d'adéquation pour les certificats Cloud. Dans la mesure où elles sont applicables, les informations tirées du document cité figurent dans la présente vue d'ensemble.

Le tableau suivant répertorie les plus importants domaines d'application des certificats spécifique au Cloud:

Certificats et normes	Spécifique Cloud	Qualité de service	Sécurité données	Confidentialité	Droit, Compliance
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 & Assurance Registry (CSA STAR)	**X**	**X**	**X**	**X**	**(X)**
ISO 27017, ISO 27018:2014	**X**	**(X)**	**X**	**X**	**(X)**

6 Exclusion de responsabilité - droits de tiers

Les normes élaborées par l'Association **eCH** et mises gratuitement à la disposition des utilisateurs, ainsi que les normes de tiers adoptées, ont seulement valeur de recommandations. L'Association **eCH** ne peut en aucun cas être tenue pour responsable des décisions ou mesures prises par un utilisateur sur la base des documents qu'elle met à disposition. L'utilisateur est tenu d'étudier attentivement les documents avant de les mettre en application et au besoin de procéder aux consultations appropriées. Les normes **eCH** ne remplacent en aucun cas les consultations techniques, organisationnelles ou juridiques appropriées dans un cas concret.

Les documents, méthodes, normes, procédés ou produits référencés dans les normes **eCH** peuvent le cas échéant être protégés par des dispositions légales sur les marques, les droits d'auteur ou les brevets. L'obtention des autorisations nécessaires auprès des personnes ou organisations détentrices des droits relève de la seule responsabilité de l'utilisateur.

Bien que l'Association **eCH** mette tout en œuvre pour assurer la qualité des normes qu'elle publie, elle ne peut fournir aucune assurance ou garantie quant à l'absence d'erreur, l'actualité, l'exhaustivité et l'exactitude des documents et informations mis à disposition. La teneur des normes **eCH** peut être modifiée à tout moment sans préavis.

Toute responsabilité relative à des dommages que l'utilisateur pourrait subir par suite de l'utilisation des normes **eCH** est exclue dans les limites des réglementations applicables.

7 Droits d'auteur

Tout auteur de normes **eCH** en conserve la propriété intellectuelle. Il s’engage toutefois à mettre gratuitement, et pour autant que ce soit possible, la propriété intellectuelle en question ou ses droits à une propriété intellectuelle de tiers à la disposition des groupes de spécialistes respectifs ainsi qu’à l’association **eCH**, pour une utilisation et un développement sans restriction dans le cadre des buts de l’association.

Les normes élaborées par les groupes de spécialistes peuvent, moyennant mention des auteurs **eCH** respectifs, être utilisées, développées et déployées gratuitement et sans restriction.

Les normes **eCH** sont complètement documentées et libres de toute restriction relevant du droit des brevets ou de droits de licence. La documentation correspondante peut être obtenue gratuitement.

Les présentes dispositions s’appliquent exclusivement aux normes élaborées par **eCH**, non aux normes ou produits de tiers auxquels il est fait référence dans les normes **eCH**. Les normes incluront les références appropriées aux droits de tiers.

Annexe A – Références & bibliographie

Notion	Description
Etude BMWi	Environnement de normalisation et de standardisation de Cloud Computing. Etude menée pour le compte du Ministère fédéral de l'économie et de la technologie (BMWi). Une étude du point de vue européen et allemand en tenant compte du programme de technologie «Trusted Cloud». Rapport final version février 2012 http://www.bmwi.de/DE/Mediathek/publikationen,did=476730.html
CloudWatch	A European Cloud observatory supporting cloud policies, standards profiles & services; éditeur de la Recommandation "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 et Assurance Registry https://cloudsecurityalliance.org/star/
EuroCloud Star Audit ECSA	Certification EuroCloud Star Audit https://eurocloud-staraudit.eu/
EuroCloud Star Audit Swiss	Certification EuroCloud Star Audit pour la Suisse 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	Directive de la Commission européenne sur la protection des données 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
Etude «Cloud Labeling»	Etude réalisée dans le cadre de la mise en œuvre GovCloud.CH par l'entreprise CBusiness Services GmbH en coopération avec la Fachhochschule Nordwestschweiz (FHNW). Version octobre 2013 http://www.isb.admin.ch/themen/projekte_programme/01752/01801/index.html?lang=fr
Certification Tier IV	TIA-942 (Telecommunications Infrastructure Standard for Data Centers), classification de l'Uptime Institut, Etats-Unis https://uptimeinstitute.com/
TÜV Trust-IT	Description relative à la certification: Trusted Cloud https://www.it-tuv.com/leistungen/cloud-security/trusted-cloud.html

Annexe B – Collaboration & vérification

Nom	Organisation/entreprise
Reto Gutmann	ETH Zurich
Claudio Giovanoli	Fachhochschule Nordwestschweiz
Pia Wittmann	anciennement CSC Switzerland GmbH
Andreas Hänecke	CSC Switzerland GmbH

Annexe C – Abréviations et glossaire

Notion	Description
Label	Par principe, un label n'est attribué qu'une seule fois. Le respect des critères correspondants ne fait pas l'objet d'évaluations répétées. Un label peut être accordé selon divers critères tels l'origine, la composition, la qualité ou les conditions de production d'un produit ou service. Un label est octroyé non pas par une instance de contrôle, mais par une organisation. Comparé à une certification, un label est une forme nettement «édulcorée», qui répond avant tout à des attentes marketing.
Norme	Une norme est un document, qui a été produit par consensus et adopté par une institution reconnue. Elle fournit, pour des usages communs et répétés, des règles, des lignes directrices ou des caractéristiques pour des activités ou leurs résultats, garantissant un niveau d'ordre optimal dans un contexte donné.
Safe Harbour	Safe Harbor est un accord portant sur la protection des données conclu entre l'UE et les Etats-Unis, qui permet aux entreprises européennes, de transmettre légalement des données personnelles vers les Etats-Unis. Les entreprises, qui demandent la certification Safe Harbor, acceptent et respectent pleinement les normes légales européennes. Le 6 octobre 2015, la Cour européenne a cependant invalidé l'accord Safe Harbor.
Standard	Une standard est une façon, comparativement homogène ou harmonisée, globalement reconnue et appliquée (ou tout au moins visée) dans la plupart des cas, de produire ou d'effectuer quelque chose, qui s'est imposée par rapport à d'autres façons de faire.
Certificat	Un certificat est contrôlé et délivré par une instance indépendante. Il stipule en principe les normes de qualité d'un produit, d'un système ou d'une prestation de service et est limité dans le temps. Le respect de cette norme fait l'objet de vérifications régulières, qui peuvent garantir le renouvellement du certificat. La certification est le processus obligatoire par lequel s'obtient le certificat.