OSCI-Transport, Version 2

– Glossar –

OSCI Leitstelle

Edition 1, veröffentlicht am 4. Juni 2009

Disclaimer

Das Glossar wird während der Erarbeitung und Fortschreibung der Dokumente für die Spezifiktaion OSCI Transport 2 zyklisch fortgeschrieben. Die Veröffentlichung erfolgt in aufsteigenden Editionsnummern.

Kommentierungen und Anregungen nehmen die OSCI Leitstelle dankend entgegen

Mit Hinsicht auf die intendierte Internationalisierung werden in den Dokumenten zu OSCI Transport teilweise international übliche englischsprachige Begriffe verwandt. Damit soll erleichtert werden, den Bezug zu anerkannten Industriestandards mit ähnlichem Anwendungsfokus herzustellen.

Fortschreibungen (nach Edition 1)

Edition	Datum	Autor	Vorgenomme Änderungen

Begriff	Erläuterung
A	
Attachment	Ergänzender Anhang zu einer Nachricht beliebigen (auch binären) Formaten.
Attribute Service (AS)	Dienst, der Profile/Attribute zu Identitäten zur Verfügung stellt (siehe auch *IdP*).
Authentifizierung	Überprüfen einer *Identität* durch Überprüfung eines *Identitätsnachweises*, den die *Identität* zu erbringen hat (z.B. Überprüfung des Personalausweises durch Gesichtskontrolle und Überprüfung der Ausweisnummer)
Authentisierung	Nachweisen einer *Identität* durch die Identität selbst (z.B. Vorlegen eines Personalausweises durch den Inhaber)
Authentisierungstoken	Attribute einer Nachricht, die zur Authentifizierung von Identitäten genutzt werden können; siehe auch Claim und Security Token.
Authentisierungszertifikat	Ein X.509-Zertifikat, das ausschließlich zum Zweck der Authentisierung genutzt werden darf.
Autor	Verfasser der Inhaltsdaten einer Nachricht und/oder Anhängen hierzu. Dieser Begriff aus OSCI Transport 1.2 wird hier synonym für den international gebräuchlicheren Begriff „Source Application“ genutzt.
B	
Benutzer/Nutzer	Menschliche *Identität*, die einen menschlichen Anwender beschreibt
Berechtigungsnachweis, Berechtigungstoken	Siehe *Sicherheitstoken*
C	
CA	Certification Authority; Anbieter von Zertifizierungsdiensten. Siehe auch *ZDA*
Claim	Aussagen, die ein Nutzer über seine Identität und Rollen trifft – meist in Form von Security Token und Attributen. Auf Basis von Claims sollen bei einem Service Provider dem anfragenden Nutzer Rechte gewährt werden; Claims müssen daher bei einer dritten, für den Service Provider vertrauenswürdigen Instanz bzgl. Gültigkeit überprüfbar sein.
Credentials	Siehe *Claim*
D	

Dienst	Siehe *Service*
E	
Empfänger	Die Instanz, an die die OSCI-Nachricht gerichtet ist. Jede OSCI-Nachricht ist genau an einen Empfänger gerichtet. Siehe auch *Recipient.*
End Point Reference (EPR)	Durch eine *URI* und weitere Parameter eindeutig identifizierte Adresse von *Services* und *Endpunkten*
Endpunkt	Aus Sicht von OSCI Transport Initiator bzw. Recipient einer OSCI-Nachricht; im asynchronen Fall kann dies auch ein Knoten sein, bei dem Nachrichten zur Abholung für den intendierten Empfänger zwischengespeichert werden (siehe *Postfach*).
F	
Fehlermeldung	Quittierung von Fehlfunktionen eines Knotens bei der Verarbeitung von Nachrichten an den/die jeweils übermittelnden Knoten (siehe auch *Statusmeldung*).
Federated Identity Management	Um einen föderierten *Service*-Zugriff zu ermöglichen müssen Technologien etabliert werden, die Identitäten in einer Vertrauensdomäne Rechte in einer anderen Vertrauensdomäne einräumen. Diese Technologien werden durch Federated Identity Management beschrieben.
G	
GUID	Globally Unique Identifier (GUID), global eindeutiger Identifier nach RFC 4122, "A Universally Unique Identifier (UUID) URN Namespace", The Internet Engeneering Task Force July 2005, http://www.ietf.org/rfc/rfc4122.txt
I	
Identität	Informationsabbild eines Teilnehmers an einem OSCI-Kommunikationsverbund.
Identitätsnachweis	Ein Nachweis der eigenen *Identität*, der geeignet ist die *Identität* zu *Authentifizieren* (z.B. Besitz eines privaten Schlüssels zu einem X.509-Zertifikat)
Identity Management	Disziplin, die sich mit der sicheren Verwaltung und Abfrage von *Identitäten* befasst.
Identity Mapping	Eine Technologie des *Federated Identity Management*, Identitäten einer Vertrauensdomäne werden dabei auf Identitäten einer anderen Vertrauensdomäne abgebildet.
Identity Provider (IdP)	Ein *Dienst* der eine *Identität authentisiert* und *Sicherheitstoken* herausgibt. Jede *Vertrauensdomäne* hat genau einen IdP, bei dem Nutzer die *OSCI-Kommunikationsverbundes* registriert sind.

Infrastruktur-Service	*Services*, die zentraler Bestandteil jeder *Vertrauensdomäne* sind
Inhaltsdaten (-container)	Die fachlichen Nutzdaten einer OSCI-Nachricht. Es können innerhalb einer Nachricht ggf. beliebig viele Container solcher Daten gebildet werden, die bei Bedarf für unterschiedliche *Target Applications* bestimmt sind. *Die Strukturierung von Inhaltsdaten obliegt der Fachlichkeit und ist nicht Gegenstand von OSCI Transport.* Inhaltsdaten können auch Anhänge in beliebigen Formaten enthalten (siehe *Attachment)*.
Initiator	Auch „Sender" einer OSCI-Nachricht. Nimmt die Inhaltsdaten entgegen, baut die Transportstruktur der Nachricht auf und übermittelt diese.
Intermediär	Logischer oder physischer Knoten auf dem Transportweg der Nachricht vom Initiator zum Empfänger. Intermediäre können Mehrwertdienste erbringen, die entsprechend den jeweiligen Bedürfnissen von Kommunikationsszenarien angefordert werden.
K	
Knoten	Sammelbegriff für logische und/oder physische Stationen, die eine OSCI-Nachricht durchläuft.
Kommunikationsdaten	Nachrichtenbestandteile, die für die Adressierung, Transport/Routing, Authentisierung, Überprüfbarkeit des Transportstatus, Sicherung der Unversehrtheit (Signatur) und Vertraulichkeit benötigt werden. Entspricht den *„Nutzungsdaten"* aus OSCI Transport 1.2 bzw. entsprechender Begriffsdefinition aus dem Telekommunikationsdienstegesetz.
L	
Leser	Die Instanz, für die die Inhaltsdaten einer Nachricht bestimmt sind. Dieser Begriff aus OSCI Transport 1.2 wird hier synonym für den international gebräuchlicheren Begriff „*Target Application*" genutzt.
M	
Message Box	Siehe *Postfach*
O	
OSCI-Gateway	Bezeichnet die Sammlung von Softwareeinheiten, die Endpunkten der OSCI-Kommunikation alle für OSCI Transport benötigen Dienste zur Verfügung stellt.
OSCI-Kommunikationsverbund	Verbund von Kommunikationsteilnehmern innerhalb einer *Vertrauensdomäne,* die auf Basis einer OSCI-Infrastruktur Nachrichten und Dokumente austauschen; i.d.R. sind solche Verbünde von fachlicher oder auch regionaler Zuordung (z.B. Meldewesen, Justiz,..).
OSCI-Nachricht	Das gesamte jeweils übermittelte Datenpaket; umfasst Kommunikations- und Inhaltsdaten sowie optionale Attachments.

P	
PKI	Mit Public-Key-Infrastruktur (PKI) bezeichnet man ein System oder eine Organisation, welches es ermöglicht, digitale Zertifikate auszustellen, zu verteilen und zu prüfen.
Policy	Beschreibt Anforderungen, Fähigkeiten und Zusicherungen von Diensten.
Postfach, Postfachdienst	Ein *Service*, der OSCI-Nachrichten im asynchronen Szenario zwischenspeichert und zur Abholung bereithält. Jedem *Initiator* und *Recipient* ist bei asynchroner Kommunikation ein Postfach zugeordnet, welches eindeutig durch seine *EPR* adressierbar ist.
R	
Rechte	Zugriff auf *Dienste* ist nur möglich, wenn eine *Identität* die entsprechenden Rechte besitzt. Dies wird bei der *Autorisierung* geprüft.
Recipient	Synonym für Empfänger
(Service-) Requestor	Softwareeinheit, die einen Dienst – i.d.R. den eines Service Providers – nachfragt; auch als „*Service Consumer*“ bezeichnet
RST-Nachricht / Request Security Token Nachricht	SOAP Nachricht nach WS-Trust um die Ausstellung eines Sicherheitstokens einzuleiten
RSTR-Nachricht / Request Security Token Response Nachricht	Teil einer SOAP Nachricht als Antwort auf ein RST oder RSTR
S	
SAK	Signaturanwendungskomponente
SAML	„Security Assertion Markup Language“, OASIS-Standard für den Austausch und die Verifizierung von Authentiserungs- und Autorisierungsinformationen in verteilten Umgebungen
SAML-Token	Ein *Sicherheitstoken* mit speziellen Claims (Nach WS-Security: SAML Token Profile 1.1)
Security Token (ST)	Von einem IdP bestätigte *Identität* und *Attribute* (z.B. *Rolle*), die zur Inanspruchnahme eines *Services* ohne zusätzliche *Authentisierung* berechtigt; i.d. R. kryptographisch gesichert
Security Token Service (STS)	Dienst, der Security Token ausstellt; dabei werden Authentisierung und Autorisierung des anfragenden Dienstes / Nutzer überprüft.

Sender, Absender	Siehe auch *Initiator* - die Instanz, die die OSCI-Nachricht übermittelt. Jede OSCI-Nachricht hat genau einen Initiator.
Service	Ein Fachlicher *Service* oder *Infrastruktur-Service*, ist in jedem Fall explizit einer *Vertrauensdomäne* zugeordnet
Service Consumer	Entität, die einen Dienst – i.d.R. den eines *Service Providers* – nachfragt
Service Provider	Anbieter eines Dienstes; dies kann ein System oder auch allgemein ein Dienstleister sein.
Sicherheitsstufe (bei Authentisierung)	Die Sicherheitsstufe sagt aus, wie groß die Sicherheit ist, dass eine durchgeführte *Authentisierung* einer *Identität* korrekt verlief und nicht kompromittiert wurde.
Signaturen, elektronische	Kryptographisch mittels eines geheimen Schlüssels aus einer Nachricht gebildetes Datum, das die Integrität der Nachricht und den Urheber prüfbar macht. Definitionen nach "Gesetz über Rahmenbedingungen für elektronische Signaturen",16.5.2001: http://bundesrecht.juris.de/sigg_2001/BJNR087610001.html: "fortgeschrittene elektronische Signaturen" sind solche die „a) ausschließlich dem Signaturschlüssel-Inhaber zugeordnet sind, b) die Identifizierung des Signaturschlüssel-Inhabers ermöglichen, c) mit Mitteln erzeugt werden, die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann, und d) mit den Daten, auf die sie sich beziehen, so verknüpft sind, dass eine nachträgliche Veränderung der Daten erkannt werden kann“ "qualifizierte elektronische Signaturen" sind solche a) bis d) und „die e) auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat beruhen und f) mit einer sicheren Signaturerstellungseinheit erzeugt werden.“
SOAP	Standardisierte Web-Service Nachricht zum Aufrufen eines Dienstes und auch zum Beantworten; Einteilung in Header und Body
Source Application	Die Instanz, die die Inhaltsdaten einer OSCI-Nachricht erzeugt. Synonym zu „Autor“ aus OSCI Transport 1.2.
Statusmeldung	Quittierung eines Knotens zur Verfügbarkeit von Diensten und/oder Status der Verarbeitung Nachrichten an den/die jeweils übermittelnden Knoten (siehe auch Fehlermeldung).
T	
Target Application	Die Instanz, für die die Inhaltsdaten einer Nachricht bestimmt sind. Synonym zu „Leser“ aus OSCI Transport 1.2. Im Sinne des Ziels der Zustellung von Inhaltsdaten der „Ultimate Recipient“

Trust	Drückt eine Vertrauensbeziehung zwischen zwei Partnern (z.B. Services) aus. Die Partner in einer Vertrauensbeziehung vertrauen darauf, dass Angaben, die nachprüfbar (signiert) vom anderen Partner kommen, korrekt sind (soweit der Partner dies prüfen kann).
Trust-Domain (TD)	*Vertrauensdomäne*, in der zwischen den Einzelkomponenten eine Vertrauensstellung hinsichtlich der Identität und deren Nachweis bestehen.
U	
Uniform Ressource Identifier (URI)	Zeichenfolge, die zur Identifizierung einer abstrakten oder physischen Ressource dient. *URI*s werden zur Bezeichnung von Ressourcen (wie Webseiten, sonstigen Dateien, Aufruf von Webservices, aber auch z. B. E-Mail-Empfängern) im Internet eingesetzt (Def. nach WIKIPEDIA).
V	
Vertrauensdomäne	Zur Aufteilung der Infrastruktur sind alle *Identitätsdatenbanken*, Dienste und *Identity-Provider* explizit einer Vertrauensdomäne zugeordnet. Alle Elemente einer Vertrauensdomäne unterhalten untereinander eine *Trust*-Beziehung. Eine Korrelation zwischen Vertrauensdomäne und Rechnerdomäne ist im Allgemeinen nicht vorauszusetzen.
Verschlüsselungszertifikat	Ein X.509-Zertifikat aus ausschließlich zum Zweck der Verschlüsselung genutzt werden darf.
W	
Web-Service	Software-Anwendung(en), die mit einem *Uniform Resource Identifier* (URI) eindeutig identifizierbar sind und deren Schnittstellen als XML-Artefakte definiert, beschrieben und gefunden werden können. Ein Webservice unterstützt die direkte Interaktion mit anderen Software-Agenten unter Verwendung XML-basierter Nachrichten durch den Austausch über internetbasierte Protokolle (Def. nach WIKIPEDIA).
Web-Services-Framework (WS-Framework)	Softwaresysteme, die den *WS-Stack* implementieren und in der Regel erweiterbar und hochkonfigurierbar sind; sollten als Basis auch für die Implementierung von OSCI Transport 2.0 eingesetzt werden
WSDL	Web Service Description Language; Spezifikationssprache für Netzwerkdienste in XML-Notation.
WS-Stack	Sammlung der für OSCI Transport relevanten OASIS- und W3C-Protokollspezifikationen für Web-Services
X	

X.509-Zertifikat	strukturierte Daten nach dem X.509-Standard, die den Eigentümer sowie weitere Eigenschaften eines öffentlichen Schlüssels bestätigen.
Z	
ZDA	Zertifizierungsdiensteanbieter im Sinne des Signaturgesetzes. Sihe auch *CA*.

Tabelle 1: Begriffsdefinitionen