

# Design eines Profil- und Zertifikatsmanagementsystems für das Service by eContract-Konzept

Andreas Friesen, Christoph Ruland

friesen,ruland@nue.et-inf.uni-siegen.de

**Abstract:** Es gibt eine Vielzahl von unterschiedlichen Konzepten und Geschäftsmodellen, die die elektronische Einbindung sowohl von Kunden als auch von Geschäftspartnern in Geschäftsprozesse ermöglichen. Diese Konzepte werden durch offene, verteilte und interoperable IT-Systeme realisiert, die aus einer Vielzahl weitgehend autonom agierender Komponenten bestehen. Die Betreiber der einzelnen Komponenten sind in der Regel nur für die Sicherheit der eigenen Komponenten zuständig, was schnell zu Inkonsistenzen bzw. Widersprüchen bzgl. der Sicherheit aus der Sicht des Gesamtsystems führen kann. Das liegt jedoch weder im Interesse der Anwender (User) noch der Betreiber solcher Systeme. Man braucht also Modellierungskonzepte, die abstrakt und mächtig genug sind, um eine in Bezug auf Sicherheit einheitliche Modellierung eines verteilten IT-Systems unabhängig von seiner Komplexität zu ermöglichen. Die Multi-Service-Multi-Provider-Architekturen (MSMP-Architekturen), in denen die autonomen Komponenten in Form von Services und deren Betreiber als Service Provider modelliert werden, stellen ein solches Modellierungskonzept dar [SCI01], [ES02]. Dieser Beitrag beschreibt das Design eines Profil- und Zertifikatsmanagementsystems, welches die Realisierung des Service by eContract-Konzepts eines Sicherheitsmodells zur Authentikation, Zugriffsrechteverwaltung und Online Service Subscription Management in MSMP-Architekturen darstellt.

## 1 Einleitung

Verteilte IT-Systeme zeichnen sich oft dadurch aus, dass deren weitgehend autonome Systemkomponenten von unterschiedlichen Betreibern mit eigenen Business- und Sicherheitsmodellen betrieben werden, und sich damit der zentralen Konfiguration und Administration entziehen. Ein anderes für die Sicherheitsüberlegungen wichtiges Merkmal dieser Systeme ist die offene Benutzergruppe, die sich aus den Benutzergruppen der einzelnen Systemkomponenten zusammensetzt und sich damit ebenfalls der zentralen Administration entzieht. Das Hinzufügen, Entfernen oder Ändern von einzelnen Systemkomponenten kann unmittelbare Auswirkungen auf die Sicherheit des Gesamtsystems haben [AAMI98].

Vereinheitlichte Mechanismen zur Authentikation und Zugriffsrechtsteuerung von Usern würden das Sicherheitsmanagement und Interoperabilität im Gesamtsystem verbessern, und die Integration von einzelnen Systemkomponenten vereinfachen. Die komplexen dynamischen Beziehungen sowohl zwischen den einzelnen Systemkomponenten als auch zwischen deren Betreibern erfordern ein flexibles, dynamisches und vor allem dezentrali-

siertes Konfigurationsmanagement, damit das Gesamtsystem korrekt funktionieren kann. Im folgenden werden die von den einzelnen Systemkomponenten erbrachten Dienste als Services, und deren Betreiber als Service Provider bezeichnet.

Moderne Sicherheitslösungen machen einen intensiven Gebrauch von der asymmetrischen Kryptographie, um einheitliche Authentikationsmechanismen und Zugriffsrechteverwaltung in verteilten Systemen zu realisieren. Die wohl populärste Lösung derzeit ist die Public Key Infrastructure (PKI) basierend auf X.509 Zertifikaten in Kombination mit der Privilege Management Infrastructure (PMI) basierend auf X.509v4 Attributzertifikaten [IETF]. Diese Lösung kann jedoch zwei wichtigen Anforderungen vom prinzipiellen Aufbau her nicht gerecht werden: dem Online Service Subscription Management und der dezentralisierten Zugriffsrechteverwaltung [AAMI98].

Die Darstellung der Architektur eines verteilten Systems als eine MSMP-Architektur ermöglicht die Anwendung des Service by eContract-Konzepts, um eine einheitliche Authentikation, Zugriffsrechteverwaltung und eine nicht abstreitbare Online Service Subscription zu realisieren [SCI01], [ES02]. Die MSMP-Architekturen und das Service by eContract-Konzept werden nun kurz beschrieben. Anschließend wird das Profil- und Zertifikatsmanagementsystem beschrieben.

## **2 Multi-Service-Multi-Provider-Architekturen**

Eine Softwarearchitektur, der ein Multi-Service-Multi-Provider-Businessmodell (MSMP-Businessmodell) zugrunde liegt, wird MSMP-Architektur genannt.

Das MSMP-Businessmodell besteht aus einer endlichen Anzahl von Entities. Es wird zwischen zwei Arten von Entities unterschieden: dem User und dem Service Provider. Ein Service Provider bietet 1,...,n Services an. Ein User kann auf eine endliche Anzahl von Services zugreifen. Ein User wird End User genannt, wenn er selbst keine Services anbietet. Ein Business User ist ein Service Provider, der die Rolle eines Users spielt indem er auf Services anderer Service Provider zugreift.

Aus der Definition des MSMP-Businessmodells ersieht man, dass eine MSMP-Architektur sehr komplex werden kann, wenn nicht nur die End User, sondern auch Service Provider die Services anderer Service Provider nutzen. Es können Relationen unterschiedlicher Komplexität zwischen den Services, und damit zwischen den Usern und den Service Providern entstehen. Diese Relationen kann man bezogen auf einen Service, als folgende Szenarien beschreiben:

Der einfache Fall: Ein Service ist nicht an andere Services angewiesen, um seine Aufgaben ausführen zu können, und schränkt die potentielle Usergruppe nicht ein. Service-Komposition: Ein Service ist an andere Services angewiesen, um seine Aufgaben auszuführen, aber schränkt die potentielle Usergruppe nicht ein. Zugriffsrechte-Komposition: Ein Service schränkt die potentielle Usergruppe ein, indem nur User, die bereits über Zugriff auf bestimmte Services haben, als potentielle User in Frage kommen. Zugriffsrechte-Delegation: Die Business User dürfen die Rechte für den Servicezugriff an ihre User delegieren. Service-Roaming: Die User erhalten Zugriff auf Services mit der gleichen oder

ähnlichen Funktionalität unterschiedlicher Service Provider.

Die kombinierte Anwendung dieser Szenarien erlaubt den Aufbau einer beliebigen MSMP-Architektur.

### **3 Das Service by eContract-Konzept**

Das Service by eContract-Konzept ist ein Sicherheitsmodell für die MSMP-Architekturen, das Authentikation, Zugriffsrechteverwaltung und Online Service Subscription unterstützt. Die gegenseitige Authentikation wird unterstützt durch eine PKI (z.B. X.509), die selbst einen Teil des Sicherheitsmodells darstellt. Die Rolle der Zertifikate und damit der Zertifizierungsinstanzen ist jedoch eingeschränkt. Die Zertifikate werden nur zu Authentikationszwecken eingesetzt. Die Zertifizierungsinstanzen sind damit nicht in die Zugriffsrechteverwaltung involviert, und deren Security Policies können homogen und einfach gehalten werden. Das vereinfacht die Cross-Zertifizierung und erhöht die Interoperabilität der PKI. Jeder Service Provider ist gleichzeitig eine Source of Privilege für seine Services. Das bedeutet, dass jeder Service Provider die Zugriffsrechte auf seine Services direkt verwaltet, und deshalb die Einbeziehung einer TTP zur Ausstellung von Attributzertifikaten unnötig wird.

Die User erhalten den Zugriff auf einen Service entweder indem sie den Service direkt abonnieren, oder durch Vorlage von Attributzertifikaten ausgestellt durch andere Service Provider, sofern diese Attributzertifikate von diesem Service Provider akzeptiert werden. Die direkte Online Subscription impliziert das Vorhandensein eines Vertrags zwischen dem User und dem Service Provider, in dem die Subscription-Konditionen unabstreitbar vereinbart sind. Das Service by eContract-Konzept definiert zusätzlich zu den Zertifikaten und Attributzertifikaten zwei weitere kryptographische Datenstrukturen (Profil und Service Policy), die online eine vertrauenswürdige Erzeugung von elektronischen Verträgen ermöglichen. Die entsprechende Anwendung der kryptographischen Datenstrukturen des Service by eContract-Konzepts auf die Szenarien aus dem vorherigen Abschnitt ermöglicht den Einsatz dieses Sicherheitsmodells in beliebiger MSMP-Architektur. Eine ausführlichere Beschreibung des Modells findet man in [ES02], [SCI01].

### **4 Profil- und Zertifikatsmanagementsystem**

Die Zertifikate, Attributzertifikate, Profile und Service Policies müssen durch eine Infrastruktur verwaltet werden, um sie für die Entities einer MSMP-Architektur verfügbar zu machen. Es gibt mehrere Ansätze für eine Infrastruktur dieser Art. In diesem Beitrag wird eine Infrastruktur vorgestellt, in der sowohl die Service Provider als auch die End-User eigene Datenstrukturen selbst verwalten. Die Infrastruktur ist damit nicht nur dezentral aufgebaut, sie reduziert auch die Funktion der Trust Center auf das absolut Notwendige, nämlich auf das Ausstellen und die Veröffentlichung von kryptographischen Zertifikaten und den Zertifikatswiderrufslisten.

Jeder Service Provider hat einen eigenen Profil- und Zertifikatsmanagementserver. Das bedeutet, dass alle kryptographischen Datenstrukturen, die mit einem Service Provider und seinen Usern assoziiert werden, auf seinem PCMS-Server verfügbar sind. Jeder End User hat einen Subscription Management Client, der zur Erstellung, Änderung und Löschung von Service Subscriptions eingesetzt wird. Die durch diese Komponente erzeugten kryptographischen Daten werden in einer verschlüsselten lokalen Datenbank abgelegt. Die Service Provider und die End User nutzen ein Directory, um die Gültigkeit der Zertifikate von ihren Kommunikationspartnern zu überprüfen. Die Attributzertifikate, Service Policies und Profiles werden durch die Service Provider ausgestellt. Da der Aussteller auch für den Widerruf verantwortlich ist, verfügen die Profil- und Zertifikatsmanagementserver über Schnittstellen über die diese Datenstrukturen eingefügt, aktualisiert, gesperrt und entfernt werden können. Ein End User erfährt allerdings von den Änderungen erst, wenn er auf einen von den Änderungen betroffenen Service zugreift, weil er nicht ständig online ist, und damit nicht immer zeitnah von den Änderungen informiert werden kann.

Der Profil- und Zertifikatsmanagementserver besteht aus drei Komponenten: Subscription Management Client (SMC), Subscription Management Server (SMS), Profile and Certificate Store. Der SMC dient dem Service Provider zur Abonnieerung von Services anderer Service Provider. Der SMS ermöglicht den Usern, die Services zu abonnieren und zu verwalten. Es werden also die folgenden drei Funktionen bereitgestellt: Subscribe, Unsubscribe und Change Subscription Conditions. Das Profile and Certificate Store verwaltet die durch SMC und SMS erzeugten kryptographischen Daten.

Das vorgestellte Profil- und Zertifikatsmanagementsystem ist hochskalierbar, weil jede Entity in einer MSMP-Architektur ihre Zugriffsrechte und die Zugriffsrechte ihrer User mit Hilfe des PCMS dezentral verwaltet.

## 5 Literaturverzeichnis

[AAMI98] C. Lynch, A White Paper on Authentication and Access Management Issues in Cross-Organisational Use of Networked Information Resources, 1998, cliff@cni.org

[CD97] D. Davis, Compliance Defects in Public-Key Cryptography, 1997, don@mit.edu

[ES02] C. Ruland, A. Friesen, Das eContract-Konzept ein Sicherheitsmodell für Multi-Service-Multi-Provider-Architekturen, Enterprise Security 2002, Enterprise Security, Patrick Horster (Hrsg.), itVerlag, Seiten 37-45, ISBN 3-936052-03-4

[IETF] <http://www.ietf.org/html.charters/pkix-charter.html>

[SCI01] A. Friesen, C. Ruland Service by e-contract a security model for authentication, access control and online subscription management in multi-service-multi-provider architectures, World Multiconference on Systemics, Cybernetics and Informatics, Orlando, v. 22.-25.7.2001, Proceedings, Volume II Information Systems, Seiten 581-585, ISBN: 980-07-7542-0