Next Generation Certification

Vertrauenswürdige Cloud-Services durch dynamische Zertifizierung qualitativer, datenschutzrechtlicher und sicherheitstechnischer Anforderungen

Ergebnisdokument für	AP 7
Titel	**Evaluierung der dynamischen Zertifizierung hinsichtlich der automatisierten und nicht-automatisierten Komponenten** **Management Summary**
Autoren	Andreas Weiss Christine Neubauer Michael Lang Prof. Dr. Helmut Krcmar Dr. Manuel Wiesche Johanna Hoffmann Prof. Dr. Alexander Roßnagel Sebastian Lins Prof. Dr. Ali Sunyaev Georg Pribyl Britta Laatzen Christian Banse Prof. Dr. Claudia Eckert
Version	5.2
Datum	10.03.2018

I. Änderungsverzeichnis

Version	Beschreibung der Änderung(en)	Autor	Datum
V1	Strukturaufbau, inhaltliche Stichpunkte, erste Ausformulierungen	Christine Neubauer	07.07.2016
V2, V3	Ergänzungen TUM	Michael Lang	08.07.2016 14.07.2016
V.3.1	Ergänzungen Provet	Johanna Hofmann	14.07.2016
V4	Ergänzung EuroCloud	Christine Neubauer	14.07.2016
V4.1	Zusammenführung Input	Christine Neubauer	18.07.2016
V4.2	Ergänzungen Uni Kassel Systementwicklung	Sebastian Lins	20.07.2016
V4.3	Update Kapitel 4	Georg Pribyl	20.07.2016
V4.5	Ergänzungen Uni Kassel Systementwicklung	Sebastian Lins	22.07.2016
V4.6	Ergänzungen EuroCloud	Christine Neubauer	22.07.2016
V4.7	Ergänzungen Uni Passau	Ramona Kühn	01.08.2016
V4.8	Britta Laatzen, Kapitel 6.3, weitere Überarbeitungen	Britta Laatzen	02.08.2016
V4.9	Ergänzungen AISEC	Christian Banse	05.08.2016
V5.0	Review aller Kapitel und Kommentierung	Andreas Weiss	12.08.2016
V5.1	Formale Änderungen	Christine Neubauer	15.08.2016
V5.2	Kapitel 4.3 Bild aktualisiert Formale Änderungen	Georg Pribyl Christine Neubauer	18.08.2016

II. Inhaltsverzeichnis

III. Abbildungsverzeichnis

1. Einleitung

1.1 Motivation

Für viele Unternehmen ist die Nutzung von Cloud-Diensten ein elementarer Bestandteil einer weiteren Digitalisierung von Unternehmensabläufen mit erkennbaren Vorteilen im Bereich der Kosten, der Unternehmenssteuerung und generellen Vorteilen bei der Wettbewerbsfähigkeit. Allerdings schrecken sie davor zurück, weil belastbare Nachweise für die Einhaltung zentraler Datenschutz- und Datensicherheitskriterien fehlen. Auch bestehende Zertifikate sind nicht ausreichend, weil sie aufgrund der hohen Dynamik der Cloud-Technologien zu unflexibel sind. Der Gültigkeitszeitraum heutiger Zertifikate liegt typischerweise im Bereich von einem bis drei Jahren. Innerhalb dieses Zeitraumes verlieren sie entweder ihre Gültigkeit, weil zentrale Hardwarekomponenten oder Softwaremodule ausgetauscht werden, oder man nimmt ein Sicherheitsrisiko in Kauf, weil auf genau diesen Austausch verzichtet wird. Darüber hinaus kann sich auch in rechtlicher Hinsicht etwas ändern, so dass ein zunächst erteiltes Zertifikat seine Gültigkeit verlieren kann.

1.2 Projekt Ziel

Forschung und Entwicklung einer dynamischen Zertifizierung zum kontinuierlichen Nachweis des Zertifizierungsstatus

1.3 Förderung

- Das Projekt **NGCert** ist Teil des Themenfeldes "Sicheres Cloud Computing" im Rahmen der Hightech-Strategie der Bundesregierung.
- Projektvolumen: 2,34 Mio. € (davon 91% Förderanteil durch das Bundesministerium für Bildung und Forschung (BMBF))

1.4 Hypothesen

- Es ist möglich, kritische Anforderungen eines Zertifikats automatisiert zu prüfen.
- Eine rein automatisierte Zertifizierung ist (nur) für einzelne Prüfschritte möglich.
- Mit Hilfe automatisierter Prüfschritte kann die Erfüllung von Anforderungen hinsichtlich Qualität, Datenschutz und Datensicherheit rechtssicher erbracht werden.
- Es ist zwischen Prüfungsinhalt und -verfahren zu unterscheiden. Ein und derselben Anforderung kann – je nach Zuordnung zum Prüfungsinhalt oder -verfahren – unterschiedliches Gewicht zukommen.
- Die Verteilung der Rollen einer dynamischen Zertifizierung darf nicht mit den Anforderungen an die Neutralität und Unabhängigkeit der Prüfungsinstanz in Konflikt stehen.

1.5 Umsetzungsziele

- Spezifikation der Anforderungen in Form von Anwendungsfällen für eine dynamische Zertifizierung, sowie Beschreibung eines Referenzmodells
- Definition eines Kennzahlensystems inklusive der (teil-)automatisierten Mess- und Vergleichsverfahren sowie eine Taxonomie zur Beschreibung von Cloud-Services als Grundlage für eine dynamische Zertifizierung

- Design der Systemarchitektur und des Vorgehens für das kontinuierliche Monitoring sowie Reporting an die unterschiedlichen Interessengruppen
- Dokumentation möglicher Vertragsrahmen, der organisatorischen und betrieblichen Aspekte, der wirtschaftlichen Betrachtung sowie der Akzeptanz
- Prototypische Implementierung von Basis-Komponenten, von Monitoring-Services sowie eines (teil)automatisierten Zertifizierungsdienstes
- Evaluationsergebnisse und Erprobungsbericht aus den Pilotierungen bei den Feldpartnern

2. Ausgangssituation:

Es gibt viele Zertifikate mit unterschiedlichem Umfang, Zielen, Gültigkeiten und Reichweiten, alle sind retrospektiv.

Abbildung 1. Cloud-Service-Zertifizierungen am Markt.

2.1 Herausforderungen

Die Herausforderung ist hier die Dynamik des Marktes gegenüber der Retrospektive der Zertifikate, denn bestehende Zertifikate beziehen sich immer nur auf einen Zustand, der in der Vergangenheit liegt. Des Weiteren ist zu berücksichtigen, dass Cloud-Dienste in vielen Fällen als Lieferkette mehrerer Dienstleistungen (Co-Lokation, Managed Service Anbieter, Cloud Anbieter...) zu betrachten ist und somit an vielen Stellen technische und organisatorische Änderungen entstehen können, die Auswirkungen auf die jeweiligen Zertifikatsaussagen haben. Für den Anwender sind die Zertifikate mit unterschiedlichen Schwerpunkten und Ausrichtungen kaum vergleichbar und auch nicht transparent.

2.2 Vorhaben zur Adressierung der Herausforderungen

- Forschung und Entwicklung einer dynamischen Zertifizierung zum kontinuierlichen Nachweis des Zertifizierungsstatus
- Verifizierte Sicherheits- und Datenschutz-Parameter
- Zertifizierung als "geeignete Garantie" nach der europäischen Datenschutz-Grundverordnung

- Sicherstellung der Rechtskonformität
- Aktualität der Zertifikatsaussage
- Schaffung von Transparenz zur Stärkung des Marktvertrauens auf einem Gebiet, das vertiefte Sach- und Fachkenntnis voraussetzt (Vertrauen zum Ausgleich mangelnder Kenntnisse)
- Automatisiertes Audit und Reporting
- Cloud Monitoring On-Demand

3. Lösungsansatz

Um den aktuellen Herausforderungen von Cloud-Service-Zertifikaten zu begegnen, ist es erforderlich, dass ausgewählte Zertifizierungsanforderungen (teil-)automatisiert und kontinuierlich überprüft werden. Hierbei stellt sich jedoch zunächst die Frage, welche Anforderungen entscheidend bei der Adoptionsbeurteilung von Cloud-Services sind, und daher besondere Relevanz für eine fortlaufende Überwachung aufweisen (siehe Kapitel 3.1). Zertifizierungsanforderungen sind in natürlicher Sprache verfasst und werden in Katalogen zusammengefasst. Diese Dokumentation erlaubt es sowohl Auditoren als auch Cloud-Service-Anbietern und -Kunden die Anforderungen leicht zu verstehen. Allerdings ist eine computergestützte Überprüfung von natürlich sprachigen Anforderungen nicht direkt möglich. Es entsteht eine semantische Lücke, die zunächst geschlossen werden muss (siehe Kapitel 3.2).

3.1 Priorisierung

Die Auswahl eines geeigneten Cloud Service Providers (CSP) ist eine der wesentlichen Herausforderungen zur Sicherstellung der späteren Cloud Sourcing Performance aus Kundensicht.

Damit der NGCert-Monitoring-Service auch die aus Kundensicht relevanten Informationen bereitstellt, wurde im Rahmen einer iterativen Umfrage (Delphi Studie) eine Priorisierung der wesentlichen Entscheidungskriterien vorgenommen[1]. Die 16 Cloud Entscheider sind zum Schluss gekommen, dass die Top 7 Kriterien wie Folgt sind:

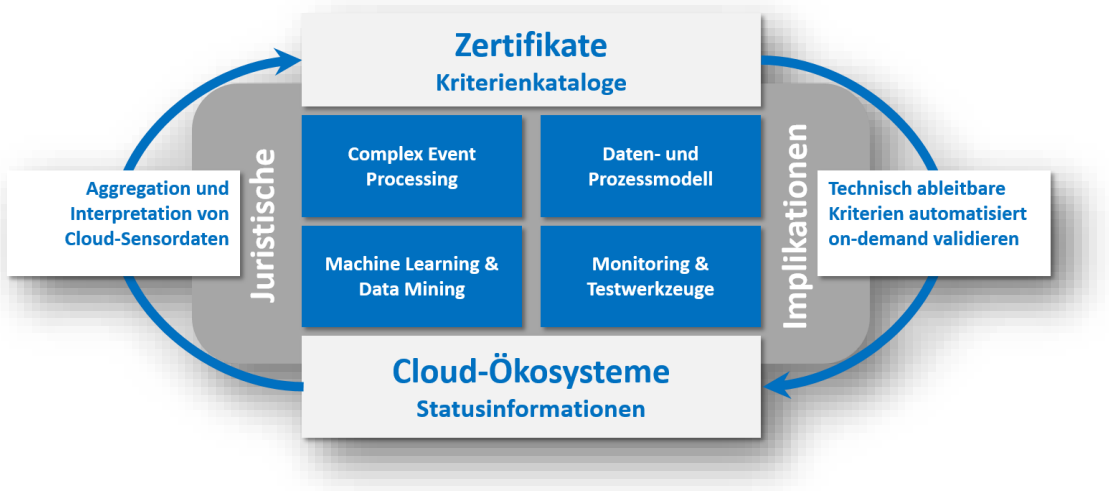
1) Funktionalität (Performance, Sicherheit, ...)
2) Rechtssicherheit
3) Vertragliche Rahmenbedingungen
4) Geolokation der Server
5) Flexibilität
6) Integrierbarkeit der Cloud-Lösung
7) Transparenz der Provider Aktivitäten

[1] Im Rahmen der Europäischen Konferenz für Informationssysteme 2016 (European Conference for Information Systems 2016) wurden die Ergebnisse der Delphi Studie veröffentlicht: Lang, Wiesche, Krcmar (2016). What are the most important criteria for cloud service provider selection? A Delphi study.

3.2 Semantische Lücke

Die sog. Semantische Lücke (Semantic Gap) zwischen den Kriterienkatalogen der Zertifikate und den Statusinformationen der Cloud-Ökosysteme muss geschlossen werden:

- über technisch ableitbare Kriterien, die automatisiert oder bei Bedarf zu validieren sind
- über die Aggregation und Interpretation von Cloud-Sensordaten
- unter rechtlichen Implikationen mit Hilfe von
    - Complex Event Processing
    - Daten- und Prozessmodellen
    - Monitoring & Testwerkzeugen
    - Machine Learning & Data Mining



3.3 Innovative Ansätze

Um die obig angesprochenen Herausforderungen zu bewältigen, sind Innovative Ansätze von Nöten. Zunächst wird ein Kriterienkatalog für dynamische Zertifizierungen erstellt, die Vergleichbarkeit zu bestehenden Zertifizierungen sichergestellt. Danach kann die Semantische Lücke für eine Auswahl von Zertifizierungsanforderungen des Katalogs geschlossen werden, wie beispielsweise die Verfügbarkeitsmessung.

3.3.1 Rechtlicher Ansatz

Die technikadäquate Entwicklung eines dynamischen Zertifizierungssystems erfordert die Erstellung eines umfassenden Kriterienkatalogs, der zwischen Zertifizierungsverfahren und -inhalt unterscheidet. Es bietet sich die Methode zur Konkretisierung rechtlicher Anforderungen zu technischen Gestaltungsvorschlägen (KORA) an.[2] Rechtliche Vorgaben sind in der Regel zu abstrakt, um konkrete technische Gestaltungsmerkmale für ein technisches System zu enthalten. Über ein stufenweises Vorgehen schafft KORA die Verbindung zwischen den zunächst inkompatibel erscheinenden Disziplinen Recht und Technik. Am Ende soll nicht nur ein rechtmäßiges Konzept stehen, das zwingende rechtliche Anforderungen erfüllt. Vielmehr verfolgt KORA das Ziel besonders vorteilhafter, das heißt rechtsverträglicher Gestaltung.

---

[2] Die Methode KORA wurde von der Projektgruppe verfassungsverträgliche Technikgestaltung an der Universität Kassel entwickelt. Zur Methode *Hammer/ Pordesch/ Roßnagel*, Informatik und Gesellschaft, 1993, 21 ff.; *dies.*, Betriebliche Telefon- und ISDN-Anlagen rechtsgemäß gestalten, 1993, 46 ff.

KORA ist in vier Stufen aufgeteilt. Den Ausgangspunkt bilden verfassungsrechtliche Vorgaben, aus denen rechtliche Anforderungen abgeleitet werden, die bereits konkreter sind, als die Vorgaben. In einem dritten Schritt erfolgt die Konkretisierung hin zu rechtlichen Kriterien. Aus diesen wiederum werden in der Folge technische Ziele entwickelt, die auf der letzten Stufe in konkrete technische Gestaltungsvorschläge münden. Durch diese Ableitung von der abstrakten normativen Quelle bis hin zu konkreten technischen Vorschlägen werden Recht und Technik nachvollziehbar miteinander in Einklang gebracht.

3.3.2 Interoperabilität

Der oben unter 3.3.2 beschriebene Kriterienkatalog für den Prüfungsinhalt dient als Vorlage für sog. NGCert-Kontrollen. Darunter sind relativ abstrakte Prüfungsfragen zu verstehen, die wiederum der Konkretisierung bedürfen, um möglichst (teil-)automatisiert überprüfbar zu sein. Die Abstraktheit der NGCert-Kontrollen liegt darin begründet, dass herkömmliche Zertifizierungskataloge auf dem Gebiet des Cloud-Computing unterschiedliche Konkretisierungsgrade aufweisen, und in einer natürlichen Sprache dokumentiert wurden. Um jedoch einen möglichst großen Nutzen des dynamischen Zertifizierungskonzepts zu erreichen, sollte der NGCert-Kriterienkatalog auf möglichst viele verschiedene herkömmliche Zertifizierungsverfahren auf dem Gebiet des Cloud-Computing anwendbar sein. Durch die Zuordnung der einzelnen NGCert-Kontrollen zu bestimmten Kontrollen in den unterschiedlichen herkömmlichen Zertifizierungskatalogen wird zum einen Transparenz geschaffen. Darüber hinaus ist für den späteren Anwender, den Auditor (im Rahmen einer externen Zertifizierung) oder den CSP (beim internen Monitoring), klar erkennbar, auf welche Kontrollen der herkömmlichen Zertifizierungskataloge die NGCert-Mechanismen anwendbar sein können. Im Einzelfall mag eine Kontrolle nach Einschätzung des Anwenders zwar nicht auf einen bestimmten herkömmlichen Katalog übertragbar sein und sich darum eine grundsätzlich möglich (teil-)automatisierte Prüfung verbieten. Allerdings dient die genannte Zuordnung dem schnelleren Auffinden des jeweiligen Einsatzgebietes. Im Ergebnis führt die taxonomische Zuordnung der NGCert-Kontrollen zur Vergleichbarkeit von bislang sehr unterschiedlichen Zertifizierungskatalogen. Sie zeigt ferner Lückenhaftigkeiten einzelner herkömmlicher Kataloge auf, deren Ursache darin liegt, dass herkömmliche Zertifizierungen stets auf der bewertenden Einschätzung eines Auditors basieren. Durch die dem NGCert-Katalog zugrundeliegende KORA-Ableitung (vgl. die Erläuterungen zu KORA unter 3.3.2) werden zudem erstmalig die normativen Grundlagen der einzelnen Prüfkriterien herkömmlicher Kataloge erkennbar.

3.3.3 Adressierung der semantischen Lücke

Entwicklung einer Domänen-spezifischen Sprache zur automatisierten Verarbeitung von Anforderungen.

3.3.4 Ein Beispiel: Verfügbarkeit vs. Kontrollfähigkeit

Eine der Kontrollen ist eine "Verfügbarkeit" der Komponenten in der Cloud, die vom Cloud Provider angegeben wird. Hier gibt es wiederum eine Semantische Lücke, da Verfügbarkeit nur eine Wahrscheinlichkeit ist, ob das System kontrollfähig ist.

Verfügbarkeit wird so beschrieben, dass sie besteht, wenn die Kontrollfähigkeit über IT-Ressourcen für Cloud-Kunden und Cloud Provider gegeben ist. Kontrollfähigkeit heißt, dass der Kunde die Ressourcen steuern und beeinflussen kann, daher auch auf ihre Funktionstüchtigkeit hin überprüfen kann. Für einen Kunden jedoch gilt das System bereits als nicht verfügbar, sobald er nicht darauf zugreifen kann bzw. seine Anforderungen nicht erfüllt werden können. Dabei spielt es für

ihn keine Rolle, ob das verbindende Netzwerk (oftmals das öffentliche Internet) dazwischen oder das System selbst ausgefallen ist.

Anders betrachtet kann ein System zwar verfügbar sein aber trotzdem nicht funktionieren. Deshalb ist die Kontrollfähigkeit der entscheidende Faktor.

Um diese festzustellen, wird überprüft, ob das System erreichbar ist, also Daten empfangen oder senden kann und ob es funktionstüchtig ist, also Steuerungsbefehle ausgeführt werden können. Unsere entwickelten Messverfahren zielen darauf ab, Verfügbarkeit im Sinne der Kontrollfähigkeit aus Sicht des Cloud-Kunden zu erfassen und zu messen.

4. Feldpartnertest

4.1 Einleitung

Die in der ersten Phase intern erprobten NGCert-Monitoring-Services sollen in einer zweiten Phase mit Auditoren und dann in einer dritten Phase mit Feldpartnern evaluiert werden. Ziel ist es, die tatsächliche Relevanz, Aussagekraft, Integrationsmöglichkeiten und Weiterverwendungsmöglichkeiten zu beurteilen und zu verbessern sowie mögliche Problemfelder zu identifizieren. All diese Aktivitäten sollen zur Verbesserung des NGCert-Monitoring-Services beitragen und zu konkreten Umsetzungen für die verschiedenen Servicemodelle der Auditoren und Feldpartner führen.

4.2 Schwerpunkt

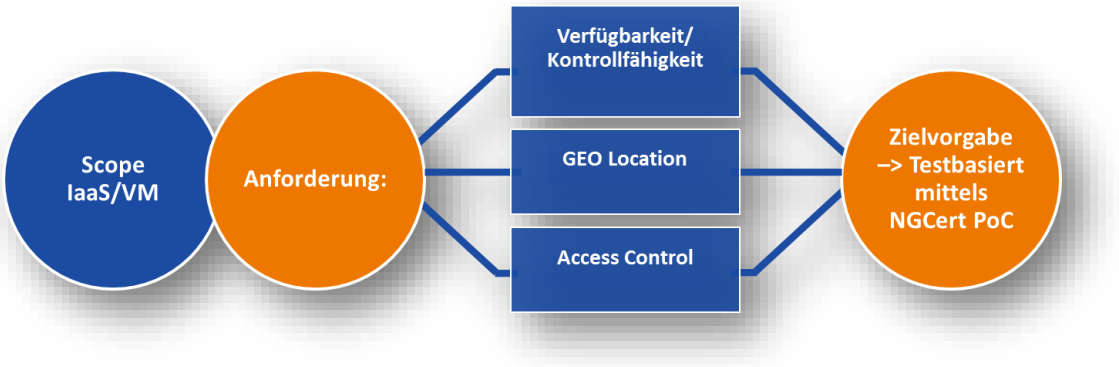
Für den Feldpartnertest haben wir 3 Kriterien ausgewählt, um die automatisierte Prüfung umzusetzen und zu testen. Basierend auf den Ergebnissen der Kundenpräferenzen, wurden für den Feldpartnertest die folgenden 3 Kriterien ausgewählt, um die automatisierte Prüfung umzusetzen und zu testen. Diese 3 Kriterien adressieren auch die wesentlichen Kriterien, die Kunden bei ihren Entscheidungsprozessen anwenden, um einen geeigneten Provider auszuwählen[3]. Diese Kriterien sind

- Verfügbarkeit / Kontrollfähigkeit,
- Geo-Lokation und
- Access Control in drei verschiedenen Ausprägungen.

Entsprechend der Kriterien Auswahl konzentrieren wir den Feldpartnertest auf fünf Anwendungsszenarien („Use Cases“) für Messverfahren, die die Funktionsfähigkeit und Integrität auf der Ebene des Infrastruktur-as-a-Services testen.

[3] Siehe: Lang, Wiesche, Krcmar (2016). What are the most important criteria for cloud service provider selection? A Delphi study. In European Conference for Information Systems 2016. Istanbul.

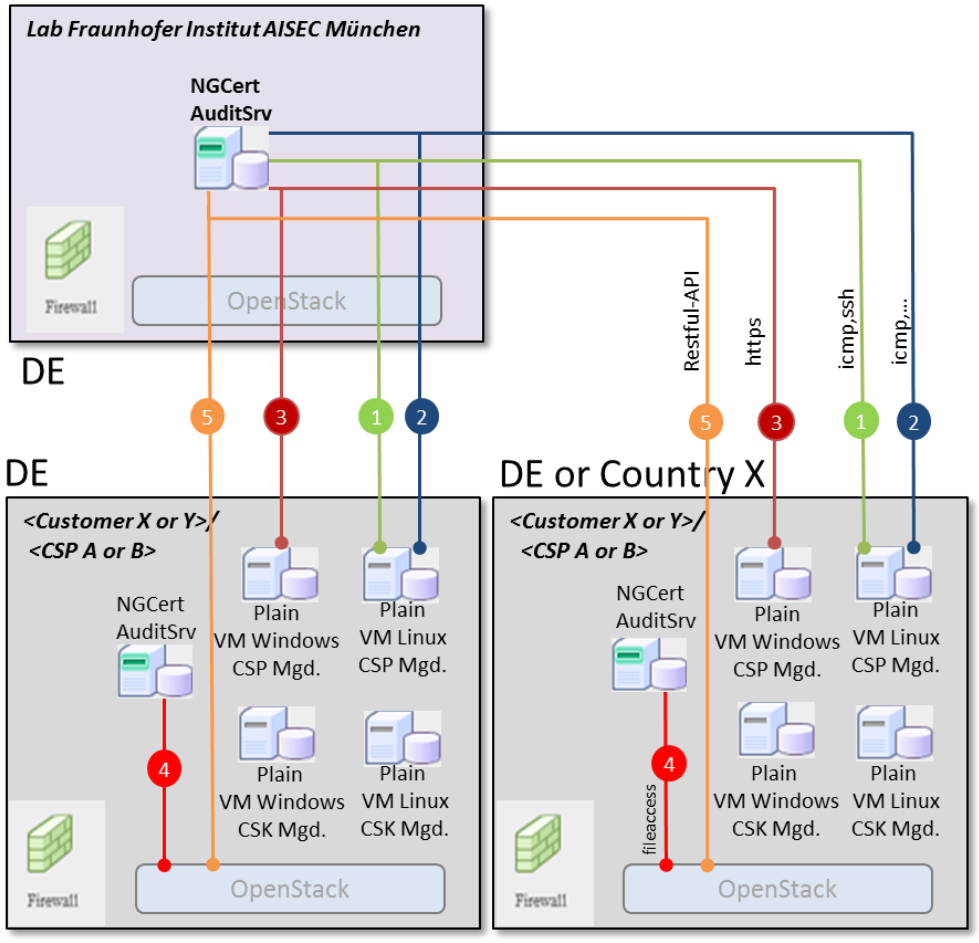
Zielvorgabe ist eine testbasierte Auditierung. Die Grafik verdeutlicht den Rahmen eines Feldpartnertests.



4.3 Messverfahren

Im Folgenden werden die fünf Use Cases und zugehörigen Messverfahren des Feldpartnertests vorgestellt und beschrieben. Die folgende Grafik vermittelt einen Überblick und zeigt das Testprinzip der fünf Use Cases:

1. Verfügbarkeit bzw. Kontrollfähigkeit
2. Geo-Lokation
3. Access Control – Windows-Sicherheitsrichtlinien
4. Access Control – Fehlgeschlagene Self-Service-Logins
5. Access Control – VM Action Log



4.3.1 Verfügbarkeit/Kontrollfähigkeit

Um die Kontrollfähigkeit im Sinne der Verfügbarkeit zu testen, wird zunächst ein Messbereich ausgewählt innerhalb dessen eine VM als Messobjekt instanziiert wird. Prinzipiell gibt es verschiedene Möglichkeiten für die Auswahl des Messbereichs. Mögliche Messbereiche zur Platzierung einer instanziierten VM sind:

- Infrastructure Tier
- Web Tier
- Database Tier (nur konzeptionell)

Darüber hinaus besteht die Möglichkeit, die Kontrollfähigkeit des Self-Service Portals als für die Kunden sichtbaren Messbereich auszuwählen, den wir im Rahmen des Feldpartnertests jedoch nicht weiter verfolgen.

Messbereiche im Feldpartnertest:
Im Rahmen des Feldpartnertests fokussieren wir den Messbereich auf eine instanziierte VM, die im Infrastructure Tier platziert wird.

Metriken und Testfälle:
Die Kontrollfähigkeit wird hierbei durch eine Kombination von mehreren einzelnen Testfällen bestimmt. Hierzu zählen unter anderem:

- Test der Erreichbarkeit einer VM durch „anpingen“, mittels ICMP-Paketen
- Test der Kontrolle einer Linux-basierten VM durch den Versuch, eine SSH-Verbindung mit gültigem User aufzubauen
- Test der korrekten Funktionsweise einer Web-Oberfläche durch Aufbau einer HTTP(S)-Verbindung und Überprüfung des zurückgelieferten Status-Codes

Die Auswahl der konkreten Testfälle bestimmt sich durch das Messobjekt (z.B. HTTP(S)-Verbindung für Web-Tier VMs).

Aus den einzelnen kontinuierlichen Testergebnissen, kann nun als Metrik die Verfügbarkeit bzw. Kontrollfähigkeit ermitteln werden. Sie ergibt sich aus den aufsummierten Zeitdistanzen fehlgeschlagener Testfälle.

Die Messverfahren sind auf ein geeignetes Messintervall abgestellt, bzw. können entsprechend eines spezifischen Zielniveaus (z.B. 99,999 %) eingestellt werden.

4.3.2 GEO Location VM

Die Aussage der geographischen Lage einer VM oder eines Netzwerkknotens kann eine entscheidende Rolle bei der Einhaltung von Gesetzen und Regeln sein. Im Rahmen des NGCert-Projektes wurden daher Methoden entwickelt, die geographische Lage einer VM möglichst genau zu bestimmen.

Hierbei muss zwischen zwei Anwendungsfällen unterschieden werden, welche jedoch auf eine gemeinsame technische Implementierung zurückzuführen ist:

- Bekannte geographische Lage einer VM und Detektion einer Änderung
- Unbekannte geographische Lage und Bestimmung der Lokation

Technisch wird die Bestimmung einer Geo-Lokation über sogenannte *traceroutes* implementiert. Hierbei werden von einem zentralen, bekannten Knotenpunk z.B. Frankfurt, ICMP-Pakete zur Ziel-VM geschickt und hierbei der Pfad (traceroute) analysiert. Mittels Machine-Learning-Verfahren kann nun bestimmt werden, ob sich die Pfade hierbei über die Zeit die Pfade stark verändern, was auf einer Änderung der Geo-Lokation zurückzuführen ist. Des Weiteren können die Pfade auch mit traceroutes anderer VMs abgeglichen werden, um so eine unbekannte geographische Lage zu bestimmen.

4.3.3 Access Control – Sicherheitsrichtlinien/Winaudit

Die lokalen Sicherheitsrichtlinien existieren auf jedem Windows-PC und legen eine Reihe von Sicherheitseinstellungen fest. Hier finden sich z.B. die Kennwort-Richtlinien, die Systemrechte der Benutzer, eine Reihe von Systemeinstellungen, die Firewall Konfiguration und Netzwerk-Zugriffsregeln, die IP-Sec-Konfiguration und die Möglichkeit, die Ausführung von Software zu verhindern (Software-Restriction-Policies und App-Locker).

Die lokalen Sicherheitsrichtlinien können zentral über das Active Directory mit Hilfe der Gruppenrichtlinien überschrieben werden. Alle Einstellungen, die in den lokalen Sicherheitsrichtlinien festgelegt sind, gibt es in den Gruppenrichtlinien ebenfalls. Wird ein Computer in die Domäne aufgenommen, werden die Kennwortrichtlinien beispielsweise sofort nur noch aus der Domäne bezogen und die lokalen Richtlinien werden überschrieben. Die meisten anderen Richtlinien sind jedoch in der Domäne standardmäßig nicht konfiguriert, so dass die lokalen Richtlinien trotzdem Gültigkeit haben.

Messbereiche im Feldpartnertest:

- Cloud Service Kunde
- Plain VM mit Windows OS (CSP Managed)
- Lokale Sicherheitsrichtlinien/Policies

Metriken:

- Password Policies
  - Maximum password age
  - Password must meet complexity requirement

- Account Lockout Policies
  - Account lockout duration
  - Account lockout threshold
  - Reset lockout counter after

- Security Options
  - Accounts: Administrator account status
  - Accounts: Block Microsoft accounts
  - Accounts: Guest account status
  - Accounts: Limit local account use of blank passwords to console logon only
  - Accounts: Rename administrator account
  - Accounts: Rename guest account

4.3.4 Access Control – Fehlgeschlagene Self-Service-Logins

Zur tiefergehenden Prüfung der Access-Log-Verfügbarkeit für Userlogin-Aktivitäten wird ein Userlogin über http-request mit einem nicht registrierten User erzeugt und die Error-Log des Apache-Servers (Dashboards) nach dem nicht erfolgreichen Logon-Eintrag des Users gesucht und ausgewertet.

Messbereiche im Feldpartnertest:

- Cloud Service Provider
- User Login Dashboard (Self-Service Portal from OpenStack)
- Access Log (Apache)

Metriken:

- Failed User Login with a non-registered user account

4.3.5 Access Control – VM Action Log

Im VM Action Log werden Informationen über Steuerungsbefehle, welche über ein Self-Service Portal an die virtuellen Maschinen gesendet werden, erfasst, um so gegebenenfalls Verstöße aufzudecken. Hierbei handelt es sich um Ereignisse wie das Beenden oder der Neustart einer VM. Diese Aktivitäten werden in einer Log-Datei aufgezeichnet.

Messbereiche:

- Cloud Service Provider
- Self-Service-Portal (OpenStack)
- Action Log der VM Änderungen

Metriken:

- Ausgeführte VM-Steuerungsbefehle der Cloud-Managementplattform
  Bsp.: Herunterfahren einer VM durch einen Admin des Cloud-Providers außerhalb des vereinbarten Wartungsfensters

4.4 Ergebnisse und Evaluation

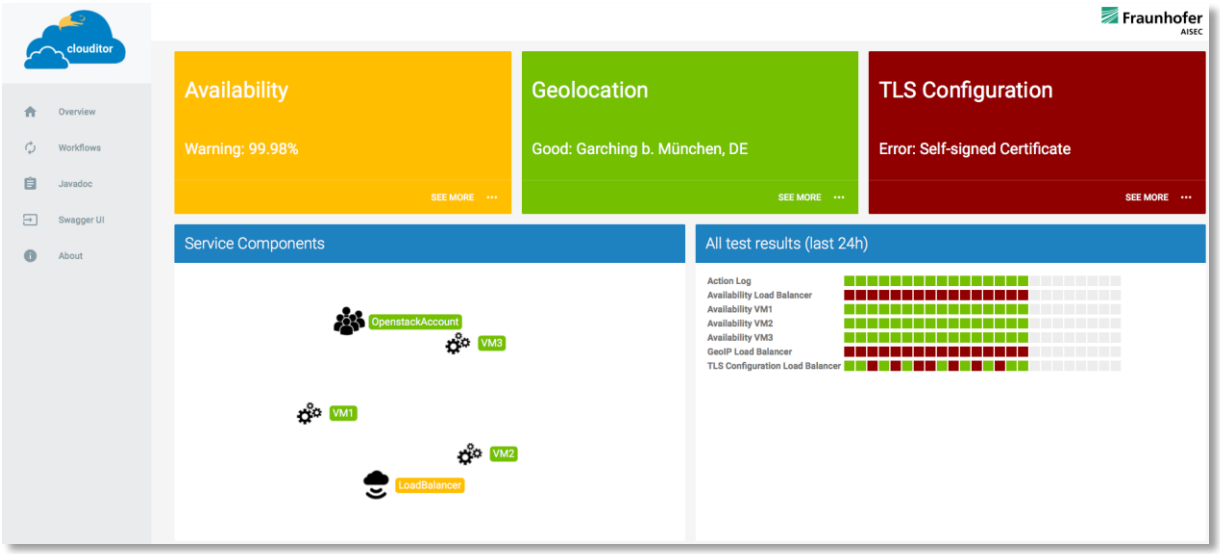
(entsprechend der Messbereiche, siehe oben)

Die Messverfahren, die Ergebnisse der Messungen und die Aussagefähigkeit der Ergebnisse sollen mit den Feldpartnern, gespiegelt an den Use Cases, evaluiert werden. Ziel ist es, die Relevanz, Aussagekraft und Integrationsmöglichkeiten des NGCert-Monitoring-Services zu beurteilen, mögliche Problemfelder zu identifizieren und daraus abgeleitet Maßnahmen zur Verbesserung des Service für einen späteren Produktiveinsatz zu verstehen und zu planen.

Im Folgenden werden die zu evaluierenden Themenfelder entlang der fünf Use Cases beschrieben.

4.4.1 Verfügbarkeit/Kontrollfähigkeit

Die Ergebnisse der Messverfahren Verfügbarkeit/Kontrollfähigkeit werden über ein Dashboard grafisch aufbereitet und ansprechend dargestellt. Die folgende Grafik zeigt exemplarisch die Gestaltung des Dashboards.

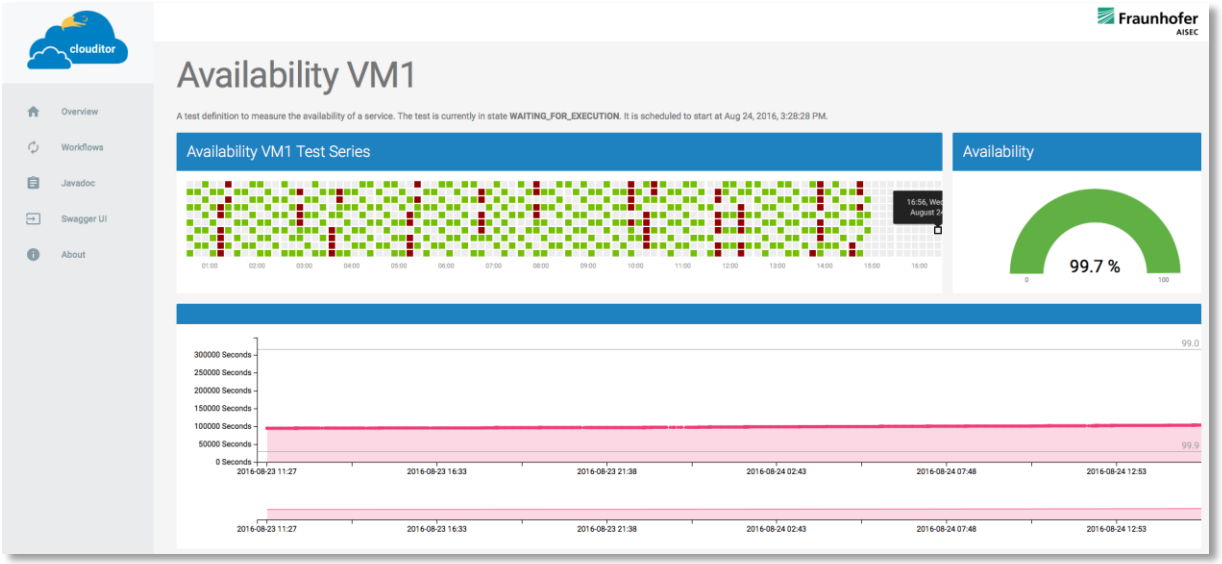


Die drei Blöcke in der Mitte - Availability, Geolokation (Geofencing), Vulnerabilities - fassen jeweils eine Eigenschaft eines Cloud-Dienstes zusammen, dessen aufbereitete Daten ein Auditor als dynamisch erzeugte Informationsquelle zu Prüfungszwecken heranziehen kann. Später können diese durch weitere Eigenschaften, z.B. Sicheres Access Management ergänzt werden.

Unterhalb der drei Blöcke befindet sich eine Zusammenfassung der Testergebnisse der letzten 48 Stunden für jeweils eine Eigenschaft - hier Availability, Geolokation (= Geofencing), OpenStack Dashboard, sowie ActionLog. Letzteres ist ein Test, der feststellt, ob ein Admin den Zustand einer VM in OpenStack unerlaubter Weise geändert hat. Im Falle von Availability sind zwei Kästchen rot, ein Ausfall wurde festgestellt.

Im Rahmen des Feldpartnertests möchten wir eine Einschätzung zum Messverfahren Verfügbarkeit/Kontrollfähigkeit erfahren und die Aussagefähigkeit sowie den Anwendungsnutzen der verschiedenen Funktionen des Dashboards, der sogenannte Clouditor, vor dem Hintergrund verschiedener Stakeholder analysieren.

Es folgt eine kurze Beschreibung zur Bedienung und zu den Anzeigen des Dashboards anhand der Ergebnisse, die wir im Rahmen des Proof-of-Concepts erzielt haben.



Testvisualisierung: Wählt man eine Eigenschaft aus der Übersicht (Figure 1) aus, so kann man sich die detaillierten Testergebnisse sowie eine geeignete Metrik anzeigen lassen. Das sehen Sie hier anhand des Beispiels Availability.

Die einzelnen Elemente im Überblick: "Availability Test Series": Dort gibt es grüne, rote, sowie graue Kästchen. Jedes Kästchen steht für eine Minute. Die Blöcke oberhalb der Uhrzeiten, z.B. 03:00, messen genau sechs Kästchen der Länge nach und zehn in der Höhe, sodass jeder diese Blöcke die Availability innerhalb einer Stunde (6*10 Minuten) anzeigt.

Nun zu den Farben: Ein grünes Kästchen bedeutet, dass ein durchgeführter Test erfolgreich ausgeführt wurde, der Cloud Service war also erreichbar. Rot bedeutet das Gegenteil: Hier schlug der Test fehl. Ist ein Feld grau, so wurde kein Test durchgeführt. Zum Abschluss dieses Elementes noch ein wichtiges Detail: Technisch gesehen handelt es sich bei den Kästchen (rot, grün, grau) um eine nominale Skala, d.h. nur weil ein Kästchen rot ist, heißt das nicht (!), dass der Cloud Service 1 Minute ausgefallen ist. Deswegen kann man die roten Kästchen auch nicht einfach addieren und erhält als Ergebnis die Summe, in der Availability nicht erfüllt war. Diese Art der Visualisierung haben wir gewählt, um minutengenau zu zeigen, wann ein Test fehlschlug, mehr zeigen die Kästchen jedoch nicht.

Weitere Details insbesondere über die gemessene, d.h. quantitative Ausfallzeit findet man im Block "Availability“ - rechts neben "Availability Test Series". 99,873 % ist das Ergebnis der bisher gemessenen Ausfallzeit im Verhältnis zu einem Jahr. Unterhalb wird mit der roten Kurve gezeigt, wie diese Availability zu Stande kommt (Tile „Accumulated Downtime"), das ist nun die gemessene Ausfallzeit. Je mehr Ausfall wir messen, desto weiter steigt die rote Kurve an ("Burn up" chart). Die grauen, horizontalen Linien zeigen übliche, jährliche Grenzwerte, etwa 99,9 %. Im Beispiel: Zum Zeitpunkt des Screenshots liegen wir zwischen 15.000 und 20.000 Sekunden. Daraus lässt sich dann (eine Art von) Availability leicht ableiten: 1 (perfekte Availability, immer erreichbar) minus Ausfallzeit, z.B. 20.000, geteilt durch die Sekunden im Jahr (~31 Millionen). Das Ergebnis dieser kleinen Rechnung ist die Zahl, die rechts oben bei „Availability“ angezeigt wird.

4.4.2 GEO Location VM

Im Rahmen des Feldpartnertests möchten wir eine Einschätzung zum Messverfahren GEO Location VM erfahren und die Aussagefähigkeit sowie den Anwendungsnutzen vor dem Hintergrund verschiedener Stakeholder analysieren.

Insbesondere möchten wir erfahren, welche Messobjekte am geeignetsten sind aus Sicht des Cloud-Providers und aus Sicht der Cloud-Kunden. Für welche Sicherheitszonen im Netzwerk eines Cloud-Providers kann das Messverfahren „minimal-invasiv" angewendet werden? Welcher Nutzen ist damit verbunden? Ist es denkbar, das Messverfahren auf Backendsysteme anzuwenden?

Es folgt eine Beschreibung der Analysemethodik und der Ergebnisse, die wir im Rahmen des Proof-of-Concepts erzielt haben.

4.4.3 Access Control

Im Rahmen des Feldpartnertests möchten wir eine Einschätzung zu den drei Messverfahren im Bereich des Access Controls erfahren.

Die Fragestellungen, die wir gemeinsam beantworten möchten, lauten:

Wie stellt sich der Nutzen, also die Aussagefähigkeit des Messverfahrens als Beispiel einer ganzen Klasse ähnlicher Verfahren, im Verhältnis zum Aufwand der Integration des Messverfahrens in die produktive Managementumgebung eines Cloud-Providers und des damit verbundenen Risikos dar? Die Fragestellung soll anhand der Risiko- und Sicherheitsbetrachtung eingehend reflektiert werden, die für die Testumgebung und Testabläufe des Feldpartnertests in Anlehnung an die Standardvorgehensweise BSI 100-2 aufgestellt worden ist und bereitgestellt wird.

Welche Managementsysteme werden zur Protokollierung und Auswertung von Access-Control-Daten eingesetzt? Wie wird die Aussagefähigkeit eines zweiten, unabhängigen Messverfahrens eingeordnet, gespiegelt an dem Bedarf verschiedener Stakeholder?

4.5 Nächste Schritte

Im weiteren Verlauf des Forschungsprojektes wird der spezifizierte Proof of Concept umgesetzt und evaluiert (siehe Abbildung 2) Dazu muss zunächst der Prozess der dynamischen Zertifizierung vollständig spezifiziert werden (bspw. in Hinblick auf involvierte Stakeholder, deren Rollen und Verantwortlichkeiten sowie notwendigen Aktivitäten und Workflows). Im Anschluss werden die im Proof of Concept dargestellten Messverfahren Verfügbarkeit, Geo-Lokation und Access Control in die Cloud-Service-Infrastruktur der am Projekt teilnehmenden Cloud-Service-Provider integriert und in Betrieb genommen. Der Betrieb wird fortlaufend überwacht und die Ergebnisse der Messverfahren analysiert, um ihre Wirksamkeit, Effektivität und Aussagekraft beurteilen zu können. Ferner sind zusätzliche Fokusgruppeninterviews mit Cloud-Service-Providern und –Auditoren geplant. Gemeinsam mit den Forschern werden die erzielten Ergebnisse diskutiert, um Feedback aus der Praxis zu erhalten. Wichtig sind hierbei die Fragestellungen, wie die Prozesse und Ergebnisse des Zertifizierungsverfahrens aufbereitet werden müssen, welche Wirkung und Wertschöpfung erzielt werden kann, und wie die Ergebnisse der Messeverfahren durch Auditoren verwendet werden können, um die Einhaltung eines Zertifikates kontinuierlich zu prüfen. Die Erkenntnisse aus dieser Evaluierungsphase fließen bei der Konzeption, dem Design und der Umsetzung des Prototypens ein, sodass dieser verbessert und optimiert werden kann. Abschließend

ist geplant, den Prototypen bei einen oder mehreren Feld- und Transferpartner zu implementieren, um die Anwendung in verschiedenen Szenarien testen zu können sowie die Robustheit des Prototypens evaluieren zu können.

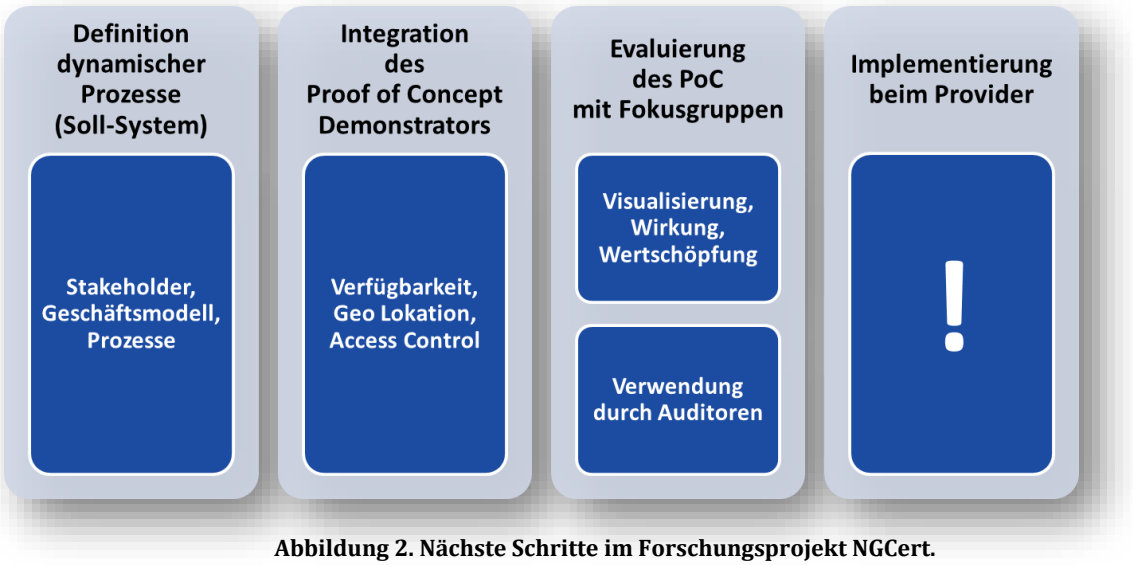


Abbildung 2. Nächste Schritte im Forschungsprojekt NGCert.

5. Prognose

- Hohe Marktrelevanz durch neue zwingende europaweite Vorgaben:
  DSGVO (Datenschutz/ Datensicherheit) und IT Sicherheitsgesetz / NIS Direktive
- Entwicklung einer universellen minimal invasiven Test Suite
  und Konfigurationssprache
- Hoher Nutzen unserer assoziierten Partner und weiterer potenzieller Kunden
  -> Fokusgruppen
- Neue rechtliche Implikationen durch Einsatz eines NGCert-Dienstes
- Hoher Impact durch wiss. Publikationen, Website und Newsletter
  (rund 300 Abonnenten)

5.1 Mögliche Verwendungen

Die Einführung einer dynamischen Zertifizierung ermöglicht aufgrund der Vielzahl von Verwendungsmöglichkeiten eine Entstehung unterschiedlicher und innovativer Geschäftsmodelle. Dazu zählen insbesondere (1) ein dynamischer Zertifizierungsdienst für Zertifizierungsunternehmen und Auditoren, und (2) ein erweiterter Monitoring-Dienst für Cloud-Service-Provider.

(1) Dynamischer Zertifizierungsdienst für Zertifizierungsunternehmen und Auditoren

Das Hauptziel des Projektes NGCert ist es, den Wandel von einer traditionellen auf eine dynamische, kontinuierliche Zertifizierung von Cloud-Services zu ermöglichen. Daher wird ein Zertifizierungsdienst prototypisch entwickelt, der sowohl Zertifizierungsunternehmen bei der Überwachung ihrer individuellen Zertifizierungsanforderungen, als auch Auditoren bei der Auditierung von Cloud-Services unterstützen soll. Auf dem Markt können sich daher zukünftig unabhängige Provider etablieren, welche einen dynamischen Zertifizierungsdienst anbieten. Diese müssen gewisse NGCert-Richtlinien erfüllen, und werden von einer Überwachungsinstanz überwacht. Ein Zertifizierungsunternehmen

kann hingegen auch den Dienst selbst betreiben und seinen Auditoren zur Verfügung stellen.

(2) Erweiterter Monitoring-Dienst für Cloud-Service-Provider

Im Gegensatz zu einem reinen Zertifizierungsdienst können die Forschungsergebnisse auch von einem Cloud-Service-Provider genutzt werden, um seine bestehenden Monitoring-Systeme zu erweitern. Dabei wäre es denkbar, dass der Provider die entwickelten Dienste selbst integriert und betreibt, oder Dritte diese erweiterten Monitoring-Dienste im Cloud-Markt anbieten. Hierbei ist jedoch zu unterscheiden, dass ein erweitertes Monitoring nicht eine dynamische Zertifizierung ersetzt, da die Unabhängigkeit der Ergebnisse eines erweiterten Monitorings nicht gegeben ist. Durch ein die Nutzung der Forschungsergebnisse im Rahmen eines erweiterten Monitorings können Cloud-Service-Provider einerseits ihre Systeme und Prozesse kontinuierlich überwachen und verbessern. Zum anderen können sie die kontinuierlichen Informationen ihren Kunden bereitstellen, um mehr Transparenz zu schaffen.

5.2 Entstehung eines neuen Wertschöpfungsnetzwerkes

Durch die Entwicklung und Umsetzung einer dynamischen Zertifizierung ergibt sich das Potential eines neuen Wertschöpfungsnetzwerks, in dem neue Akteure mit innovativen Geschäftsmodellen auftreten können, und bestehende Akteure neue Rollen und Verantwortlichkeiten einnehmen können. Eine schematische Darstellung des Wertschöpfungsnetzwerkes ist unter Abbildung 3 zu finden. Im Folgenden werden einige Akteure besonders herausgegriffen.

5.2.1 NGCert-Monitoring-Service-Provider

Der NGCert-Monitoring-Service-Provider bietet einem Auditor individuelle Services zur Unterstützung der Auditierung oder zum Monitoring eines seitens des CSP angebotenen Cloud-Dienstes an. Hierbei sei bspw. auf die verschiedenen Messverfahren des Projektes verwiesen. So könnte der NGCert-Monitoring-Service-Provider zum Beispiel einen Service anbieten, der die Verfügbarkeit, die Latenz und die Bandbreite kontinuierlich überwacht. Der NGCert-Monitoring-Service-Provider kann eine vom CSP unabhängige Dritte Partei sein, welche einen NGCert-Monitoring-Service gemäß den NGCert-Richtlinien anbietet. Denkbar wäre auch, dass ein Auditor den NGCert-Monitoring-Service selbst betreibt. Es bestehen bestimmte Anforderungen, die der NGCert-Monitoring-Service-Provider wiederum selbst einhalten und ggf. nachweisen muss. Beispielsweise können Anforderungen an Standort der Rechenzentren bestehen. Auch kann der NGCert-Monitoring-Service-Provider in der Nutzung von Sub-Providern eingeschränkt sein. Insbesondere muss die Einhaltung der Anforderungen durch den NGCert-Monitoring-Service-Provider möglichst automatisiert überprüft werden. Die Ergebnisse dieser Überprüfung sollten zur Steigerung des Vertrauens in den NGCert-Dienst öffentlich zugänglich und durch die Überwachungsstelle überprüfbar sein.

5.2.2 NGCert-Infrastruktur-Betreiber

Die technische Infrastruktur die für den Betrieb eines NGCert-Monitoring-Services benötigt wird kann entweder vom NGCert-Monitoring-Service-Provider selbst oder durch einen Dritten bereitgestellt und betrieben werden. Ein NGCert-Infrastruktur-Betreiber könnte daher die notwendigen Rechen- und Speicherkapazitäten anbieten. Diese Rolle könnte daher von bestehenden Re-

chenzentrumsanbietern übernommen werden. Sollte diese Rolle durch einen Dritten wahrgenommen werden, ist zu berücksichtigen, dass ggf. Beschränkungen in der Auswahl bestehen und der Dritte wiederum gewisse Sicherheitsanforderungen erfüllen muss.

5.2.3 Überwachungsstelle

Eine Überwachungsstelle ist eine unabhängige Instanz, welche sicherstellt, dass NGCert-Monitoring-Services, Auditoren und CSP im Rahmen einer dynamischen Zertifizierung konform zu den NGCert-Richtlinien sind.

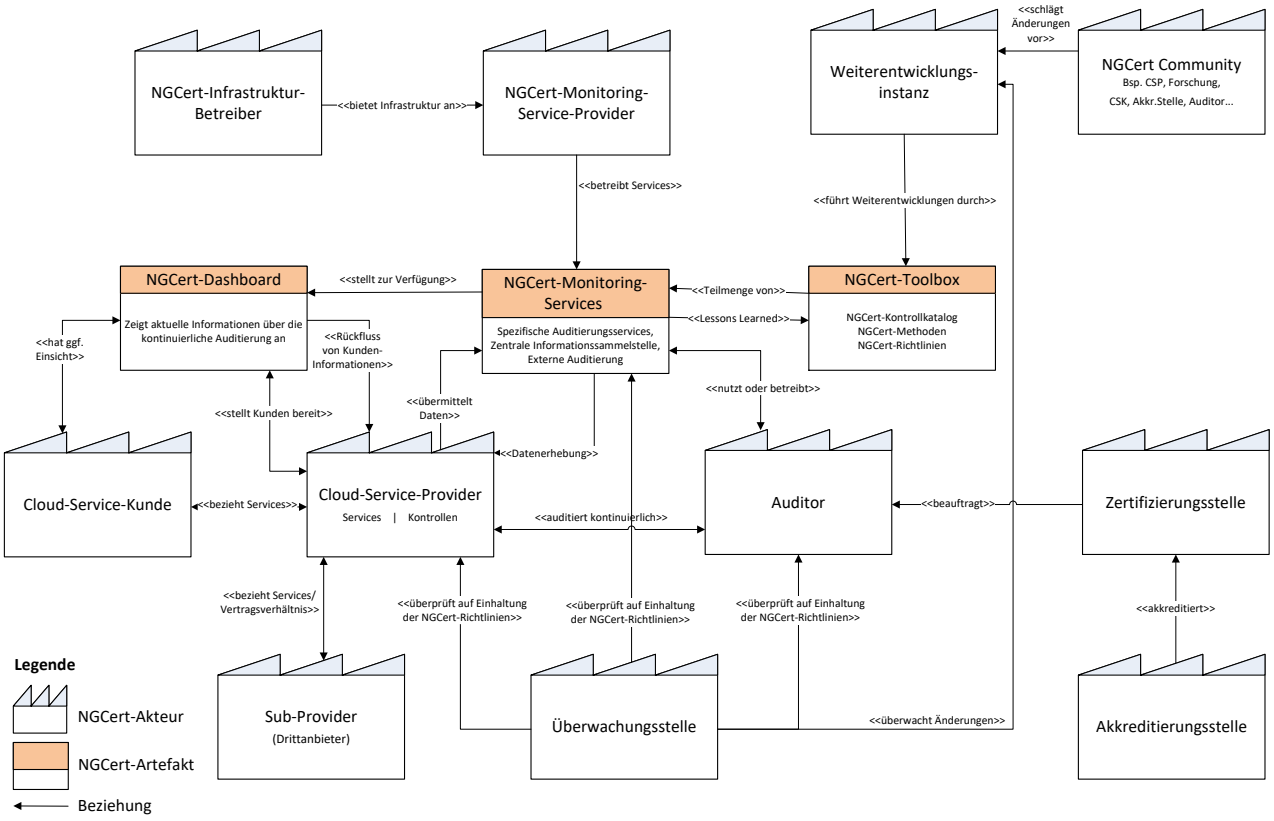


Abbildung 3. Wertschöpfungsnetzwerk der dynamischen Zertifizierung.

6. Notwendige Evaluierung für den Praxiseinsatz

6.1 Bedarf für die Evaluierung

Ziel dieses Forschungsprojektes ist eine praxisnahe Entwicklung und Evaluierung der geschaffenen Prototypen. Daher ist nach einem projektinternen Feldtest mit beteiligten Cloud-Service-Providern auch ein Praxiseinsatz mit externen Feld- und Transferpartnern gewünscht. Nur durch diese externe Diskussion und Validation können wir Forscher sicherstellen, dass erarbeitete Konzepte und Prototypen eine tatsächliche Verwendung in der Wirtschaft nach sich ziehen, und somit ein Mehrwert geschaffen wird.

6.2 Analyse zum Einsatz von NGCert bei Feldpartnern

Als Entscheidungsgrundlage für den Einsatz von NGCert bei Feldpartnern soll die folgende SWOT-Analyse behilflich sein. Neben den Stärken und Chancen von NGCert, werden insbesondere auch die damit verbundenen Schwächen und Risiken diskutiert:

Stärken	Schwächen
• NGCert adressiert relevanten Informationsbedarf potenzieller Cloud-Kunden • Einfache Anwendung von NGCert durch intuitives Dashboard möglich • Kontinuierlicher Anforderungsabgleich von Key-Parametern	• Teilweiße sind invasive Kontrollen unumgänglich • Zeit- und Ressourceninvestment durch CSP erforderlich
Chancen	**Risiken**
• Competitive Advantage durch Vertrauensvorsprung • Steigende Attraktivität bei Neu- und Bestandskunden • Interne Prozessverbesserungen durch kontinuierliche Messungen möglich	• Neue Sicherheitslücken möglich, durch invasive Kontrollmechanismen • NGCert Service ist aktuell ein Forschungsprojekt, dessen Marktreife noch aussteht

6.3 Risiko- und Sicherheitsbetrachtung

Für den Praxiseinsatz des NGCert-Monitoring-Services sind Risiko- und Sicherheitsbetrachtungen aus zwei Perspektiven erforderlich: aus Sicht der Feldpartner und aus der Perspektive eines späteren NGCert-Monitoring-Produktes.

Im Rahmen des geplanten Feldpartnertests wird eine Risiko- und Sicherheitsbetrachtung aus Sicht der potenziellen Partner erstellt, die entsprechend der ausgewählten Messverfahren die Risiken eines Testdurchlaufs in Produktionsumgebungen identifiziert und entsprechende Maßnahmen zur Risikominimierung und Vermeidung belegt.

Hierzu wird eine IT-Sicherheitsbetrachtung für die Testumgebung und Testabläufe des Feldpartnertests in Anlehnung an die Standardvorgehensweise BSI 100-2 vorgenommen. Die IT-Sicherheitsbetrachtung wird mit Blick auf die unterschiedlichen Messverfahren und damit verbundenen spezifischen Risiken modular aufgestellt. Es wird unterschieden zwischen Messverfahren, die seitens der Feldpartner minimale Eingriffe erfordern (nicht-invasiv) und solchen Messverfahren, die die Platzierung von Messinfrastruktur innerhalb der Produktivsysteme bei den Partnern erfordern (invasiv).

Für den späteren angedachten produktiven Einsatz ist eine Risiko- und Sicherheitsbetrachtung erforderlich, um die Basis für eine solide Produktentwicklung zu schaffen, die einen stabilen und verlässlichen NGCert Monitoring-Service garantiert. Risiken werden identifiziert und entsprechende Maßnahmen zum Umgang mit den Risiken im Sinnen eines Anforderungskatalogs vorgeschlagen.