ASSA ABLOY

CLIQ® FAQs

Technische Informationen zur Netzwerkauthentifizierung (802.1x) bei WallPD Gen.2

Technische Details zu den 802.1x-Zertifikaten:

Authentifizierungsverfahren:

- Das System nutzt EAP-TLS (Extensible Authentication Protocol - Transport Layer Security)
- Client-ID entspricht automatisch dem IP-Hostnamen des WPDs

Client-Zertifikat (für das WPD):

- Format: .p12 (PKCS#12)
- RSA-Schlüssellänge: Mindestens 2048 Bit
- Hash-Algorithmus: Mindestens SHA-2/SHA256
- Formate unterstützt: DER und PEM (Klartext, keine Verschlüsselung)
- Braucht ein Passwort zum Hochladen
- Muss von der eigenen CA ausgestellt werden

Server-CA-Zertifikat(e):

- Format: .pem
- Bis zu 3 CA-Zertifikate können hochgeladen werden
- Das ist das Root-/Intermediate-CA-Zertifikat des 802.1x-Servers (meist RADIUS)

Ablauf der Authentifizierung:

1. WPD startet 802.1x-Authentifizierung mit dem RADIUS-Server
2. Mutual Authentication über EAP-TLS mit dem Client-Zertifikat
3. Erst danach bekommt das WPD Netzwerkzugang
4. Dann normale CLIQ-Verbindung mit DCS-Zertifikaten zum CLIQ-Server

Benötigt wird:

- Ein .p12-Client-Zertifikat aus der eigenen CA/PKI
- Das .pem CA-Root-Zertifikat des 802.1x-Servers
- Den Hostnamen des 802.1x-Servers (meist RADIUS)