S!MPATI online

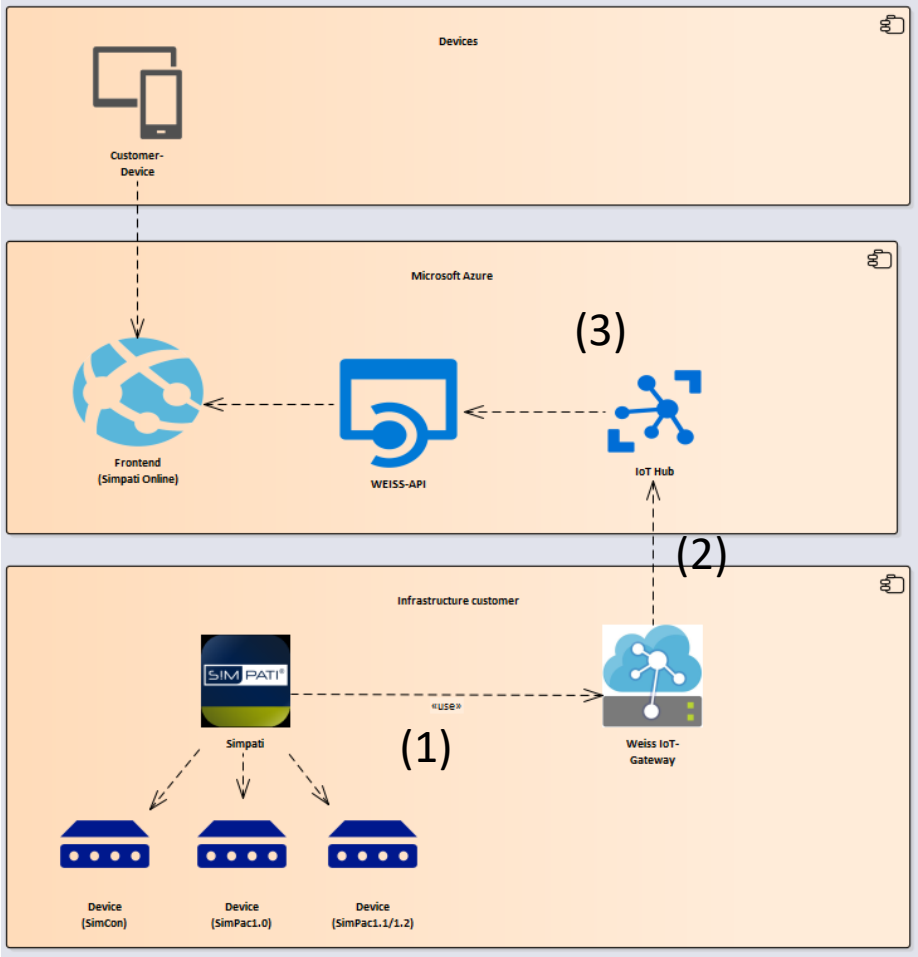
Security

Main security components

- Architecture view on S!MPATI online / Weiss IoT Gateway and Microsoft Cloud Access Security Broker
- Connection and data storage
- Cryptographic strategy
- Authentication and tenant administration
- Testing
- References

Architecture view on S!MPATI online

Weiss Umwelttechnik S!MPATI online



(1) Fetching data from S!MPATI via SimServ at localhost to the Gateway

(2) Gateway is sending Data with Microsoft IoT SDK to the IoT Hub.
Protocol is secure AMQP

(3) Data is identified by a token. A device can connect to the IoT Hub with a valid token only .
Tokens are saved encrypted on the S!MPATI system at the customer.
The Weiss IoT Gateway is registered at Azure Active Directory B2C with a unique identifier.

Connection and data storage

Connection Customer Internet

- Due to the fact that all communication is encrypted the connection between the Weiss IoT Gateway and the internet for accessing Microsoft Azure services has no needs to be underlied with e.g. an additional VPN.
- Ports 5671 and 443 have to be opened **outwards** in the customer IT infrastructure for communication.

Trusted CA

- Weiss Umwelttechnik GmbH relies on the cooperation partner Microsoft.
- All services including the IoT Hub use the Certificate Authority made available via Microsoft Azure.

Data storage

- All data is stored in Europe, Amsterdam.
- Data access is done by token.
- Tenants are strictly separated on access level (multi-client capability).

Cryptographic strategy

All communication is encrypted (API, Database, IoT Communication)

Crypto standard is state of technology.

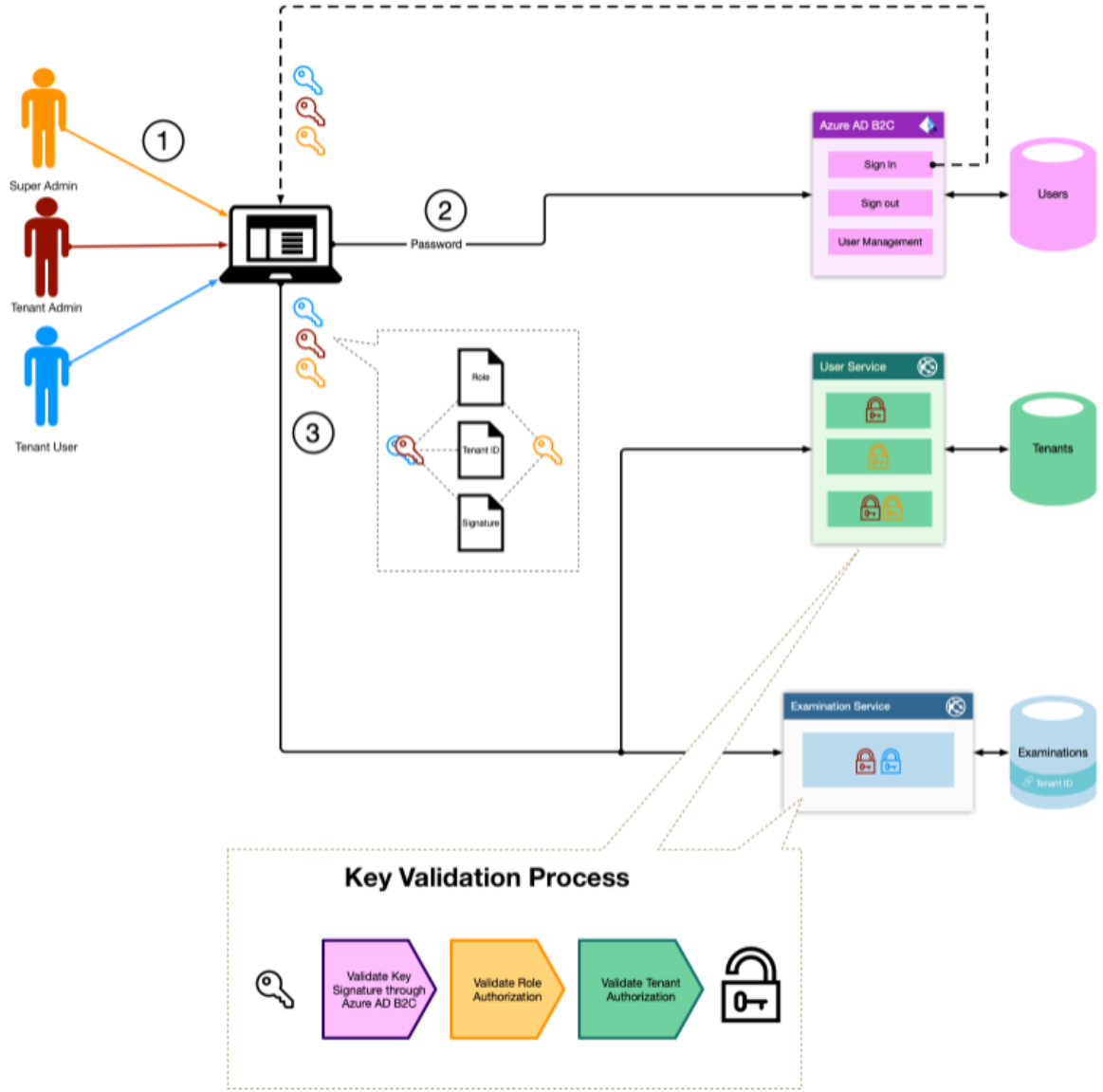
Weiss Umwelttechnik GmbH uses the Cipher Suites with

- key exchange: RSA 2048bits
- encryption : SHA256withRSA
- TLS1.2 and TLS1.3 are available

Authentication and tenant administration

Authentication and tenant administration is based on the Microsoft Azure B2C solution.

Key signature, role validation and tenant authorization are administered on seperate systems



Testing

Additional security testing with external specialist following standard rules.

In penetration tests the following topics have been checked:

- transport security http
- transport layer security configuration
- certificate configuration
- key exchange configuration
- e-mail policies
- database security

References

[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 Certificate

Further technical information:

- 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