Bundesministerium
für Wirtschaft
und Technologie

Trusted Cloud

Presseinformation

SkIDentity

Vertrauenswürdiges Cloud Computing braucht starke Authentisierung

Cloud-Dienste ermöglichen das gemeinsame Arbeiten an Projekten, egal wo sich die Kollegen gerade befinden. In rund um den Globus 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 könnten sich durch Hackerangriffe oder gezielte Betrugsversuche die Zugangsdaten eines Mitarbeiters verschaffen und so unerlaubten Zugriff auf sensible Daten erhalten. Um dies zu verhindern müssen in der Cloud starke, auf mehreren Faktoren (Besitz, Wissen, Sein etc.) basierende Authentisierungsmechanismen eingesetzt werden.

Brücke zwischen sicheren Ausweisen und Cloud

Genau hier setzt das Projekt SkIDentity an. Es schlägt eine Brücke zwischen sicheren elektronischen Ausweisen (eID) in Form von Chipkarten, wie z. B. dem neuen Personalausweis, der elektronischen Gesundheitskarte, Signatur- und Bankkarten oder Mitarbeiterausweisen, und dem wachsenden Markt der Cloud-Computing-Infrastrukturen. Ziel ist es, vertrauenswürdige Identitäten für die Cloud bereitzustellen und dadurch alle Arten von Geschäftsprozessen für Konsumenten und Unternehmen 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 und in breitenwirksamen Pilotprojekten erprobt.

Nutzung bestehender Ausweise für eine sichere Authentifizierung

Besondere Berücksichtigung finden hierbei die Bedürfnisse der kleinen und mittleren Unternehmen und Behörden. Kern der SkIDentity-Infrastruktur ist ein eID-Broker, der die Dienstnutzer entsprechend den Sicherheitsvorgaben (Wünschen) des Clouddienstes an einen Authentifizierungsdienst aus einer Auswahl bestehender Dienste weitervermittelt. Der Authentifizierungsdienst führt die Nutzerauthentifizierung durch. Dabei können bestehende existierende elektronische Ausweise zum Einsatz kommen. Mit Hilfe der SkIDentity Infrastruktur können sich Dienstnutzer so mit ihren bereits vorhandenen sicheren Ausweisen für verschiedenste Clouddienste anmelden.

Zweifelsfreie Identitäten für die Cloud und aus der Cloud

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. Bei einem Login-Versuch prüft SkIDentity die Echtheit des genutzten Ausweises und

stellt bei der erstmaligen Registrierung auf Wunsch weitere Benutzerattribute (z.B. Name, Adresse) bereit. Auf Basis dieser Information kann der Cloud-Dienst entscheiden, ob und auf welche Funktionen und Daten ein Benutzer Zugriff hat. Um diese Vorteile nutzen zu können, muss der Cloud-Anbieter keine eigene aufwändige IT-Infrastruktur betreiben, sondern kann die sicheren Authentisierungsdienste bequem aus der Cloud beziehen.

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 den auch zum Trusted Cloud-Technologieprogramm gehörenden Projekten MimoSecco und SealedCloud sorgt SkIDentity für rundum sichere Cloud-Lösungen. Während MimoSecco und SealedCloud vor allem die auf den Servern der Cloud-Anbieter gespeicherten und verarbeiteten Daten schützen, verhindert SkIDentity den unautorisierten Zugriff auf diese Systeme aus der Cloud.

Ausgangssituation

- Log-In ist bedeutender Sicherheitsaspekt bei Cloud-Diensten
- Angreifer überwinden schwache Authentisierungsverfahren und können Daten entwenden oder missbrauchen
- Kein einheitliches, starkes Authentisierungsverfahren für Anwender von mehreren Cloud-Diensten

Zielsetzung

- Sicheres und benutzerfreundliches Authentifizierungssystem verhindert unbefugte Zugriffe auf Daten in der Cloud
- Hochsichere Anmeldung für die Cloud auf Basis etablierter Technologien und bewährter Ausweissysteme
- Broker-basierte Architektur ermöglicht kosteneffizientes Identitätsmanagement, das selbst für KMU und Kommunen geeignet ist

Koordinator	Ecsec GmbH, Dr. Detlef Hühnlein
E-Mail	detlef.huehnlein@ecsec.de
Telefon	+49 9571 896479
Laufzeit	15.01.2012 – 14.01.2015
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 www.skidentity.de