Webservice-Verfahrensanbindung an das USP

Allgemeine Informationen für Software-Lieferanten

von Webservice-Client Software

Version: 1.0

Inhalt

1 Allgemeines 3
1.1 Kurzbeschreibung des beschriebenen Services 3
1.2 Zielgruppe und benötigtes Vorwissen 3
1.3 Abgrenzung des Dokumentenumfanges 3
1.4 Glossar und verwendete Begriffe 4
2 Anbindung von Webservice-Verfahren an das USP 5
2.1 Allgemeine technische Architektur 5
2.2 Verbindungsaufbau zu einem USP-Webservice 5
2.2.1 Webservice-Endpunkte 6
2.2.2 TLS-Verbindungsparameter 6
2.3 Zertifikat- und Schlüsselmanagement für USP-Webservices 6
3 Empfehlungen an den Webservice-Client Software-Hersteller 7
3.1 Schlüsselmanagement 7
3.2 Verbindungen zum Webservice & Authentifizierung 7
3.3 Migration von SOAP-Security auf mTLS 7
Änderungsprotokoll 9

1 Allgemeines

1.1 Kurzbeschreibung des beschriebenen Services

Über das Unternehmensserviceportal können bestimmte Webservices erreicht werden, die von Webservice-Client Software aufgerufen werden.

Der Aufruf von Webservice-Verfahren findet üblicherweise automatisiert über Programm-zu-Programm Kommunikation statt, und verwendet mTLS für die Authentifizierung des Clients gegenüber des Webservices.

Dieses Dokument beschreibt die allgemeinen technischen Aspekte für Webservice-Client Softwarehersteller und Webservice-Verfahrensanbieter, mit dem Ziel, ihre jeweilige Software für diese Authentifizierungsmethode vorbereiten zu können.

Dieses Dokument liefert keine spezifischen Informationen zu den einzelnen Webservice-Verfahren wie z.B. die genauen Endpunkte usw. Diese Informationen pro Webservice sind weiterführender Dokumentation zu den spezifischen Verfahren zu entnehmen.

1.2 Zielgruppe und benötigtes Vorwissen

Dieses Dokument richtet sich an zwei Gruppen:

- gegenwärtige und zukünftige Anbieter von Webservice-Client Software
- gegenwärtige und zukünftige Anbieter von Webservices im Unternehmensserviceportal

Dieses Dokument bietet technische Informationen über die notwendigen Verbindungsparameter, damit sich ein Webservice-Client erfolgreich mit einem Webservice in USP verbinden, an einem solchen authentifizieren und ein solches benutzen kann.

Das Dokument eignet sich für folgende Zielgruppen:

- Software-Entwicklerinnen und -Entwickler
- IT-Architektinnen und -Architekten

Für die erfolgreiche Authentifizierung von Webservice-Clients an vom USP angebundene Webservices wird mTLS (Mutual TLS) verwendet.

Um den Inhalt dieses Dokuments vollständig nachvollziehen und in der Praxis anwenden zu können, sollten Leser über folgende Voraussetzungen verfügen:

- Kenntnisse der Funktionsweise von HTTPS
- Grundlegendes Verständnis von TLS bzw. mTLS bzw. grundlegendes Verständnis von Zertifikaten, Zertifikatsketten und asynchroner Verschlüsselung

1.3 Abgrenzung des Dokumentenumfanges

Dieses Dokument erhebt keinen Anspruch darauf, die zugrunde liegenden Konzepte, Protokolle und Technologien der Themenbereiche Authentifizierung, mTLS und Webservices vollständig zu erläutern.

Die beschriebenen Inhalte setzen ein bestehendes Verständnis der relevanten Grundlagen voraus und dienen primär der Einordnung, Orientierung und Unterstützung bei der Anwendung in einem spezifischen fachlichen oder technischen Kontext. Es liegt nicht im Verantwortungsbereich dieses Dokuments, die erwähnten Themen in einer Form aufzubereiten, die ein vollständiges Erlernen oder Ersetzen weiterführender Fachliteratur, Standardspezifikationen oder Trainingsmaterialien ermöglichen würde.

1.4 Glossar und verwendete Begriffe

Begriff	Beschreibung
Portal	Ein Portal ist im digitalen Kontext eine Website oder Anwendung, die als zentraler Einstiegspunkt fungiert, um Informationen, Dienste und Applikationen aus verschiedenen Quellen gebündelt bereitzustellen.
Stammportal	Das Unternehmensserviceportal (USP) fungiert im PVP-Kontext als sogenanntes Stammportal und bietet dem Anwendungsportal damit vertrauenswürdige Aussagen über Authentizität, Autorisierung und andere Informationen des angemeldeten Benutzers.
Reverse Proxy	Ein Reverse Proxy ist ein Vermittlerserver, der vor einem oder mehreren Webservern im Internet oder Netzwerk steht. Er nimmt eingehende Client-Anfragen (z.B. vom Browser) entgegen, leitet sie an den passenden internen Server weiter und sendet die Antwort zurück. Er schützt und optimiert die Backend-Server, ohne dass der Client dies bemerkt.
Verfahrensintegration	Um eine neue Anwendung bzw. ein neues Verfahren den Benutzern in USP zugänglich zu machen, müssen diese zuvor in das USP "integriert" werden, d.h. das Portal wird entsprechend konfiguriert, damit die Anwendung anschließend im USP aufrufbar ist. Integrierte Anwendungen sind unter https://mein.usp.gv.at (https://mein.usp.gv.at) aufrufbar, sofern der angemeldete Benutzer Berechtigungen für diese Anwendung hat.
Verfahrensmigration	Die technische Infrastruktur des Unternehmensserviceportals muss kontinuierlich modernisiert und weiterentwickelt werden, um zukunftsfähig zu bleiben. Dies kann für bereits integrierte Anwendungen die Notwendigkeit einer Migration auf die neue Systemarchitektur des USP mit sich bringen. Das Verfahren ist danach über die neue Architektur verfügbar und wird anschließend im „Altsystem“ deaktiviert. Eine Verfahrensmigration bewirkt üblicherweise keine funktionalen Änderungen, allerdings ist unter Umständen die Mitwirkung des Verfahrenspartners bei der Testdurchführung und bei organisatorischen Aspekten notwendig. Es können sich auch technische Änderungen ergeben, die der Verfahrenspartner in seiner Anwendung implementieren muss.
Verfahrenspartner	Der Verfahrenspartner ist der technische und/oder organisatorische Verantwortliche eines Webservices, das in USP integriert wurde oder wird.

2 Anbindung von Webservice-Verfahren an das USP

2.1 Allgemeine technische Architektur

Das Unternehmensserviceportal können verschiedene Webservices erreicht werden, die von Webservice-Clients aufgerufen werden können.

Jedes Webservice wird dabei als Subdomain unter *.ws.usp.gv.at zur Verfügung gestellt. Zwischen dem Client und dem Webservice befindet sich ein Reverse-Proxy, welcher unter anderem die Authentifizierung und ein entsprechendes Routing zum Backend-Service durchführt.

Dadurch ergibt sich folgende einfache Architekturdarstellung:

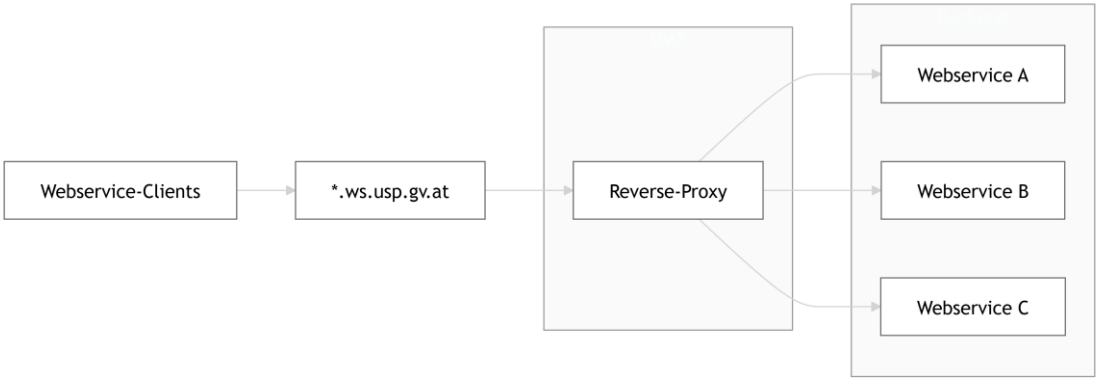


Abbildung 1 - Architektur Webservices in USP

2.2 Verbindungsaufbau zu einem USP-Webservice

Für die Kommunikation mit dem Webservice wird Mutual TLS (mTLS) verwendet. Dabei authentifizieren sich sowohl der Webservice-Client als auch der Webservice gegenseitig auf Transportebene mittels X.509-Zertifikaten.

1. Der Webservice-Client baut eine TLS-Verbindung zum HTTPS-Endpunkt des Webservice auf.
2. Das Webservice präsentiert während des TLS-Handshakes sein Serverzertifikat.
3. Der Client prüft das Serverzertifikat anhand der konfigurierten Zertifizierungsstelle (CA), der Zertifikatsgültigkeit sowie des Hostnamens.
4. Das Webservice fordert anschließend ein Client-Zertifikat an.
5. Der Client sendet sein X.509-Client-Zertifikat sowie den Nachweis des Besitzes des zugehörigen privaten Schlüssels.
6. Das Webservice validiert das Client-Zertifikat gegen die vertrauenswürdigen Zertifizierungsstellen und prüft dessen Gültigkeit.
7. Nach erfolgreicher gegenseitiger Authentifizierung wird der TLS-Handshake abgeschlossen und die verschlüsselte Webservice-Kommunikation gestartet.

2.2.1 Webservice-Endpunkte

Der allgemeine Webservice-Endpunkt hat folgendes Format:

```
https://app.ws.usp.gv.at/webservice-path
```

`app` … dreistelliger Code, der für jedes Webservice-Verfahren eindeutig ist

`webservice-path` … URI-Pfad des entsprechenden Webservice-Verfahrens. Falls ein Webservice-Verfahren Test- und Produktionsumgebungen anbietet, müssen diese innerhalb des Pfades unterschieden werden

Ein einzelnes Webservice-Verfahren selbst kann mehrere Endpunkte anbieten. Die genaue Bezeichnung alle Endpunkte ist der Dokumentation des jeweiligen Webservice-Verfahrens zu entnehmen.

2.2.2 TLS-Verbindungsparameter

Verbindungen zu den vom USP bereitgestellten Webservices benötigen eine TLSv1.3 (empfohlen) oder TLSv1.2 Verbindung.

Für TLSv1.2 werden die folgenden Cipher-Suites unterstützt:

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256

2.3 Zertifikat- und Schlüsselmanagement für USP-Webservices

Client-Zertifikat und der dazugehörige Schlüssel werden durch den USP-Administrator des Unternehmens in der USP-Administration (Benutzeroberfläche) generiert und anschließend als PKCS#12 (siehe: https://en.wikipedia.org/wiki/PKCS_12) heruntergeladen. Die generierte PKCS#12-Datei und der darin enthaltene Schlüssel ist mit einem Passwort geschützt, welches dem USP-Administrator beim Download angezeigt wird. Das Passwort für die PKCS#12-Datei und für den darin enthaltenen Schlüssel ist identisch.

Die Schlüsselinformationen werden dabei innerhalb der USP-Administration nicht persistiert und sind nach einem Download nicht mehr erneut abrufbar. Lediglich das (öffentliche) Zertifikat wird innerhalb der USP-Infrastruktur abgelegt.

Der USP-Administrator muss entsprechend dafür Sorge tragen, dass er die PKCS#12-Datei und das zugehörige Passwort sicher aufbewahrt und unbefugten Dritten nicht zur Verfügung stellt. Die Webservice-Client Software muss in der Lage sein, diese Zertifikats- und Schlüsselinformationen in dieser Datei für den Aufbau der mTLS-Verbindung zu nutzen.

3 Empfehlungen an den Webservice-Client Software-Hersteller

In diesem Abschnitt geben wir Empfehlungen an die Hersteller der Webservice-Client Software. Diese Empfehlungen folgen der Idee einer flexiblen Konfiguration und sollen einerseits helfen, die Benutzererfahrung für die Anwender zu gestalten, und andererseits für Client-Entwickler zusätzlich hilfreiches Verständnis zu übermitteln.

Selbstverständlich liegt es im eigenen Ermessen des Softwarehersteller, inwieweit diese Empfehlungen umgesetzt werden.

3.1 Schlüsselmanagement

Direkte Verwendung von PKCS#12 als Schlüsselbund

Da Client-Zertifikat und Schlüssel als PKCS#12 zur Verfügung gestellt werden, sollte die Webservice-Client Software in der Lage sein, diese direkt zu importieren bzw. zu verwenden

PKCS#12 mit Passwort

Da sowohl die PKCS#12-Datei selbst als auch der darin enthaltene Schlüssel mit einem Passwort versehen ist, sollte die Webservice-Client Software es dem Benutzer gestatten, beim Import dieses Passwort anzugeben. Die PKCS#12-Datei und der darin enthaltene Schlüssel sind mit demselben Passwort gesichert, daher ist die Eingabe eines einzelnen Passworts ausreichend.

Zertifikats-Ablaufdatum anzeigen

Da das Client-Zertifikat mit einem Ablaufdatum versehen ist, sollte die Webservice-Client Software in der Lage sein, ein bevorstehendes Ablaufen des Zertifikats zu erkennen und diesen Zustand dem Benutzer rechtzeitig zur Anzeige bringen, damit dieser ein neues Zertifikat generieren kann.

3.2 Verbindungen zum Webservice & Authentifizierung

Konfigurierbarkeit des Endpunktes bzw. des Hosts

Für Benutzer des Clients sollte es möglich sein, den Webservice-Endpunkt oder zumindest den Host anzupassen. Wie in Abschnitt 2.2.1 beschrieben, bietet das Unternehmensserviceportal für die verschiedenen Webservice-Verfahren verschiedene Sub-Domains an.

3.3 Migration von SOAP-Security auf mTLS

Dieser Abschnitt enthält spezielle Empfehlungen für Webservice-Client Software, die bereits SOAP-Security implementiert hat, um mit den vom Unternehmensserviceportal bereitgestellten Webservices zu interagieren.

Die Idee hinter diesen Empfehlungen ist es, den Benutzer einen Migrationspfad zu mTLS-Authentifizierung anzubieten, der nicht von einem Upgrade der Client-Software erzwungen wird. Stattdessen liegt die Überlegung zugrunde, dass Benutzer nach einem Upgrade auf mTLS-fähige

Client-Software Zeit haben, um den Wechsel auf mTLS schrittweise durchzuführen bzw. kurzzeitig die Möglichkeit haben, die bisherige Authentifizierungsmethode zu verwenden:

Auswahl der Authentifizierungsmethode

Um eine reibungslose Migration aller Anwender auf die neue Authentifizierungsmethode zu gewährleisten, empfiehlt sich, kurzzeitig zwischen zwei Software-Releases eine Auswahlmöglichkeit der Authentifizierungsmethode zu schaffen:

SOAP-Security … Angabe von Username und Passwort

mTLS … Angabe einer PKCS#12 Datei & zugehöriges Passwort

SOAP-Security als „deprecated“ darstellen und Entfernen dieser Funktionität einplanen

Mit der Verfügbarkeit von „mTLS“ als Authentifizierungsmethode gegen die vom Unternehmensserviceportal bereitgestellten Webservices ist es ratsam, dass „SOAP-Security“ als veraltet markiert wird und dass diese Methode in zukünftigen Releases nicht mehr angeboten werden kann.

Das Unternehmensserviceportal wird voraussichtlich ab Ende Oktober 2027 eine Authentifizierung über SOAP-Security nicht mehr anbieten.

Änderungsprotokoll

Version 1.0	**Datum: 30.10.2026**	Initiale Version