SOA, aber sicher!

Serviceorientierte Architekturen (SOA) besitzen die Flexibilität, IT-Prozesse unternehmensübergreifend zu verbinden. Für die Sicherheit hat dies weitreichende Konsequenzen, da die klassische Abschottung an den Unternehmensgrenzen nicht mehr hinreichend funktioniert. Dieser Artikel stellt die Herausforderungen und Konzepte bei der Umsetzung von Sicherheit in SOA dar.

Von Christoph Meinel, Michael Menzel und Ivonne Thomas, Potsdam

Kaum ein anderer Trend im IT-Bereich hat in den vergangenen Jahren so viel Aufmerksamkeit auf sich gezogen wie SOA. Aus der ursprünglichen Idee, Funktionalität als Dienst verfügbar zu machen, ist mittlerweile die Vision eines Internets der Dienste erwachsen – eines globalen Marktplatzes, auf dem jeder Teilnehmer Dienste sowohl konsumieren als auch anbieten kann.

Der Dienst als „Ware“ ist eine Vision, die Unternehmen große Flexibilität in der Planung und Zusammenstellung ihrer Geschäftsprozesse verspricht. Mit einem solchen Marktplatz könnten Unternehmen Dienste aus einem breiten Portfolio auswählen und je nach Bedarf in ihre eigenen Prozesse einbinden, aber auch selbst Dienste anderen Nutzern anbieten. Um eine solche Vision Realität werden zu lassen, sind jedoch noch viele Stufen zu erklimmen. Ein Schritt von zentraler Bedeutung ist dabei die Garantie und Umsetzung von Sicherheit in serviceorientierten Architekturen.

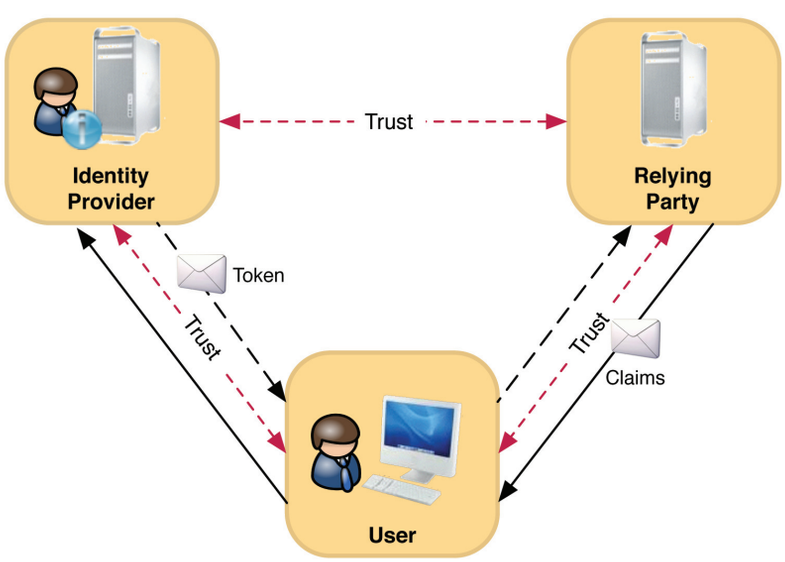

Abbildung 1: „Dreieck des Vertrauens“ zwischen SOA-Rollen

Komposition von Diensten

Das Paradigma der serviceorientierten Architekturen löst komplexe Probleme durch das Zusammenschalten vieler kleiner Bausteine, der Dienste, die unabhängig voneinander existieren und gewartet werden können. Dabei müssen die Komponenten nicht binär-kompatibel sein, da sie lose über einen Nachrichtenaustausch gekoppelt sind. Diese Unabhängigkeit ist eine Eigenschaft, die den SOA-Ansatz von der bisherigen Entwicklung klassischer verteilter oder komponentenbasierter Applikationen unterscheidet. Webservice-Spezifikationen, beispielsweise das SOAP-Protokoll und WSDL (Web Service Definition Language), bieten offene Standards für die Umsetzung einer SOA, die garantieren, dass Systeme unabhängig von ihrer Architektur und ihren Betriebssystemen miteinander kommunizieren können.

Die Überbrückung von Technologieunterschieden machen SOA

und Webservices zu einer wichtigen Integrationsarchitektur. Um eine einfache und flexible Komposition von verschiedenen Diensten zu ermöglichen, wird oftmals eine Kommunikationsinfrastruktur wie ein Enterprise-Service-Bus (ESB) zugrunde gelegt: Dieser erleichtert es, abstrakte Beschreibungen von Geschäftsprozessen auf eine konkrete Komposition von Diensten abzubilden. Zudem können IT-Prozesse von Partnern, Zulieferern und Kunden leicht in die eigenen Geschäftsprozesse eingebunden werden, um schnell und flexibel auf sich verändernde Geschäftsanforderungen zu reagieren.

Sicherheitsimplikationen

Eine derartige Infrastruktur hat jedoch auch Implikationen für die Umsetzung von Sicherheit. Neue Sicherheitsmechanismen für SOA sollten auch selbst der SOA-Philosophie folgen und Dienste so offen und so einfach nutzbar wie möglich halten. Der Anspruch der Wiederverwendbarkeit von Diensten in verschiedenen Kontexten verbietet es dem Anwendungsentwickler, Sicherheit isoliert und dienstspezifisch umzusetzen. Stattdessen sollte man Sicherheit ebenfalls interoperabel, auf offenen Standards basierend implementieren.

Für die Absicherung einer mit Webservices realisierten SOA gibt es bereits eine Reihe von Spezifikationen. Möchte man beispielsweise einen Flugbuchungsdienst anbieten, dann sollten persönliche und vertrauliche Daten (z. B. Kreditkarteninformation des Kunden) dem Dienst nicht ungeschützt übermittelt werden. Die Spezifikation WS-Security kann dazu verwendet werden, Integrität und Vertraulichkeit dieser auszutauschenden Nachrichten sicherzustellen. Die Eigenschaft eines Dienstes, selbstbeschreibend zu sein, impliziert, dass die Dienstbeschreibung auch die Anforderungen an die Verschlüsselung und Integrität der Kundendaten fordern muss. Die Spezifikationen WS-Policy und WS-SecurityPolicy ermöglichen es einem Dienst diese Anforderungen zu definieren, die dann von allen Aufrufern erfüllt werden müssen. So kann vom Flugbuchungsdienst zum Beispiel die Art der Verschlüsselung verschiedener Nachrichtenteile genau vorgegeben werden.

Welt ohne Grenzen

Zusätzlich zur Absicherung der in den ausgetauschten Nachrichten enthaltenen Informationen muss der Zugriff der Benutzer auf den Dienst eingeschränkt werden. Das Abrufen von Buchungsinformationen darf etwa im Beispiel unseres Flugbuchungsdienstes nur dem Benutzer erlaubt sein, der diese Buchung tatsächlich vorgenommen hat. Die Autorisierung von Benutzern setzt allerdings die Kenntnis über ihre Identität voraus. Diese wird ebenfalls benötigt, um nachvollziehen zu können, wer eine bestimmte Aktion ausgeführt hat, oder um einen Dienst personalisiert anzubieten.

Im Rahmen der Entwicklung des Internets zum Internet der Dienste führen serviceorientierte Architekturen auch zu einer Vernetzung von Systemen über Unternehmensgrenzen hinweg. Für die Sicherheit hat dies erhebliche Konsequenzen, da Unternehmensgrenzen zunehmend „aufgeweicht“ werden. Es stellt sich die Frage: Wie lassen sich Benutzer identifizieren und verwalten, wenn Dienste öffentlich über das Internet verfügbar sind?

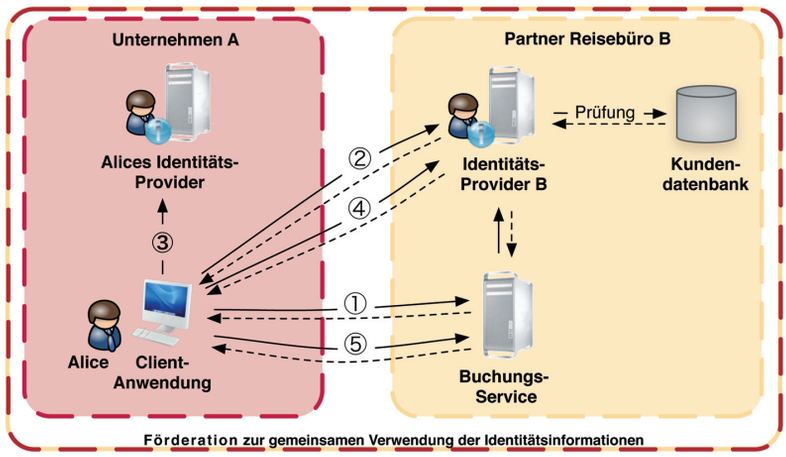

Abbildung 2: Beispiel für die föderative Integration eines Flugbuchungsdienstes

Um Benutzer in der digitalen Welt zu repräsentieren, wird üblicherweise ein Account angelegt, hinter dem sich eine so genannte digitale Identität verbirgt.

Die Rolle der Identität

Eine digitale Identität eines Benutzers fasst eine Menge an Informationen über ihn zusammen, die durch ein Authentifizierungsmerkmal verifiziert werden können – sie bildet die Grundlage, um den Zugriff auf einen Dienst autorisieren zu können. Der Schutz und die vertrauenswürdige Verwaltung von Identitätsdaten stellen jedoch in einer globalen Welt wie dem Internet, in der es keine regelnde Instanz gibt, eine besondere Herausforderung dar. Auch technisch gesehen gibt es im WWW keinen einheitlichen Identity-Layer, über den Benutzer vertrauenswürdig identifiziert werden könnten.

Aus dem Bedarf der Absicherung von Diensten im Internet erwächst folglich die Notwendigkeit, dass jeder Dienstanbieter seine Nutzer individuell verwaltet und – üblicherweise über Benutzername und Passwort – authentifiziert. Für die Benutzer bedeutet dies, dass sie ihre digitale Identität bei jedem Dienstanbieter erneut registrieren müssen. So entstehen „Identitätsinseln" im Netz, welche typischerweise die gleichen Benutzerinformationen wie Name, Adresse oder Alter umfassen. Darüber hinaus sind diese Identitäten nicht portabel: Es gibt beispielsweise keine Möglichkeit, eine hart verdiente Ebay-Reputation bei anderen Diensten zu nutzen.

Betrachtet man das heutige Identitätsmanagement (IDM) in Unternehmen, so ist dieses üblicherweise über ein Verzeichnis zentralisiert, beispielsweise Active Directory mit Kerberos zur Authentifizierung. Kerberos ermöglicht zwar den Zugriff auf alle Dienste im Unternehmen, ohne dass eine erneute Authentifizierung notwendig ist, und der Verzeichnisdienst stellt allen Anwendungen zusätzliche Informationen über die Benutzer bereit, allerdings ermöglichen es diese Sicherheitsansätze nicht, Anwendungen über Unternehmensgrenzen hinaus bereitzustellen oder zu nutzen. Somit stellen auch Unternehmen vom öffentlichen Netz abgeschottete Identitätsinseln dar.

Hat ein Unternehmen beispielsweise eine Kooperation mit dem Anbieter des beispielhaften Flugbuchungsdienstes, so müssten sich erst alle Mitarbeiter bei diesem Dienst registrieren, bevor sie hierüber buchen können. Mit den bisherigen Lösungen für das unternehmens-

WS-*-Standards

WS-Security definiert Erweiterungen für das SOAP-Protokoll, um die Vertraulichkeit und Integrität von Nachrichten basierend auf XML-Encryption und XML-Signature sicherzustellen. Zudem wird ein Mechanismus spezifiziert, um Sicherheitstokens mit einer Nachricht zu verknüpfen.

WS-SecureConversation ist quasi „SSL für SOAP" – es definiert einen beiderseitig authentifizierten Nachrichtenkontext, in dem Nachrichten sicher ausgetauscht werden können.

WS-Trust spezifiziert eine auf WS-Security basierende Möglichkeit, um Sicherheitstoken anzufordern und auszustellen.

WS-Federation definiert Protokolle, um Identitäten, Attribute, Authentifizierungs- und Autorisierungsentscheidungen in verschiedenen unabhängigen Administrationsdomänen zu nutzen, die in einer Föderation vereint sind.

WS-Policy beschreibt die Definition, Gruppierung und Kommunikation von Anforderungen (sog. Policy-Assertions).

WS-SecurityPolicy definiert eine Menge von Policy-Assertions, um sicherheitsbezogene Anforderungen hinsichtlich der Verwendung von WS-Security, WS-Trust und WS-SecureConversation auszudrücken.

weite Identitätsmanagement wäre kein Portal realisierbar, das im Sinne des Internets der Dienste dynamisch einen Flugbuchungsdienst selektiert und im Hintergrund nutzt.

Eine offensichtliche Lösung für dieses Problem böte die Festlegung eines einheitlichen Standards zur Verwaltung von Identitäten im Internet – allerdings hat jede Verfahrensweise ihre Vor- und Nachteile und es ist kaum anzunehmen, dass eine einzige Methode alle Anwendungsfälle sowie zukünftige Szenarien abdecken kann. Microsoft hatte im Jahre 1999 „Passport" als Authentifizierungssystem für das Internet eingeführt, welches die Lücke eines einheitlichen Authentifizierungssystems im Internet schließen sollte – allerdings waren die verwendeten Protokolle proprietär, Microsoft stellte die zentrale Authentifizierungsinstanz dar und das System funktionierte nur im Zusammenspiel mit Microsoft-Technologie, weshalb Passport kein umfassender Erfolg vergönnt war. Auch hat sich bisher keine weltumspannende Public-Key-Infrastruktur durchgesetzt, die für alle Menschen Zertifikate erzeugt, um global sicher kommunizieren zu können.

Portable Identitäten

Gleichwohl hat jedes Identitätsmanagementsystem seine Daseinsberechtigung und erfüllt jeweils die Anforderungen für das Anwendungsszenario, für das es erdacht wurde. Deshalb ist es auch nicht ratsam (und technisch kaum möglich), alle diese Systeme durch ein umfassendes, einheitliches Verfahren zu ersetzen. Kerberos zum Beispiel erfüllt seinen Zweck hervorragend, solange sich Benutzer innerhalb einer abgeschlossenen Administrationsdomäne bewegen, versagt aber, wenn Dienste über diese Grenzen hinaus angeboten werden sollen. Eine Identitätsmanagementlösung, die im globalen Raum funktioniert, muss deshalb in der Lage sein, bestehende Systeme miteinander zu verbinden, ohne diese ersetzen zu wollen.

Eine mögliche Lösung ist die Schaffung eines Metasystems, das eine Abstraktionsschicht bildet, die verfahrensspezifische Details verbirgt (so wie es beispielsweise bei IP über Ethernet oder Token-Ring geschieht). Ein Metasystem für Identitäten sollte Interoperabilität zwischen verschiedenen IDM-Lösungen herstellen, auf freier und interoperabler Technologie beruhen, herstellerunabhängig sein sowie die Privatsphäre des Benutzers achten. Diese Anforderungen, die Kim Cameron in den so genannten Laws of Identity (www.identityblog.com) zusammengefasst hat, repräsentieren die Erfahrungen aus den Vor- und Nachteilen verschiedener Identitätsmanagementlösungen.

Das Identity-Metasystem

Eine konkrete Spezifikation für ein solches Metasystem ist das Identity-Metasystem, das ursprünglich von Microsoft vorgeschlagen wurde. Seine Architektur wird durch die WS-*-Spezifikationen (s. a. Kasten) umgesetzt, die in der Organization for the Advancement of Structured Information Standards (OASIS) fortentwickelt werden – insbesondere durch die Spezifikationen WS-Trust und WS-Federation (www.oasis-open.org/committees/documents.php?wg_abbrev=wsfed).

Das Identity-Metasystem fasst eine Identität abstrakt als einen Satz von Behauptungen – so genannten Claims – auf, die eine Person über sich selbst macht oder die von einer anderen Person gemacht werden, beispielsweise: „Ich bin über 18 Jahre alt", „Alice kennt den symmetrischen Schlüssel" oder „Meine Kreditkartennummer lautet 1234 5678 3333 3333".

Um Claims über den Benutzer eines Dienstes sicher und verifizierbar bereitstellen zu können, werden diese Informationen in ein Credential, das so genannte Security-Token, verpackt und können so über Sicherheitsdomänen hinaus weitergegeben werden. Auffällig ist, dass mit dieser Terminologie (Claim = Behauptung) auch eine gewisse Unsicherheit zum Ausdruck gebracht wird. In einer geschlossenen Sicherheitsdomäne, wie beispielsweise einer Windows Server 2003 Domäne, wird in der Regel von Security-Assertions gesprochen, die also eine gesicherte Tatsache über einen Benutzer repräsentieren. In einem offenen System hängt die Glaubwürdigkeit dieser Aussagen von der ausstellenden Instanz des Credentials ab und erfordert gegenseitiges Vertrauen zwischen den involvierten Parteien (vgl. Abb. 1). Das Identity-Metasystem abstrahiert diese Parteien durch eine Unterteilung in drei Rollen: Subjects (Benutzer), Identity-Provider (die ausstellende Instanz) und Relying Parties (beispielsweise Dienste oder Portale).

Mit dieser Abstraktion der Rollen lassen sich Interaktionen nachbilden, wie sie uns im täglichen Leben begegnen: Angenommen, jemand möchte in einem Geschäft einen neuen Mobilfunkvertrag abschließen, dann würde diese Person das Subject darstellen, während der Verkäufer der Dienst, also die Relying Party, wäre. Die identitätsbestätigende Instanz könnte gleichermaßen das Einwohnermeldeamt wie eine Universität oder Bank sein – je nachdem, wem der Verkäufer vertraut, wird er den vorgelegten Ausweis (das Security-Token) akzeptieren oder ablehnen und folglich dem Kunden einen Mobilfunkvertrag verkaufen oder nicht.

Möchte man das Konzept des Identity-Metasystems in service-

TeleTrusT-Fachkonferenz „Trusted Computing“

Am 4. März findet von 14:00 Uhr bis 17:00 Uhr die diesjährige CeBIT-Fachkonferenz des TeleTrusT Deutschland e. V. in Raum 15 des Convention Center (Messegelände Hannover) statt. Zum Thema “Trusted Computing” werden in jeweils etwa halbstündigen Vorträgen voraussichtlich Redner aus dem Bundesministerium des Innern, dem (if)is – Institut für Internet-Sicherheit der FH Gelsenkirchen, der Sirrix AG und der WIK Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste GmbH sprechen. Für die letzte halbe Stunde ist eine Diskussionsrunde mit allen Teilnehmern vorgesehen; die Moderation der Veranstaltung obliegt TeleTrusT-Vorstand Prof. Dr. Norbert Pohlmann.

orientierten Architekturen anwenden, so kommt eine ganze Reihe von Spezifikationen zum Tragen: Der Standard WS-Trust spezifiziert beispielsweise das Interface eines Identity-Providers, der Identitäten als Dienst anbietet, indem er Security-Tokens ausstellen kann, um die Authentifizierung eines Benutzers oder bestimmte Claims zu attestieren. Die Anforderungen einer Relying Party an die Credentials, mit denen Claims bereitgestellt werden sollen, lassen sich genauso wie die Sicherheitsanforderungen über WS-Policy kommunizieren. Für die Beschreibung eines Security-Tokens selbst kommt üblicherweise die Security-Assertion-Markup-Language (SAML) zum Einsatz.

Metasystem-Szenarien

Basierend auf Standards und Konzept des Identity-Metasystems lassen sich verschiedene Szenarien umsetzen: Beim benutzerzentrischen Identitätsmanagement steht der Benutzer im Zentrum der Interaktion und hat maximale Kontrolle über den Austausch der Informationen zwischen den Instanzen: Um auf einen Dienst zuzugreifen, wählt er aus einer Reihe von Identitätsprovidern denjenigen aus, durch den er seine Identität bestätigen lassen möchte. Er erhält dadurch ein Security-Token, das er an den Dienst seiner Wahl weiterleitet. Der Dienst

Information-Card und CardSpace

„Information-Card“ ist Microsofts Ansatz für eine interoperable Architektur zur Verwaltung und Verwendung digitaler Identitäten und stellt eine spezifische Ausprägung des im Haupttext besprochenen Identity-Metasystems dar. Die Identitätsinformationen eines Benutzers werden von einem Identitätsprovider, dem der Benutzer vertraut, verwaltet und können von diesem bei Bedarf bestätigt werden. Entsprechend den Sicherheitsanforderungen einer Relying Party kann der Benutzer beim Zugriff auf den Dienst eine entsprechende Sicherheitsbestätigung von einem der Identitätsprovider abrufen und seiner Anforderung mitgeben.

Für die Wahl eines geeigneten Identitätsproviders schreibt Information-Card eine Komponente vor, welche diese Aufgabe für alle Anwendungen übernimmt; dieser so genannte Identity-Selector wurde bereits für verschiedene Plattformen implementiert. Die Implementierung von Microsoft heißt CardSpace und ist in Windows Vista und Windows XP mit .net 3.5 integriert.

Für eine einfache Benutzerführung orientiert sich CardSpace an der Verwaltung von Identitäten im täglichen Leben: Wird eine Person nach ihrer Identität gefragt wird, so identifiziert sie sich üblicherweise über eine „Karte“, beispielsweise in Form einer Visitenkarte oder eines Ausweises. Dies imitiert CardSpace durch die Verwendung einer Benutzeroberfläche, die eine Reihe von Visitenkarten darstellt, aus denen der Benutzer auswählen kann (s. Abb. 3). Der Ablauf bei Cardspace ist wie folgt:

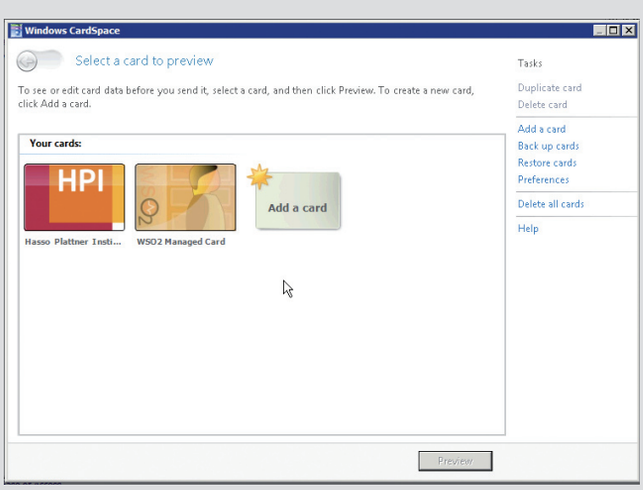

Abbildung 3: CardSpace Identity-Selector

_____ Nach Erstellung eines Accounts bei einem Information-Card-fähigen Identitätsprovider erhalten Anwender eine Information-Card in Form einer XML-Datei.

_____ Der Anwender kann diese Karte in CardSpace importieren. Jede Karte dient als Referenz auf den Identitätsprovider und speichert die Informationen (Claims) über den Benutzer, welche dieser Identitätsprovider bestätigen kann.

_____ Sobald ein Benutzer auf einen Dienst zugreift, ruft die Clientsoftware CardSpace auf und übergibt die Anforderungen in Form von Claims; im Internet Explorer ist diese Funktion bereits integriert.

_____ Cardspace erscheint auf dem Bildschirm und zeigt dem Anwender einen Satz von Karten an, welche die vorliegenden Anforderungen erfüllen können.

_____ Der Anwender selektiert einen Identitätsprovider seiner Wahl, von dem sich CardSpace das Token holt, um es an die Clientanwendung zurückzuliefern.

_____ Die Clientsoftware kann im Anschluss den Dienst mit diesem Token aufrufen.

entscheidet anhand des Ausstellers des Tokens sowie des Inhaltes, ob er der Identität vertraut.

Ein anderes Szenario ist das förderative Identitätsmanagement: Eine Förderation stellt einen Vertrauensbereich über verschiedene unabhängige administrative Domänen dar, in dem Identitäten und Aussagen über Identitäten als glaubwürdig eingestuft werden, wenn einer der teilnehmenden Identitätsprovider sie bestätigt. Während die Benutzer weiterhin in der eigenen Domäne verwaltet werden, lassen sich Dienste so auch nahtlos in anderen Partnerdomänen nutzen. Die für die Ausführung des Dienstes notwendigen Identitätsinformationen werden als Claims mit den Nachrichten ausgetauscht.

Das Zusammenspiel der Spezifikationen lässt sich am besten am Beispiel ersehen (vgl. Abb. 2). Bleiben wir beim Flugbuchungsdienst und nehmen an, dass Alice für das Unternehmen A arbeitet. In die firmeneigene Software zur Buchung von Geschäftsreisen möchte Unternehmen A einen Buchungsdienst integrieren und entscheidet sich für das Reisebüro B, das einen entsprechenden Dienst über das Internet bereitstellt. Unternehmen A und Reisebüro B schließen einen Kooperationsvertrag mit einer Reihe von Bedingungen, die für B ausreichend sind, um den Aussagen von A's Identitätsprovider zu vertrauen.

Möchte Alice fliegen, so sucht sie sich einen Flug über die Firmensoftware und bestätigt die Buchung. Die zugrunde liegende dienstbasierte Architektur stellt sicher, dass ihre persönlichen Daten sicher übertragen werden und der Flug auf ihren Namen gebucht wird. Dazu ruft die Client-Software auf Alices Rechner als erstes die Policy des Flugbuchungsdienstes ab, die eine Reihe von benötigten Claims enthält, die von einer vertrauenswürdigen Instanz bestätigt werden müssen. Diese Policy könnte zum Beispiel besagen, dass der Dienst eine Bestätigung vom domäneninternen Identitätsprovider braucht, dass Alice sicher authentifiziert wurde. Die Client-Software, welche die Policy auswertet, würde daraufhin zusätzlich die Policy vom Identitätsprovider vom Reisebüro B abrufen.

Da Unternehmen A und Reisebüro B eine Föderation bilden, vertraut der Identitätsprovider von B dem Identitätsprovider von A und fordert von ihm ein beglaubigtes Token an, das die Authentifizierung von Alice bestätigt. Da der Identitätsprovider von A Alice bereits zuvor authentifiziert hat, stellt er das gefor-

derte Token aus. Dieses kann vom Identitätsprovider von B in ein Token konvertiert werden, das in B's Dienstdomäne gültig und damit zum Aufruf des Flugbuchungsdienstes nutzbar ist.

Fazit

Die Umsetzung der Sicherheit in einer serviceorientierten Architektur sollte der SOA-Philosophie folgen und die Eigenschaften der losen Kopplung und Selbstbeschreibung von Diensten erhalten. Dies wird erreicht, indem Sicherheitsanforderungen in die Dienstbeschreibung einbezogen oder verlinkt werden. Diese Sicherheitsanforderungen können sich auf den Schutz der ausgetauschten Nachrichten (Integrität und Vertraulichkeit) beziehen, auf die in der Nachricht übermittelten Claims über die Identität eines Benutzers (Identifizierung) sowie deren Richtigkeit (Authentifizierung) und den Aussteller festlegen, durch den die Richtigkeit geprüft werden soll (Vertrauen).

Diese Informationen bilden die Entscheidungsbasis für die Autorisierung des Zugriffs eines Benutzers zur Nutzung eines Dienstes. Ebenso wie die Beschreibung digitaler Identitäten erfolgt auch die Autorisierung über die vom Dienst angeforderten Claims. Das klassische Rollenmodell der Zuweisung von Zugriffsrechten zu einer Benutzerrolle tritt dabei zunehmend in den Hintergrund, da die Semantik, die mit einer Rolle verbunden ist, in den Claims widergespiegelt werden kann – im einfachsten Fall kann ein Claim auch eine Rolle enthalten, weshalb die claimbasierte Zugriffskontrolle als umfassenderes Modell anzusehen ist.

Ein für den domänenübergreifenden Fall essenzieller Aspekt ist das Vertrauen zwischen ausstellender und abhängiger Instanz, das sich auf das Vertrauen zwischen den involvierten Organisationen zurückführen lässt. Eine Möglichkeit, um Vertrauensbeziehungen herzustellen, ist die Bildung einer Föderation auf der Grundlage von vertraglichen Vereinbarungen. ■

Prof. Dr. Christoph Meinel ist Institutsdirektor und Geschäftsführer des Hasso-Plattner-Instituts (HPI) an der Universität Potsdam (www.hpi.uni-potsdam.de), Dipl.-Inf. Michael Menzel und MSc. Ivonne Thomas sind Doktoranden im Forschungskolleg „Service-oriented Systems Engineering" am HPI.

Sind Sie verantwortlich für die IT-Sicherheit?

<kes> liefert alle relevanten Informationen zum Thema IT-Sicherheit – sorgfältig recherchiert von Fachredakteuren und Autoren aus der Praxis.

In jeder Ausgabe finden Sie wichtiges Know-how, Hinweise zu Risiken und Strategien, Lösungsvorschläge und Anwenderberichte zu den Themen:

Internet/Intranet-Sicherheit
Zutrittskontrolle
Virenabwehr
Verschlüsselung
Risikomanagement
Abhör- und Manipulationsschutz
Sicherheitsplanung
Elektronische Signatur und PKI

<kes> ist seit 20 Jahren *die* Fachzeitschrift zum Thema Informations-Sicherheit - eine Garantie für Zuverlässigkeit.

Jetzt Probeheft anfordern!

<kes>-online

<kes>-Leser können neben der Print-Ausgabe auch <kes>-online unter www.kes.info nutzen. Hier finden Sie ohne Zugangsbeschränkung, das Thema der Woche, viele interessante Links, Stichwort-Lexikon IT-Security-Begriffe, Verzeichnis relevanter Veranstaltungen und außerdem aktuelle Artikel zum Probelesen.

Abonnenten erhalten zusätzlich ein Passwort mit dem sie Zugriff auf alle aktuellen Artikel und auch auf das Online-Archiv erhalten.

PROBEHEFT-ANFORDERUNG

☐ **ja,** bitte schicken Sie mir gratis und unverbindlich ein Exemplar der <kes> - Die Zeitschrift für Informations-Sicherheit zum Probelesen zu.

Es kommt nur dann ein Abonnement zustande, wenn ich es ausdrücklich wünsche.

Das Abonnement beinhaltet ein Passwort zur Nutzung des Abo-Bereichs auf www.kes.info

Datum | Zeichen | Unterschrift

Lieferung bitte an

Telefon Durchwahl

FAX an +49 6725 5994

SecuMedia Verlags-GmbH
Abonnenten-Service
Postfach 12 34
55205 Ingelheim