Bundesministerium
für Wirtschaft
und Energie

Trusted Cloud

# Trusted Cloud

## Innovatives, sicheres und rechtskonformes Cloud Computing

# Impressum

**Herausgeber**
Bundesministerium für Wirtschaft
und Energie (BMWi)
Öffentlichkeitsarbeit
11019 Berlin
www.bmwi.de

**Text und Redaktion**
Kompetenzzentrum Trusted Cloud
A&B One Kommunikationsagentur GmbH

**Gestaltung und Produktion**
PRpetuum GmbH, München

**Stand**
aktualisierte Neuauflage, Februar 2014

**Druck**
Bonifatius GmbH, Paderborn

**Bildnachweis**
George Doyle/getty (Titel), zothen/fotolia (S. 2),
alehdats/fotolia (S. 4), Nicholas Rigg/getty (S. 6),
snapfoto105/fotolia (S. 20), sfam_photo/shutterstock (S. 30),
Kurhan/fotolia (S. 38), Scanrail/fotolia (S. 44)



Zertifikat seit 2002
audit berufundfamilie

Das Bundesministerium für Wirtschaft und Energie ist mit dem audit berufundfamilie® für seine familienfreundliche Personalpolitik ausgezeichnet worden. Das Zertifikat wird von der berufundfamilie gGmbH, einer Initiative der Gemeinnützigen Hertie-Stiftung, verliehen.

FSC
www.fsc.org
MIX
Papier aus verantwortungsvollen Quellen
FSC® C011558

**Diese und weitere Broschüren erhalten Sie bei:**
Bundesministerium für Wirtschaft und Energie
Referat Öffentlichkeitsarbeit
publikationen@bundesregierung.de
www.bmwi.de

**Zentraler Bestellservice:**
Telefon: 030 182722-721
Bestellfax: 030 18102722-721

# Inhaltsverzeichnis


fcomplex Csqrt(fcomplex z)
fcomplex c;
float w;
if ((z.r == 0.0) && (z
c.r=0.0;
c.i=0.0;
} else {
w = sqrt((sqr
if (z.r >= 0.
return ans;
} else {
temp=x/y;
ans=y*sqrt(1.0+
temp=y/x;
ans=x*sqrt(1.0+
if (x > y) {
ans=x;
} else {
temp=x/y;
ans=y*sqrt(1.0+
return ans;
fcomplex RCmul(float x, fcomplex a)
fcomplex c;
c.r=x*a.r;
c.i=x*a.i;
return c;
fcomplex Cinv( fcomplex z)
float s = 1.0 / (z.r*z.r + z.i*z.i);
c.r = z.r * s;
c.i = -z.i * s;
return c;
int main()
fcomplex a, b, c;
a = Cmplx( 10, 6 );
b = Cmplx( 4, 9 );

# Vorwort

Die Cloud ist längst in unserem Alltag angekommen: Viele nutzen schon heute webbasierte E-Mail-Dienste, streamen ihre Musik online auf ihr Smartphone oder speichern und verwalten ihre Kontakte und sonstige Dateien im Internet. Und dabei ist es egal, ob gerade der Tablet-PC, der Laptop oder das Smartphone genutzt wird – Dokumente, Bilder, Videos und Musik sind überall abrufbar.

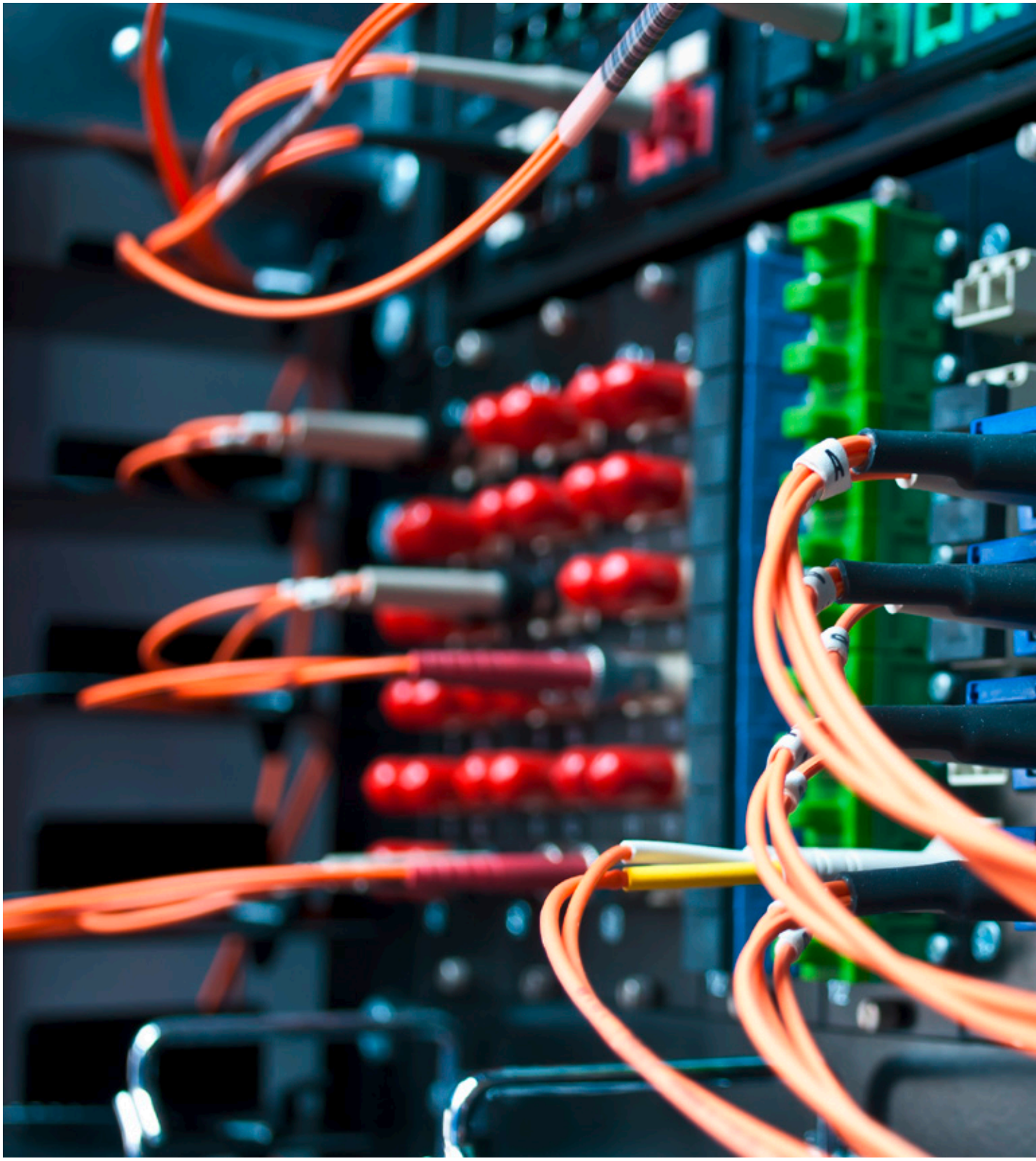
Auch für Unternehmen eröffnet Cloud Computing vielfältige Möglichkeiten – etwa wenn es darum geht, aktuelle passgenaue Software, Rechenleistung und Speicherplatz über das Internet zu beziehen. Dadurch müssen Unternehmen nicht selbst in eine große IT-Infrastruktur investieren – gerade auch für Start-ups ein entscheidender Vorteil. Gezahlt wird verbrauchsabhängig nur für die tatsächlich benötigten Ressourcen. So können Unternehmen auf innovative Technologien zugreifen, die bislang vor allem den Großen der Branche vorbehalten waren. Und: Mitarbeiter können mobil auf ihre Daten zugreifen. Das ermöglicht Flexibilität im Unternehmen und eröffnet viel Raum für neue Geschäftsmodelle.

Mit dem Technologieprogramm Trusted Cloud wollen wir die großen Innovations- und Marktpotenziale von Cloud Computing gerade für den Mittelstand weiter erschließen. In verschiedenen Gebieten werden exemplarisch die Chancen und die Vielfalt der neuen Anwendungen demonstriert – von Industrie und Handwerk über die Gesundheitsbranche bis zum öffentlichen Sektor.

Es gibt aber auch Gründe, die ein Unternehmen beim Einsatz der Cloud noch zögern lassen. Gerade bei den rechtlichen Rahmenbedingungen besteht noch Handlungsbedarf. Mit dem Aktionsprogramm Cloud Computing gehen wir auch auf solche Fragen ein und arbeiten gemeinsam mit der Wirtschaft und der Wissenschaft an verlässlichen Lösungen.

Deutschland hat alle Chancen, sich in diesem zukunftsträchtigen Markt weiter als führender Standort zu etablieren. Sicheres Cloud Computing „Made in Germany“ eröffnet viele neue Möglichkeiten – vielleicht auch für Sie.

Sigmar Gabriel
Bundesminister für Wirtschaft und Energie




# Das Technologieprogramm Trusted Cloud

## Einleitung

Die Informations- und Kommunikationstechnologien (IKT) bilden eine entscheidende Grundlage für den Erfolg des Wirtschaftsstandorts Deutschland. Sie leisten als Querschnittstechnologien einen zentralen Beitrag zur Produktivität sowie Innovationsfähigkeit und damit für die Wettbewerbsfähigkeit der gesamten Wirtschaft.

Eine derzeit besonders vielversprechende Entwicklung ist Cloud Computing. Damit können Unternehmen aktuelle Software, Rechenleistung und Speicherplatz direkt über das Internet beziehen. Dies geht einher mit einer stärkeren Industrialisierung der IT: Standardisierung und Automatisierung, Modularisierung, Konzentration auf Kernkompetenzen und kontinuierliche Qualitätsverbesserungen. Mit hohen jährlichen Wachstumsraten gehört Cloud Computing derzeit zu den wichtigsten Entwicklungen der IT-Branche weltweit. Auch in Deutschland hat Cloud Computing eine hohe Dynamik erreicht. Zunächst ging die Entwicklung besonders von den privaten Konsumenten aus. Mittlerweile setzen auch immer mehr Unternehmen Cloud-Lösungen ein.

## Cloud Computing bietet Vorteile für alle Unternehmen

Cloud Computing bietet vielfältige Chancen für die deutsche Wirtschaft – und zwar für alle Branchen. Über die Cloud können mittelständische Firmen und Start-ups auf innovative Technologien zugreifen, die bislang vor allem großen Unternehmen vorbehalten waren. Sie müssen nicht mehr selbst in eine große IT-Infrastruktur investieren, da sie alle Ressourcen von einem professionellen IT-Anbieter quasi mieten können. Gezahlt wird nutzungsabhängig nur für die tatsächlich benötigten Leistungen. Das Internet wird damit zu einer immer bedeutsameren Infrastruktur für die Wirtschaft. Cloud Computing ermöglicht ebenso die mobile Nutzung von Unternehmensanwendungen weltweit, wodurch neue Formen der Zusammenarbeit entstehen und der steigende Informationsbedarf effektiver gedeckt werden kann. Weiterhin können ganz neue Geschäftsmodelle und innovative Produkte entstehen.

Für die IT-Unternehmen ist Cloud Computing aktuell ein zentraler Wachstumsmarkt. Kleinere Software-Anbieter können die Cloud-Ökosysteme größerer Anbieter nutzen und dadurch einen breiteren Kundenkreis erschließen. Software-Entwickler können durch Cloud-Plattformen mit aktuellen Entwicklerwerkzeugen neue Software flexibel und kostengünstig entwickeln. Außerdem können Rechenzentren bestehende Kapazitäten mittels Cloud-Lösungen besser auslasten. Gleichzeitig kann der meist hohe und kostenintensive Energieverbrauch reduziert werden. Insgesamt können IT-Anbieter durch standardisierte und automatisierte Prozesse ihre Kosteneffizienz verbessern.

Cloud Computing führt aber auch zu neuen Herausforderungen. Dazu gehören Fragen der Sicherheit und des Schutzes von Betriebsgeheimnissen, der Rechtskonformität, der Interoperabilität und Datenportabilität sowie der Wirtschaftlichkeit. Lösungen hierfür zu finden ist eine wichtige Grundlage, um das notwendige Vertrauen der Anwender in Cloud-Dienste zu etablieren. Mit dem Technologieprogramm Trusted Cloud nimmt sich das Bundesministerium für Wirtschaft und Energie (BMWi) dieser Fragen an.

## Cloud-Lösungen für mittelständische Unternehmen im Fokus

Ziel des Technologieprogramms Trusted Cloud ist die Entwicklung und Erprobung innovativer, sicherer und rechtskonformer Cloud-Computing-Lösungen. Von diesen neuen, cloud-basierten Diensten sollen insbesondere mittelständische Unternehmen profitieren.

An den 14 Projekten sind insgesamt 36 Unternehmen verschiedener Branchen, 27 wissenschaftliche Einrichtungen und vier weitere Institutionen beteiligt. Sie erarbeiten prototypisch grundlegende Technologien sowie Cloud-Anwendungen für die Bereiche Industrie, Handwerk, Gesundheit und den öffentlichen Sektor, die auf andere Anwendungsgebiete übertragbar sein sollen. Damit werden die Vorteile von Cloud Computing anhand konkreter Pilotanwendungen verdeutlicht und praxisnah erprobt. Durch einen offenen und transparenten Markt sollen im Wettbewerb innovative Anwendungen entstehen, sodass IT-Anwender zukünftig aus einem breiten Angebot die für sie passenden Dienste auswählen können. Insgesamt soll dies zu einer Stärkung des IKT-Standorts Deutschland beitragen.

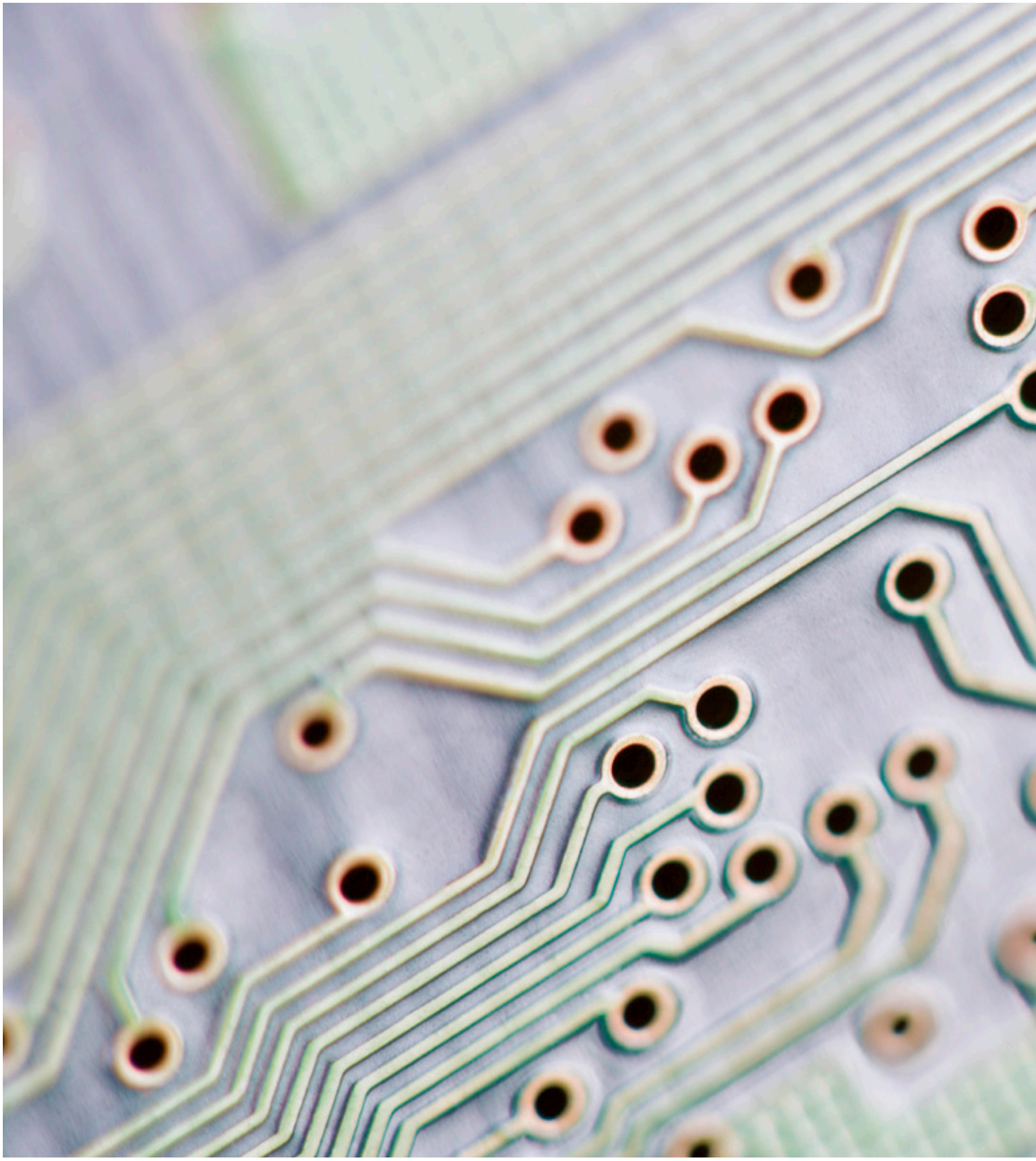
## Förderung von Technologie- und Marktentwicklung

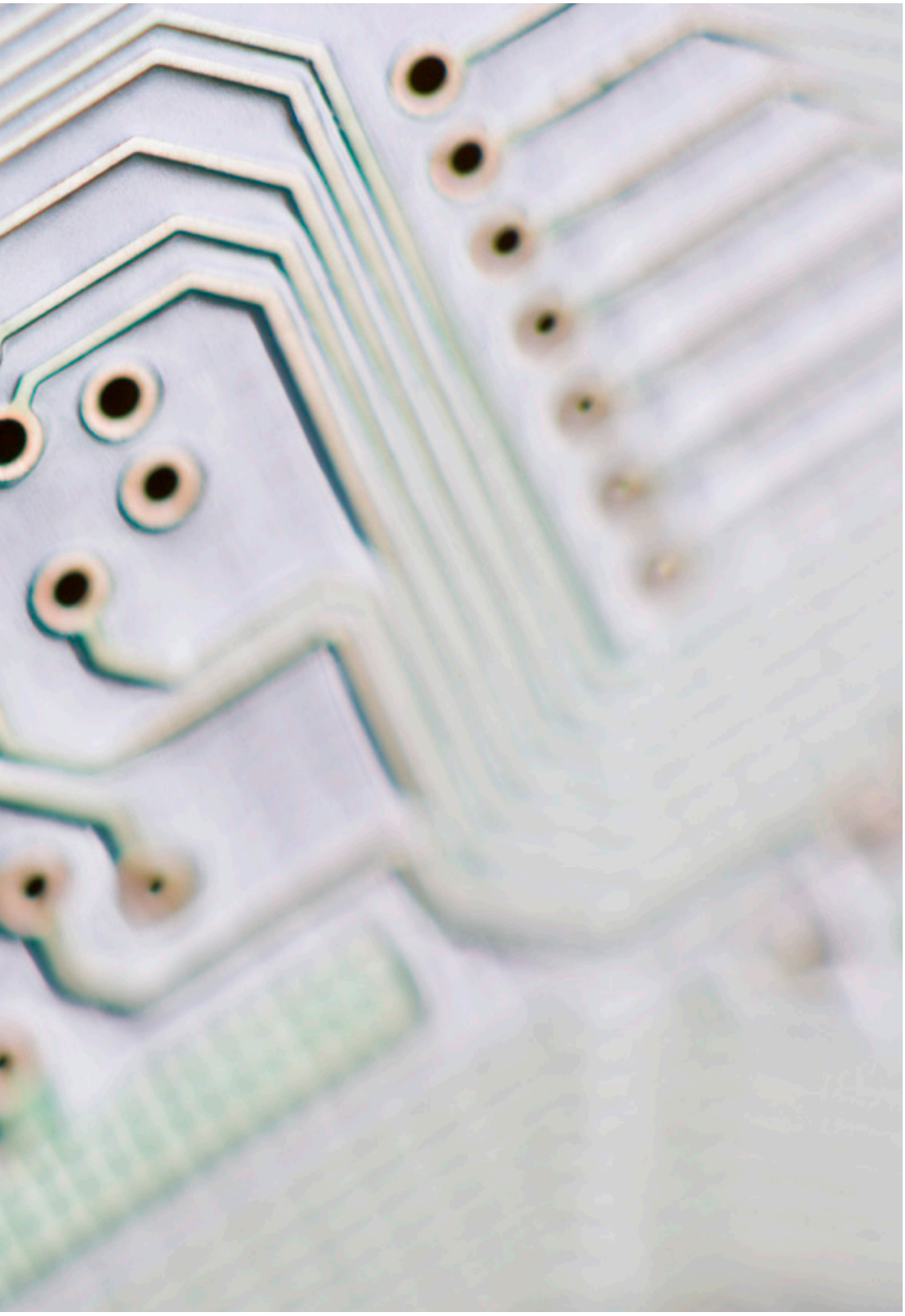
Um in einem so dynamischen Markt wie dem für Technologien und Dienste im Cloud Computing Transparenz zu schaffen, ist es nötig, die Angebote vergleichbar zu machen. Nur wenn Unternehmen in der Lage sind, die besten Angebote für eine spezifische Nutzung innerhalb eines Marktes auszuwählen, werden neue Technologien nachgefragt und genutzt. Das Technologieprogramm Trusted Cloud trägt dazu bei, Kriterien für eine einheitliche Bewertung und Beurteilung von Cloud-Diensten zu schaffen. Sie sollen in den Bereichen Funktionalität, Sicherheit, Schutz und Wirtschaftlichkeit beschrieben und beurteilt werden. Das ermöglicht nicht nur einen Vergleich einzelner Angebote untereinander, sondern auch eine Beschreibung und Charakterisierung von Angebot und Nachfrage – der Grundlage für eine gute Entwicklung des Marktes für Cloud-Technologien und -Dienste.

## Vom Technologiewettbewerb zum Technologieprogramm

Das Bundesministerium für Wirtschaft und Energie (BMWi) hat Trusted Cloud im September 2010 als Technologiewettbewerb gestartet. Insgesamt sind 116 Projektvorschläge eingereicht worden. In einem mehrstufigen Prozess wurden mit Unterstützung einer unabhängigen Expertenjury die 14 erfolgversprechendsten Projekte ausgewählt. Die Forschungs- und Entwicklungsaktivitäten haben 2011 begonnen und laufen bis Anfang 2015. Das BMWi stellt dafür ein Fördervolumen von rund 50 Millionen Euro bereit. Durch Eigenbeträge der Projektpartner liegt das Gesamtvolumen von Trusted Cloud bei rund 100 Millionen Euro.

Das Technologieprogramm Trusted Cloud ist der zentrale Beitrag des BMWi zum „Aktionsprogramm Cloud Computing“, das gemeinsam mit Partnern aus Wirtschaft und Wissenschaft im Oktober 2010 gestartet wurde. Trusted Cloud ist Bestandteil der IKT-Strategie und der Hightech-Strategie der Bundesregierung.





# Entwicklung von Basistechnologien

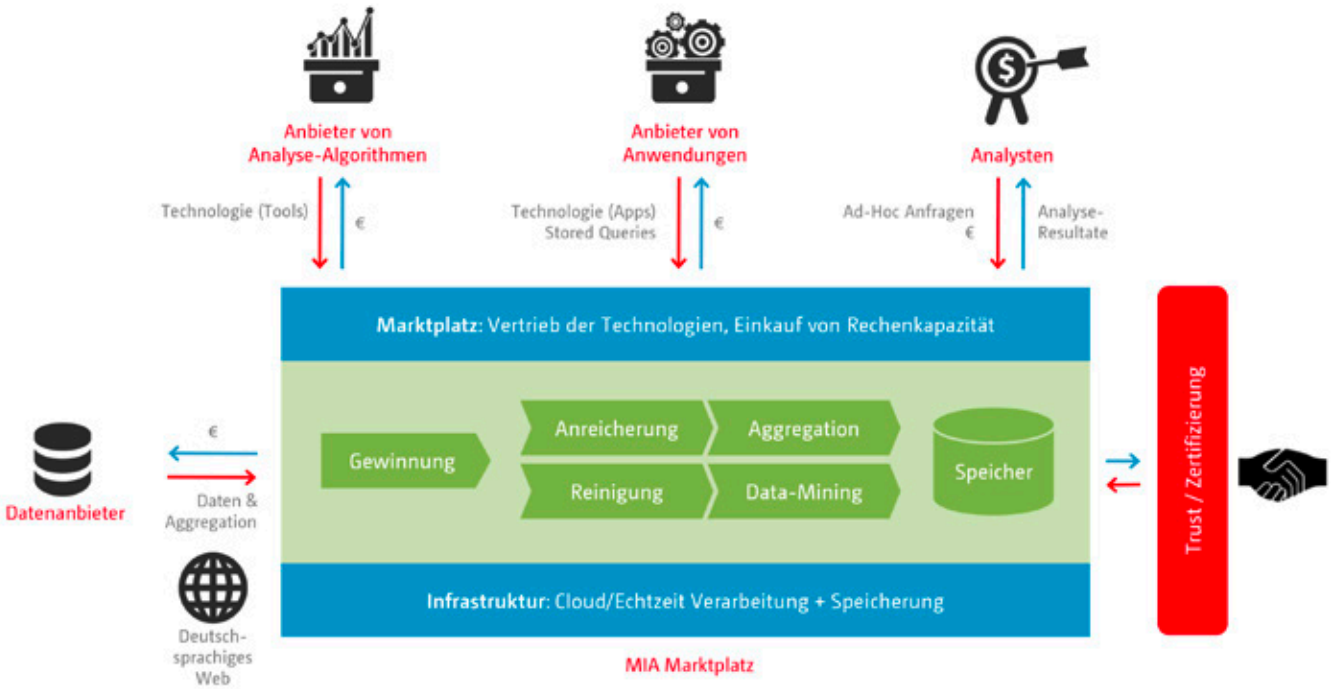
# MIA

## Informationsmarktplatz für das deutschsprachige Web

Das deutschsprachige Web enthält mehr als sechs Milliarden Webseiten voller öffentlich zugänglicher Informationen, Meinungen und Inhalte. Dieser gewaltige Datenfundus bietet ein außerordentliches Potenzial für die Markt- und Trendforschung, den Vertrieb von Nachrichten und für intelligente Geschäftsentscheidungen (Business Intelligence). Um dieses Potenzial nutzbar zu machen, entwickelt das Projekt MIA einen Cloud-Marktplatz für Informationen und Analysen auf Basis der Daten des deutschen Web. MIA stellt den Datenbestand, eine Plattform zur Verarbeitung und einen Marktplatz zum Vertrieb von Daten und Anwendungen bereit. Die geplante Marktplatz-Infrastruktur umfasst die Bereitstellung, Veredelung, Vermarktung sowie die Abrechnung von Daten und Mehrwertdiensten. Über diese Plattform sollen Cloud-Anbieter Analysewerkzeuge entwickeln und über den Marktplatz bereitstellen können, die Anwender dann flexibel und kosteneffizient nutzen können. So können auch mittelständische Unternehmen gängige Analysewerkzeuge nutzen und damit beispielsweise Produkte und Dienstleistungen gezielter an Kundenwünsche anpassen.

## Eine Datenbank für alle deutschsprachigen Web-Inhalte

Bisher mussten Unternehmen für eine Analyse der Daten des deutschen Web eine eigene Infrastruktur aufbauen, die Daten selbst sammeln und speichern und schließlich Analysewerkzeuge entwickeln. MIA will hingegen einen Großteil der relevanten deutschsprachigen Netzinhalte in einer speziellen Datenbank (Data Warehouse) zusammenfassen. Außerdem werden die gesammelten Textdaten mit Informationen über ihre Herkunft, ihren Inhalt und ihre sprachliche Struktur angereichert. So können die Daten einer Vielzahl von Unternehmen als Grundlage von Analysen zur Verfügung stehen. Dazu ist die Entwicklung von Datenstrukturen und Algorithmen nötig, die auch hohe Datenmengen bewältigen können. Herausforderungen liegen dabei in der Verbesserung der Ressourcenzuordnung in Cloud-Architekturen und in der Parallelisierung von Rechenjobs in verteilten Systemen. Kurze Datenzugriffs- und Ausführungszeiten sollen eine hohe Benutzerinteraktivität sicherstellen.



## Marktplatzteilnehmer kombinieren Daten und Algorithmen zu neuen Dienstleistungen

Auf Basis dieses Data Warehouse schafft MIA einen Cloud-Marktplatz, über den Informationen, Softwarekomponenten und Analysen elektronisch gehandelt werden können. Unternehmer können sich darauf konzentrieren, Lösungen zu entwickeln, die das implizite und unstrukturierte Wissen der von MIA gesammelten Daten durch algorithmische Verfahren explizit und damit nutzbar machen. Beispielsweise könnte ein Softwareanbieter eine Softwarekomponente für das Text-Mining auf dem Marktplatz als Basis-Werkzeug anbieten. Dann kann ein Marktforschungsunternehmen Nutzungsrechte an dieser Technologie erwerben und das Basis-Werkzeug auf unternehmensspezifische Fragestellungen anpassen. Damit können mit ausgewählten Web-Daten detaillierte Analysen erstellt und auf dem MIA-Marktplatz als Beratungsdienstleistung vertrieben werden. Zusätzlich ist es möglich, die Web-Daten mit kundeneigenen Daten zu verknüpfen, um besondere kundenspezifische Analysen zu erhalten.

## MIA senkt die Eintrittsbarrieren für den Geschäftsbereich der Datenanalyse

Durch das zentrale Data Warehouse und den Marktplatz müssen Datenanalysten wie Marktforschungs- und Beratungsunternehmen nicht in eine eigene aufwändige Infrastruktur investieren. Stattdessen können sie über die Cloud flexibel Analysewerkzeuge nachfragen, die genau auf ihre Bedürfnisse zugeschnitten sind. Unternehmen können dadurch kostengünstigere und spezifischere Analysen erhalten, wodurch Barrieren für Innovationen und den Eintritt in neue Märkte gesenkt werden. Das Projekt betrachtet prototypisch drei Anwendungsfälle: die Branchen Medien, Marktforschung und Beratung – unter besonderer Berücksichtigung der hierfür spezifischen Anforderungen an Datenschutz und Datensicherheit am Standort Deutschland.

### Ausgangssituation

- Deutschsprachiges Web bietet großen Datenschatz für verschiedenste Analysen
- Erfassung, Analyse und Verwertung dieser Daten sind aufwändig
- Verschiedene Algorithmen zur Analyse von Webinhalten sind nicht zentral zugängig

### Zielsetzung

- Zentraler Informationsmarktplatz für das Handeln von Daten, Analyseverfahren und Beratungsdienstleistungen
- Datenanalysen werden vereinfacht und vergünstigt
- Marktplatzteilnehmer kombinieren existierende Daten und Algorithmen zu neuen Diensten

### Kontakt

**Technische Universität Berlin**
Institut für Softwaretechnik und Theoretische Informatik, Fachgebiet Datenbanksysteme und Informationsmanagement
**Dr. Holmer Hemsen**
**E-Mail** holmer.hemsen@tu-berlin.de
**Partner**
- Fraunhofer-Institut für Rechnerarchitektur und Softwaretechnik (FIRST)
- Neofonie GmbH
- ParStream GmbH
- TEMIS Deutschland GmbH
- VICO Research & Consulting GmbH

**Internet** www.mia-marktplatz.de

# MimoSecco

## Vertrauensvolles Datenmanagement für Cloud-Dienste

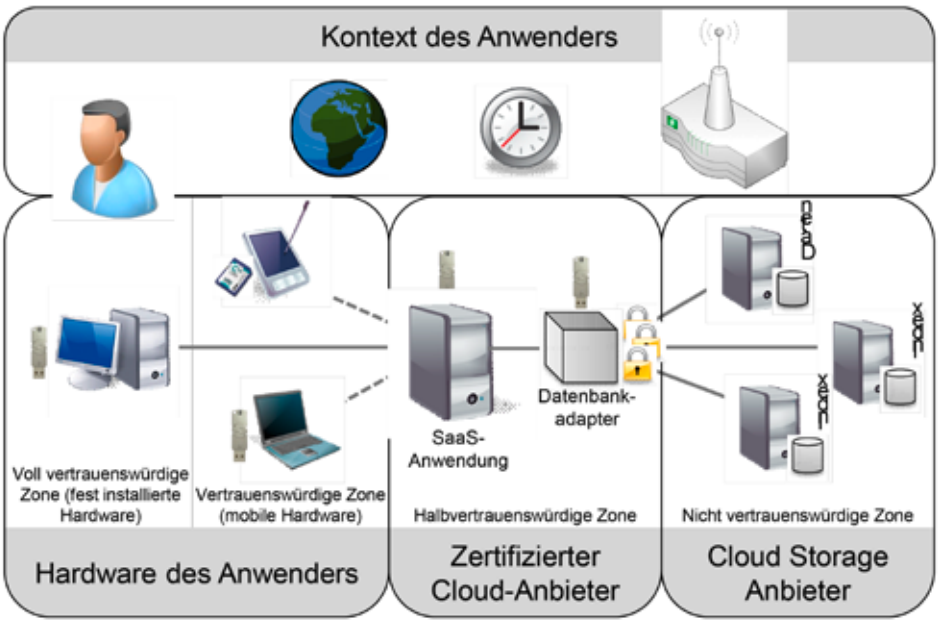
Die Daten von Unternehmen müssen auch in der Cloud sicher sein. Sie müssen bei der Datenverarbeitung so geschützt sein, dass nur die Anwender, nicht aber Mitarbeiter des Cloud-Anbieters auf sie zugreifen können. Gleichzeitig muss sichergestellt sein, dass auch beim Zugriff über mobile Endgeräte nur befugte Anwender Datensätze öffnen können. Es ist allerdings problematisch und sehr aufwändig, verschlüsselte Daten zu verarbeiten. Ziel von MimoSecco ist daher eine ganzheitliche Lösung für die Absicherung des Datenmanagements in der Cloud.

Konzeptionelle Grundlage bildet das MimoSecco-Zonenmodell. Es klassifiziert die Hardware des Anwenders und die beteiligten Cloud-Anbieter nach dem Grad ihrer Vertrauenswürdigkeit in drei Zonen. Die fest installierte Hardware des Anwenders bildet die voll vertrauenswürdige Zone, in der uneingeschränkt auf alle Daten zugegriffen werden kann. Die vertrauenswürdige Zone umfasst auch seine mobile Hardware. Einschränkungen der Vertrauenswürdigkeit ergeben sich hier allerdings etwa dadurch, dass jemand anderes den Arbeitenden beobachten könnte („shoulder sniffing“). Zertifizierte Cloud-Anbieter, mit denen ein direktes Vertragsverhältnis besteht und die den deutschen Rechtsanforderungen zum Datenschutz unterliegen, bilden die halb vertrauenswürdige Zone. Hier sind nur die Daten temporär im Speicher verfügbar, welche gerade für die Verarbeitung benötigt werden, sofern der Anwender über die entsprechende Berechtigung verfügt. Die nicht vertrauenswürdige Zone bilden Drittanbieter unbekannter Vertrauenswürdigkeit. In dieser Zone erfolgt die Ablage aller Daten generell nur verschlüsselt.

Die Kontrolle über die Datennutzung erfolgt mittels eines universell anwendbaren Hardware-Tokens unter Einbeziehung des Zugriffskontexts. Dazu entwickelt das Projekt eine Middleware, die sich auf den Client der Anwender und den Servern des Cloud-Anbieters positioniert und dort die sichere Anmeldung, den sicheren Datenzugriff und die sichere Speicherung der Daten regelt. Die Middleware wird als Baukasten gestaltet, sodass auf den jeweiligen Systemen (Endgerät, Cloud-Anwendung, Datenbankadapter usw.) aus diesem Baukasten die dort jeweils benötigten Komponenten ausgewählt und eingesetzt werden können.

## Sicherheitsmanagement durch Datenbanktransformation

MimoSecco erlaubt es, Daten geschützt in der Cloud abzulegen und dennoch effizient an diesen Daten zu arbeiten. Dies wird erreicht, indem die Datenbank geschickt transformiert wird. Auf dem Datenserver liegen die Daten in verschlüsselter Form. Der Betreiber des Servers hat somit keine



Kenntnis über den Inhalt der Daten. Eine über die Datenbank vorgenommene Indizierung wird mit unverschlüsselten Suchbegriffen, aber verschlüsselter Zuordnung auf weitere Server verteilt. Die Indizierung und das Verschlüsseln der Daten übernimmt der vertrauenswürdige Datenbankadapter, den die Cloud-Anwendung für Anfragen verwendet.

## Token-basierte Verschlüsselungsmethoden

Ein zentrales Element zur Identifizierung berechtigter Nutzer ist der Einsatz zertifizierter Hardware-Sicherheitstoken. Dies sind gegen physische Angriffe gesicherte Smartcards oder USB-Sticks, die an den Datenbankadapter angeschlossen sind. Der benötigte Schlüssel liegt nur im Sicherheitstoken vor. Liegen gleichzeitig aktuell gültige Zertifikate des Cloud-Anwenders und der vertrauenswürdigen Cloud-Anwendung vor, gibt der Sicherheitstoken des Datenbankadapters den Schlüssel temporär frei, sodass die benötigten Daten entschlüsselt werden können. Nach erfolgter Bearbeitung der Daten werden der Schlüssel im Datenbankadapter und alle temporäre Kopien der Daten wieder gelöscht. Weitere Einsatzgebiete der Sicherheitstoken sind eine Zwei-Faktor-Authentifizierung des Anwenders und die Verschlüsselung von vertraulichen Dokumenten, auf deren Inhalt auch die Cloud-Anwendung keinen Zugriff haben soll.

## Einbeziehung des Zugriffskontexts

Als Ergänzung zu klassischen Berechtigungssystemen entwickelt MimoSecco Ansätze, die den Zugriffskontext berücksichtigen. Dies kann beispielsweise der Ort sein, von dem aus ein Datenzugriff erfolgt, der Zeitpunkt des Datenzugriffs, das Vorhandensein des Sicherheitstokens am Client oder das zum Zugriff verwendete Netzwerk. Dadurch wird es z. B. möglich, den Zugriff auf sensible Daten aus einer Cloud-Anwendung auf die Geschäftsstellen eines Unternehmens und dessen Geschäftszeiten zu beschränken, oder die Übertragung von Daten über eine als unsicher eingestufte Infrastruktur zu verhindern.

**Ausgangssituation**

- Mitarbeiter wollen mobil und sicher auf Unternehmensdaten zugreifen
- Unbefugte dürfen keinen Zugriff auf die Daten erlangen
- Cloud-Anbieter hat theoretisch Zugang zu allen Daten
- Effiziente Verarbeitung von verschlüsselten Daten nicht möglich

**Zielsetzung**

- Mehrstufiges Sicherheitszonenkonzept erschwert Insider-Angriffe bei Cloud-Anbietern
- Einsatz von Sicherheitstoken und Verschlüsselung ermöglichen bessere Kontrolle des Zugriffs auf die Daten durch den Nutzer
- Einbeziehung des Zugriffskontexts zur Absicherung des mobilen Datenzugriffs

**Kontakt**

CAS Software AG
Spiros Alexakis
E-Mail spiros.alexakis@cas.de
Partner
- Karlsruher Institut für Technologie (KIT)
- WIBU-Systems AG

Internet www.mimosecco.de

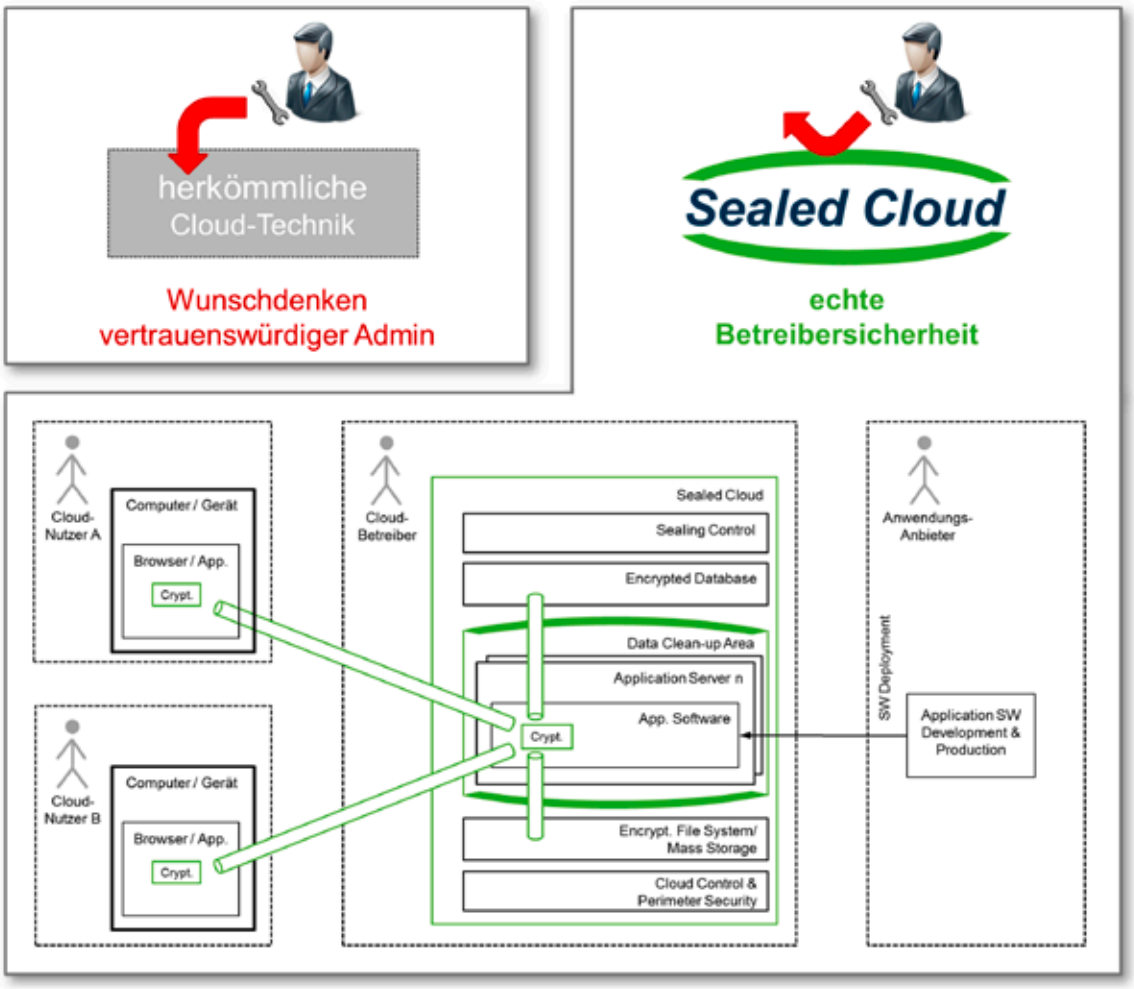
# Sealed Cloud

## Technisch abgesichertes Cloud Computing

Wenn Unternehmen ihre Daten in der Cloud speichern und verarbeiten, ist der Schutz der Informationen vor Angriffen und Diebstahl von größter Bedeutung. Viele Cloud-Anwendungen verschlüsseln deshalb den Datenverkehr zwischen Nutzer und Cloud-Anbieter, sodass Unbefugte von außen nicht darauf zugreifen können. Trotzdem erscheint es vielen Unternehmen immer noch riskant, ihre Daten in die Cloud auszulagern. Denn dort liegen sie nicht mehr auf Servern im eigenen Haus, sondern bei einem Drittanbieter, der theoretisch darauf Zugriff nehmen könnte. Daher entwickelt das Projekt Sealed Cloud ein umfassendes Konzept und Technologien zur Sicherung der Daten gegen unbefugten Zugriff sowohl von Dritten als auch vom Cloud-Anbieter selbst. Ziel ist eine „versiegelte" Infrastruktur für Cloud Computing, der Unternehmen ihre Daten und Geschäftsgeheimnisse sicher anvertrauen können.

## „Versiegelung" der Datenverarbeitung schafft Sicherheit

Daten wären generell geschützt, wenn aufgrund einer technischen „Versiegelung" vom Sender bis zum Empfänger gar kein physischer Zugriff auf die Kommunikationssignale möglich wäre. Bei den üblichen Telekommunikationsverbindungen ist dies in der Praxis jedoch ökonomisch nicht durchführbar. Deshalb greifen Unternehmen für die sichere Übertragung auf eine Ende-zu-Ende-Verschlüsselung von Daten zurück. Allerdings wird oft nicht bedacht, dass die Vermittlungsknoten in der Cloud noch immer bei jedem Datenverkehr offenbaren, wer mit wem wann und wie oft kommuniziert. Diese Verbindungsdaten, so genannte Metadaten, lassen sich sehr leicht analysieren und ermöglichen vielfältige Rückschlüsse auf die eigene Geschäftstätigkeit. Wendet man eine technische „Versiegelung" zusätzlich auch an den Vermittlungsknoten an, schützt man auf ökonomische Weise neben den Inhalten auch die Metadaten. Dies wird mittels der Technologie von Sealed Cloud umgesetzt.



## „Data Clean-up“ schützt zuverlässig gegen Insider-Angriffe

Im Rechenzentrum des Cloud-Infrastruktur-Betreibers sorgen eine Reihe technischer Maßnahmen für eine solche „Versiegelung“, sodass kein Mitarbeiter des Betreibers je Zugriff auf die dort gespeicherten Daten erhält. Selbst wenn physische Arbeiten an einem der Server nötig werden, bleiben die Daten vor neugierigen Blicken verborgen. Dazu sind die Daten auch im Rechenzentrum mittels eines bewährten Verschlüsselungsstandards (AES 256) verschlüsselt gespeichert. Jeder einzelne Datensatz erhält dabei seinen eigenen Schlüssel, der jedes Mal neu generiert wird und nur dem Nutzer – niemals dem Cloud-Betreiber – bekannt ist. Ein Aufbrechen dieser Verschlüsselung ist praktisch unmöglich und müsste für jeden einzelnen Datensatz neu erfolgen.

Zentral für den Schutz der Daten ist jedoch die Möglichkeit, sie auch dann noch abzusichern, wenn sie unverschlüsselt vorliegen. Das ist unter anderem der Fall, wenn sie gerade durch den Nutzer von Ferne bearbeitet werden. Dafür setzt Sealed Cloud auf das so genannte „Data Clean-up“. Unverschlüsselte Daten werden ausschließlich in Bereichen ohne persistente Speicherung verarbeitet. Kommt es zu einem Zugriff auf den Server, löscht das System mittels „Data Clean-up“ alle temporär unverschlüsselten Daten. Dabei ist egal, ob es sich um einen ungeplanten, potenziell unbefugten Zugriff handelt oder um eine Öffnung des Servers zu Wartungszwecken. Für den „Clean-up“ werden bestehende Nutzer-Sessions auf andere, vom Zugriff nicht betroffene Server migriert und verschlüsselt. Dann werden die Daten auf dem betroffenen Server gelöscht und der Server abgeschaltet. Nach 15 Sekunden ohne Strom sind die Daten aus den nicht-persistenten Speichern zuverlässig verschwunden.

## Offene und standardisierte Schnittstellen für Cloud-Dienste

Sealed Cloud bietet eine offene und standardisierte Schnittstellenschicht für Cloud-Dienste. Das umfassende Sicherheitskonzept der versiegelten Cloud wird so für eine ganze Reihe von Diensten nutzbar. Demonstriert wird dies am Beispiel zweier Cloud-Anwendungen. Mit „deleGate“ soll zum einen ein Dienst angeboten werden, mit dem der Verfügungsberechtigte eines Unternehmens Zugangsberechtigungen zu Cloud-Diensten verwalten und kontrolliert delegieren kann. Der Cloud-Dienst IDGARD ermöglicht eine sichere und abhörsichere Kommunikation, über die zum Beispiel Unternehmen geschäftsrelevante Informationen austauschen können, ohne Angst vor Datendiebstahl haben zu müssen. Beide Dienste nutzen über die offenen Schnittstellen die von Sealed Cloud entwickelten Sicherheitstechnologien.

### Ausgangssituation

- Schutz von Daten ist in der Cloud nicht generell sichergestellt
- Auch beim Einsatz von Ende-zu-Ende-Verschlüsselung sind Metadaten ungeschützt
- In Rechenzentren von Cloud-Anbietern können Administratoren potenziell Daten einsehen

### Zielsetzung

- Die versiegelte Cloud-Infrastruktur unterbindet unbefugten Zugriff auf alle Daten des Cloud-Anwenders
- Auch der Cloud-Anbieter bzw. dessen Mitarbeiter können nicht auf die Daten zugreifen
- Neben den Inhalten der Kommunikation sind auch die Metadaten geschützt

### Kontakt

**Uniscon universal identity control GmbH**
**Dr. Hubert Jäger**
**E-Mail** hubert.jaeger@uniscon.de
**Partner**
- Fraunhofer-Institut für Angewandte und Integrierte Sicherheit (AISEC)
- SecureNet GmbH
- Universität Kassel, Fachgebiet Wirtschaftsinformatik und Projektgruppe verfassungsverträgliche Technikgestaltung (provet) – im Forschungszentrum für Informationstechnik-Gestaltung (ITeG)

**Internet** www.sealedcloud.de

# SkIDentity

## Vertrauenswürdiges Cloud Computing braucht starke Authentifizierung

Cloud-Dienste ermöglichen das gemeinsame Arbeiten an Projekten, egal wo sich die Kollegen gerade befinden. In weltweit verteilten Büros, auf einem Notebook zu Hause oder auch unterwegs mit Smartphone oder Tablet-PC, überall haben die Mitarbeiter Zugriff auf wichtige Daten oder gemeinsam nutzbare IT-Dienste. Diese Flexibilität ist jedoch mit einem Risiko verbunden: Unbefugte können sich durch Hackerangriffe oder gezielte Betrugsversuche die Zugangsdaten eines Mitarbeiters verschaffen und so unerlaubten Zugriff auf sensible Unternehmensdaten und Geschäftsgeheimnisse erhalten. Um dies zu verhindern, müssen in der Cloud starke, auf mehreren Faktoren basierende Authentifizierungsmechanismen eingesetzt werden.

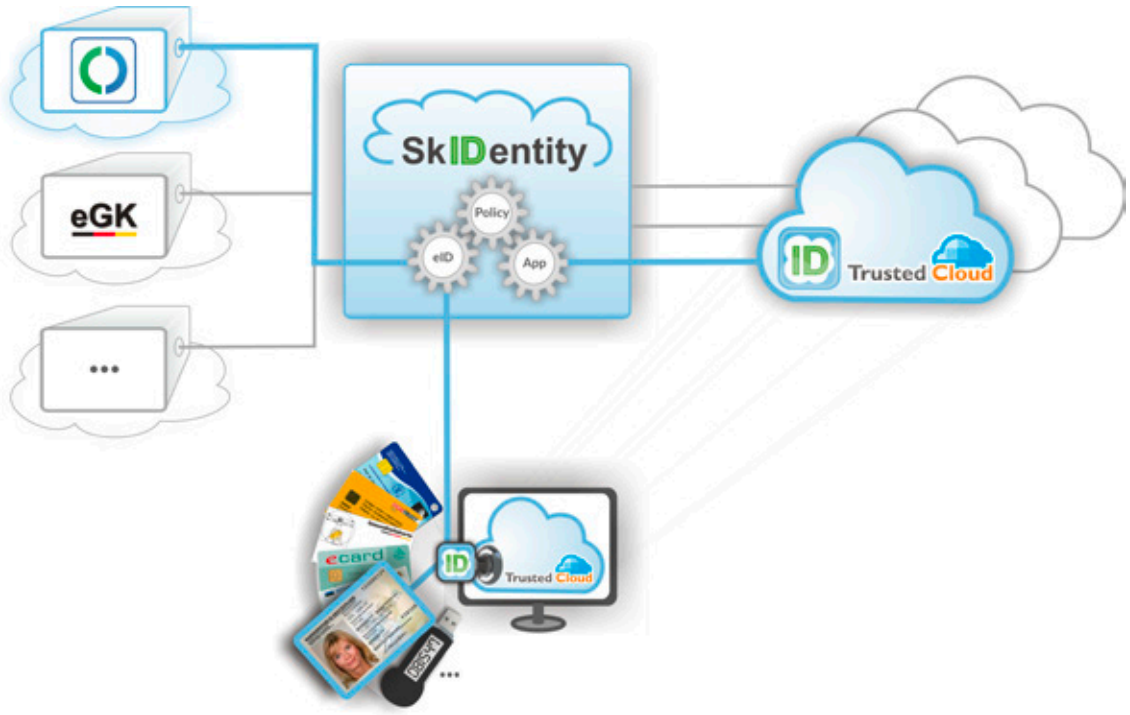
## Brücke zwischen sicheren Ausweisen und Cloud

Genau hier setzt das Projekt SkIDentity an und entwickelt ein sicheres Authentifizierungssystem für Cloud-Anwendungen. Dafür setzt SkIDentity auf bestehende sichere elektronische Ausweise (eID) wie den neuen Personalausweis. Das ist deutlich sicherer als eine Anmeldung durch Benutzernamen und Passwort.

Ziel ist es, vertrauenswürdige Identitäten für die Cloud bereitzustellen und dadurch alle Arten von Geschäftsprozessen für Konsumenten, Unternehmen und Behörden besser abzusichern. Hierfür werden bereits existierende sowie neu zu entwickelnde Komponenten, Dienste und Vertrauensinfrastrukturen zu einer umfassenden, rechtskonformen, wirtschaftlich sinnvollen und hochsicheren Identitätsinfrastruktur für die Cloud integriert.

## Flexible Nutzung verschiedener eID-Services für eine sichere Authentifizierung

Besondere Berücksichtigung finden hierbei die Bedürfnisse von mittelständischen Unternehmen und Behörden. Für sie bündelt SkIDentity eine Reihe von eID-Services und macht sie flexibel für die sichere Anmeldung bei einer Cloud-Anwendung nutzbar. Kern der SkIDentity-Infrastruktur ist ein eID-Broker. Seine Aufgabe ist es, zwischen den Vorgaben des Cloud-Dienstes, seinem Rechtemanagement und den eingesetzten Authentifizierungsdiensten zu vermitteln. Im ersten Schritt kann der Cloud-Anbieter festlegen, welche eID für eine Anmeldung akzeptiert werden soll. Dabei kann es sich zum Beispiel um Ausweistoken wie einen Mitarbeiterausweis, Bank- und Signaturkarten, einen Heilberufsausweis, die elektronische Gesundheitskarte, den neuen Personalausweis oder ähnliche europäische Ausweiskarten handeln.



## Zweifelsfreie Identitäten für die Cloud und aus der Cloud

Bei einem Login-Versuch vermittelt der Broker die Authentifizierungsanfrage vom Cloud-Dienst an den entsprechenden eID-Service und erfährt so, ob der präsentierte Ausweistoken gültig ist. Darüber hinaus können hierbei auf Wunsch weitere Benutzerattribute wie Name und Adresse des Anwenders vom Cloud-Dienst angefragt werden. Auf Basis dieser Information kann der Cloud-Anbieter entscheiden, ob und auf welche Cloud-Anwendungen, Funktionen und Daten der Benutzer Zugriff hat. Am Ende steht ein auf bewährten und hochsicheren Technologien basierendes Anmeldeverfahren, das in den Cloud-Dienst integriert wird und dort als eine Art Wächter fungiert. Der Cloud-Anbieter muss nicht selbst eine eigene Authentifizierungsstruktur aufbauen und dafür nötige Berechtigungszertifikate erwerben, sondern kann die sicheren Authentifizierungsdienste bequem über SkIDentity aus der Cloud beziehen.

### Ausgangssituation

- Die Anmeldung zu Cloud-Diensten ist sicherheitskritisch
- Angreifer überwinden schwache Authentifizierungsverfahren und können Daten entwenden oder missbrauchen
- Kein einheitliches, starkes Authentifizierungsverfahren für Anwender von mehreren Cloud-Diensten

### Zielsetzung

- Sicheres und benutzerfreundliches Authentifizierungssystem verhindert unbefugte Zugriffe auf Daten in der Cloud
- Einsatz von etablierten Technologien und bewährter Ausweissysteme, damit der Anwender keinen neuen Ausweistoken benötigt
- Broker-basierte Architektur ermöglicht kosteneffizientes Identitätsmanagement, das selbst für mittelständische Unternehmen und Kommunen geeignet ist

## Rundum sicheres und vertrauensvolles Datenmanagement für Cloud-Dienste

Zusätzliche Einsatzgebiete hat SkIDentity in weiteren Projekten, die ebenfalls die Absicherung von Daten und Informationen in der Cloud zum Ziel haben. Gemeinsam mit Trusted-Cloud-Projekten wie beispielsweise Sealed Cloud sorgt SkIDentity für rundum sichere Cloud-Lösungen. Während verschiedene Projekte die auf den Servern der Cloud-Anbieter gespeicherten und verarbeiteten Daten schützen, verhindert SkIDentity den unautorisierten Zugriff auf diese Systeme aus der Cloud.

### Kontakt

**Ecsec GmbH**
**Dr. Detlef Hühnlein**
**E-Mail** detlef.huehnlein@ecsec.de

**Partner**

- ENX Association
- Fraunhofer-Institut für Arbeitswirtschaft und Organisation (IAO)
- Fraunhofer-Institut für Graphische Datenverarbeitung (IGD)
- OpenLimit SignCubes GmbH
- Ruhr-Universität Bochum, Lehrstuhl Netz- und Datensicherheit
- Universität Passau, Lehrstuhl für Öffentliches Recht, Informationstechnologierecht und Rechtsinformatik
- Urospace GmbH
- Versicherungswirtschaftlicher Datendienst GmbH

**Internet** www.skidentity.de

# Value4Cloud

## Marktunterstützende Mehrwertdienste für mehr Vertrauen in Cloud Computing

Cloud Computing verschafft Unternehmen mehr Flexibilität, macht sie mobiler und kann ihnen dabei helfen, Kosten zu reduzieren und ihre Innovationsfähigkeit zu verbessern. Dennoch scheuen gerade mittelständische Unternehmen oft die Nutzung. Die ständig wachsende Zahl von Cloud-Anbietern und -Angeboten hat den Markt unübersichtlich gemacht. Zudem fehlt es vielen IT-Verantwortlichen an Erfahrung und Expertise, um die Besonderheiten des IT-Bereitstellungsmodells Cloud umfassend zu beurteilen. Gleichzeitig stehen auch die Anbieter von Cloud-Diensten vor der Herausforderung, ihre Angebote marktgerecht bereitzustellen. Dazu müssen sie zum einen wissen, welche Anforderungen ihre Kunden an einen Cloud-Dienst stellen. Zum anderen müssen sie ihr Angebot so beschreiben, dass es für Interessenten aussagekräftig und mit anderen vergleichbar wird.

Genau hier setzt das Projekt Value4Cloud an. Es entwickelt einen strukturierten Leitfaden zur Unterstützung von Interessenten bei der Analyse von Cloud-Angeboten, eine Methode zur Integration von Kunden in den Innovationsprozess des Dienst-Anbieters sowie Best Practices, mit denen Anbieter ihre Dienste rechtsverträglich und vertrauenswürdig gestalten können. Darüber hinaus werden rechtliche Anforderungen der Nutzung von Cloud-Computing-Angeboten untersucht.

## Mehr Übersicht und Vertrauen für Cloud-Anwender

Zur Erreichung dieser Ziele entwickelt Value4Cloud marktunterstützende Mehrwertdienste, die in bestehende Marktplätze für Cloud-Dienste und Informationsportale eingebunden werden können. Dort sollen Cloud-Dienste einheitlich beschrieben, kategorisiert und durch Anwender bewertet werden können. Dies sorgt für mehr Transparenz in der Beschaffung, Auswahl und Nutzung von Cloud-Diensten.

Value4Cloud setzt hier in drei Bereichen an. Erstens benötigen Anwender für ihre Entscheidung bezüglich eines Cloud-Dienstes strukturierte Informationen. Dazu entwickelt das Projekt Konzepte, mit denen die Dienste beschrieben werden können, um sie so leichter vergleichbar zu machen. Eine Kategorisierung der Dienste und Fallstudien erleichtert zusätzlich den Überblick. Zweitens entwickelt das Projekt ein auf der Dienstebeschreibung aufbauendes Benchmarking von Cloud-Diensten nach einheitlichen Kriterien, in dem wichtige Diensteigenschaften wie Leistungsumfang, Rechtskonformität und Dienstqualität vergleichbar werden. Drittens will Value4Cloud die Anwender bei der Qualitätsbewertung unterstützen. Dazu entwickelt das Projekt Möglichkeiten der Bewertung von Cloud-Diensten durch andere Anwender und erarbeitet ein Rahmenwerk zur Zertifizierung der Dienste durch unabhängige Dritte.

Value4Cloud Dienste
(Fokus: Anwender)

- Strukturierte Information
- Qualitätsbewertung
- Benchmarking
- Vertrauensunterstützung


Value4Cloud Dienste
(Fokus: Anbieter)

- Open Service Innovation
- Rechtsverträglichkeit

## Unterstützung von Cloud-Anbietern bei der Entwicklung marktgerechter Dienste

Mit der so geschaffenen Transparenz und Vergleichbarkeit wird es für die Cloud-Anbieter noch wichtiger, marktgerechte Angebote zu schaffen, die den Anforderungen der Kunden an Qualität, Vertrauenswürdigkeit und Verlässlichkeit genügen. Cloud-Anwender erwarten von ihren Cloud-Anbietern einerseits eine kostengünstige und effiziente Bereitstellung. Andererseits fordern sie kundenspezifische Entwicklungen. Value4Cloud unterstützt Cloud-Anbieter dabei, diesen Zielkonflikt zu meistern. Durch den Einsatz offener Innovationsmethoden wird das Wissen der Anwender und externer Partner genutzt, um kundenorientiert Lösungen zu schaffen. Die Rechtsverträglichkeit neuer Angebote wird durch Leitfäden zur rechtskonformen Servicegestaltung adressiert. Diese beziehen sich auf Fragen des Datenschutzes, des IT-Strafrechts und der Haftung.

### Ausgangssituation

- Anwendern fehlen verlässliche Ansätze zur Bewertung der Qualität von Cloud-Diensten
- Mangelnde Vergleichsmöglichkeit von Cloud-Diensten
- Erfahrungen und Bedarfe der Cloud-Anwender werden nur von wenigen Anbietern zur Weiterentwicklung ihres Angebots aufgegriffen
- Bewertungsansätze zu Rechtskonformität von Cloud-Diensten fehlen

### Zielsetzung

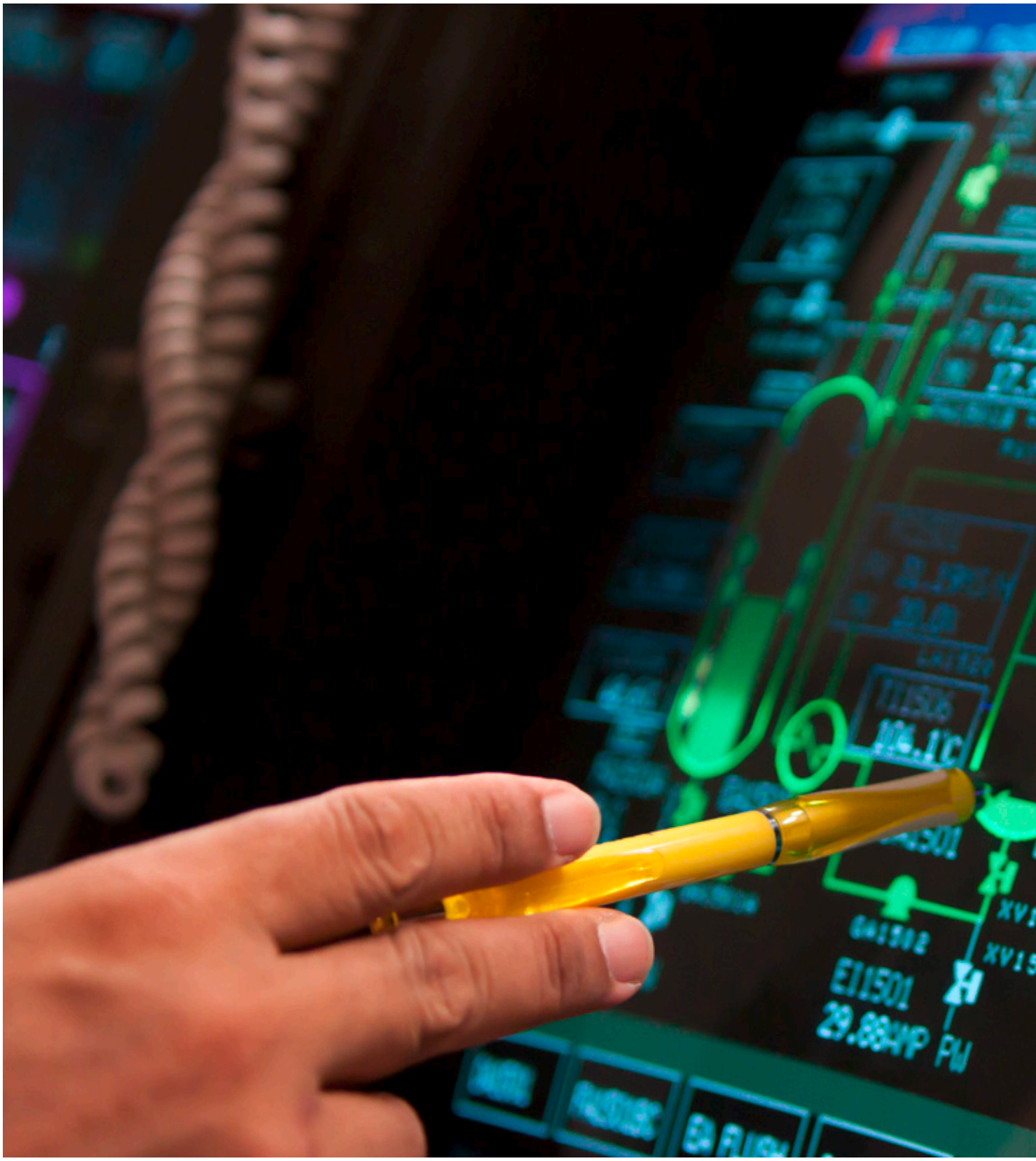
- Erleichterung des Vergleichs und der Bewertung der Qualität von Cloud-Diensten, wodurch Aspekte wie Sicherheit und Rechtskonformität besser beurteilt werden können
- Kundenerfahrungen und -bewertungen helfen bei der Orientierung und Auswahl von Angeboten
- Systematische Integration der Kundenbedürfnisse in den Entwicklungsprozess von Cloud-Anbietern

### Kontakt

**fortiss** – An-Institut der
Technischen Universität München
Forschungsbereich Information Systems
**Prof. Dr. Helmut Krcmar**
**E-Mail** krcmar@fortiss.org

**Partner**
- gate Garchinger Technologie- und Gründerzentrum GmbH
- SpaceNet AG
- Universität Kassel, Fachgebiet Wirtschaftsinformatik und Projektgruppe verfassungsverträgliche Technikgestaltung (provet) – im Forschungszentrum für Informationstechnik-Gestaltung (ITeG)
- Universität zu Köln, Wirtschafts- und Sozialwissenschaftliche Fakultät

**Internet** www.value4cloud.de


E11501
29.88MP
PM


# Anwendungen für Industrie und Handwerk

# Cloud4E

## Flexible Simulationslösungen in der Cloud für mittelständische Unternehmen

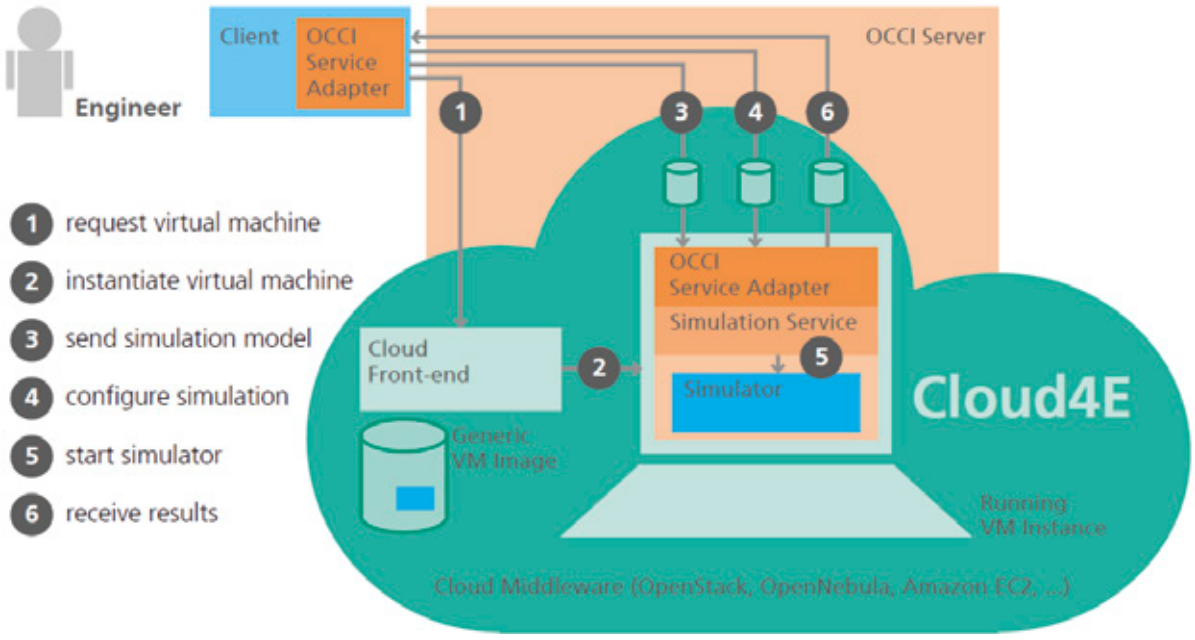
Moderne Produktentwicklungen erfordern umfangreiche Simulationen. Kaum ein Ingenieur kommt heute ohne massive Berechnungen bei der Konstruktion einzelner Bauteile oder ganzer Maschinen aus. Der finanzielle und personelle Aufwand für die Beschaffung der notwendigen Software sowie die Implementierung, Wartung und der Unterhalt der Hardware ist für mittelständische Unternehmen kaum wirtschaftlich zu leisten. Das Projekt Cloud4E will deshalb den Zugang zu professionellen Simulationslösungen bedarfsgerecht als Dienst über die Cloud ermöglichen. Damit erhalten Ingenieure in mittelständischen Unternehmen Zugang zu technischen Simulationslösungen, deren Einsatz bisher meist nur in großen Unternehmen wirtschaftlich ist. Dies erhöht die Innovationsfähigkeit von mittelständischen Unternehmen und ermöglicht ihnen, in neue Märkte einzutreten.

## Flexible und kostengünstige Simulations- und Optimierungsmethoden für Ingenieure

Dazu bietet Cloud4E über die Cloud Zugang zu allen Ressourcen, die für das Ausführen professioneller Simulationen im Engineering-Bereich notwendig sind. Dies umfasst neben der Software auch die nötige Rechenkapazität, die für die Berechnung heterogener, hochkomplexer Modelle in konkurrenzfähiger Zeit nötig ist. Dies bietet klare Vorteile für die entwickelnden Unternehmen: Investitionen in Hardware, Software und Personal können reduziert werden, laufende Kosten für die Installation und Pflege der Simulationssoftware entfallen. Auch die Ausfallsicherheit der Systeme wird durch die Cloud entscheidend erhöht, da die Ressourcen in der Cloud redundant und hochverfügbar sind, was bei lokal betriebenen Systemen oftmals aus Kostengründen nicht der Fall ist. Dies verhindert auch Ressourcen-Engpässe bei aufwändigen Analysen oder vor Lieferterminen und Produktfreigaben, wenn viele Ingenieure gleichzeitig Simulationen ausführen müssen. Die Cloud macht die Nutzung von Simulationslösungen also effizienter und flexibler.

## Individuell konfigurierbare Nutzung von Software und Rechenkapazitäten über die Cloud

In der Anwendung wird der Start einer Simulation für Ingenieure nicht komplizierter sein als bei der Nutzung lokaler Ressourcen. Statt auf einem lokalen Computer läuft die Simulationssoftware flexibel buchbar auf einer virtuellen Maschine in der Cloud. Diese virtuelle Maschine greift dabei auf Speicher- und Rechenkapazität der Cloud zurück, die die nötige Rechenleistung für die Simulation liefert und flexibel an aktuelle Anforderungen anpassbar ist. Cloud4E implementiert dazu offene, standardisierte Schnittstellen wie Open Cloud Computing Interface (OCCI), über die Software-,



Plattform- und Infrastruktur-Ebene miteinander kommunizieren. Dabei werden Ingenieure ihre Simulationen genauso individuell konfigurieren und ausführen können wie eigene Software innerhalb des Unternehmens. Gleichzeitig sorgen die offenen Schnittstellen dafür, dass sie bei Bedarf einen Wechsel des Anbieters vornehmen können, ohne dabei bisher erzielte Ergebnisse zu verlieren.

Im ersten Schritt wird Cloud4E den Cloud-Zugang für Modelica- und FEM-Simulationen als Modellanwendung bereitstellen, mit deren Hilfe Prototypen hinsichtlich ihrer Schwachstellen überprüft und bereits frühzeitig in der Entwicklungs- bzw. Konstruktionsphase verbessert oder aufgegeben werden können. In Zukunft werden die Anbieter von Simulationssoftware jedoch in der Lage sein, anhand der Projektergebnisse von Cloud4E beliebige Lösungen über die Cloud anzubieten.

## Einheitliche Sicherheitsinfrastruktur über den gesamten Workflow

Von zentraler Bedeutung für das Projekt ist die Sicherheit. Die bei der Entwicklung neuer Baugruppen oder Maschinen entstehenden Simulationsdaten sind für Konkurrenten von größtem Interesse. Sie müssen auf Rechnern in der Cloud bestens vor dem Zugriff Unbefugter geschützt sein. Cloud4E entwickelt deshalb eine vertrauenswürdige Sicherheitsinfrastruktur, die jeden Schritt im Lebenszyklus einer Simulationsaufgabe schützen kann. Übertragung und Verarbeitung der Daten werden dabei stets verschlüsselt sein. Hierzu stellt Cloud4E konfigurierbare und einfach zu nutzende Werkzeuge auf Basis von erprobten Open-Source-Technologien zur Verfügung, die sich entsprechend den jeweiligen Anforderungen in Cloud-Simulationsdienste integrieren lassen.

### Ausgangssituation

- Simulationsverfahren sind fester Bestandteil moderner Produktentwicklungen und erfordern hohe Rechenkapazitäten
- Für mittelständische Unternehmen sind Investitionen in notwendige Hardware, Software und Personal oft zu hoch
- Hohes Interesse von Mitbewerbern an Simulationsergebnissen erfordert Sicherheitsvorkehrungen

### Zielsetzung

- Flexible, cloud-basierte Simulationsumgebungen werden für mittelständische Unternehmen verfügbar
- Kostengünstige Nutzung professioneller Modelica- und FEM-Simulationslösungen
- Datensicherheit wird durch einheitliche Sicherheitsinfrastruktur gewährleistet

### Kontakt

**ITI Gesellschaft für ingenieurtechnische Informationsverarbeitung mbH**
**Dr. Andreas Uhlig**
**E-Mail** Andreas.Uhlig@itisim.com
**Partner**
- ERAS GmbH
- Fraunhofer-Institut für Integrierte Schaltungen (IIS)
- Friedrich-Alexander-Universität Nürnberg-Erlangen, Lehrstuhl für Rechnerarchitektur
- GWDG – Gesellschaft für wissenschaftliche Datenverarbeitung mbH

**Internet** www.cloud4e.de

# CLOUDwerker

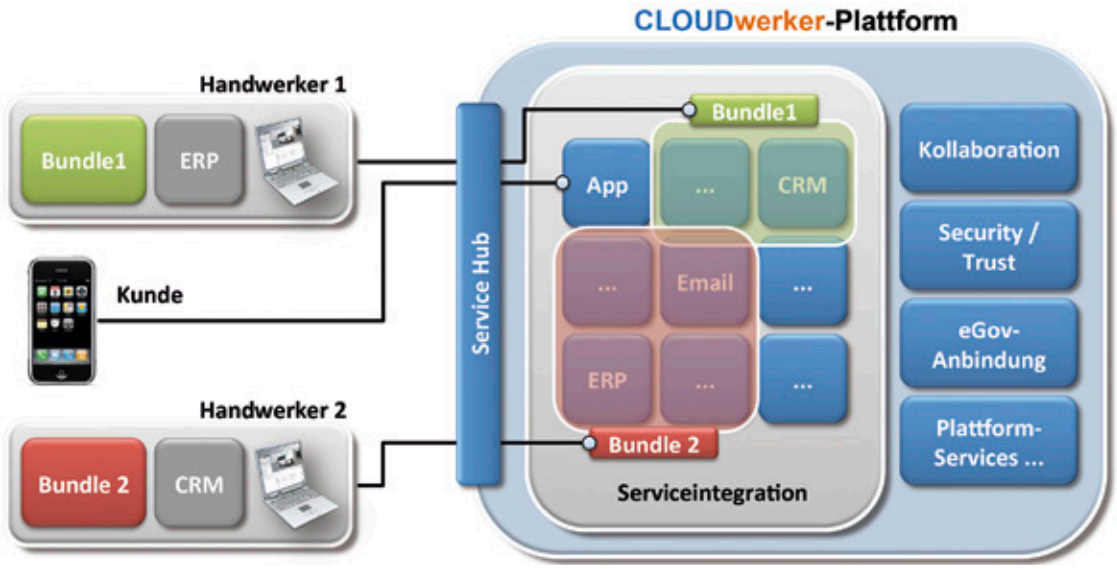
## Vertrauenswürdige, offene Cloud-Plattform für Handwerksbetriebe

In modernen Unternehmen ist der Einsatz von Software zur Unterstützung von Geschäftsprozessen und zur Verwaltung der Kundenbeziehungen mittlerweile unerlässlich. Denn das bringt zahlreiche Vorteile: Die Rechnungsstellung wird einfacher, die Zusammenarbeit mit Lieferanten als auch Projektpartnern kann besser koordiniert werden und die Programme bieten Übersichten zu wichtigen Geschäftsdaten. Wartung und Betrieb dieser Software erfordern jedoch laufende Investitionen und auch die Lizenzen selbst sind meist teuer und viel umfangreicher als benötigt. Und zusätzlich wird auch noch entsprechendes Personal benötigt, um diese nützlichen Werkzeuge einsatzbereit zu halten. Für die meisten Handwerksunternehmen ist dies nicht zu leisten – der Einsatz von Software beschränkt sich dort auf das Nötigste. Dabei könnten gerade Handwerker mit relativ festen und etablierten Abläufen vom Einsatz professioneller Software-Lösungen stark profitieren. Das Projekt CLOUDwerker will deshalb speziell für Handwerksunternehmen den Schritt hin zum Einsatz moderner IT-Werkzeuge vereinfachen.

## Baukasten integrierter IT-Lösungen in Form von Cloud-Diensten

Wichtige und nützliche Software-Pakete sollen deshalb über die Cloud angeboten werden. Ziel ist es, eine vertrauenswürdige, offene Service-Plattform zu schaffen, über die Software-Hersteller ihre Software anbieten können, während auf der anderen Seite Handwerker diese Software komfortabel und flexibel buchen können. Dabei werden die Dienste vom Office-Paket bis hin zu professionellen Lösungen für das Kundenbeziehungsmanagement (CRM) und zur Steuerung von Geschäftsprozessen (ERP) reichen. Sie sollen sich quasi modular in individuell konfektionierbare, integrierte Service-Bündel zusammenstellen lassen. Dienste können dabei von unterschiedlichen Diensteanbietern stammen, sind flexibel anpassbar und lassen sich so kombinieren, dass eine durchgängige Bearbeitung von Geschäftsprozessen möglich ist.

Zusätzlich soll zur Vereinfachung der Interaktion mit Ämtern und Behörden das Zusammenspiel mit eGovernment-Lösungen vereinfacht werden. Über spezielle Kollaborationswerkzeuge können zum Beispiel mit anderen Handwerksunternehmen gemeinsam Angebote, Rechnungen oder Bewerbungsunterlagen für öffentliche Ausschreibungen erstellt werden. Am Ende sollen sich alle wesentlichen Organisationsanforderungen von Handwerksunternehmen über die Dienste erfüllen lassen.



## Cloud-basierte kollaborative Bearbeitung von Aufträgen

Da die angebotenen Dienste nahtlos miteinander kommunizieren können, bietet CLOUDwerker eine kooperative Bearbeitung von Geschäftsprozessen zwischen verschiedenen Handwerksbetrieben. Betriebe, die zusammen an einem Gewerk oder Bauprojekt arbeiten, können über die im Rahmen des Projekts entwickelte CLOUDwerker-Plattform ihre Geschäftsprozesse zusammenführen, gemeinsam Rechnungen stellen, auf Ressourcen zugreifen oder die Kommunikation mit dem Kunden regeln. Der Kunde wiederum kann über die Plattform mit seinen Auftragnehmern in Kontakt treten und von ihm beispielsweise über den aktuellen Status und die Planungen informiert werden.

Eine besondere Bedeutung haben das Vertrauen und die Akzeptanz der Plattform. Hierzu unterstützt CLOUDwerker Handwerksbetriebe bei der Auswahl geeigneter, vertrauenswürdiger Cloud-Dienste mit dem so genannten „Trusted Service Finder“, der Handwerksbetriebe elektronisch durch die einzelnen Schritte des Auswahlprozesses führt. Verschiedene technische und nicht-technische Maßnahmen sorgen für Qualität und Rechtskonformität. Hinzu kommen weitere Optionen wie die Möglichkeit der Zusammenarbeit und des Datenaustauschs zwischen verschiedenen Handwerkern. Außerdem soll eine Migration bestehender Software zu den über CLOUDwerker angebotenen IT-Diensten unterstützt werden.

### Ausgangssituation

- Bestehende Softwarelösungen zur Unterstützung von Geschäftsprozessen sind meist teuer und kaum für Handwerksbetriebe geeignet
- Einrichtung, Wartung und Betrieb erfordern laufende Investitionen und professionelle IT-Experten
- Für die Zusammenarbeit zwischen mehreren Handwerksbetrieben fehlen passende Software-Programme

### Zielsetzung

- Zentrale Cloud-Plattform versorgt Handwerksbetriebe modular mit passender Software
- Nutzung von Cloud-Diensten reduziert IT-Investitionen und IT-Personaleinsatz
- Die Zusammenarbeit zwischen verschiedenen Handwerksbetrieben wird einfacher und professioneller

### Kontakt

CAS Software AG
Dr. Mark Hefke
E-Mail mark.hefke@cas.de
Partner
- 1&1 Internet AG
- CAS Software AG
- Fraunhofer-Institut für Arbeitswirtschaft und Organisation (IAO)
- Haufe Lexware GmbH & Co. KG
- Karlsruher Institut für Technologie (KIT)

Internet www.cloudwerker.de

# PeerEnergyCloud

## Sicherer virtueller Marktplatz für den lokalen Stromhandel

Private Haushalte verbrauchen rund ein Drittel des Stroms in Deutschland. Sie beziehen ihn meist aus großen überregionalen Kraftwerken. Gleichzeitig werden immer mehr Haushalte selbst zu Produzenten regenerativer Energie. Sie speisen diese jedoch genau wie die großen Kraftwerke in das gleiche Stromnetz ein. Bisher ist das Stromnetz jedoch nicht in der Lage, den Mix aus lokal und überregional erzeugter Energie intelligent zu nutzen. Dadurch können Haushalte bislang keinen lokal erzeugten Strom direkt verbrauchen. Mit Hilfe der Cloud will PeerEnergyCloud diese Situation verbessern. Lokal erzeugten Strom will das Projekt auf intelligente Weise an lokale Verbraucher vermitteln. Ziel ist die Konzeption und Entwicklung eines so genannten Microgrids und eines entsprechenden Cloud-Marktplatzes für den Handel mit lokal erzeugtem Strom über die Cloud. Dabei soll zum Beispiel der Preis Anreiz für die Verbraucher sein, bevorzugt den lokal erzeugten Strom zu nutzen.

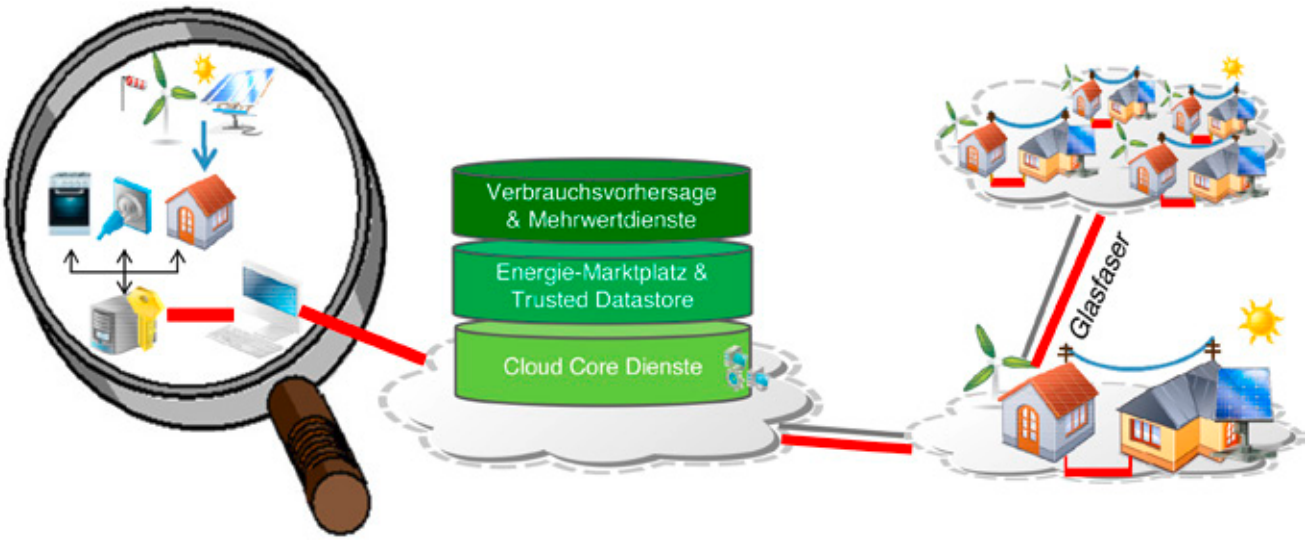
## Multi-Agentenhandel und Mehrwertdienste für Microgrids

Microgrids sind lokale Stromnetze mit wesentlichen Vorteilen: Durch PeerEnergyCloud-Marktplätze vermeiden sie lange Wege und Energieverluste und sorgen so für Netzstabilität und Versorgungssicherheit. Die urbane Netzstruktur wird optimal ausgenutzt, während überregionale Netze entlastet werden.

In der Modellstadt Saarlouis mit zunächst 50 angeschlossenen Wohneinheiten und mehreren Photovoltaikanlagen will PeerEnergyCloud mit innovativen Erfassungs- und Prognoseverfahren den produzierten Strom möglichst genau beziffern und über einen virtuellen Marktplatz den lokalen Energiehandel ermöglichen. Erzeugungs- und Verbrauchsschwankungen – so genannte Lastspitzen – können über die Cloud automatisch ausgeglichen werden, ohne dass der Netzbetreiber eingreifen muss.

## Intelligente Energienutzung mit vernetzten Sensoren und Aktoren

Grundlage dafür ist die sichere Vernetzung von Sensoren und Aktoren in den angeschlossenen Haushalten. Die Sensoren erfassen Stromverbrauch und -produktion und speisen die erfassten Daten in eine private Cloud der Stadtwerke ein. Verbrauch und Erzeugung lassen sich so teilweise in Echtzeit erfassen und lokal miteinander synchronisieren. Entsteht nach Abzug des Verbrauchs ein Stromüberschuss, fließt er in die überregionalen Netze. Reicht die lokale Erzeugung nicht aus, wird zusätzlicher Strom aus den überregionalen Netzen eingespeist. Eine noch effizientere Nutzung des Stroms ermöglichen die Aktoren in den Haushalten. Sie erhalten ebenfalls die Daten über den lokal erzeugten Strom. Ist viel Strom vorhanden, startet zum Beispiel die Waschmaschine. Fehlt der Strom, werden energieintensive Vorgänge aufgeschoben. Hinzu kommt die Möglichkeit für Drittanbieter, auf Basis der lokalen Daten eigene Mehrwertdienste bereitzustellen. Werden ausgewählte Daten vom



Verbraucher freiwillig für eine weitere Verwendung freigegeben, kann er zusätzliche energiebezogene Dienste buchen. Dann werden die Sensoren im Haus nicht nur für den intelligenten Einsatz von Haushaltsgeräten verwendet, sondern für ein so genanntes Energie-Auditing genutzt, das die Energieeffizienz des Haushaltes ermittelt und Stromsparpotenziale aufdeckt. Genauso können die Sensoren für eine Gebäudeüberwachung zum Objektschutz genutzt werden.

## Sichere Kommunikationsverbindung für die Weitergabe der Daten

Diese Weitergabe von Daten aus dem Haushalt an weitere Dienste-Anbieter macht hohe Sicherheitsstandards notwendig. Zum Schutz der Daten vor unberechtigtem Zugriff und vor unkontrollierter Nutzung implementiert PeerEnergyCloud hohe Verschlüsselungsstandards für alle Kommunikationsverbindungen zwischen Sensoren, Aktoren und der Cloud. Von der Kommunikation zwischen Sensoren und Aktoren bis hin zur Verbindung zwischen Nutzern und dem Online-Marktplatz sind Verbindungen verschlüsselt und können auch vom Cloud-Anbieter nicht eingesehen werden.

### Ausgangssituation

- Keine sichere und skalierbare Verarbeitung der Energiedaten
- Keine Mechanismen zur Angleichung von Angebot und Nachfrage von lokalem Strom
- Energiekontingente aus der Produktion privater Haushalte nicht frei handelbar

### Zielsetzung

- Bereitstellung von Energiediensten und Nutzung von günstiger Cloud-Infrastruktur für Endkunden durch Versorger
- Sichere Speicherung und Übertragung der Energiedaten durch Cloud-Infrastruktur
- Intelligentes „Microgrid“ regelt die Verteilung des lokal erzeugten Stroms an Abnehmer in der Umgebung über einen Cloud-Marktplatz

### Kontakt

SEEBURGER AG
Holger Kirchner
E-Mail h.kirchner@seeburger.de
Partner
- AGT Group (R&D) GmbH
- Deutsches Forschungszentrum für Künstliche Intelligenz (DFKI)
- Karlsruher Institut für Technologie (KIT)
- Stadtwerke Saarlouis GmbH

Internet www.peerenergycloud.de

# SensorCloud

## Hochskalierbare Cloud-Plattform für vernetzte Sensoren und Aktoren

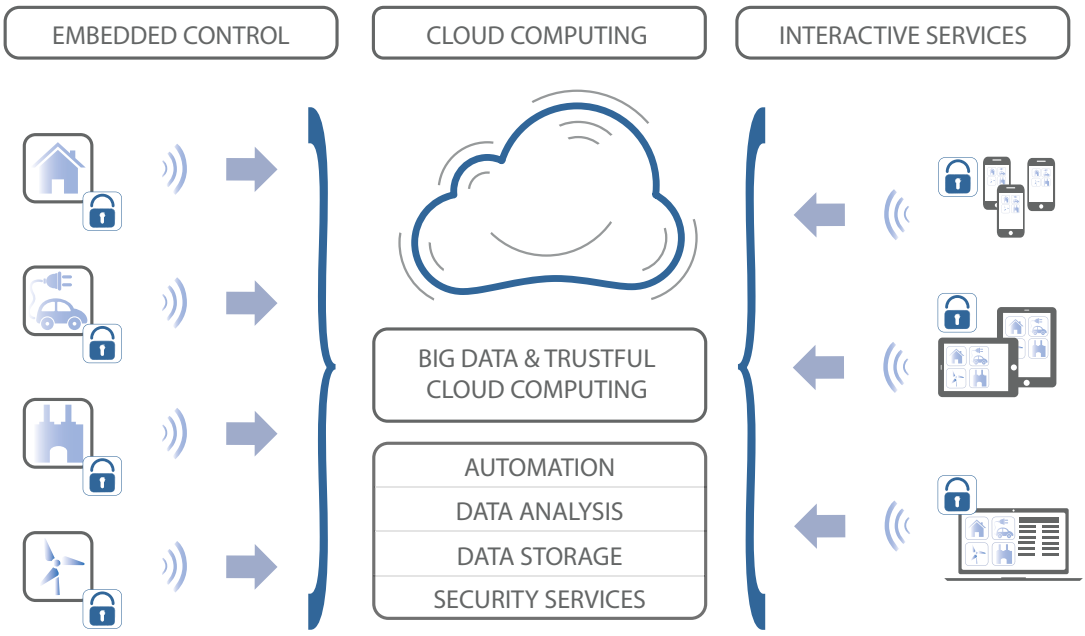
Sensoren und automatisch gesteuerte Aktoren sind aus vielen Bereichen des täglichen Lebens nicht mehr wegzudenken. Umweltsysteme in großen Gebäuden etwa messen über Sensoren Lichtstärke und Temperatur. Wird es zu hell oder zu heiß, dann fährt das Gebäude automatisch Jalousien herunter und regelt über Luftaustauschsysteme das Klima im Inneren. Aber auch Stromnetze oder Gesundheitssysteme reagieren heute auf Sensordaten und verbessern oder automatisieren danach ihre eigenen Funktionen. Für diese Anwendungsfälle werden Sensoren und Aktoren mit der dazwischengeschalteten Informationstechnologie heute noch lokal vernetzt. Einzellösungen werden für jeden Einsatz neu konzipiert oder anwendungsspezifisch angepasst; gemeinsame Standards gibt es kaum.

Das Projekt SensorCloud will deshalb die Vernetzung von Sensoren, Aktoren und die entsprechende Datenverarbeitung über die Cloud ermöglichen. Bislang zueinander inkompatiblen Inselanwendungen stellt das Vorhaben ein breit aufgestelltes, technisch innovatives Konzept entgegen. Ziel ist es, einen industriellen Standard zu haben, der spezialisierte und damit teure Leitungsnetze unnötig macht und die Nutzung dieser Technologien in Unternehmen und in privaten Haushalten vereinfacht.

## Intelligente Infrastrukturen für Stromnetze und Straßenverkehr

Mit SensorCloud ist es möglich, Sensordaten aller Art in der Cloud zu speichern und zu verarbeiten. Die Möglichkeiten dafür sind vielfältig. Ein Beispiel ist die Stromversorgung: Heute speichert die Daten eines Haushalts der jeweilige Stromanbieter bei sich. Wechselt der Haushalt zu einem anderen Anbieter, müssen bisherige Verbrauchsdaten mühsam übertragen und aktuelle Zählerstände vor Ort abgelesen werden. Mit SensorCloud wird es möglich sein, die Verbrauchsdaten über einen vernetzten Sensor zentral in der Cloud zu speichern und zu verarbeiten. Da der Kunde von Anfang an alleiniger Eigentümer der Daten ist und die volle Kontrolle über die Vergabe und den Entzug der Zugriffsrechte gegenüber Dritten hat, gestaltet sich ein Anbieterwechsel inklusive der Datenübernahme einfach und unkompliziert. Durch den Einsatz sicherer Verschlüsselungsmethoden wird eine Ende-zu-Ende-Sicherheit gewährleistet.

Ein weiteres Beispiel ist die intelligente, zentrale Steuerung des Straßenverkehrs: Sensoren in der Straßendecke oder in Form von Kameras messen die Verkehrsdichte, Aktoren wie etwa elektronische Anzeigetafeln regeln die Geschwindigkeit entsprechend und helfen so bei der Vermeidung von Staus. Mit Cloud-Technologien wäre dafür kein eigenes Steuerungsnetz nötig. Wenn Sensoren und Aktoren an das Internet angeschlossen sind, kann die Steuerung über die SensorCloud erfolgen.



## Vielfältiges Ökosystem innovativer Anwendungen

Die SensorCloud wird aus drei Komponenten bestehen: einer Cloud-Plattform, flexibel einsetzbaren, so genannten Cloud-Devices und den SensorCloud-Anwendungen. Als eine Art Betriebssystem vermittelt die Plattform zwischen der grundlegenden technischen Infrastruktur, bestehend aus einem Netzwerk virtualisierter Server und Datenspeicher, und den übrigen Komponenten der SensorCloud. Darauf basieren die Cloud-Devices: Das sind die über die SensorCloud vernetzten Sensoren und Aktoren. Sie können flexibel und benutzerspezifisch mit der SensorCloud verbunden werden. Offene Schnittstellen (APIs) ermöglichen schließlich, diese Devices in verschiedensten Anwendungen anzusprechen und zu nutzen.

Entwickler können so eigene, innovative Anwendungen entwickeln, mit Sensorinformationen aus der Cloud verknüpfen oder vernetzte Aktoren ansprechen. Auf der Basis der intelligenten und sicheren Infrastruktur von SensorCloud kann so ein vielfältiges Ökosystem innovativer Anwendungen entstehen. Der Besitzer eines Devices entscheidet selbst über die Freigabe seiner Sensordaten. Im Beispiel der Stromversorgung: Der Haushalt, der dem Stromanbieter das Auslesen seines Stromzählers erlaubt, könnte den Zugriff auch einer Anwendung freigeben, die ihm beim Stromsparen hilft, indem sie die Verbrauchsdaten intelligent interpretiert. Dem Nutzer ist es in diesem Fall selber überlassen, welchen Teil der Daten er welchem Anbieter zur Verfügung stellt. Gepaart mit Daten über den aktuellen Strompreis könnten Cloud-Devices mit Aktoren dann energieintensive Vorgänge wie das Wäschewaschen automatisch starten.

### Ausgangssituation

- Einzellösungen, die anwendungsspezifisch aufgebaut oder angepasst werden
- Die Anwendungen sind lokal begrenzt
- Intelligente Systeme in Unternehmen und privaten Haushalten bieten viele Chancen, sind aber meist proprietär

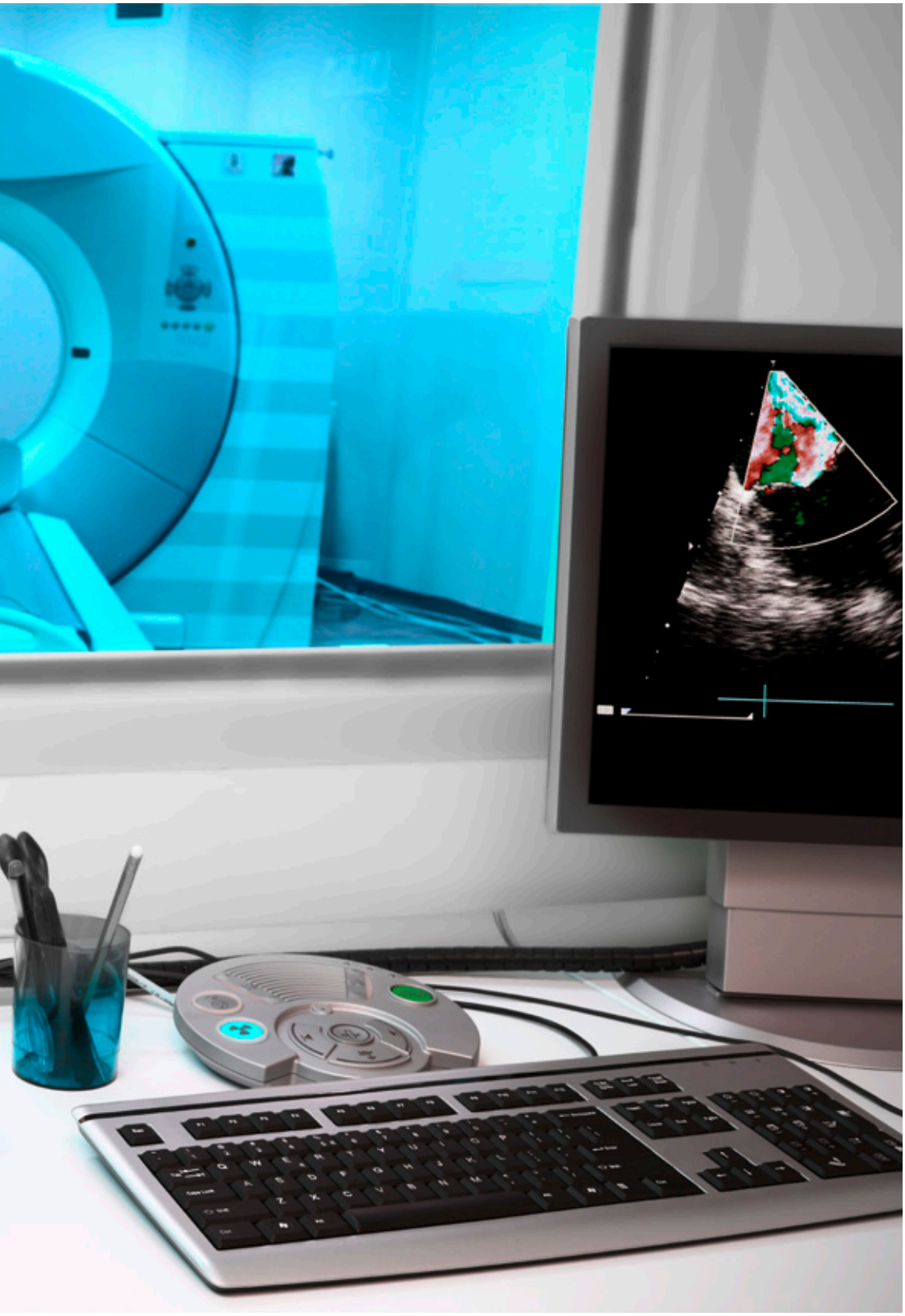
### Zielsetzung

- Vernetzung von Sensoren und Aktoren über eine hochverfügbare Cloud-Infrastruktur
- Schaffung eines Industriestandards, der die Vernetzung vieler unterschiedlicher Systeme über die Cloud ermöglicht
- Einbindung zahlreicher Anwendungen über offene Schnittstellen
- Sichere Kommunikationsinfrastruktur mit Ende-zu-Ende-Verschlüsselung
- Datenverarbeitung in Echtzeit

### Kontakt

QSC AG
Fred Schmidt
E-Mail fred.schmidt@qsc.de
Partner
- Fachhochschule Köln, Institut für Nachrichtentechnik
- RWTH Aachen University
- symmedia GmbH

Internet www.sensorcloud.de



# Anwendungen für den Gesundheitssektor

# cloud4health

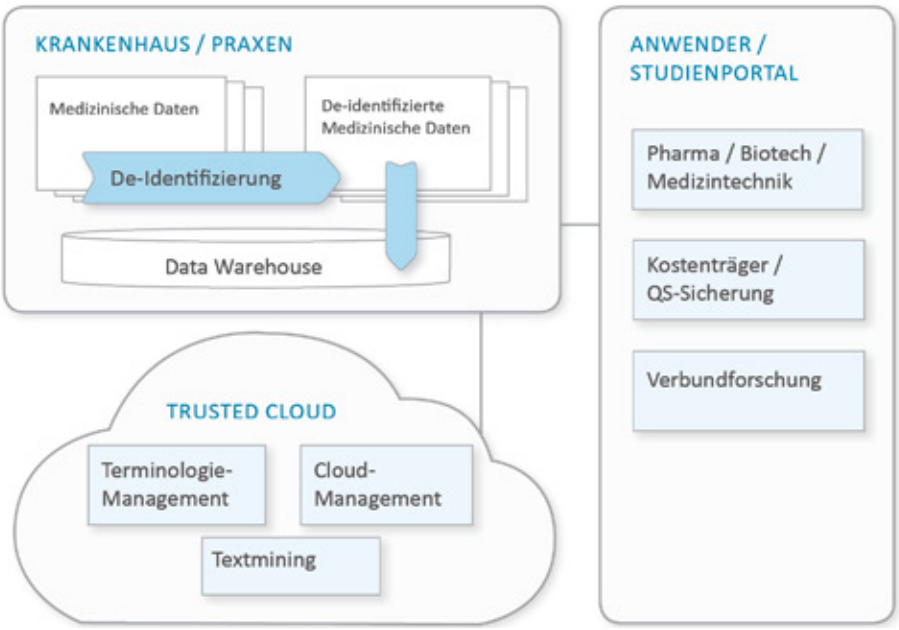
## Sichere Cloud-Architektur für Anwendungen im Gesundheitswesen

Bei der Behandlung von Patienten fallen in Kliniken viele Daten an. Diese können dabei helfen, Therapien und Medikamente zu verbessern. Die Daten zeigen zum Beispiel, wie gut neue Heilverfahren tatsächlich wirken und wo sie weiterentwickelt werden können. Auch in der Erforschung von Krankheiten können diese Informationen von unschätzbarem Wert sein. Doch wie lässt sich dieser Datenschatz im Gesundheitswesen am besten nutzen, ohne dass dabei die Privatsphäre der Patienten und der Schutz ihrer persönlichen Daten gefährdet werden? Diese Fragen beantwortet das Projekt cloud4health. Hier entstehen Lösungen für die zentrale Speicherung und Analyse von medizinischen Daten und die Nutzung der wertvollen Erkenntnisse aus den Analysen über die Cloud. Gleichzeitig entwickelt das Projekt ein Sicherheitskonzept für den Schutz dieser Daten, das den besonderen datenschutzrechtlichen Anforderungen gerecht wird.

## Semantisches Annotationsframework zur Sekundärnutzung medizinischer Rohdaten

Cloud4health kombiniert dazu Textanalyse- und Data-Warehouse-Technologien, die je nach Bedarf als private oder Community-Cloud bereitgestellt werden. So können Kliniken entscheiden, ob sie nur ihre eigenen Patientendaten analysieren und die Ergebnisse nur ihren Mitarbeitern zur Verfügung stellen wollen, oder ob sie ihre Daten gemeinsam mit anderen Einrichtungen des Gesundheitswesens nutzbar machen und selbst von der größeren Datenbasis profitieren wollen. In beiden Fällen werden die Daten zentral in der Cloud verarbeitet. Dabei werden sie anonymisiert, um die Privatsphäre der Patienten zu schützen.

Diese zentral gespeicherten Daten lassen sich dann inhaltlich analysieren, auch wenn sie in unstrukturierter Form vorliegen. Bisher beschränkt sich die Sekundärnutzung von Daten aus der elektronischen Krankenakte fast ausschließlich auf die Nutzung strukturierter Daten. Das sind Daten, die von jedem Patienten in gleicher Form dokumentiert werden und so leicht miteinander vergleichbar sind. Der größte Teil medizinischer Informationen liegt aber elektronisch als Freitext in Befunden und Arztbriefen vor. Cloud4health analysiert auch diese Texte, findet semantische Sinnzusammenhänge und Wortbeziehungen und macht sie so intelligent durchsuch- und analysierbar.



## Konkrete Anwendungsszenarien zur Verbesserung der Patientenbehandlung

Was das bedeutet, wird an den konkreten Modellanwendungen von cloud4health deutlich. Die erste Anwendung ist das frühzeitige Erkennen unerwünschter Nebenwirkungen bei neu eingeführten Medikamenten. Aus den unstrukturierten Patientendaten erkennt cloud4health, zu welchen Nebenwirkungen es im Zusammenhang mit dem Medikament kommt und wie oft diese auftreten. So lässt sich schneller und besser erkennen, wann und wie das Medikament einzusetzen ist. Das erhöht die Sicherheit der Patienten entscheidend und verbessert die Effektivität der Erfassung von unerwünschten Wirkungen nach Markteinführung.

Die zweite Anwendung ist die Auswertung der Behandlung von Patienten mit künstlichen Hüftgelenken. Hier macht cloud4health die Erfahrungen über den Einsatz verschiedener heute bereits verwendeter Hüftgelenksprothesen miteinander vergleichbar. Immer wieder auftretende Komplikationen nach Hüftgelenksoperationen lassen sich so erkennen, Operationstechniken können entsprechend verbessert werden. Ärzte können besser entscheiden, welches Implantat in welchem Patientenfall die besten Ergebnisse verspricht.

In einem dritten Anwendungsszenario werden Verfahren zu automatisierten Plausibilitäts- und Wirtschaftlichkeitsprüfungen medizinischer Behandlungen entwickelt. Dabei soll geprüft werden, inwieweit ärztliches Handeln zweckmäßig und wirtschaftlich erfolgt. Vor dem Hintergrund begrenzter Mittel im Gesundheitswesen wäre es möglich, Therapien nicht nur rein wirtschaftlich, sondern auch aufgrund des medizinischen Nutzens zu bewerten. So lässt sich zum Beispiel überprüfen, ob angeordnete Behandlungen bedarfsgerecht erfolgten.

### Ausgangssituation

- Sensibilität von Patientendaten verhindert oft deren Nutzung für die Allgemeinheit
- Unstrukturierte Datensammlungen verhindern Analysen zur Qualitätsverbesserung
- Fehlende computergestützte Qualitäts- und Wirtschaftlichkeitsprüfungen für medizinische Behandlungen

### Zielsetzung

- Sichere Cloud-Architektur ermöglicht zeitnahe, semantische Analyse medizinischer Daten
- Strenges Datenschutz- und Sicherheitskonzept ermöglicht Umgang mit hochsensiblen Daten
- Verbesserung der Patientensicherheit und Versorgungsqualität

### Kontakt

Averbis GmbH
Dr. med. Philipp Daumke
E-Mail daumke@averbis.de

Partner
- Fraunhofer-Institut für Algorithmen und Wissenschaftliches Rechnen (SCAI)
- Friedrich-Alexander-Universität Erlangen-Nürnberg, Lehrstuhl für Medizinische Informatik
- RHÖN-KLINIKUM AG
- TMF – Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V.

Internet www.cloud4health.de

# GeneCloud

## Kostenreduzierte Arzneimittelentwicklung durch cloud-basiertes Wirkstoff-Screening

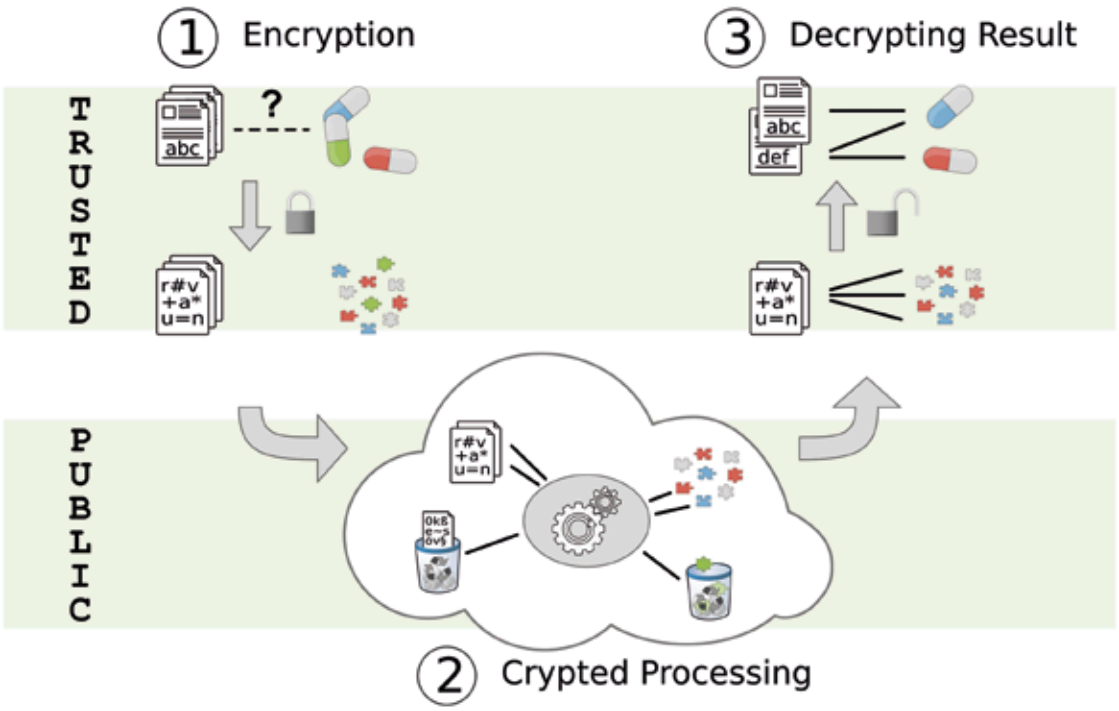
Die schnellere und kostengünstigere Entwicklung dringend benötigter Medikamente ist das Ziel des Projekts GeneCloud. Neue so genannte Hochdurchsatzverfahren erlauben der Pharmaindustrie die Analyse und Messung einer großen Anzahl von Proben in vergleichsweise kurzer Zeit. Die dabei entstehenden Datenmengen bergen jedoch eine große Herausforderung. Die zu ihrer Speicherung und Verarbeitung nötigen Rechenkapazitäten stehen gerade kleinen und mittelständischen Unternehmen selten zur Verfügung, denn die Investition in zahlreiche eigene Server wäre zu hoch. Darüber hinaus erfordern diese aufwändigen und rechenintensiven Verfahren ein hohes Maß an Sicherheit.

## Parallelisierung von Hochdurchsatzverfahren der Pharmaindustrie für die Cloud

Eine Lösung dieses Problems ist der Zugang zu benötigten Rechenkapazitäten für parallele Hochdurchsatzverfahren über die Cloud. Entsprechend müssen die Algorithmen zur Bearbeitung der Daten so gestaltet sein, dass sie parallelisiert und damit verteilt berechenbar, sind. Dafür teilt die im Rahmen des Projektes entwickelte Software die notwendigen Rechenschritte so intelligent auf, dass möglichst viele von ihnen gleichzeitig ausgeführt werden und auf mehrere Prozessoren verteilt werden können. Dies spart Zeit und beschleunigt die Entwicklung. Forscher können so bedarfsgerecht die Rechenleistung buchen, die sie für ihre Analysen gerade benötigen. Für einige Stunden oder Tage steht ihnen dann die Leistung eines Großrechners ganz nach den jeweiligen Anforderungen zur Verfügung.

## Cloud-basierte Wirkstoffanalysen zur Krebsbekämpfung

GeneCloud will genau diese flexible, elastische Nutzung ermöglichen und dabei den besonderen Anforderungen der Pharmaunternehmen genügen. Denn pharmazeutische Daten bedürfen eines besonderen Schutzes. Zum einen möchten die Unternehmen ihre Geschäftsgeheimnisse besonders schützen. Zum anderen unterliegen sie speziellen Datenschutzbestimmungen. Das Projekt wird drei Anwendungen des Wirkstoffscreenings entwickeln. Die erste Anwendung soll Biomarker im Krebs vorhersagen, um



Prognosen über den Krankheitsverlauf bei Krebserkrankungen zu verbessern. Bei der zweiten Anwendung geht es darum, Wirkstoffe auf ihre Bindefähigkeit an Zielproteine zu testen, um die Wirkung von Medikamenten zu verstehen. Dadurch können zukünftig noch wirksamere Folgesubstanzen entwickelt werden. Ein wesentliches Problem in der Wirkstoffforschung sind ungewollte Effekte von Wirkstoffen. Im dritten Anwendungsfall werden Arzneimittelinteraktionen durch automatisierte Textanalysen entsprechender Fachliteratur identifiziert.

## Verbesserter Schutz durch kryptografische und steganografische Verfahren

Eine weitere Herausforderung ist die notwendige Absicherung der bearbeiteten Daten, um sie vor dem Zugriff Unbefugter zu schützen. Einfache Verschlüsselungsverfahren reichen dazu nicht aus, da auch der Cloud-Anbieter keinen Einblick haben darf. GeneCloud hat dazu ein neuartiges steganografisch-kryptografisches Sicherheitskonzept entwickelt. Herkömmlich verschlüsselte Daten werden dabei zusätzlich anonymisiert, vermischt und in einem Trägermedium versteckt, um so einen flexiblen und skalierbaren Schutz zu realisieren.

### Ausgangssituation

- Die Entwicklung von neuen Medikamenten in der Pharmaforschung ist teuer und langwierig
- Der Einsatz von neuen, rechenintensiven Verfahren ist für die Arzneimittelforschung unerlässlich
- Mittelständische Unternehmen können sich die hohen Investitionen in notwendige Rechenkapazitäten nicht leisten

### Zielsetzung

- Rechenkapazitäten für neue Analyseverfahren können über die Cloud genutzt werden
- Cloud-basiertes Wirkstoffscreening ermöglicht auch mittelständischen Unternehmen eine moderne Arzneimittelentwicklung
- Die Daten bleiben durch kryptografische und steganografische Verfahren gesichert

### Kontakt

Transinsight GmbH
Dr. Michael R. Alvers
E-Mail malvers@transinsight.com
Partner
- antibodies-online GmbH
- Qualitype AG
- Technische Universität Dresden, Zentrum für Informationsdienste und Hochleistungsrechnen

Internet www.transinsight.com/genecloud/

# TRESOR

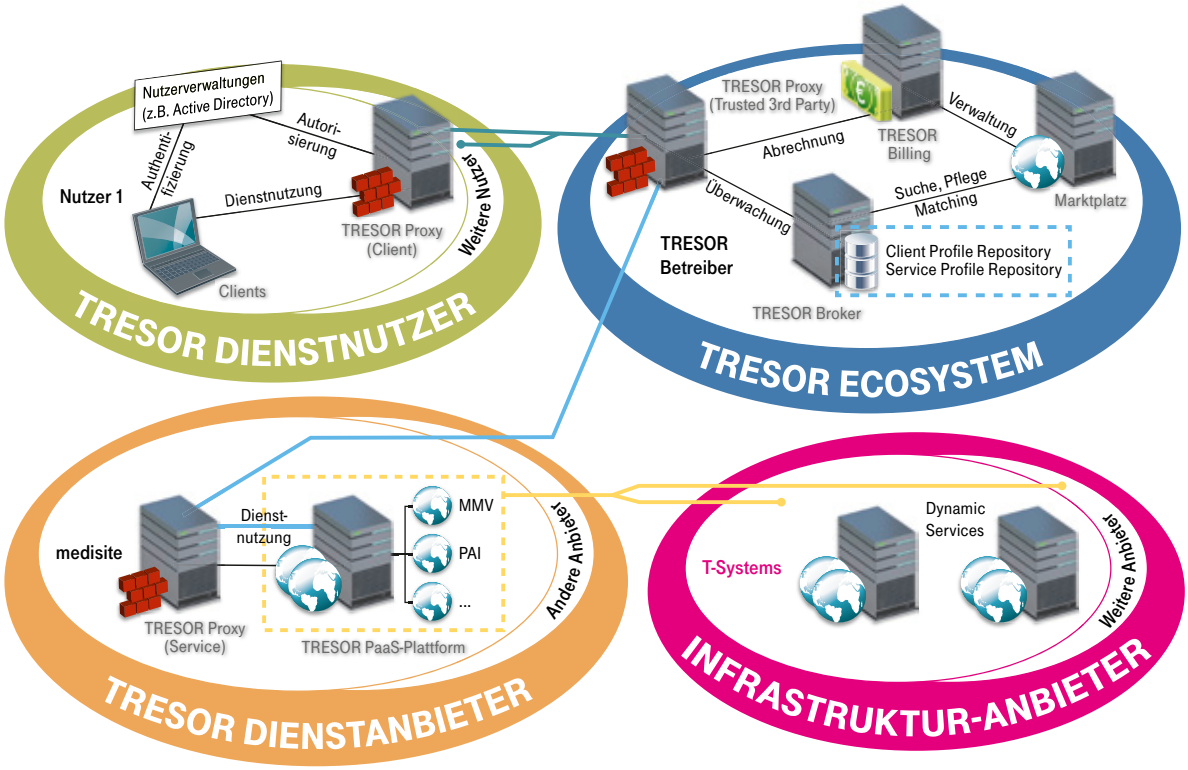
## Sichere Nutzung von Cloud-Diensten im Gesundheitswesen

Oftmals müssen Patienten im Rahmen der Behandlung von Erkrankungen in andere Kliniken verlegt werden. Bei Patienten mit Herzerkrankungen erfolgen beispielsweise erste Untersuchungen bei einem Kardiologen oder in der kardiologischen Abteilung eines Krankenhauses. Wird eine Operation erforderlich, müssen diese Patienten in ein Herzzentrum oder eine herzchirurgische Abteilung verlegt werden. Es folgt eine Behandlung in spezialisierten Kliniken und anschließend in Rehabilitationseinrichtungen. Bei all diesen Stationen einer Therapie fallen Daten an, die jeweils auch für die anderen medizinischen Einrichtungen für eine erfolgreiche Behandlung wichtig sind – von den persönlichen Daten, der medizinischen Anamnese über die Diagnose der Krankheit bis hin zu ihrer medikamentösen oder operativen Behandlung. Die sichere und vertrauenswürdige elektronische Übergabe dieser Daten an eine andere medizinische Einrichtung ist heute jedoch nur eingeschränkt möglich.

## Vertrauenswürdiges Cloud-Ökosystem

Das Projekt TRESOR schafft deshalb eine vertrauenswürdige Infrastruktur, die gesetzliche Vorschriften sowie Sicherheits- und Datenschutzvorgaben berücksichtigt. Ziel ist ein Cloud-Ökosystem mit Anwendungen für das Gesundheitswesen, das eine datenschutzkonforme, geschlossene und institutsübergreifende Prozesskette ermöglicht. Lokale und zueinander inkompatible Insellösungen können durch Cloud-Anwendungen auf der Basis gemeinsamer Standards ersetzt werden.

Das Cloud-Ökosystem besteht dabei unter anderem aus einer dynamischen Cloud-Plattform, einem Cloud-Broker und einem Cloud-Proxy. Die Plattform schafft eine technische Basis für modulare und dynamische Cloud-Anwendungen auf der Grundlage etablierter Standards wie OSGi. Auf einem Marktplatz können Dienste-Anbieter ihre Anwendungen bereitstellen. Gesundheitseinrichtungen wählen verschiedene Cloud-Dienste zur Nutzung aus. Diese können



untereinander kommunizieren und Daten austauschen. Einzelne Dienste lassen sich jederzeit einfach austauschen, wodurch Lock-in-Effekte vermieden werden. Der Cloud-Broker steuert dabei für Gesundheitseinrichtungen die Bündelung der gebuchten Dienste und sorgt als zentrales Service- und Profile-Repository für den sicheren Austausch der Daten zwischen den Diensten und den Anwendern.

## Datensicherheit im Fokus

Gleichzeitig schützt der Cloud-Broker Anwendungen und Daten vor dem Zugriff Unbefugter. Dazu identifiziert er eindeutig und zuverlässig die Anwender und gewährt ihnen nur Zugang zu den Cloud-Diensten, zu denen sie auch berechtigt sind. Die innovative Zugriffssteuerung setzt dabei zusätzlich auf eine ortsbasierte Autorisierung, bei der die Daten nur von bestimmten Orten abrufbar sind. Für die sichere Übermittlung und Speicherung von Daten entwickelt TRESOR flexible hierarchische Verschlüsselungsmethoden. Kern ist hierbei das Trusted Cloud Transfer Protocol (TCTP), das eine getrennte Verschlüsselung von Nutzdaten und Metainformationen möglich macht. Dies erlaubt eine echte Ende-zu-Ende-Verschlüsselung und damit einen vertrauensvollen Austausch von sensiblen Daten über alle Zwischenstationen hinweg.

## Beispielhafte Anwendungen im Bereich der Behandlung von Patienten

Zur Veranschaulichung des TRESOR-Ökosystems werden zwei Demonstratoren umgesetzt. Zum einen werden die Projektpartner eine medienbruchfreie medizinische Verlaufsdokumentation zwischen den am Projekt beteiligten Krankenhäusern zeigen – eben jenen notwendigen sicheren Datenaustausch zwischen kooperierenden Einrichtungen bei der gemeinsamen Versorgung von Patienten. Zum anderen soll ein cloud-basierter Dienst zur Prüfung von Arzneimittelinteraktionen demonstriert werden, der aktuelle Informationen aus dem Behandlungsprozess eines Patienten nutzt.

### Ausgangssituation

- Datensicherheit in der Cloud entspricht vielfach nicht den hohen Anforderungen des Gesundheitswesens
- Sicherer elektronischer Datenaustausch zwischen Gesundheitseinrichtungen fehlt
- Cloud-Dienste haben Potenzial, sind im Gesundheitswesen jedoch noch selten

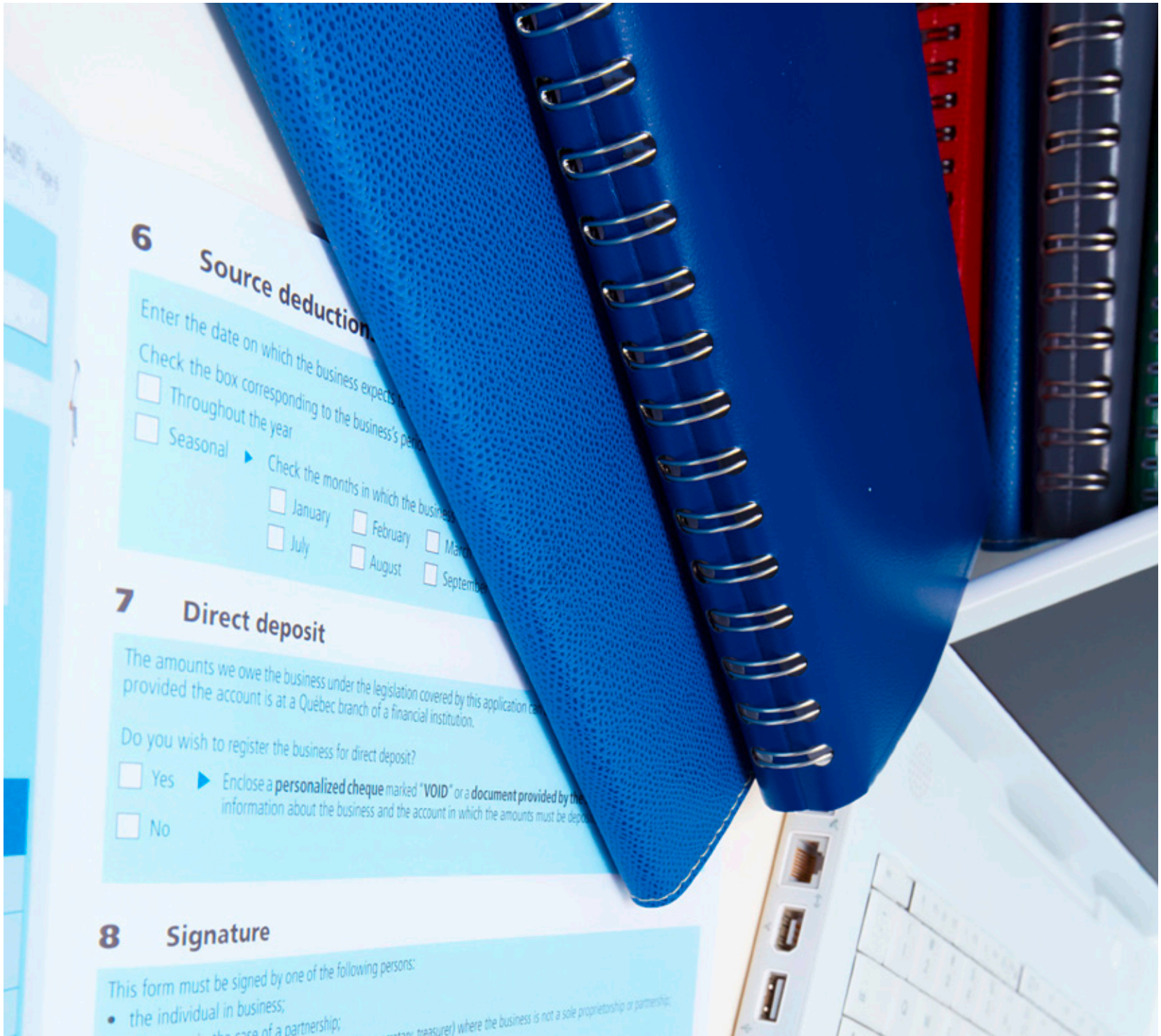
### Zielsetzung

- Cloud-Ökosystem für sichere und rechtskonforme Bereitstellung und Nutzung von Diensten im Gesundheitswesen
- Demonstration einer sicheren cloud-basierten medienbruchfreien Verlaufsdokumentation für medizinische Einrichtungen
- Ortsbasierte sichere Authentifizierung und Autorisierung von Cloud-Anwendern

### Kontakt

**medisite Systemhaus GmbH**
**Torsten Frank**
**E-Mail** torsten.frank@medisite.de
**Partner**
- Deutsches Herzzentrum Berlin
- Paulinenhaus Krankenanstalt e.V.
- Technische Universität Berlin, Fachgebiet Service-centric Networking
- Technische Universität Berlin, Fachgebiet Informations- und Kommunikationsmanagement
- T-Systems International GmbH
- Bitplaces GmbH

**Internet** www.cloud-tresor.de


6 Source deduction
Enter the date on which the business expects
Check the box corresponding to the business's
Throughout the year
Seasonal
Check the months in which the
January
February
July
August
7 Direct deposit
The amounts we owe the business under the legislation covered by this application
provided the account is at a Québec branch of a financial institution.
Do you wish to register the business for direct deposit?
Yes
Enclose a personalized cheque marked "VOID" or a document provided by the
information about the business and the account in which the amounts must be
No
8 Signature
This form must be signed by one of the following persons:
the individual in business;


# Anwendungen für den öffentlichen Sektor

# CloudCycle

CLOUDCYCLE
Sicherheit. Standards. Services.

## Sichere und rechtskonforme Cloud-Lösungen für Schulverwaltungen und Bürgerportale

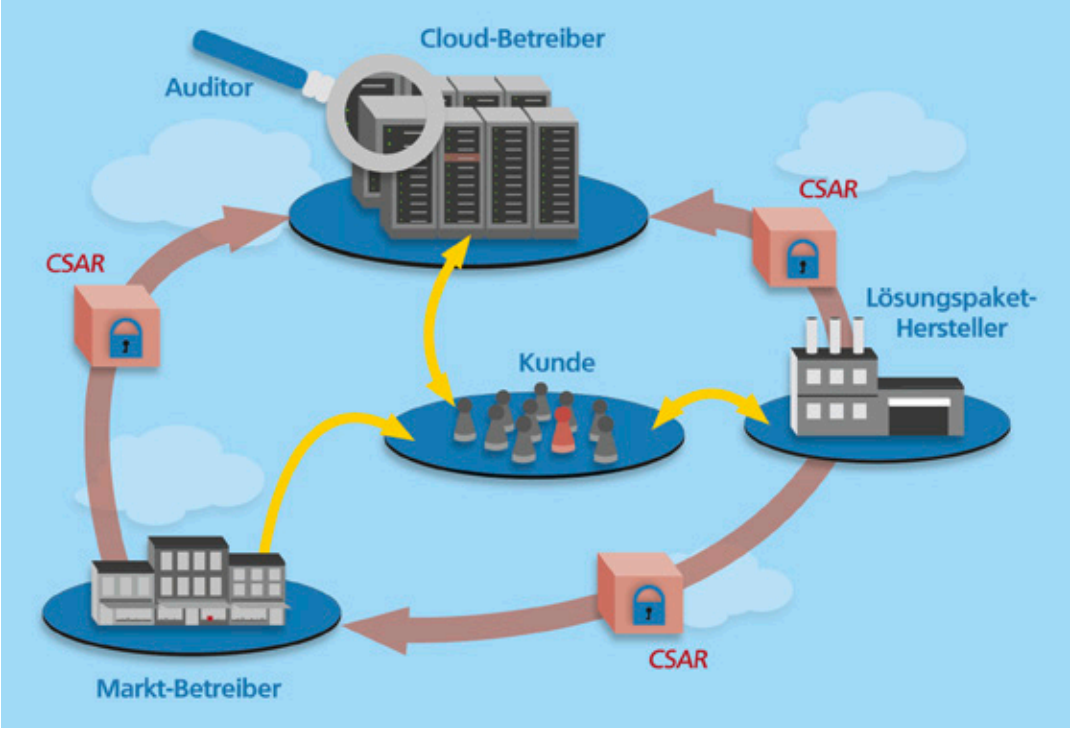
Cloud-Dienste bieten kleinen und mittleren Unternehmen sowie der öffentlichen Verwaltung zahlreiche Chancen. Sie ermöglichen die vernetzte und flexible Zusammenarbeit, selbst unter Kollegen an verschiedenen Standorten. Allerdings verhindern rechtliche Unsicherheit und Sicherheitsbedenken den Schritt gerade von Schulen, Behörden und Verwaltungen in die Cloud. CloudCycle will dieser Zurückhaltung begegnen und sichere sowie kostengünstige Cloud-Dienste für diese Zielgruppen ermöglichen. Beispielhaft geschieht dies anhand einer Bildungs-Cloud, die innerhalb des Projekts erstmalig definiert wird. Sie stellt eine auf die Bedürfnisse von Schulen zugeschnittene Auswahl an Cloud-Diensten zur Verfügung. Dabei werden die für Schulen und den öffentlichen Bereich besonderen Rechts- und Sicherheitsanforderungen berücksichtigt.

Im Bildungssektor müssen bislang Daten der Schulverwaltung und Daten aus dem pädagogischen Bereich physisch getrennt gespeichert und bearbeitet werden, was sehr aufwändig und ineffizient sein kann. Durch die Technologie von CloudCycle könnten zukünftig das Schulverwaltungsnetz und das pädagogische Netz lediglich virtuell getrennt in einer Bildungs-Cloud genutzt werden, was zu einer deutlichen Vereinfachung führen würde.

## CloudCycle-Ökosystem als gemeinsame, standardisierte Basis für Cloud-Dienste

Dazu schafft CloudCycle ein Cloud-Ökosystem, das eine gemeinsame, standardisierte Basis für den gesamten Lebenszyklus eines Cloud-Dienstes bietet. Sämtliche Komponenten, die für das Angebot eines Cloud-Dienstes nötig sind, sollen zueinander kompatibel werden. Die Anbieter einer Cloud-Plattform können so problemlos zu einem anderen Rechenzentrum umziehen, solange die Infrastruktur CloudCycle nutzt. Die Anbieter eines Cloud-Dienstes wiederum können ihr Angebot auf eine andere Cloud-Plattform umziehen. Die Kunden eines Cloud-Dienstes schließlich können ihre Daten nahtlos zwischen Cloud-Diensten auf der Basis von CloudCycle migrieren.

Ziel ist es, das Format von Cloud-Diensten im Zusammenspiel der unterschiedlichen Akteure zu standardisieren und damit einen einfachen Wechsel zwischen verschiedenen Anbietern zu ermöglichen. Die Standardisierung betrifft den gesamten Lebenszyklus eines Cloud-Dienstes: von der Cloud-Plattform, die der Dienst als technische Basis nutzt, über die Erstellung kompatibler Anwendungen bis hin zur Nutzung durch den Anwender und darüber hinaus die Migration zu einer anderen Plattform oder das Löschen einer Anwendung am Ende ihres Lebenszyklus. Der Nutzer soll die Wahl zwischen verschiedenen Softwareherstellern



und Cloud-Betreibern haben und bei einem Wechsel seine Daten nahtlos weiterverwenden können. Der gemeinsame Standard stellt dabei ebenfalls sicher, dass auch bei dem neuen Anbieter dasselbe Maß an IT-Sicherheit und Rechtskonformität gewährleistet ist wie vor dem Wechsel.

## Interoperabilität zwischen den Anbietern von Cloud-Plattformen und -Lösungen

Um das zu erreichen, verwendet CloudCycle den bei dem Standardisierungsgremium OASIS spezifizierten Standard TOSCA (Topology and Orchestration Specification for Cloud Applications). TOSCA ermöglicht die formale Beschreibung der Topologie und Lebenszyklus-Operationen von Cloud-Anwendungen. Damit ist es möglich, den Aufbau der Anwendung zu beschreiben und in einem Plan einheitlich eine Abfolge von Operationen zu definieren, durch die eine Cloud-Anwendung installiert, verwaltet und überwacht werden kann. Dabei können die Dienstanbieter definieren, welche Anforderungen etwa an Sicherheit oder Rechtskonformität ihre Anwendung erfüllen soll. Innerhalb des von CloudCycle entwickelten erweiterten Standards kann jeder Cloud-Betreiber diesen Anforderungen schnell, kostengünstig und verbindlich entsprechen.

### Ausgangssituation

- Gemeinsame technische Basis für den vollständigen Lebenszyklus eines Cloud-Dienstes nicht vorhanden
- Keine einheitliche Lösung für Fragen der Interoperabilität, Sicherheit und Rechtskonformität zwischen Plattformen
- Migration von Daten zwischen öffentlich-rechtlichen und privatwirtschaftlichen Cloud-Anbietern schwierig

### Zielsetzung

- Entwicklung einer Dienstebeschreibungssprache zur vollständigen Abbildung eines Cloud-Dienst-Lebenszyklus
- Flexible Nutzung von Cloud-Anwendungen auf unterschiedlichen Plattformen bei garantierter Sicherheit und Rechtskonformität
- Vereinfachung der Interoperabilität und Migration durch standardisierte Schnittstellen

## Automatisierte Audits zur Kontrolle von Sicherheit und Datenschutz

Die gemeinsame technische Basis ermöglicht zudem Mehrwertdienste, die alle Cloud-Dienste auf der Basis von CloudCycle nutzen können. Ein Beispiel dafür sind automatisierte Auditing- und Monitoring-Lösungen. Unternehmen und die öffentliche Verwaltung haben eine Reihe von Sicherheitsanforderungen und rechtlichen Anforderungen zu erfüllen. Dabei wird die Einhaltung der Vorgaben meist von unabhängigen Dritten überprüft. Diese Kontrollen können im CloudCycle-Ökosystem zu einem großen Teil automatisiert geschehen. Dazu definiert der Kunde seine spezifischen Prüfkriterien in einer so genannten Policy. Danach ist es möglich, den Cloud-Dienst anhand der Kriterien automatisch zu prüfen und festzustellen, ob er den darin festgeschriebenen Sicherheitsanforderungen des Kunden genügt. Die Automatisierung der Prüfungen erlaubt regelmäßige Audits in kurzen Abständen und somit eine kontinuierliche, kostengünstige und effiziente Kontrolle der Anforderungen während des gesamten Lebenszyklus eines Cloud-Dienstes.

### Kontakt

**regio iT gesellschaft für informationstechnologie mbh**
**Peter Niehues**
**E-Mail** peter.niehues@regioit-aachen.de
**Partner**
- Fraunhofer-Institut für Sichere Informationstechnologie (SIT)
- IBM Deutschland Research and Development
- Kommunale Informationsverarbeitung Baden-Franken
- Universität Stuttgart, Institut für Architektur von Anwendungssystemen
- Universität Stuttgart, Institut für Parallele und Verteilte Systeme

**Internet** www.cloudcycle.org

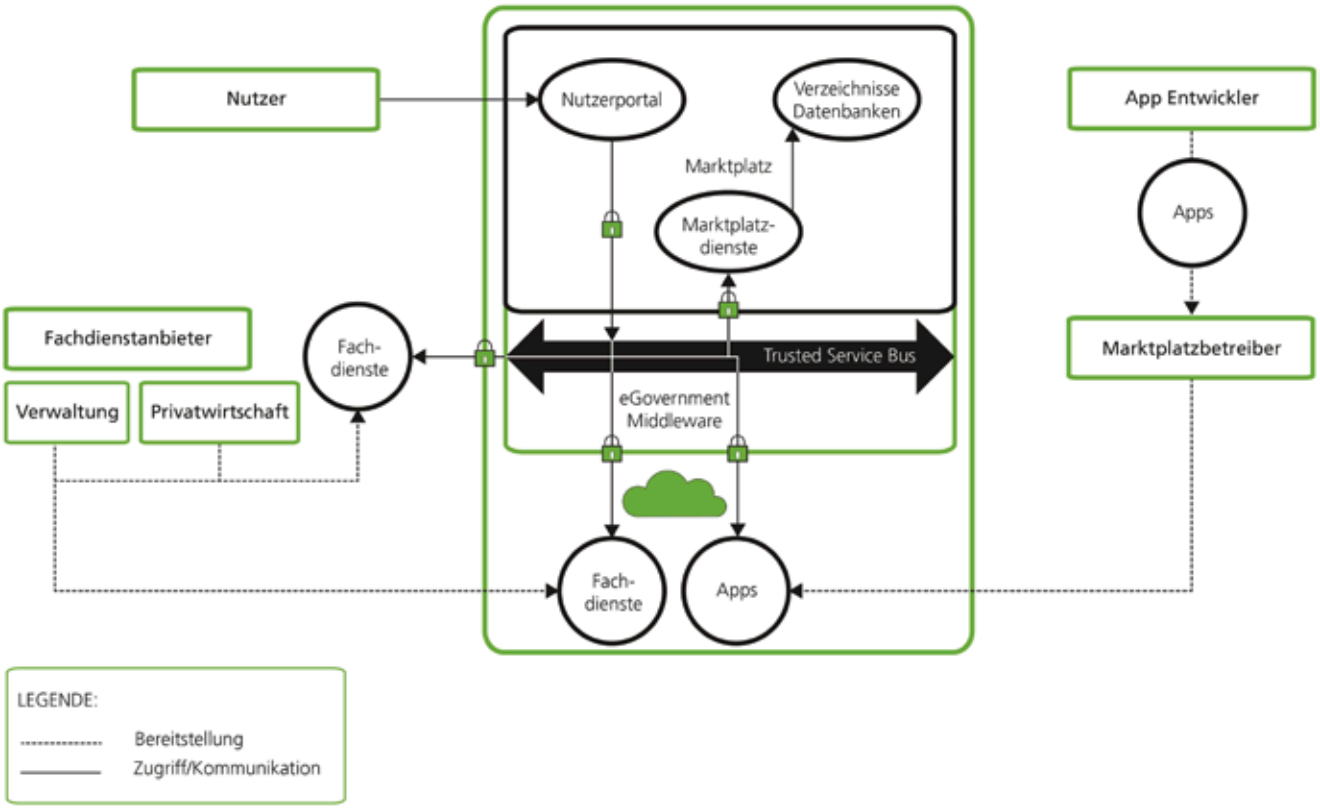
# goBerlin

## Vertrauenswürdiger Cloud-Marktplatz für Bürger, Wirtschaft und Verwaltung

Ob Heirat, Geburt eines Kindes oder Gründung eines Unternehmens – in diversen Lebenslagen sind Bürger auf zahlreiche gewerbliche und öffentliche Dienstleistungen angewiesen. Deren Auswahl und Abwicklung kosten Zeit und Geld und sind meist recht aufwändig. Zum Beispiel beim Umzug: Möbel müssen in das neue Heim transportiert werden, die Nachsendung der Post muss organisiert werden und zahlreiche Behördengänge sind zu erledigen. Das Projekt goBerlin will dazu beitragen, dass Berlins Bürgerinnen und Bürger künftig Online-Dienste von Behörden und Unternehmen ebenso leicht finden wie nutzen können. goBerlin baut dazu einen Cloud-Marktplatz auf, der eGovernment-Leistungen der öffentlichen Verwaltung mit Angeboten privater Firmen verbindet. Bürger finden so an einer Stelle, was sie bislang selbst mühsam zusammensuchen müssen. Eine Pilotanwendung wird für die Lebenslage „Umzug“ erarbeitet.

## Cloud-Infrastruktur zur Kombination von Dienstleistungen

goBerlin schafft dazu eine Struktur aus drei Ebenen: Infrastruktur-, Plattform- und eine Anwendungsebene für die Entwicklung und Bereitstellung von Apps. Basis ist eine Cloud-Infrastruktur, auf der eine Plattform-Ebene aufsetzt, über die Basisdienste und fachliche Dienste angeboten werden können. Basisdienste sind dabei Komponenten für den sicheren und zuverlässigen Betrieb von Anwendungen, beispielsweise für das Identitäts- oder Prozessmanagement. Ein hier integrierter Baustein ist die sichere Identifikation über den neuen Personalausweis (nPA). Fachliche Dienste sind Schnittstellen zu Dienstleistungsangeboten aus Verwaltung und Wirtschaft. Neben der Ummeldung online finden sich hier Dienste für die Wohnungssuche, den Abschluss relevanter Versicherungen oder für die Suche nach Handwerkern. Ein von goBerlin etabliertes Anbieterportal ermöglicht es Behörden und Unternehmen, sich als Anbieter zu registrieren und ihre Dienste in einheitlicher Form auf dem Portal bereitzustellen. Auch die Bezahlung und Abrechung der Dienstleistung lassen sich darüber abwickeln.



## Cloud-Dienste zur Unterstützung von Lebenslagen

Diese so bereitgestellten Basisdienste und fachlichen Dienste können Softwareentwickler zur Entwicklung innovativer Apps nutzen. Dafür schafft goBerlin ein Portal, über das die Entwickler alle angebotenen Dienste finden, sie zu Apps verknüpfen und diese schließlich veröffentlichen können. Die Bürgerinnen und Bürger können die Apps und die darin enthaltenen Dienstleistungen schließlich über das Lebenslagenportal abrufen. Dort erscheinen die Apps gruppiert nach den Lebenslagen, zu denen sie Dienstleistungen anbieten. Im Fall eines Umzugs können dies zum Beispiel Dienstleistungen der Behörden wie Meldevorgänge sowie behördliche Informationen zu Mietspiegel und Wohnlage sein. Diese können verknüpft werden mit Angeboten privater Dienstleister wie Immobilienanzeigen und Handwerkerleistungen.

## Sicherheit und Vertrauen für öffentliche und private Dienstleistungen

goBerlin will eine vertrauensvolle und sichere Umgebung für Bürger, Dienstleister und App-Entwickler schaffen. So wird der Marktplatz durch die öffentliche Hand in einer lokalen und hochsicheren Cloud-Infrastruktur betrieben. Grundlegende Sicherheitsdienste werden als Teil der Plattform-Basisdienste bereitgestellt, die Anwendungsentwickler je nach Sicherheitsbedarf der jeweiligen Anwendung flexibel einbinden können. Bürgerinnen und Bürger werden die Möglichkeit haben, ihre persönlichen Daten in einer sicheren Umgebung zu verwalten und transparent und genau zu steuern, welche Apps und fachlichen Dienste Zugriff auf welche Daten erhalten. Schließlich durchlaufen alle angebotenen Apps einen Zertifizierungsprozess zu Aspekten wie Sicherheit, Datenschutz und Nutzerfreundlichkeit. So entsteht ein Cloud-Marktplatz, über den Unternehmen und die Verwaltung ihre Dienstleistungen anbieten und auf dem Bürgerinnen und Bürger diese Dienstleistungen sicher und bequem nachfragen können.

### Ausgangssituation

- Bürger müssen sich in verschiedenen Lebenslagen die benötigten Dienstleistungen aufwändig einzeln zusammensuchen
- Ein gemeinsames Angebot von Behörden und Wirtschaft fehlt
- Viele Dienstleistungen sind nicht elektronisch als Dienst verfügbar

### Zielsetzung

- Über ein Portal finden Bürger gebündelt verschiedene Dienstleistungen zu einzelnen Lebenslagen
- eGovernment und gewerbliche Dienstleistungen werden kombiniert angeboten
- Die Regelung von Lebenslagen wird durch webbasierte Dienste einfacher und bequemer

### Kontakt

**IT-Dienstleistungszentrum Berlin AöR**
**Christian Langenfeld**
**E-Mail** christian.langenfeld@itdz-berlin.de

**Partner**
- Atos IT Solutions and Services GmbH
- Berliner Senatsverwaltung für Inneres und Sport
- Fraunhofer-Institut für Offene Kommunikationssysteme (FOKUS)
- HSH Soft- und Hardware Vertriebs GmbH
- Immobilien Scout GmbH

**Internet** www.goberlin-projekt.de


LAN1
LAN2
LAN3
LAN4
19.52

# Das Kompetenzzentrum Trusted Cloud

## Wissenschaftliche Begleitung der Technologieprojekte

Das Technologieprogramm Trusted Cloud umfasst ein breites Spektrum an Themen. Zum einen arbeiten die 14 Projekte an verschiedenen Technologien und Innovationen. Zum anderen gibt es eine Reihe übergreifender Herausforderungen beim Einsatz von Cloud Computing, die alle Unternehmen betreffen. Das Kompetenzzentrum Trusted Cloud unterstützt die Technologieprojekte und das Bundesministerium für Wirtschaft und Energie (BMWi) bei der erfolgreichen Umsetzung der Programmziele.

Das Kompetenzzentrum begleitet zum einen die Projekte bei der Realisierung ihrer Innovationen durch fachliche und organisatorische Unterstützung, Aufzeigen von Synergien, Vernetzung mit nationalen und internationalen Akteuren, Transfer von Wissen und Technologien und bei der nachhaltigen Verwertung ihrer Ergebnisse. Als zentraler Ansprechpartner für das Technologieprogramm Trusted Cloud informiert das Kompetenzzentrum die interessierte Fachöffentlichkeit und Medien über den Fortschritt des Programms und der Technologieprojekte. Das Kompetenzzentrum Trusted Cloud arbeitet zum anderen gemeinsam mit der Fach-Community an den übergreifenden Herausforderungen für die Nutzung von Cloud Computing.

## Das Kompetenznetzwerk Trusted Cloud

Das Kompetenzzentrum Trusted Cloud etabliert dazu ein Kompetenznetzwerk. In das Kompetenznetzwerk Trusted Cloud sollen insbesondere mittelständische Entwickler und Nutzer vertrauenswürdiger Cloud-Angebote einbezogen werden, wenn sie Beiträge zu den folgenden Themen leisten:

- Entwicklung vertrauenswürdiger Cloud-Angebote
- Bewertung und Nutzung der Geschäftspotenziale der Cloud-Technologien in unterschiedlichen Anwendungen und Einsatzumgebungen
- Erfassung und Berücksichtigung der rechtlichen Rahmenbedingungen von Cloud Computing
- Entwicklung von Sicherheitstechnologien für Cloud Computing
- Vermeidung von Abhängigkeiten der Nutzer von einmal in Anspruch genommenen Cloud-Diensten

Das Kompetenznetzwerk ist ein Netzwerk von mittelständischen Unternehmen für mittelständische Unternehmen. Denn die Vielfalt der Anforderungen an vertrauenswürdige Cloud-Angebote kann nur in unterschiedlichen mittelständischen Nutzungsumgebungen erfüllt werden.

Das Kompetenznetzwerk Trusted Cloud entwickelt eine so genannte Plattformstrategie als „Referenz-Dienste-Infrastruktur“. Innerhalb dieser können Dienste sehr unterschiedlicher Art in einem einheitlichen Rahmen dargestellt werden, beispielsweise Anwendungsdienste, Basisdienste, Sicherheitsdienste, Datenschutzdienste etc. Die Darstellung der Projektergebnisse des Trusted-Cloud-Programms und Cloud-Angebote Externer können in dieser Architektur positioniert werden, sodass der Kontext für die Nutzung jedes Dienstes charakterisiert wird und Schnittstellen zu anderen Diensten festgelegt werden können. Mit der Plattformstrategie soll darüber hinaus gezeigt werden, dass die in den Projekten des Trusted-Cloud-Programms erarbeiteten Ergebnisse übertragbar und für den gesamten Mittelstand von Relevanz sind.

## Rechtlicher Rahmen für Cloud Computing

Cloud Computing kann in Deutschland nur wirtschaftlich erfolgreich sein, wenn die rechtlichen Rahmenbedingungen eine effiziente Nutzung von Cloud-Diensten ermöglichen. Ein innovationsfreundlicher Rechtsrahmen ist daher von besonderer Bedeutung. Für die rechtlichen Aspekte von Cloud Computing hat das BMWi daher innerhalb des Kompetenzzentrums Trusted Cloud eine eigene Arbeitsgruppe einrichten lassen. In der Arbeitsgruppe „Rechtsrahmen des Cloud Computing“ erarbeiten Experten aus Wirtschaft, Anwaltschaft und Wissenschaft sowie Vertreter aus Datenschutzbehörden gemeinsam mit Projektbeteiligten aus dem Trusted-Cloud-Programm Lösungsvorschläge für rechtliche Herausforderungen. Aktuelle Themenschwerpunkte sind: Datenschutz, Vertragsgestaltung, Urheberrecht sowie Haftungsfragen und Strafbarkeitsrisiken. Darüber hinaus wird ein Pilotprojekt zur datenschutzrechtlichen Zertifizierung von Cloud-Diensten betrieben, das Impulse für die rechtssichere Nutzung von Cloud Computing und die Gewährleistung eines hohen Datenschutzniveaus setzen soll.

## Ansprechpartner

**Trusted Cloud** ist ein Technologieprogramm des Bundesministeriums für Wirtschaft und Energie (BMWi).
**Internet** www.trusted-cloud.de

**Kompetenzzentrum Trusted Cloud**
c/o INNOVA Beratungsgesellschaft mbH
**Adresse** Schopenhauerstraße 47
14129 Berlin
**Telefon** 030 3463-7590
**E-Mail** kompetenzzentrum@trusted-cloud.de

**Redaktionsbüro Trusted Cloud**
c/o A&B One Kommunikationsagentur GmbH
**Adresse** Burgstraße 27
10178 Berlin
**Telefon** 030 24086-770
**E-Mail** presse@trusted-cloud.de

www.bmwi.de