S!MPATI online

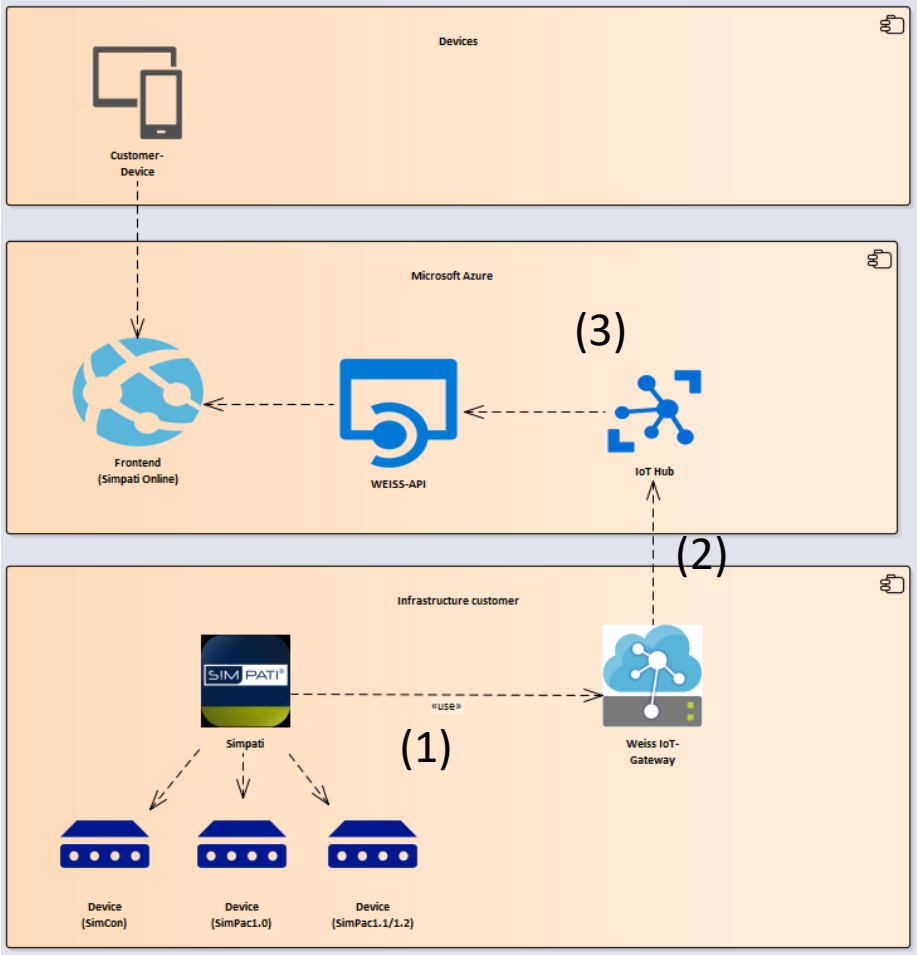
Security

Sicherheitskomponenten

- Architektursicht auf S!MPATI online / Weiss IoT Gateway und den Microsoft Cloud Access Security Broker
- Verbindungen und Datenspeicherung
- Verschlüsselung
- Authentifizierung und Benutzerverwaltung
- Testing
- Referenzen

Architektursicht auf S!MPATI online

Weiss Umwelttechnik S!MPATI online



(1) S!MPATI liest Daten über SimServ auf dem localhost und leitet diese zum Gateway

(2) Das Gateway sendet die Daten mit dem Microsoft IoT SDK zum IoT Hub. Das Protokoll ist verschlüsseltes AMQP.

(3) Die Daten werden über einen Token identifiziert. Ein Gerät kann sich nur mit einem gültigen Token am IoT Hub anmelden.
Tokens werden verschlüsselt auf dem S!MPATI System des Kunden gespeichert.
Das Weiss IoT Gateway ist mit einem einmaligen und eindeutigen Token am Azure Active Directory B2C angemeldet.

Verbindung und Datenspeicherung

Verbindung Kunde - Internet

- Da die gesamte Kommunikation verschlüsselt ist, muss keine weitere Massnahme (z.B. VPN) zur Verbindung zwischen dem Weiss IoT Gateway und den Microsoft Azure Services vorgesehen werden.
- Die Ports 5671 and 443 müssen **ausgangsseitig** in der Kunden IT Infrastruktur geöffnet werden.

Vertrauenswürdige Zertifikatsstelle

- Weiss Umwelttechnik GmbH vertraut auf die Kooperation mit dem Partner Microsoft.
- Alle Services inklusive dem IoT Hub benutzen die Zertifikatsstelle, die von Microsoft Azure zur Verfügung gestellt wird.

Datenspeicherung

- Alle Daten werden in Europa, Amsterdam, gespeichert.
- Der Datenzugriff erfolgt über Token.
- Mandanten sind strikt voneinander auf Zugriffsebene getrennt (Multi-Client Fähigkeit).

Verschlüsselung

Die gesamte Kommunikation ist verschlüsselt (API, Datenzugriffe, IoT Kommunikation)

Der Verschlüsselungsstandard entspricht dem Stand der Technik.

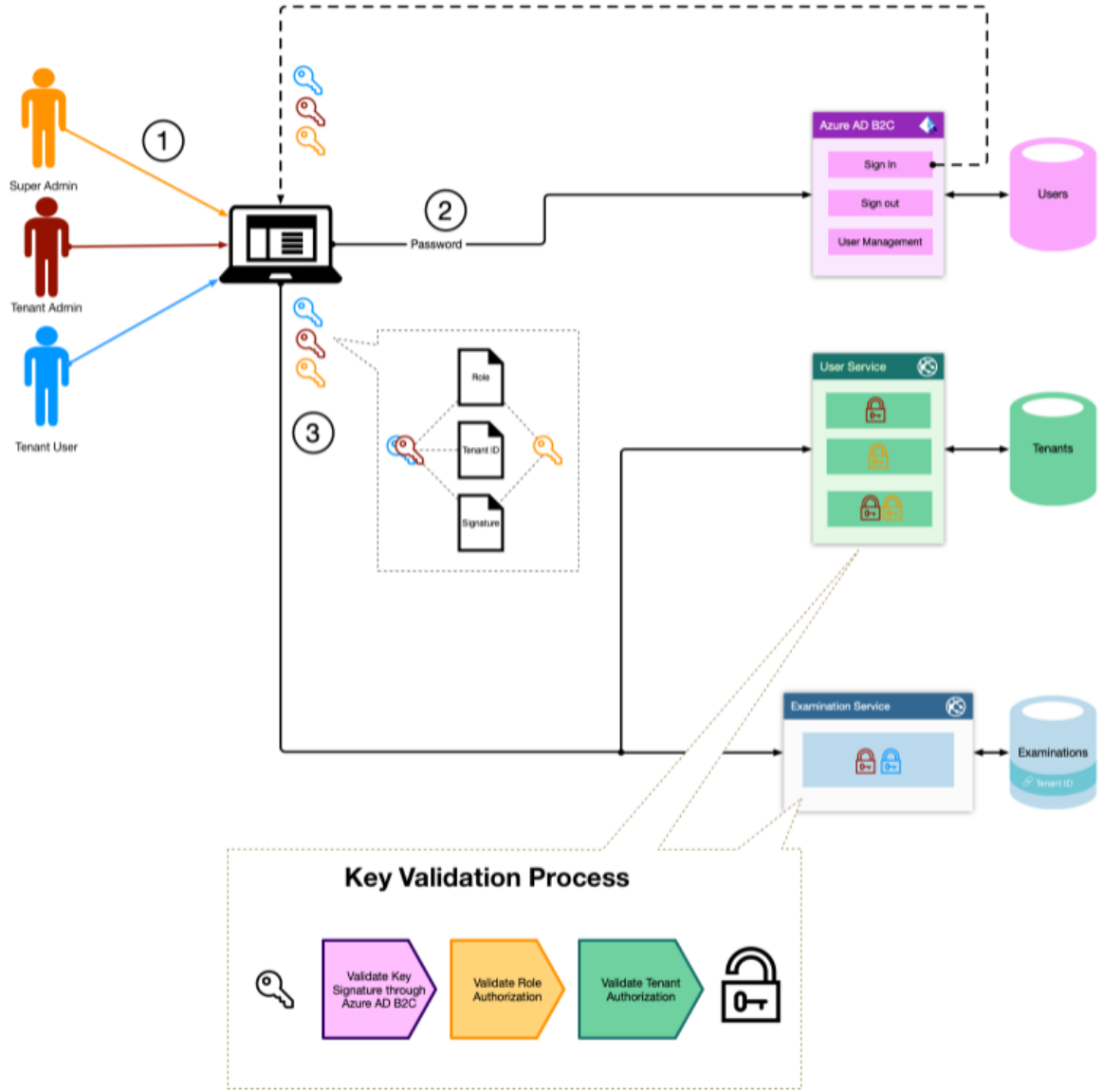
Weiss Umwelttechnik GmbH nutzt die Cipher Suites mit

- Schlüsselaustausch: RSA 2048bits
- Verschlüsselung : SHA256withRSA
- TLS1.2 und TLS1.3 stehen beide zur Verfügung

Authentifizierung und Benutzerverwaltung

Authentifizierung und Benutzerverwaltung basieren auf der Microsoft Azure B2C Lösung.

Schlüssel- und, Rollenverifizierung sowie Benutzerautorisierung werden auf verteilten Systemen verwaltet.



Testing

Zusätzliche Sicherheits Tests werden mit externen Spezialisten nach dem Stand der Technik durchgeführt.

In Penetration Tests wurden unter anderem die folgenden Gesichtspunkte geprüft:

- Transport Sicherheit http
- Konfiguration der Transport Schicht Sicherheit
- Zertifikats Konfiguration
- Konfiguration des Schlüsselaustauschs
- eMail Verteilungs- und Verwaltungs-Regeln
- Datenzugriffs Sicherheit

Referenzen

[Microsoft, 2020-09-16] Statement of Applicability for Microsoft Azure, Dynamics 365, and other Online Services - ISO 27001, 27018 and 27701

[Microsoft, 2020-08-19] Certificate demonstrating Microsoft Azure, Dynamics 365, and Other Online Services' compliance with ISO27001 and 27701 (Privacy Information Management Systems) framework.

[Microsoft, 2020-08-19] Assessment report demonstrating Microsoft Azure, Dynamics 365, and other Online Services' compliance with the ISO 27001, 27018, 27017 and 27701 (PIMS) frameworks.

[Microsoft, 2020-03-31] ISO 27001:2013 Zertifikat

Weitere technische Informationen:

- https://github.com/Azure/azure-iot-sdk-csharp
- https://en.wikipedia.org/wiki/Advanced_Message_Queuing_Protocol
- https://docs.microsoft.com/de-de/azure/active-directory-b2c/technical-overview

Weiss Umwelttechnik GmbH
Greizer Straße 41 - 49
35447 Reiskirchen ¬ Germany
Tel +49 6408 84-0
info@weiss-technik.com
www.weiss-technik.com