

Glossar zum S.A.F.E. Feinkonzept

Thema:	Secure Access to Federated E-Justice/E-Government
Verantwortlich:	Bund-Länder-Kommission für Datenverarbeitung und Rationalisierung in der Justiz
Version.Release:	1.3
Erstellt am:	01.02.2008
Zuletzt geändert am:	03.04.2008
Zustand:	in Bearbeitung / vorgelegt / <u>fertiggestellt</u>
Anzahl der Seiten:	8
Autoren:	Klaus Lüttich. (bremen online services GmbH & Co KG) Birger Streckel (Dataport)
Dateiname:	20080330_SAFE_Glossar_V1-3_veroeff.doc
Zusammenfassung:	Sammlung von Begriffen und Abkürzungen, die im S.A.F.E.-Feinkonzept genutzt werden.
Anfragen/Hinweise:	BLK-AG „IT-Standards in der Justiz“ <ul style="list-style-type: none">• Jürgen Ehrmann (Justizministerium Baden-Württemberg) Telefon: 0711 279-2142 ehrmann@jum.bwl.de• Meinhard Wöhrmann (Oberlandesgericht Düsseldorf) Telefon: 0211 4971-647 meinhard.woehrmann@olg-duesseldorf.nrw.de
Status:	Freigegeben durch die BLK am 8. Mai 2008

A	
Administrator	Im EGVP-System derjenige, der im zentralen Adressbuch des Registrierungsservers Änderungen, Sperrungen, Freischaltungen und Löschungen vornehmen darf.
Adressbuch	Im EGVP-System die Liste der adressierbaren Teilnehmer
Aktion	Atomare, fundamentale Einheit ausführbarer Funktionalität
Aktivität	Eine <i>Aktion</i> oder ein einfacher Ablauf von <i>Aktionen</i>
Aktivitätsdiagramm	Beschreiben das Verhalten von Systemen mit <i>Aktionen</i> : Ablauf, Verschachtelung, Parallelität, Verantwortungsbe- reiche, Ausnahmen
Anwendungsfall	Menge von <i>Aktionen</i> , die von einem System bereitgestellt werden; erkennbarer Nutzen für Akteure; Außensicht des Systems
Attribut	Datum, das einer <i>Identität</i> zugeordnet ist (z.B. Nachname, Email-Adresse oder Authentisierungszertifikat); jede Identität wird durch eine Menge von Attributen beschrieben
Attribute-Service (AS)	Der Attribute-Service ist ein zentraler <i>Infrastrukturservice</i> , der die Abfrage von <i>Attributen</i> einer oder mehrerer <i>Identitäten</i> dient
Authentifizierung	Überprüfen einer <i>Identität</i> durch Überprüfung eines <i>Identitätsnachweises</i> , den die <i>Identität</i> zu erbringen hat (z.B. Überprüfung des Personalausweises durch Gesichtskontrolle und Überprüfung der Ausweisnummer)
Authentisierung	Nachweisen einer <i>Identität</i> 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 Sicherheitstoken

Authentisierungszertifikat	Ein X.509-Zertifikat aus ausschließlich zum Zweck der Authentisierung genutzt werden darf.
Autorisierung	Einräumen von <i>Rechten</i> anhand einer bereits festgestellten (authentifizierten) <i>Identität</i> und <i>Rolle</i> (z.B. Jeder authentifizierte EU-Bürger ist autorisiert, in die Schweiz einzureisen)
<i>B</i>	
Backend	OSCI-Client bei Gericht/Verwaltung, der von allen Teilnehmern am EGVP-System adressiert werden kann (für jeden im Adressbuch sichtbar)
Benutzer/Nutzer	Menschliche <i>Identität</i> , die einen menschlichen Anwender beschreibt
Berechtigungsnaehweis	Siehe <i>Sicherheitstoken</i>
<i>C</i>	
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.
<i>D</i>	
Dienst	Siehe <i>Service</i>
DoS-Attacke	Angriff mit Serviceanfragen an einen <i>Service-Provider</i> die zu so starker Auslastung führen, dass der <i>Service-Provider</i> seinen <i>Dienst</i> nicht oder nur sehr langsam erbringt (Denial of Service)
<i>E</i>	
EGVP	Von der deutschen Justiz betriebenes System aus Server- und Client-Komponenten für den sicheren elektronischen

	Rechtsverkehr über OSCI.
F	
Fachlicher Service	<i>Services</i> die eine spezielle fachliche Anwendung implementieren, die aber die <i>Authentisierungs-</i> und <i>Autorisierungsmechanismen</i> einer <i>Vertrauensdomäne</i> nutzen und damit genau einer <i>Vertrauensdomäne</i> explizit zugeordnet sind
Favoritenliste	Ab Version 2.3 im EGVP-System lokal anlegbare Liste von Adressaten
Föderation	Eine Föderation (von <i>Vertrauensdomänen</i>) entsteht, wenn eine <i>Identität</i> , die in einer Vertrauensdomäne registriert ist, <i>Dienste</i> einer anderen Vertrauensdomäne nutzen möchte. Dazu ist eine <i>Trust</i> -Beziehung zwischen den Vertrauensdomänen notwendig.
Federated Identity Management	Um einen föderierten <i>Service</i> -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	
Generalisierung	Verallgemeinern von spezifischen <i>Anwendungsfällen</i> (s. Spezialisierung)
I	
Identität	Ein Eintrag in der <i>Identitätsdatenbank</i> , i.A. Informationsabbild eines menschlichen Benutzers, Systems oder einer Anwendung
Identitätsdatenbank	(eng: Identity-Store) Datenbank zur Speicherung von <i>Identitäten</i> mit deren <i>Attributen</i> , zentraler Bestandteil jeder <i>Vertrauensdomäne</i>
Identitätsnachweis	Ein Nachweis der eigenen <i>Identität</i> , der geeignet ist die <i>Identität</i> zu <i>Authentifizieren</i> (z.B. Besitz eines privaten Schlüssels zu einem X.509-Zertifikat)
Identity-Management	Disziplin, die sich mit der sicheren Verwaltung und Abfrage von <i>Identitäten</i> befasst.

Identity-Mapping	Eine Technologie des <i>Federated Identity Management</i> , Identitäten einer Vertrauensdomäne werden dabei auf Identitäten einer anderen Vertrauensdomäne abgebildet.
Identity-Provider (IdP)	Ein <i>Dienst</i> der eine <i>Identität authentisiert</i> und <i>Sicherheitstoken</i> herausgibt. Jede <i>Vertrauensdomäne</i> hat genau einen IdP.
Infrastruktur-Service	<i>Services</i> , die zentraler Bestandteil jeder <i>Vertrauensdomäne</i> sind
Intermediär	Bei OSCI definierte Einheit (Server), die einen Postfachdienst anbietet sowie kryptografische und Zertifikatsprüfungen bereitstellt, beinhaltet den OSCI-Manager für die OSCI-Kommunikation.
<i>J</i>	
Justiz-Backend	<i>EGVP</i> -Behörden-Client mit <i>Rolle</i> „Gericht“, der die Adressen aller Teilnehmer sieht (Backends, Slaves und Clients)
Justiz-Slave	<i>EGVP</i> -Behörden-Client, der im Adressbuch des Kunden der Justiz (Kunden-Client) nicht sichtbar ist
<i>K</i>	
Kunden-Client	<i>EGVP</i> -Client mit <i>Rolle</i> „Kunde der Justiz“, der ausschließlich die Adressen der Gerichte (Backends) sieht
<i>L</i>	
LK EGVP	Gremium, das über die Weiterentwicklung des <i>EGVP</i> -Systems entscheidet.
<i>O</i>	
OSCI	Protokollstandard der deutschen Öffentliche Verwaltung auf Basis internationaler Standards (SOAP, XML usw.) für eine sichere Kommunikation über potentiell unsichere Netze (wie z.B. da Internet)

<i>P</i>	
Provisioning	Anlegen, Ändern, Löschen und Auslesen von <i>Identitätsdaten</i> und <i>Attributen</i> (auch CRUD für Create, Read, Update, Delete)
Provisioning-Service	<i>Service</i> , der <i>Provisioning</i> -Funktionalität bereitstellt
PKI	Mit Public-Key-Infrastruktur (PKI) bezeichnet man ein System oder eine Organisation, welches es ermöglicht, digitale Zertifikate auszustellen, zu verteilen und zu prüfen.
<i>R</i>	
Registrierungsserver	Im EGVP-System das zentrale Verzeichnis, bei dem sich alle Teilnehmer registrieren, und wo ihre Daten verwaltet werden.
Replikation	siehe Change Request 06/009 zum <i>EGVP</i>
Rechte	Zugriff auf <i>Dienste</i> ist nur möglich, wenn eine <i>Identität</i> die entsprechenden Rechte besitzt. Dies wird bei der <i>Autorisierung</i> geprüft.
Requestor	Dienstnutzer, der Anfragen an <i>Services</i> stellt (auch Client)
Rolle	Ein Rollenkonzept kann die Prüfung der <i>Rechte</i> vereinfachen, da die Rechte in diesem Fall nur anhand des <i>Attributes</i> „Rolle“ vergeben werden.
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
<i>S</i>	
SAML	„Security Assertion Markup Language“, OASIS-Standard für den Austausch und die Verifizierung von Authentisie-

	rungs- und Autorisierungsinformationen in verteilten Umgebungen
SAML-Token	Ein <i>Sicherheitstoken</i> mit speziellen Claims, z.B. Rolle im EGVP-Kontext (Nach WS-Security: SAML Token Profile 1.1)
Service	Ein Fachlicher <i>Service</i> oder <i>Infrastruktur-Service</i> , ist in jedem Fall explizit einer <i>Vertrauensdomäne</i> zugeordnet
Service Provider	stellt einen <i>Service</i> zur Verfügung
Sicherheitstoken	Von einem IdP bestätigte <i>Identität</i> und <i>Attribute</i> (z.B. <i>Rolle</i>), die zur Inanspruchnahme eines <i>Services</i> ohne zusätzliche <i>Authentisierung</i> berechtigt; i. d. R. kryptographisch gesichert
Sicherheitsstufe	Die Sicherheitsstufe sagt aus, wie groß die Sicherheit ist, dass eine durchgeführte <i>Authentisierung</i> einer <i>Identität</i> korrekt verlief und nicht kompromittiert wurde.
Signatur	Kryptographisch mittels eines geheimen Schlüssels aus einer Nachricht gebildetes Datum, das die Integrität der Nachricht und den Urheber prüfbar macht.
Slave	EGVP-Client eines Mitarbeiters der Justiz/Verwaltung, der OSCI-Nachrichten versenden und von Kollegen erhalten, aber nicht von Kunden adressiert werden kann (für diese nicht im Adressbuch sichtbar)
SOAP	Standardisierte Web-Service Nachricht zum Aufrufen eines Dienstes und auch zum Beantworten; Einteilung in Header und Body
Spezialisierung	Verfeinerung eines allgemeinen <i>Anwendungsfalls</i> zu einem spezifischeren (Generalisierung beschreibt dieselbe Beziehung in umgekehrter Richtung)
<i>T</i>	
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 (so-

	weit der Partner dies prüfen kann).
Trust-Domain	Siehe <i>Vertrauensdomäne</i>
V	
Vertrauensdomäne	Zur Aufteilung der Infrastruktur sind alle <i>Identitätsdatenbanken</i> , Dienste und <i>Identity-Provider</i> explizit einer Vertrauensdomäne zugeordnet. Alle Elemente einer Vertrauensdomäne unterhalten untereinander eine <i>Trust-Beziehung</i> . 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.
Visitenkarte	Vom Teilnehmer am EGVP-System einzugebende Daten zu seiner Identität.
X	
X.509-Zertifikat	strukturierte Daten nach dem X.509-Standard, die den Eigentümer sowie weitere Eigenschaften eines öffentlichen Schlüssels bestätigen.