kontron

The Power of IoT

Kontron AIS GmbH

Datensicherheit

EquipmentCloud® &
KontronGrid

2024-09

Agenda

Kontron AIS GmbH

Systemansatz

Datenbank

Sichere Kommunikation

Nutzermanagement

Datensicherheit und -qualität

KontronGrid Dienste

kontron
The Power of IoT
Kontron AIS GmbH

01
Systemansatz

01 SYSTEMANSATZ

EquipmentCloud®- Digitalisierungslösung für Service & After-Sales

kontron
The Power of IoT
Kontron AIS GmbH

- Cloudbasierte Lösung
  - Die EquipmentCloud® ist eine webbasierte Anwendung
  - Software-as-a-Service (SAAS) bietet weltweiten Zugriff auf den Dienst und Maschinendaten
  - App-basierte Nutzung auf multiplen Endgeräte (Smartphone, Tablet, Laptop) für iOS oder Android
  - Keine eigene IT-Infrastruktur und administrativer Aufwand notwendig
    - Geringe initiale Kosten durch SAAS-Model
    - Minimiertes Investitionsrisiko durch die Verlagerung von CapEx zu OpEX
    - Erhöhte Flexibilität und effiziente Skalierung
  - Gemeinsame Datenbasis aller Module
  - Zugriff auf neuste technische Innovationen wie Data Analytics und KI
  - Dokumentierte generische Schnittstellen (REST) für die Kommunikation mit Drittsystemen

01 SYSTEMANSATZ

KontronGrid - IoT Device Management für Geräteflotten

Kontron AIS GmbH

- Cloudbasierte Lösung und Edge Service
  - Das KontronGrid teilt sich die gleiche technologische Basis wie die EquipmentCloud®, was webbasierte User Interface anbelangt
  - Eigenständige Software-as-a-Service (SAAS) oder Add-On Modul der EquipmentCloud®
    - Kompatibel
    - Integriert
    - Erweiterbar
  - Bietet weltweiten Zugriff auf den Dienst und IoT-Gerätedaten
  - Vorinstallierter Agent auf dem Edge Gerät stellt die Verbindung zur Webanwendung her
  - Dokumentierte generische Schnittstellen (REST) für CLI-Kommunikation und Docker Compose Integration

kontron
The Power of IoT
Kontron AIS GmbH

02

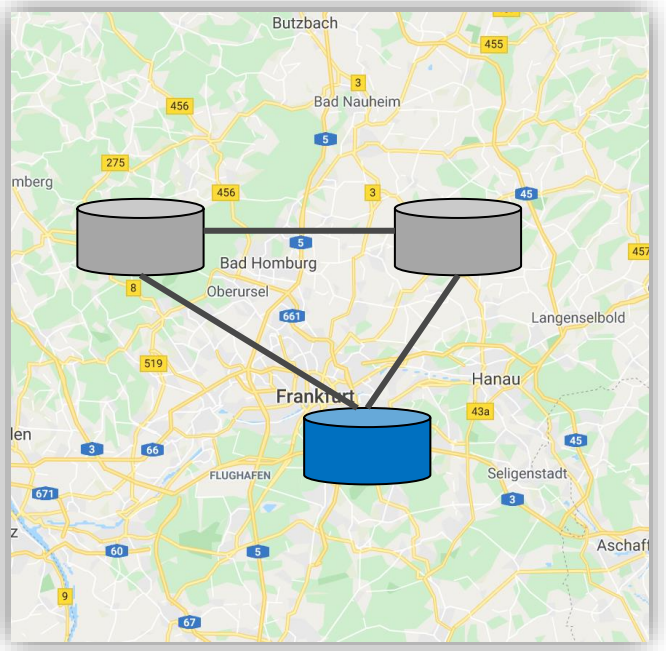
Datenbank

02 Datenbank

Datenbankserver

Kontron AIS GmbH

- Die EquipmentCloud® und das KontronGrid basieren auf der Oracle Cloud Infrastructure (OCI) Gen 2.0
- Hauptserver und Back-Up Server der Oracle Cloud Serversysteme befinden sich in Deutschland
- Oracle unterhält drei Server Standorte gleichzeitig um Frankfurt a.M.
  - Spiegelung der Daten zur Sicherheit
  - Flexibles Umschaltung bei Problemen
  - Highspeed-Internetverbindungen zwischen den Standorten vorhanden

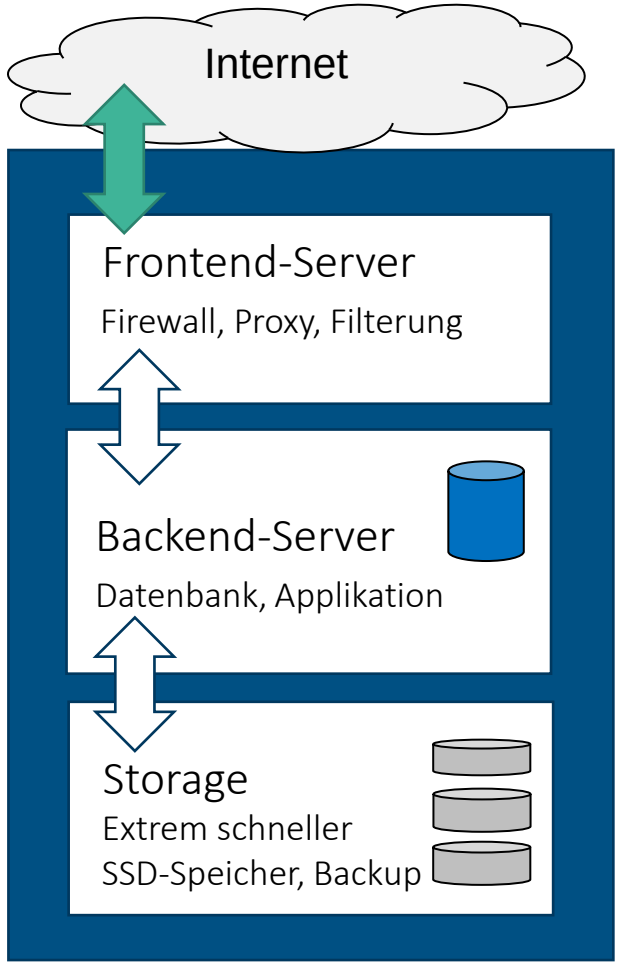


Datenbankserver in Frankfurt a.M.

02 Datenbank

Aufbau Datenbank in der Cloud

- Trennung von Frontend und Backend
- Frontend zur Sicherung der Kommunikation, Filterung von unberechtigten Anfragen
- Backend mit der Datenbank und Applikation
- Storage (SSD) zur Speicherung der Daten und Sicherstellung eines schnellen Zugriff



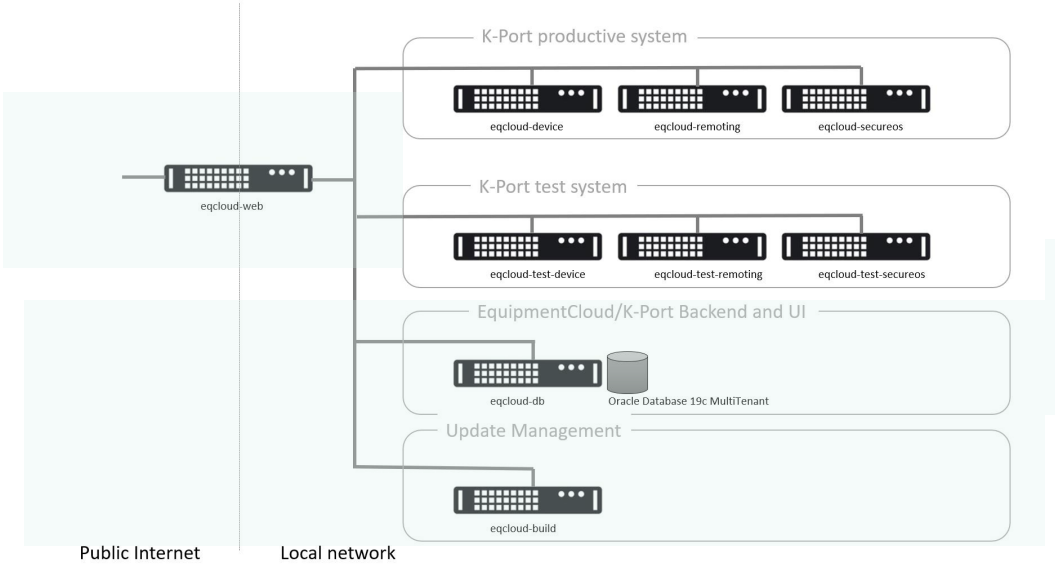
02 Datenbank

Aufbau Datenbank in der Cloud (EquipmentCloud & KontronGrid)

Kontron AIS GmbH

Die einzelne Systeme übernehmen folgende Aufgaben:

- **eqcloud-web**: Front-End-Server als Zugangspunkt aus dem öffentlichen Internet
  - Hostet ORDS (Oracle REST Data Service) sowie TomCat
  - NGINX-Server dient als Proxy-Anwendung für Zugang von außen
- **eqcloud-db:** Oracle Datenbankserver als Multi-Tenant-System mit den Kundencontainern
  - Ausführung von Oracle Datenbanksoftware sowie der APEX-Anwendungen
- **eqcloud-build:** Betrieb des Build-Agent, über den die Aktualisierung der Oracle-Datenbank und der APEX-Anwendung erfolgt
  - Server wird nur für Updates gestartet und ist die restliche Zeit ausgeschaltet



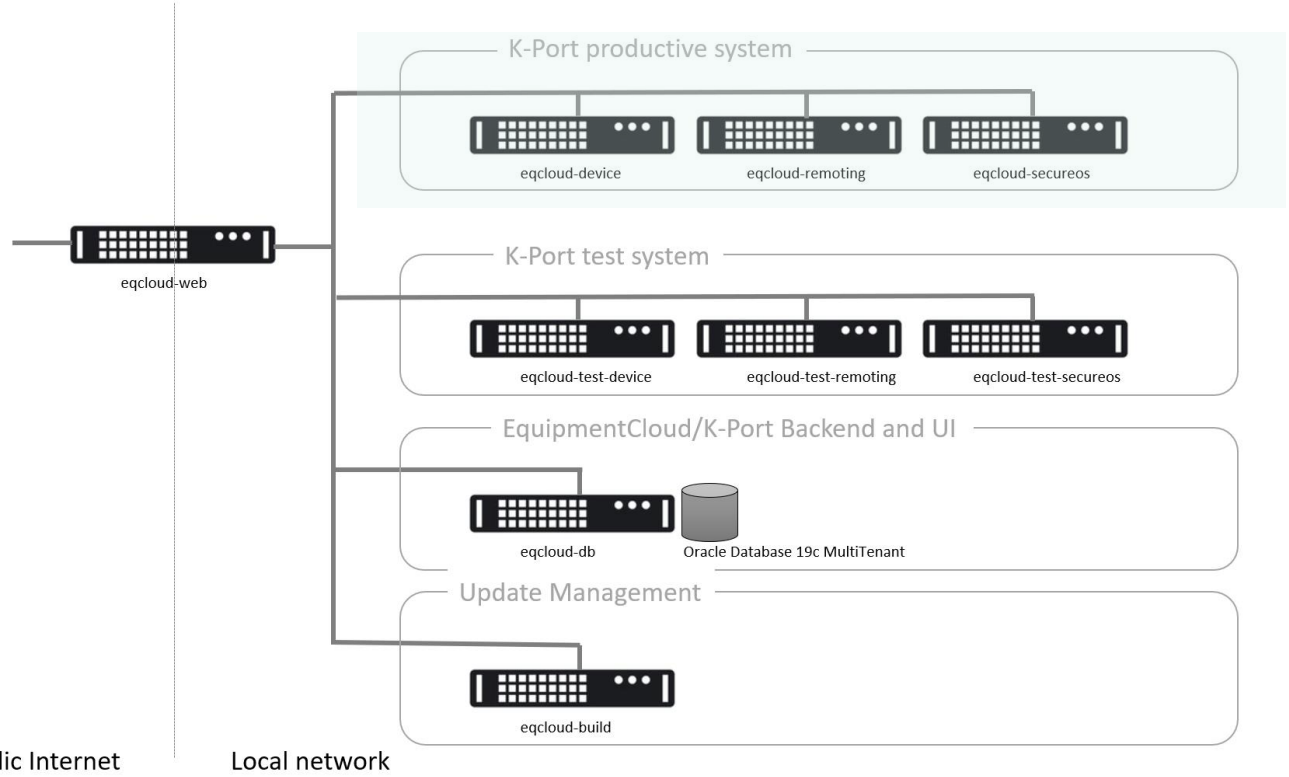
02 Datenbank

Aufbau Datenbank in der Cloud (KontronGrid)

Kontron AIS GmbH

KontronGrid Produktivsystem übernimmt folgende Aufgaben:

- **eqcloud-device:** Server handelt die lokalen Agenten der angeschlossenen Geräte im KontronGrid
  - Gewinnung von Monitoring-Daten
  - Übermittlung von Kommandos zum Download
  - Start und Löschen der Docker-Anwendungen
- **eqcloud-remoting**: Server dient als Manager für die Remoting-Verbindungen zu den Geräten im KontronGrid
  - Ausführung Guacamole, das die Kommunikation im Browser über SSH und RDP sicherstellt
- **eqcloud-secureos:** Server dient als Endpunkt für die Auslieferung von KontronOS Updates an die Geräte



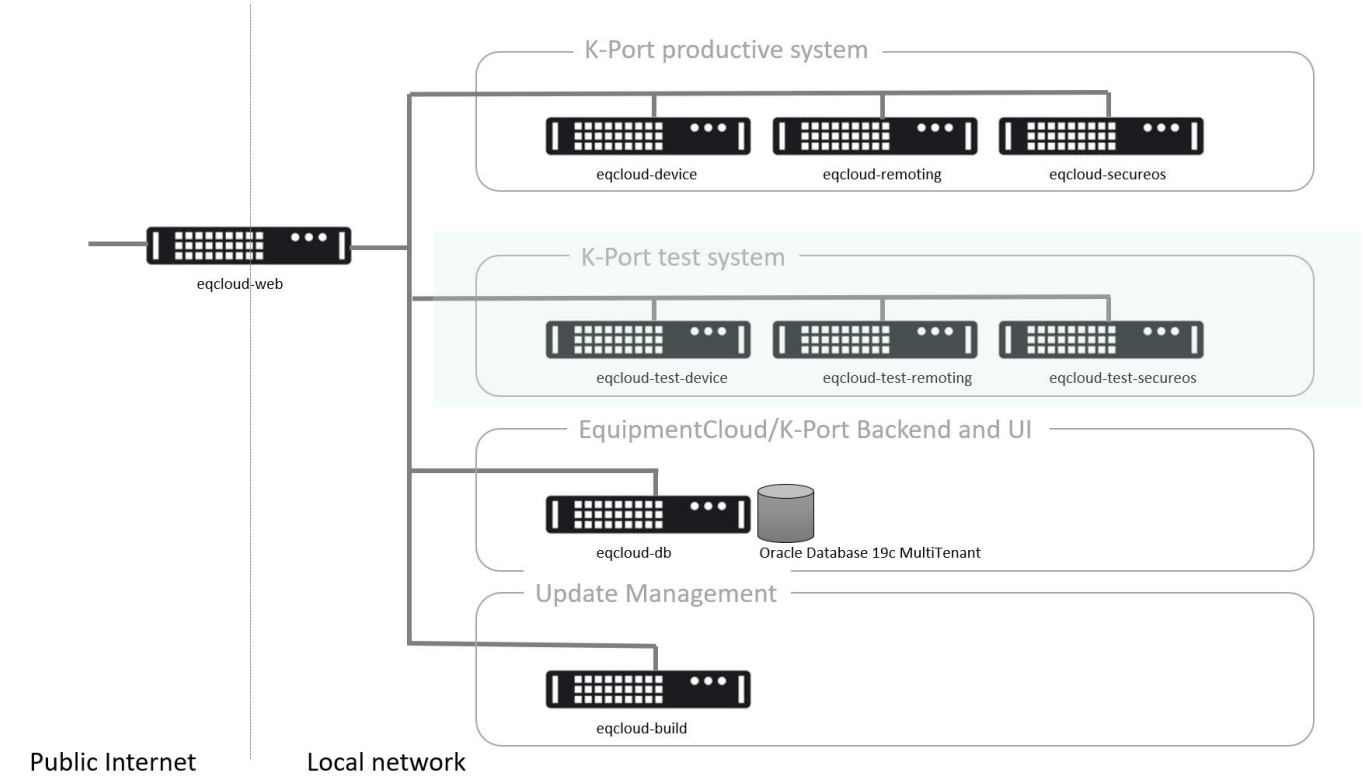
02 Datenbank

Aufbau Datenbank in der Cloud (KontronGrid)

Kontron AIS GmbH

KontronGrid Testumgebung übernimmt folgende Aufgaben:

- **eqcloud-test-device, eqcloud-test-remoting, eqcloud-test-secureos:** Testumgebung für die produktiven Systeme im KontronGrid sind funktionell identisch.
  - Erprobung neuer Versionen zur Sicherstellung der Zuverlässigkeit und Qualität von ausgelierten Updates, indem ein Test in realer Umgebung auf einem limitierten Set an Testgeräten der Kontron AIS erfolgt

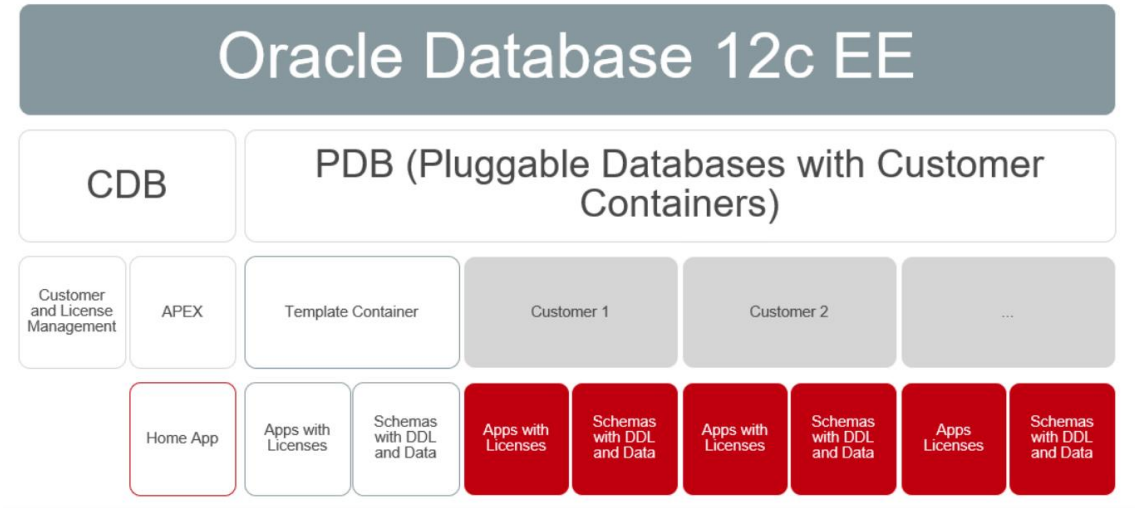


02 Datenbank

Aufbau Oracle Datenbank

Kontron AIS GmbH

- Jede Kunde erhält Zugriff auf eigene physische Datenbank (Plugable Database – PDB)
- Jede PDB besitzt getrennt verschlüsselte Daten-Dateien nach AES128 (Advanced Encyrption Standard) auf dem Datenbankserver in einem eigenen Kundenverzeichnis

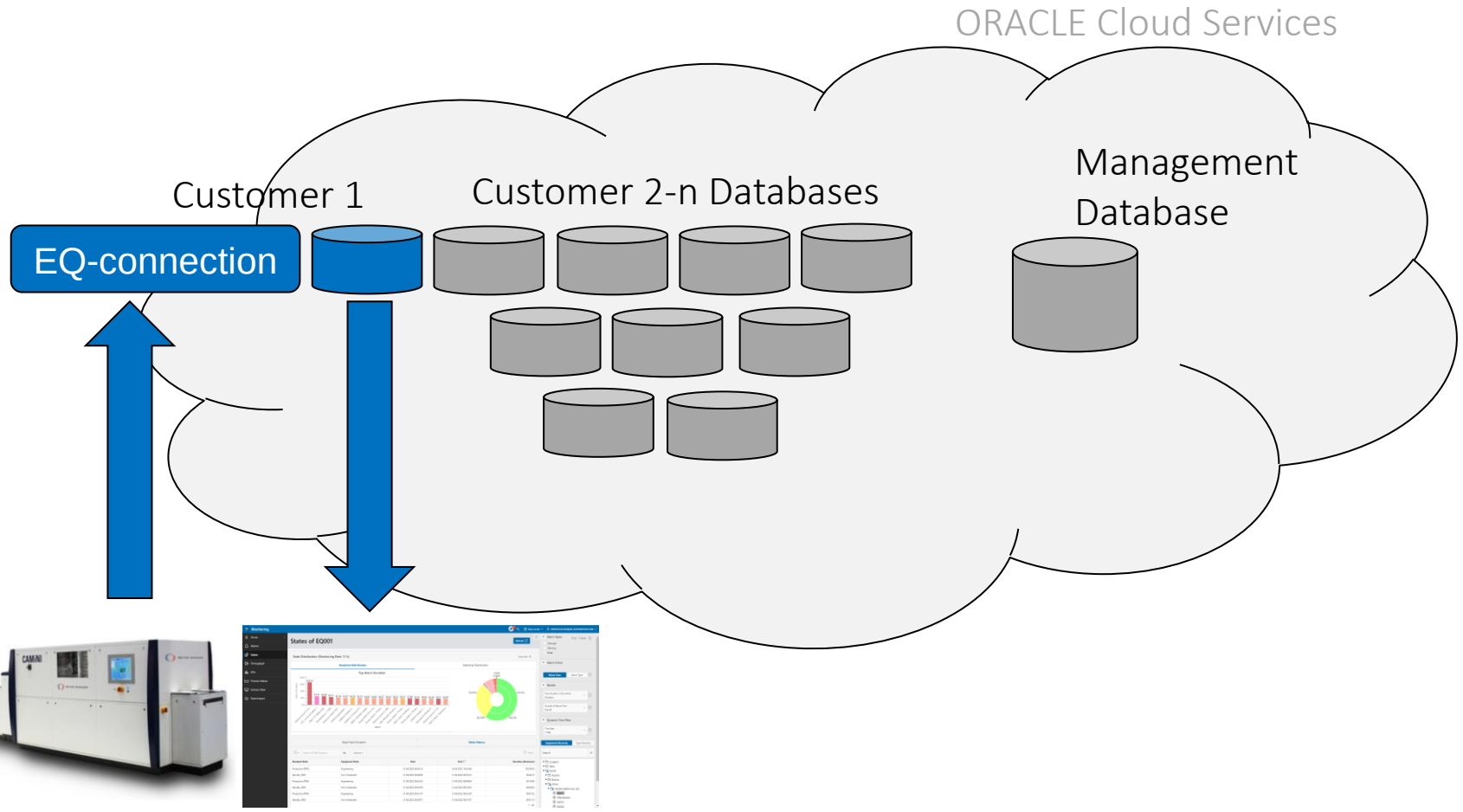


02 Datenbank

Physische getrennte Kundendatenbanken

Kontron AIS GmbH

Aufbau
Backend
Struktur

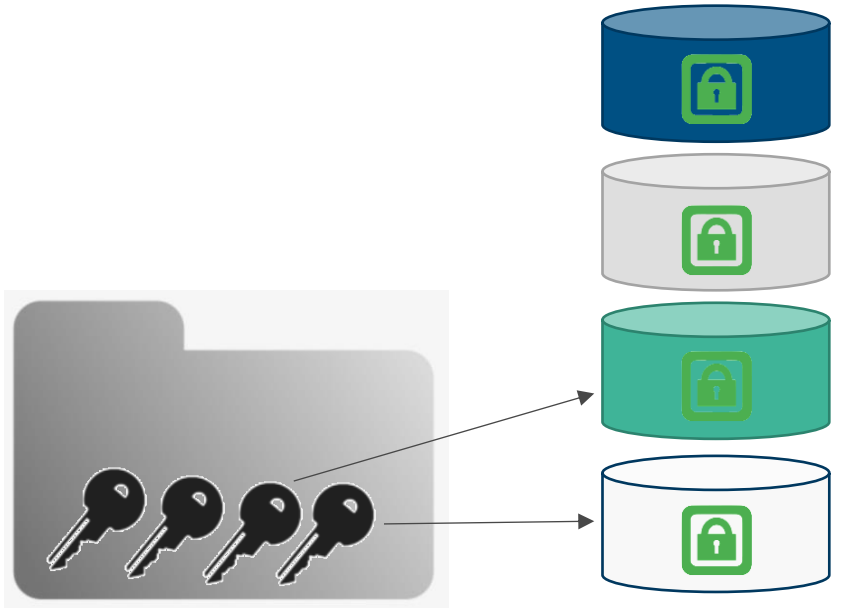


02 Datenbank

Verschlüsselte Datenbanken

Kontron AIS GmbH

- Kontron AIS erzeugt bei der Datenbank-Erstellung für jeden Kunden einen eigenen Schlüssel
- Jeder Kundencontainer ist einzeln gesichert
- Back Up der Kundencontainer sind separat verschlüsselt
- Niemand (außer Kontron AIS) kann die Datenbank lesen
- Schlüssel befindet sich außerhalb der Datenbank
- Im Storage sind nur „nutzlose“ Daten gespeichert
- Zugriff durch die Kontron AIS erfolgt ausschließlich auf Rückfrage oder Aufforderung des Kunden um
  - Daten zu entschlüsseln
  - Wiederherstellen des Backups
  - Unterstützung bei Problemen (Passwort Vergessen des Admins)
- Daten werden wie eine Blackbox behandelt



Key Wallet verwaltet die AIS

Kunden-Container verschlüsselt

kontron
The Power of IoT
Kontron AIS GmbH

“

Wie sicher sind die Maschinendaten in der Cloud?

”

kontron
The Power of IoT
Kontron AIS GmbH

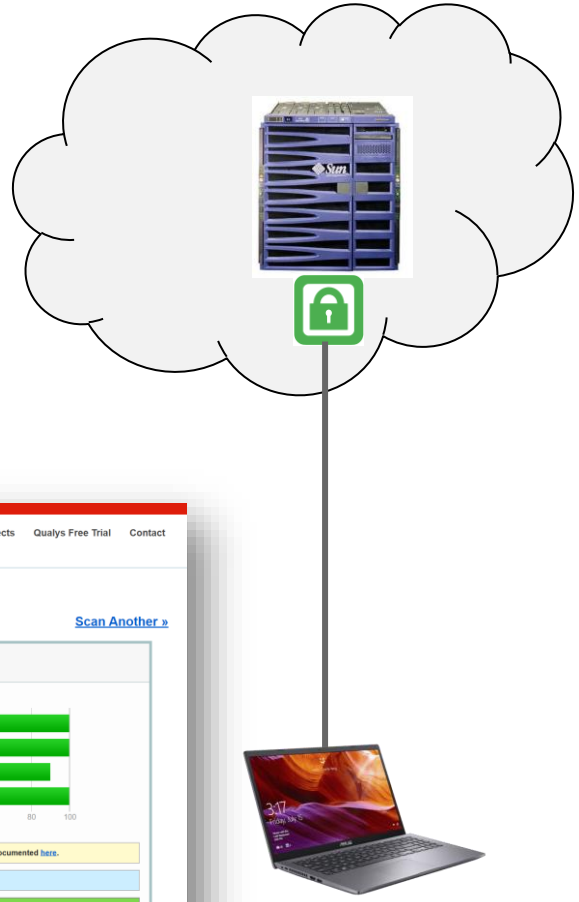
03
Sichere Kommunikation

03 Sichere Kommunikation

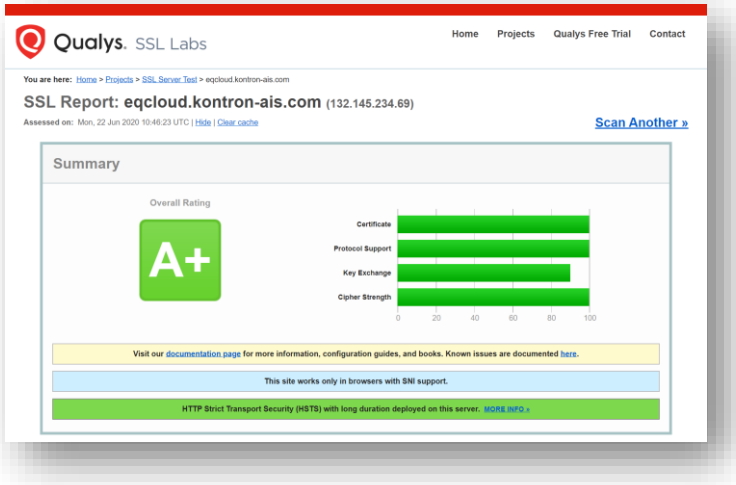
Kommunikation zur Cloud

kontron
The Power of IoT
Kontron AIS GmbH

- End-to-End-Verschlüsselung
- Jede Kommunikation zwischen Maschinen, Anlagen und IoT-Gateways ist per REST über Forward Secrecy (HTTPS – SSL/TLS 1.2, 2048 Bit) abgesichert
- Neuste Internetstandards, ähnlich des Onlinebankings und aktuellste Sicherheitsstandards (A+) werden angewendet
- Sicherheit gegen Datenklau



Testen Sie die Sicherheit des Frontend über einen Klick auf den SSL Report selbst

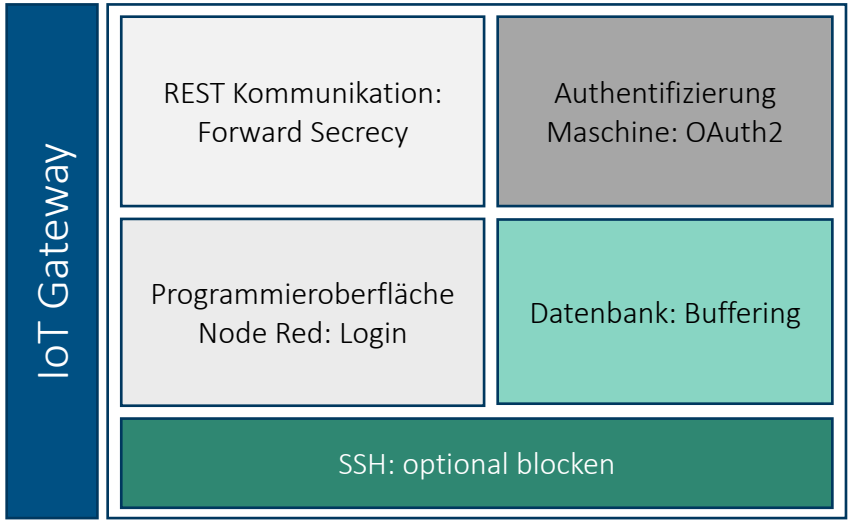


03 Sichere Kommunikation

Kommunikation der IoT Gateways zur Cloud

Kontron AIS GmbH

- Gleiche Sicherheitsstandards wie REST Kommunikation
- Authentifizierung erfolgt per OAuth2
- Bei Ausfall Internetverbindung puffert IoT Gateway Maschinendaten in einer lokalen Datenbank bis zur Wiederherstellung oder Erreichen der vorkonfigurierten Datenbankgröße
- Zugriff auf Programmieroberfläche nur per Login
- SSH (Secure Shell) Zugang zur Herstellung von sicheren Verbindungen zu anderen Netzwerken lässt sich optional blocken



03 Sichere Kommunikation

Kommunikation innerhalb der Cloud

kontron
The Power of IoT
Kontron AIS GmbH

- Potentielle Angriffsmöglichkeiten:
  - Cross-Site-Scripting
  - URL-Tampering
  - SQL-Injections

Etablierte Sicherheitsmaßnahmen:

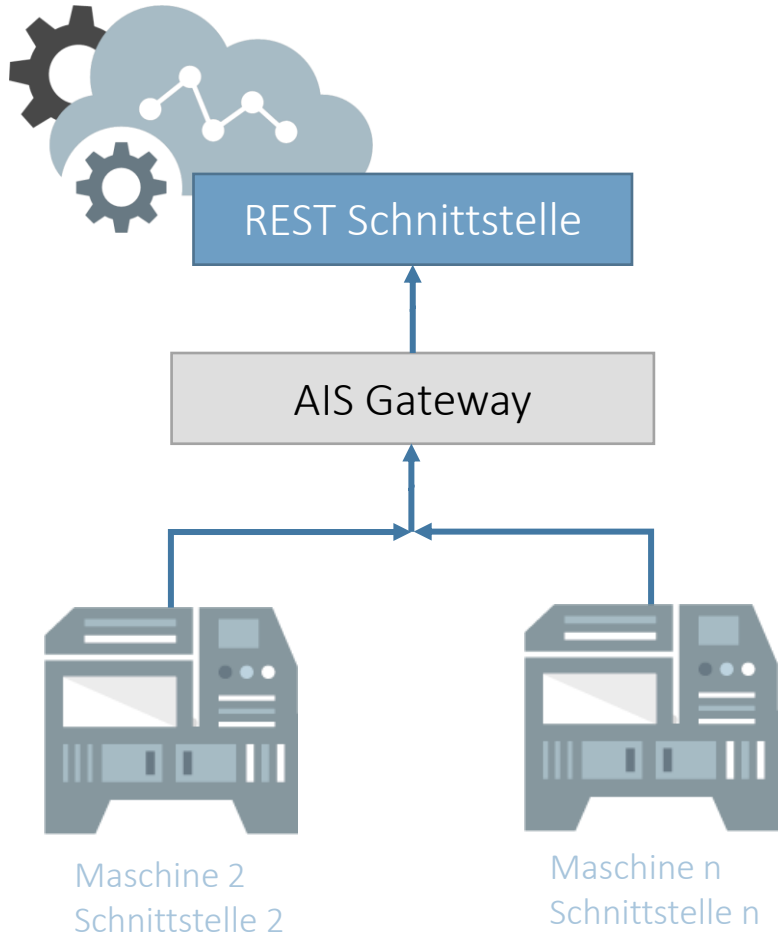
- Automatisierte Tests
- Escaping
- Whitelisting
- Serverseitige Validierung
- Statusautomation (Session State Protection)

03 Sichere Kommunikation

Sicherheit im Kundennetzwerk bei Einsatz von IoT-Gateways

Kontron AIS GmbH

- Keine Verbindungen von außen zu IoT-Gateway notwendig
- Keine aktive Portweiterleitung erforderlich
- Sämtliche ausgehende Ports (bis auf 443 für HTTPS) des am IoT-Gateway angeschlossenen Routers sind geschlossen oder können geblockt werden
- Konfiguration der Verbindung zu einer festgelegten, öffentlichen IP Adresse / Domain der EquipmentCloud®



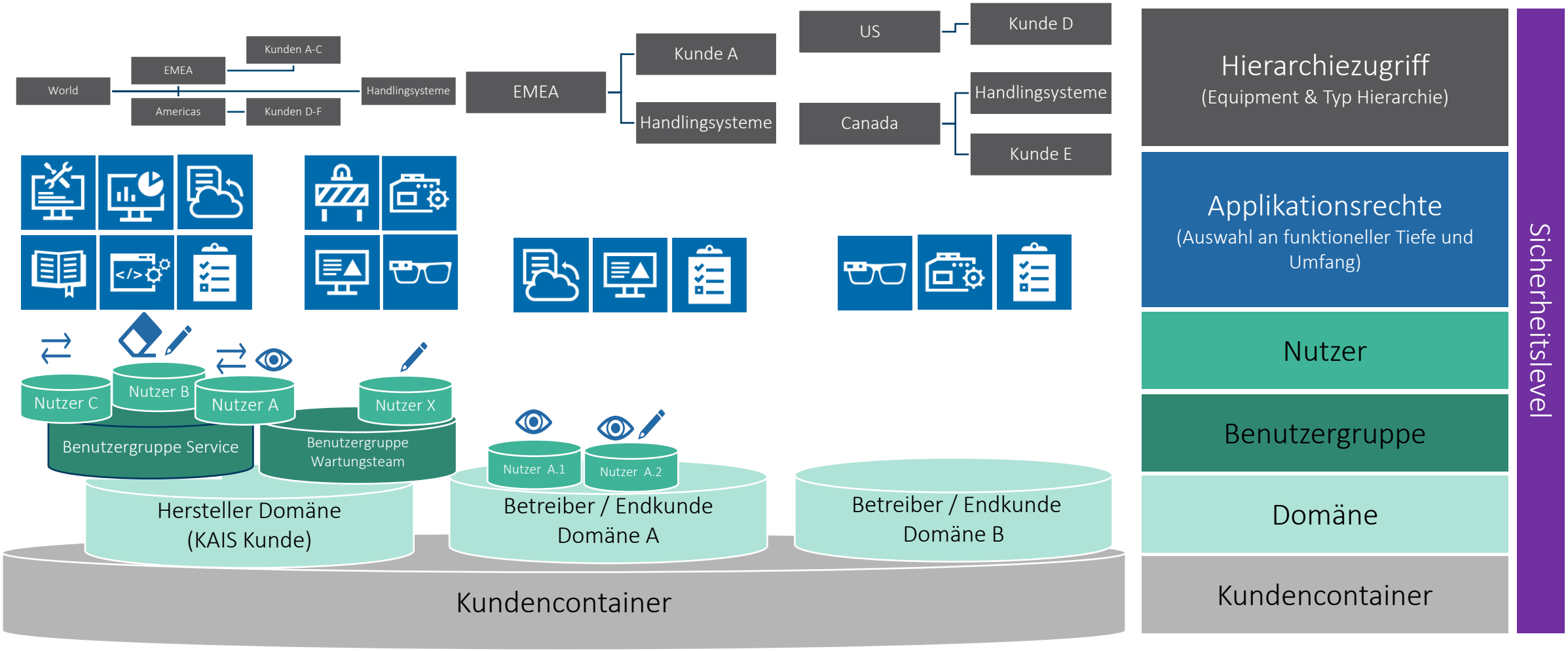
kontron
The Power of IoT
Kontron AIS GmbH

04
Nutzermanagement

04 Nutzermanagement

Überblick Rollen- und Berechtigungskonzept

Kontron AIS GmbH



04 Nutzermanagement

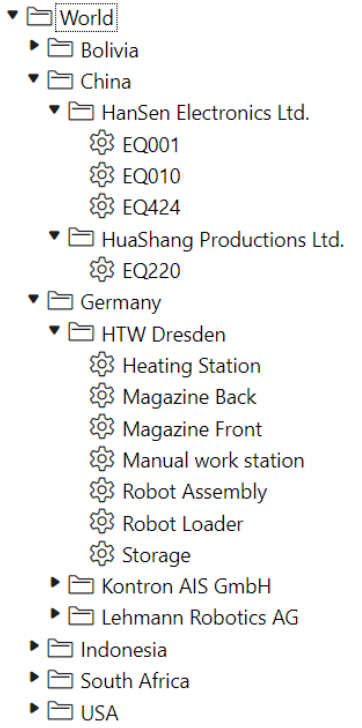
Rechtegesteuerter Zugriff

kontron
The Power of IoT
Kontron AIS GmbH

- Nutzerbezogene Sichtbarkeiten per Rechte geschützt
- Jeder Nutzer ist registriert
- Jeder Nutzer ist einer Domäne und / oder Benutzergruppe zugeordnet
- Jeder Nutzer hat einen spezifischen Rechte-Satz, dieser setzt sich zusammen aus:
  - Hierarchiezugriff (Typen und Equipments)
  - Applikationsrechten
  - Sichtbarkeitslevel
  - Standard-Dashboards
- Rechtesätze lassen sich an Unterdomänen vererben
- Benutzergruppen und zugehörige Rechtesätze lassen sich auf neue Benutzer kopieren
- Alle Abfragen nutzen den konfigurierten Rechtesatz
- Schutz bis hin zur API gegeben

Hierarchiezugriff

Nutzer 1



Nutzer 2

04 Nutzermanagement

Applikationsrechte

kontron
The Power of IoT
Kontron AIS GmbH

- Nutzern oder Benutzergruppen kann ein bestimmter Umfang von Applikationsrechten zugewiesen werden

- Die Applikationsumfang kann sich aus folgenden Modulen* zusammensetzen:
  - Basis Module: eDocs / EquipmentHub / OpenIssues / Workflows / Maintenance / SpareParts / Monitoring / SoftwareCenter / KnowledgeBase
  - Zusatz Module: RemoteAssistance / SpareParts Pro / DeviceManagement
  - Administration: Nutzer Management / Equipment Konfiguration / Global

- Die Applikationstiefe kann je App variieren:
  - Leserechte: Login & Anzeigen
  - Bearbeitungsrechte: Editieren & Durchführen & Ausfüllen & Downloaden & Beenden
  - Administrationsrechte: Erstellen & Definieren & Verwalten & Löschen

* Voraussetzung dafür sind gültige Lizenzen

04 Nutzermanagement

Applikationsrechte KontronGrid

Kontron AIS GmbH

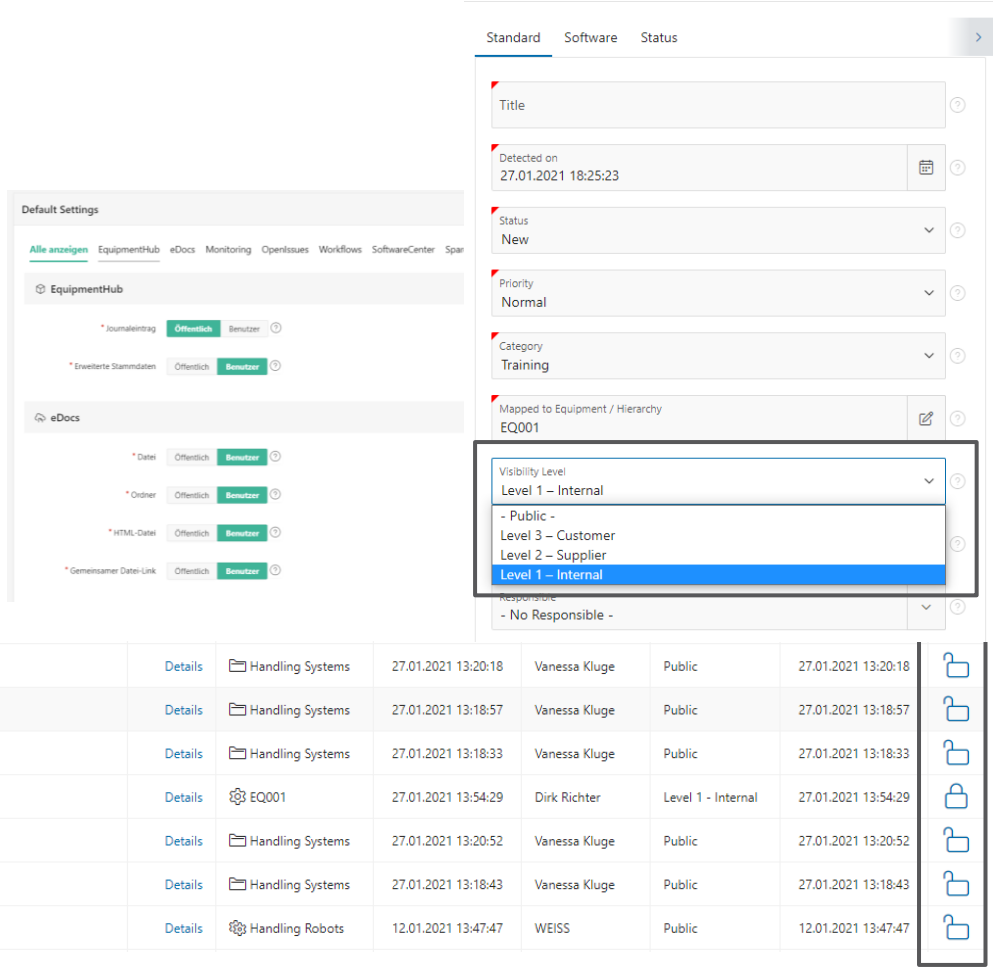
- Benutzer-verwaltung
  - Benutzer
    - Erstellen
    - Bearbeiten
  - Benutzergruppen
    - Erstellen
    - Bearbeiten
- Equipment Konfiguration
  - Hierarchien
    - Erstellen
    - Bearbeiten
    - Löschen
  - Equipment
    - Erstellen
    - Bearbeiten
    - Löschen
  - Equipment-Typen
    - Erstellen
    - Bearbeiten
    - Löschen
- Global
  - Eigenes Dashboard erstellen
  - Öffentliche Berichte festlegen
  - Standard-Dashboards festlegen
  - Branding, Sichtbarkeitslevel, Fähigkeiten und erweiterte Stammdaten administrieren
  - Globale Benachrichtigungen verwalten
  - Bearbeiten von zugeordneten Objekten
  - Feeds verwalten
  - Artikel verwalten
- DeviceManagement
  - Anmelden
  - Container starten und stoppen
  - Container verwalten
  - Fernzugriff aufbauen
  - VPN-Verbindung herstellen
  - KontronOS managen
  - Geräte verwalten
  - Equipment Beziehungen verwalten
  - Download Images
  - Images verwalten

04 Nutzermanagement

Zeilenweise Sichtbarkeit

kontron
The Power of IoT
Kontron AIS GmbH

- Sichtbarkeitslevel werden Domänen zugeordnet und an jeweilige Benutzer vererbt
- Sicherbarkeitslevel lassen sich individuell konfigurieren: Name und Anzahl:
  - z.B. Extern, Intern, Öffentlich
- Es können zwei Default Sichtbarkeitslevel für Modul-Daten definiert werden:
  - Öffentlich oder
  - Benutzerbezogen
- Sichtbarkeitslevel für folgende Modul-Daten definiert werden:
  - EquipmentHub: Journaleinträge, Erweiterte Stammdaten
  - eDocs: Datei, Ordner, HTML-Datei
  - OpenIssues: Issue, Kommentar
  - Monitoring: Profil
  - Workflows: Workflows, Phase, Checkliste
  - SoftwareCenter: Freigabe
  - SpareParts: Katalog, Stammdaten
  - SpareParts Pro: Stammdaten
  - KnowledgeBase: Themen



kontron
The Power of IoT
Kontron AIS GmbH

05

Datensicherheit & -Qualität

05 Datensicherheit & -Qualität

Datenschutz & externe Dienste

kontron
The Power of IoT
Kontron AIS GmbH

- Datenverarbeitung erfolgt DS-GVO konform
- Datenspeicherung erfolgt in Deutschland auf Servern von Oracle
- Das Geschäftsmodell der EquipmentCloud® und des bereitgestellten Service besteht **nicht** in der Analyse und Weiterverarbeitung der Nutzerdaten
- Die ORACLE Cloud Infrastructure dient der Bereitstellung der EquipmentCloud®-Infrastruktur
- ORACLE Maps wird zur Visualisierung von Standorten von Maschinen genutzt*
- Google Firebase Cloud Messaging wird zum Senden von Push Nachrichten eingesetzt*
- Google ReCaptcha dient der Nutzerauthentifizierung beim Einloggen und Registrieren*
- Deepl API dient der automatisierte Übersetzung von GUI und Nutzertexten*

*Externe Dienste: auf Wunsch deaktivierbar

05 Datensicherheit & -Qualität

Passwortrichtlinie und Multifaktor-Authentifizierung

kontron
The Power of IoT
Kontron AIS GmbH

- Passwortrichtline laut IT-Durchführungskonzept
  - 12 Zeichen (Großbuchstaben, Kleinbuchstaben und Zahl sind verpflichtend)
  - Sonderzeichen optional
  - 5 maximale Versuche, dann wird Zugang gesperrt
  - Gültigkeit Passwort 180 Tage (aktuell so zentral festgelegt)
- Identitätsprovider Integration auf Domänenebene
  - Dient des einfachen und sicheren Logins von Nutzern sowie der erleichterten Zugangsverwaltung von Administratoren
  - Ermöglicht die Einbindung von multiplen Identitätsanbietern (z.B. Azure AD) auf verschiedenen Domänenebenen
  - Single-Sign-On und Multi-Faktor-Authentifizierung kann von Administratoren erzwungen warden
  - MFA mittels beliebiger Authentifizierung App
  - Nutzbar für Web und native App

05 Datensicherheit & -Qualität

ISO-Zertifizierungen Kontron AIS

kontron
The Power of IoT
Kontron AIS GmbH

- ISO/IEC 27001:2017: DE / EN (2024)
- TISAX Zertifizierung auf Anfrage erhältlich
- Entwicklung von Software als ein Service in der Cloud
- Anwendbarkeitserklärung auf Anfrage erhältlich

05 Datensicherheit & -Qualität

ISO-Zertifizierungen Oracle

Kontron AIS GmbH

- **ISO/IEC 27001:2013**
- Services basierend auf der Oracle Cloud Infrastructure (OCI)
- Zertifikat auf Anfrage erhältlich

- **ISO/IEC 27018:2019**
- Schutz personenbezogener Daten in öffentlichen Cloud-Diensten als Auftragsdatenverarbeitung für die Oracle Cloud Infrastructure
- Zertifikat auf Anfrage erhältlich

- **ISO/IEC 27017:2015**
- Oracle Cloud Infrastructure – Classic (OCI-C) als Infrastructure as a Service & Platform as a Service
- Zertifikat auf Anfrage erhältlich

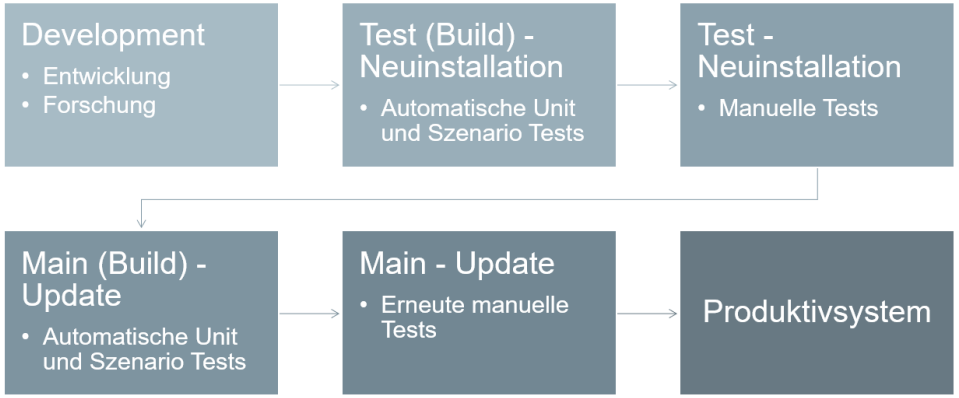
- **ISO/IEC 20000-1:2018**
- Zertifikat auf Anfrage erhältlich

05 Datensicherheit & -Qualität

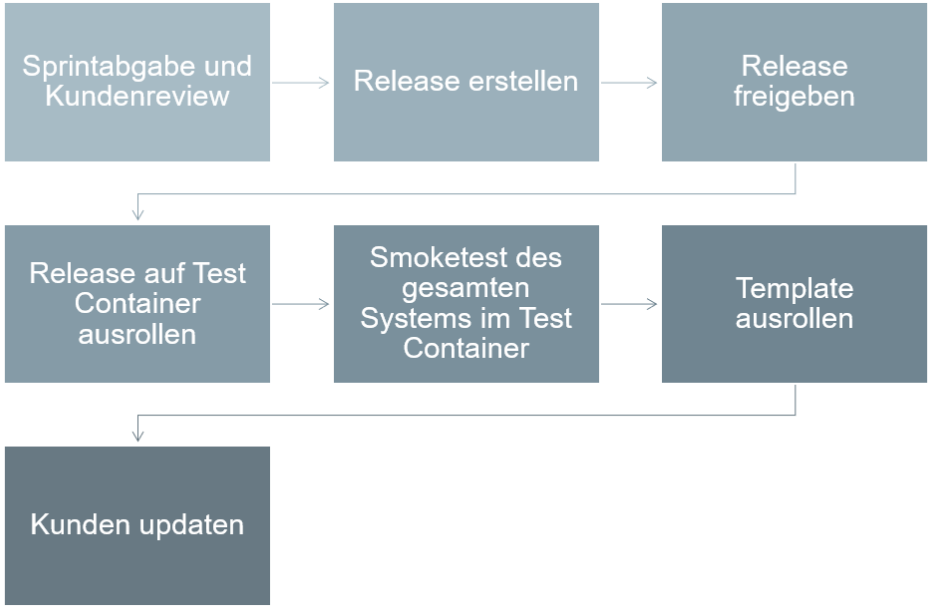
Entwicklungs- und Rolloutprozess

Kontron AIS GmbH

› Entwicklungsprozess



› Rolloutprozess

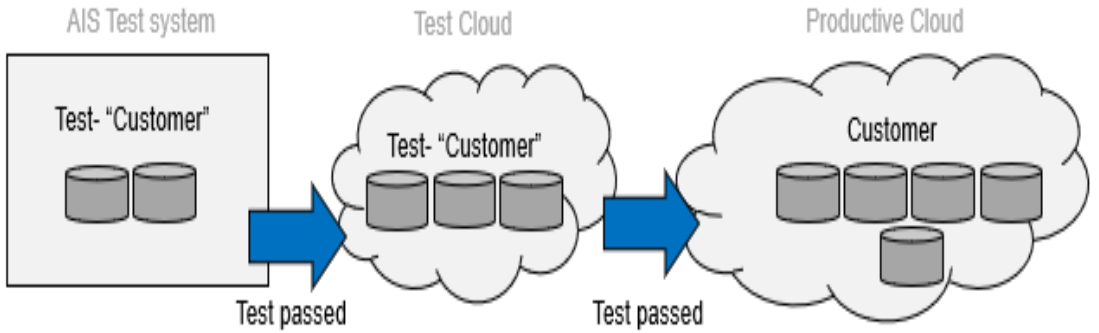


05 Datensicherheit & -Qualität

Agile Produktentwicklung

kontron
The Power of IoT
Kontron AIS GmbH

- Erfolg durch das gelebte Projekt- und Produktmanagement nach SCRUM
- Rapid Development für neue Features (APEX Entwicklungsumgebung)
- Automatisierte Build-Prozesse (Continuous Integration) sorgen für kurze Entwicklungszyklen
- Automatisiertes Testen ermöglicht eine Version innerhalb des kurzen Entwicklungszyklus von zwei Wochen fertigzustellen



05 Datensicherheit & -Qualität

Agile Operationen

kontron
The Power of IoT
Kontron AIS GmbH

- Skriptbasierte Infrastruktur ermöglicht schnell auf Änderungen und Anforderungen zu reagieren
- Regressionstests / Integrationstests mit Risikobewertung (Szenarientests)
- Automatisierter Rollout neuer Versionen auf allen Staging-Systemen (Testserver, Spiegelsystem, Produktivsystem) erfolgt schrittweise nach erfolgreichen Tests auf jedem System
  - Codierte Infrastruktur
  - Skript Konfiguration auf Team Foundation Server (TFS)
  - Paralleles Ausrollen auf multiplen Servern
  - Verfolgung und Registrierung jedes Updates
  - komplette Übersicht über installierte Versionen in jedem Server
  - Freigabe-Prozess nach Vier-Augen-Prinzip (*auch HotFixes)*
- Performance- und Trendanalyse sowie Überwachung von Systemparametern zur Vermeidung von Unterbrechungen des produktiven Systems bei Rollout oder während des Betriebs
- Monitoringsystem Nagios:
  - Datenbank bezogen: CPU Auslastung, Speicherauslastung (Arbeitsspeicher, für Stabilität auschlaggebend), Festplattenüberwachung (Verfügbarkeit)
  - Security Checks: SSL Labs – Verschlüsselungsalgorithmen werden getestet, damit diese nicht kompromittiert sind (alle 3 Wochen)

Kontron AIS GmbH

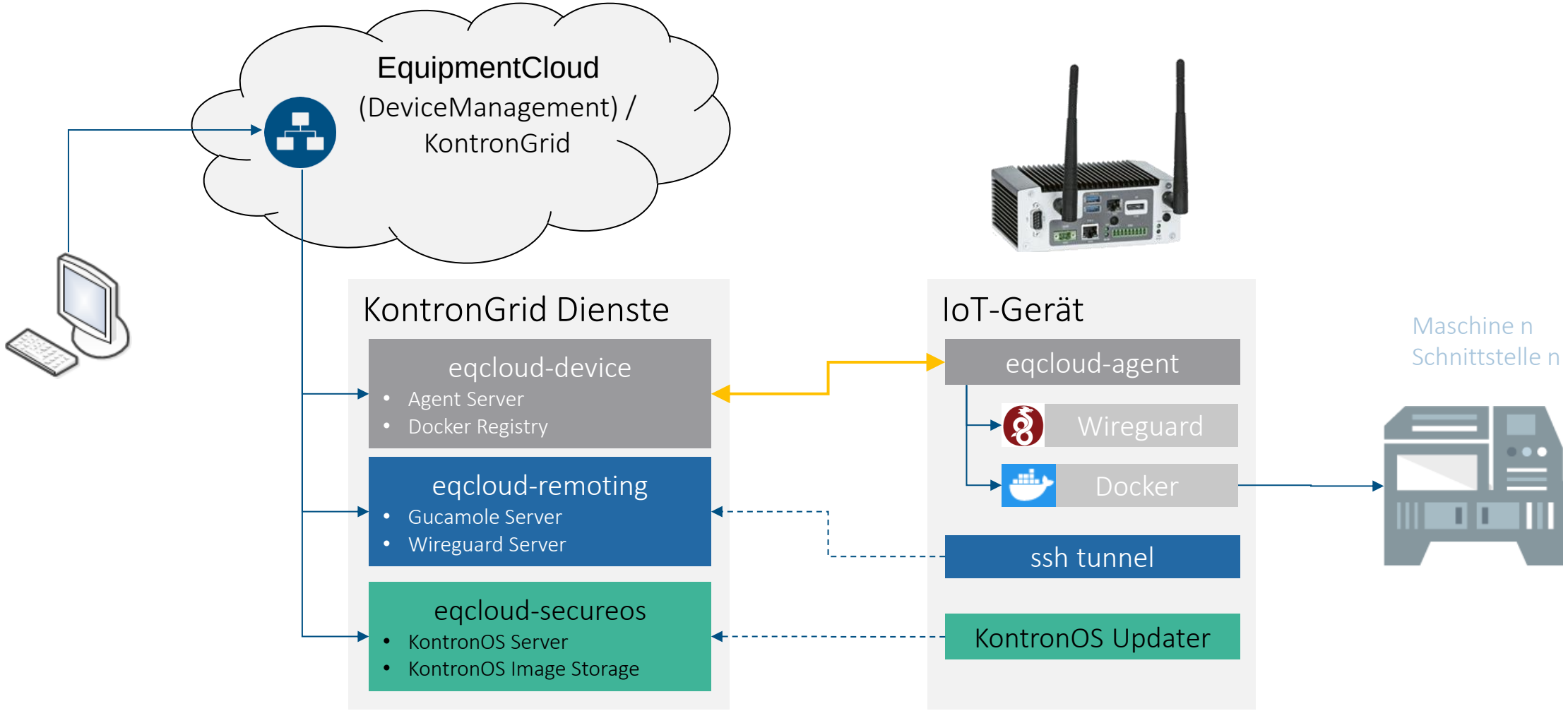
06

KontronGrid Dienste

06 KontronGrid Dienste

Überblick

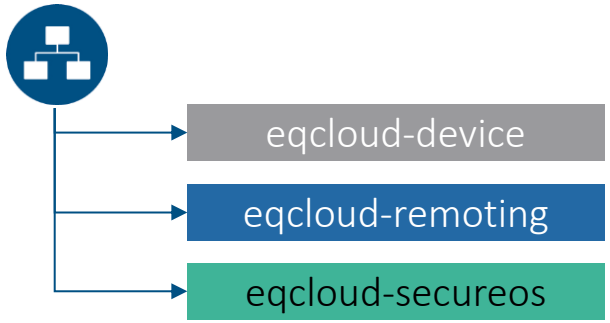
Kontron AIS GmbH

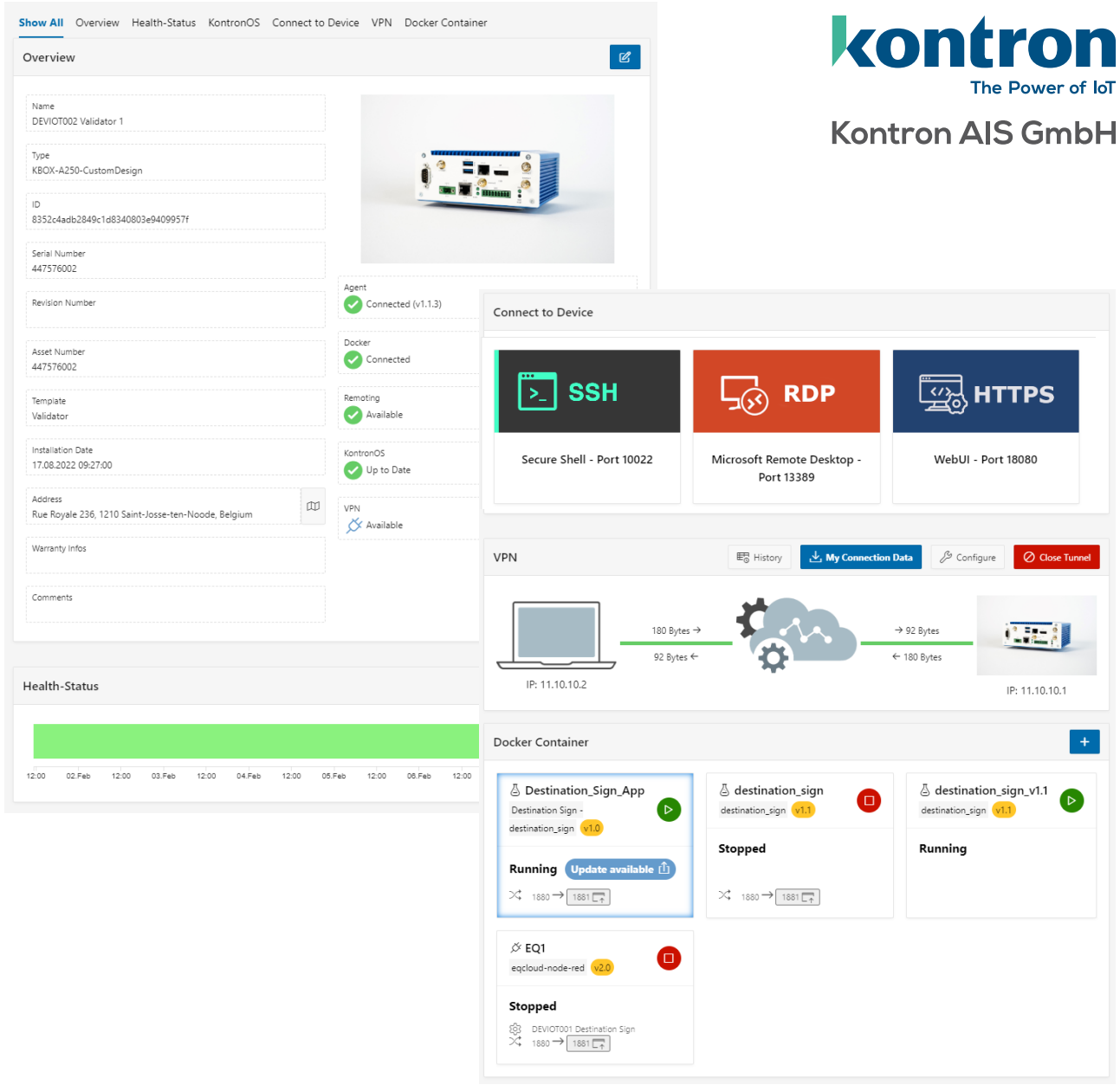


06 KontronGrid Dienste

DeviceManagement Modul

- Jeder Nutzer ist registriert
- Granulare Zuordnung von Applikationsrechten
  - Benutzergruppen/ Domänen
  - Hierarchisches Gerätemanagement
  - Separate Rechte für jeden Funktion (e.g. VPN, Docker, etc.)
- Server zu Server basierte Kommunikation
  - Cloud interne REST Calls
  - SSL geschützt
  - Zugangsauthentifizierung für jeden Service



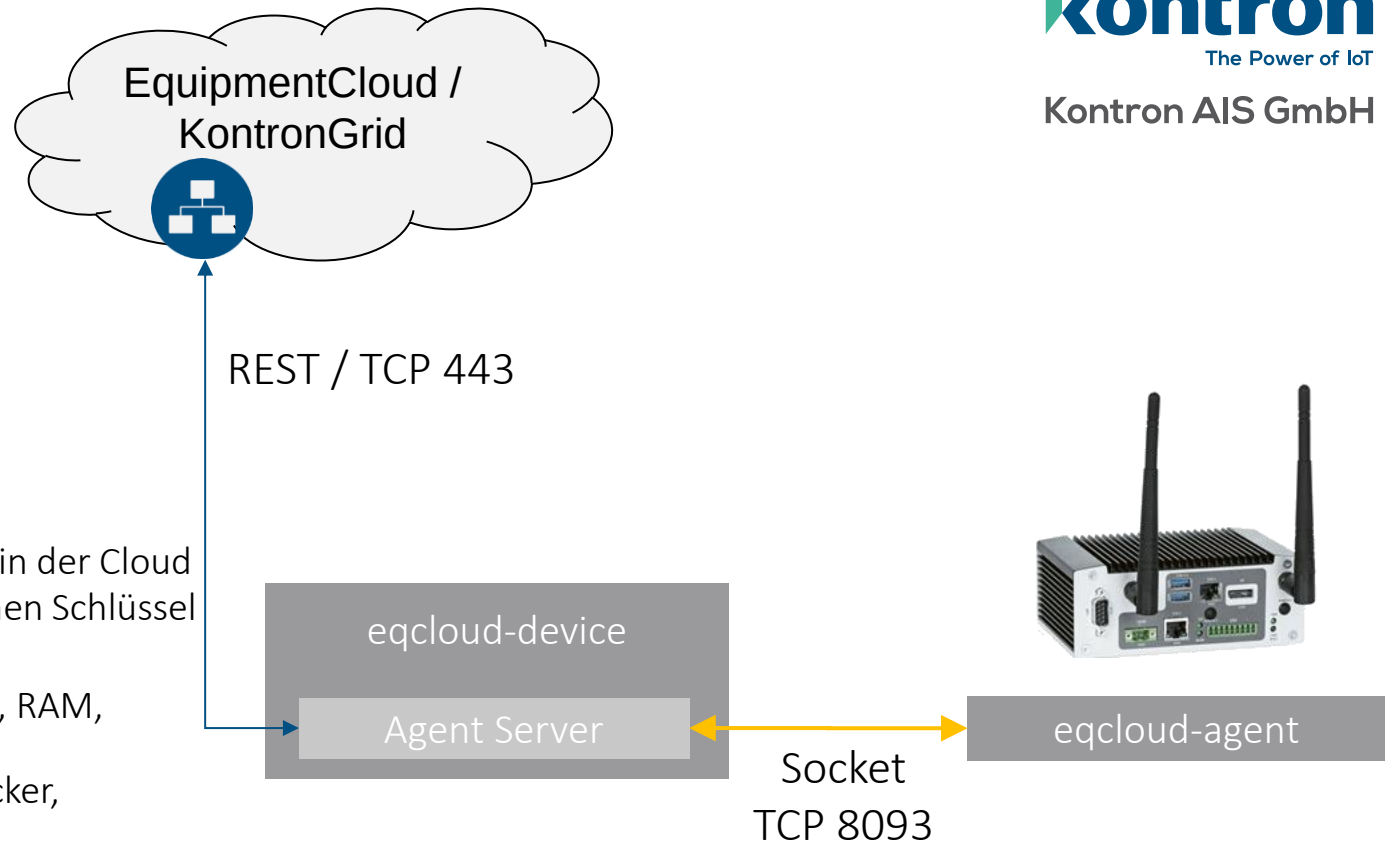


kontron
The Power of IoT
Kontron AIS GmbH

06 KontronGrid Dienste

Geräte Agent

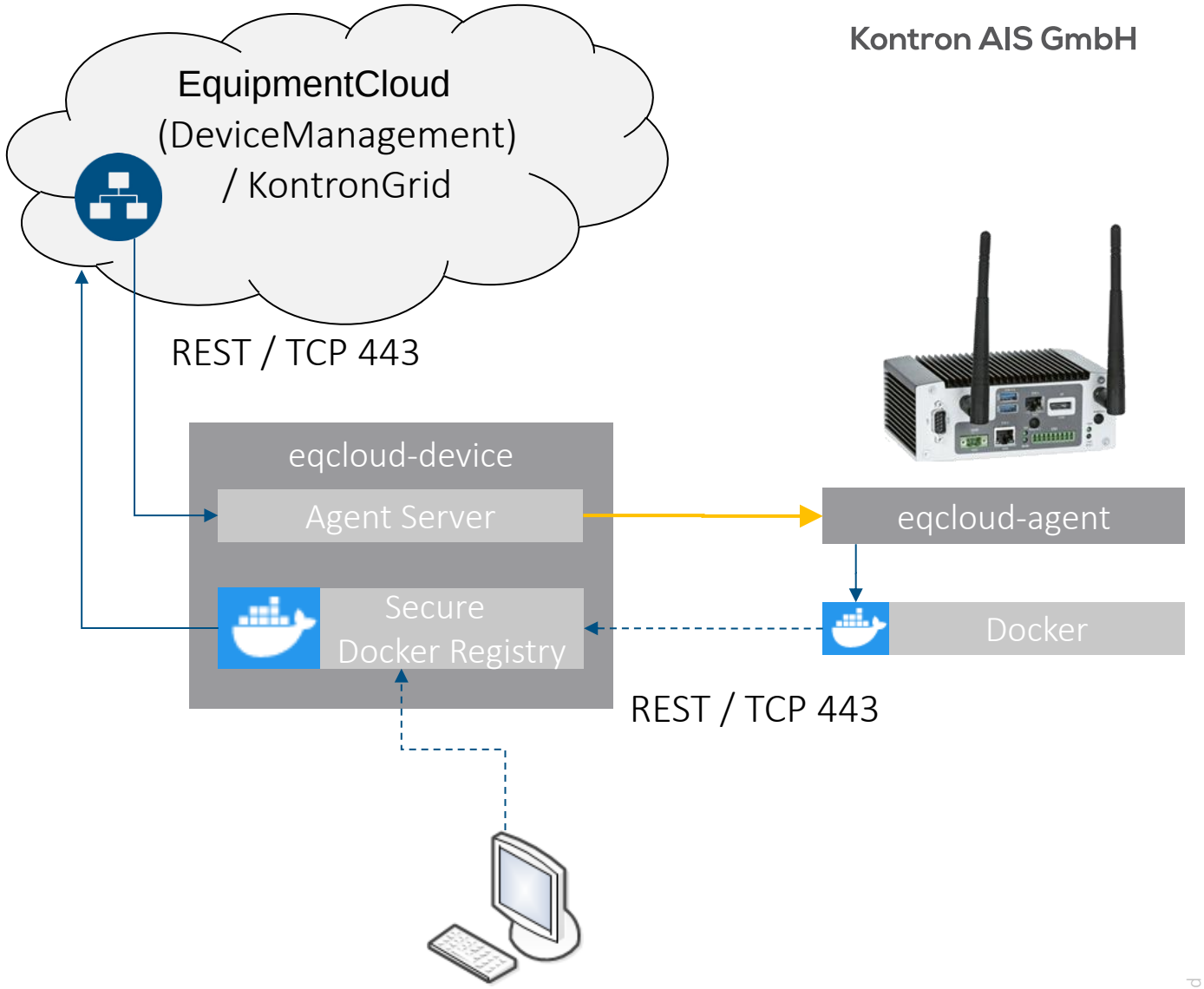
- Socket basierte Kommunikation
  - Framework socket.io
  - Proprietäres Protokoll
  - SSL geschützt
  - Automatische Verbindungsaufbau nach Verbindungsunterbrechnung
  - Geräte Authentifizierung
  - Agent Server überprüft Authorisierung des Geräts in der Cloud
  - SSL / Zugans Authentifizierung mit Gerätespezfischen Schlüssel
- Agent Funktionen
  - Zyklisches Monitoring des Gesundheitsstatus (CPU, RAM, Storage, etc.)
  - Fernsteuerung von optionalen Funktionen wie Docker, Wireguard, Systemneustart usw.



06 KontronGrid Dienste

Docker

- Fernsteuerung von Docker Containern
  - Befehle werden indirekt über den Agent Server und eqcloud-agent ausgeführt
  - Benutzer benötigt Zugriff auf Gerät im DeviceManagement-Modul + Docker verwalten Recht
  - Optionale Unterstützung von Docker Compose
  - Bulk-Rollout von Updates
- Docker Registry
  - Trennung von Images zwischen Kunden
  - Gerät zieht Images aus der Registry
  - SSL-geschützt
  - Registry prüft Autorisierung des Geräts UND des angeforderten Images in der EquipmentCloud
  - Registry prüft Autorisierung der Nutzer beim Push eines Images (z.B. Integration von Build-Pipelines)

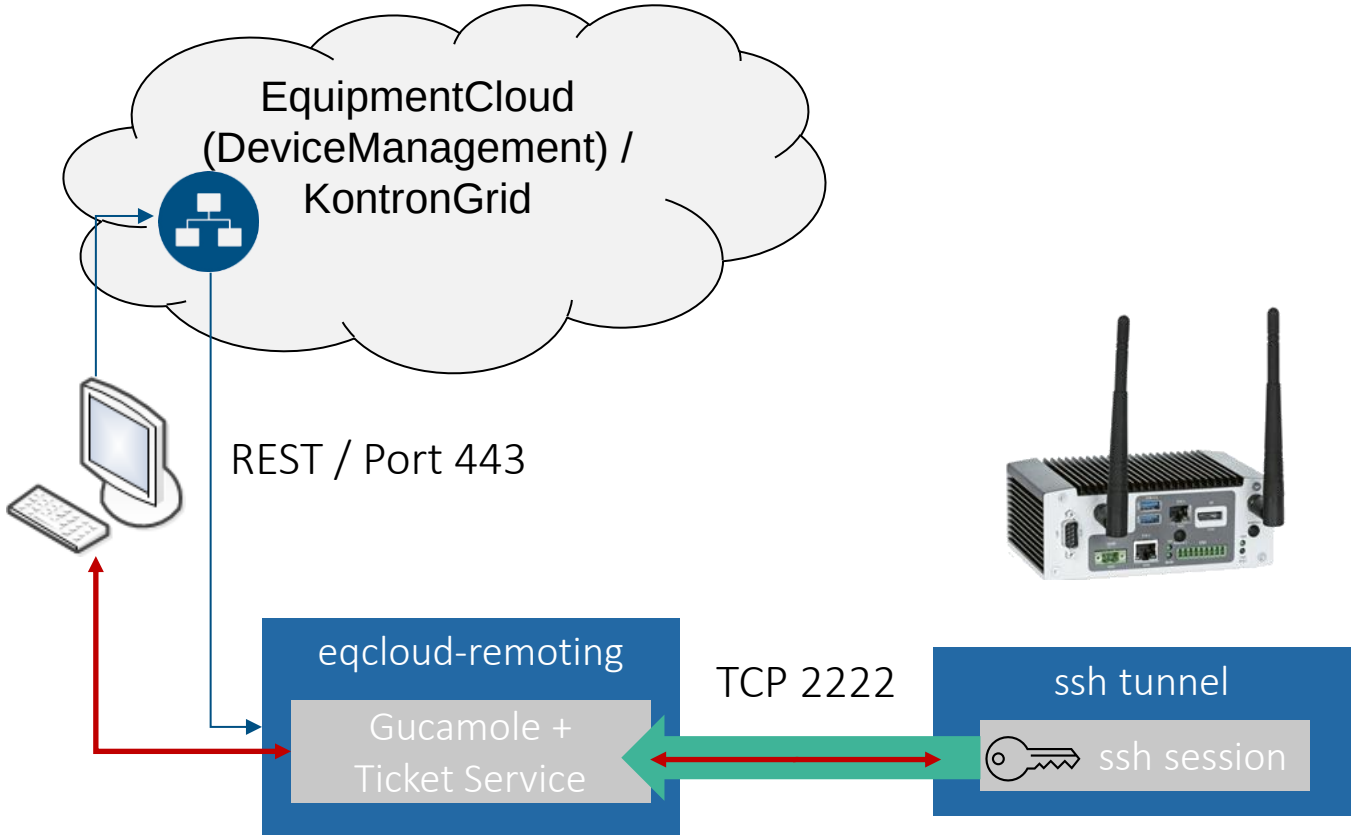


06 KontronGrid Dienste

Remoting

Kontron AIS GmbH

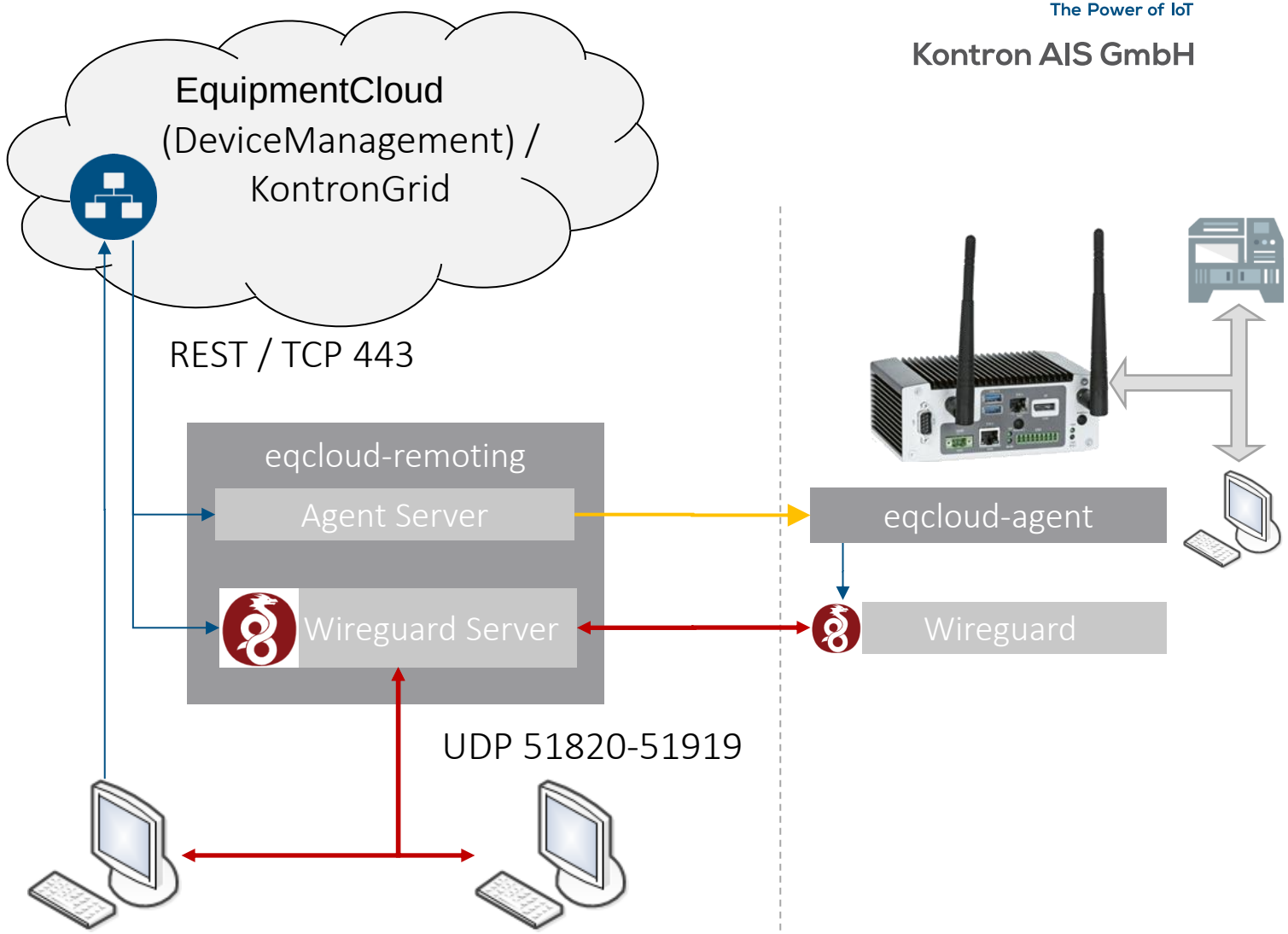
- Browser basierte SSH und RDP Sitzungen
  - Benutzer fordert Verbindung über DeviceManagement an
  - Interner Ticketdienst zum Schutz der Browsersitzung
- Zweistufige Authentifizierung
  - Benutzer benötigt Zugriff auf das Gerät im DeviceManagement-Modul + Fernzugriff-Aufbauen-Recht
  - Benutzer benötigt lokale Anmeldedaten für das Gerät
- Gerät baut einen ssh-Tunnel zum Remoting-Server auf
  - RSA 2048bit Schlüssel
  - Server prüft Berechtigung
  - Strikte Trennung der einzelnen Geräte



06 KontronGrid Dienste

VPN

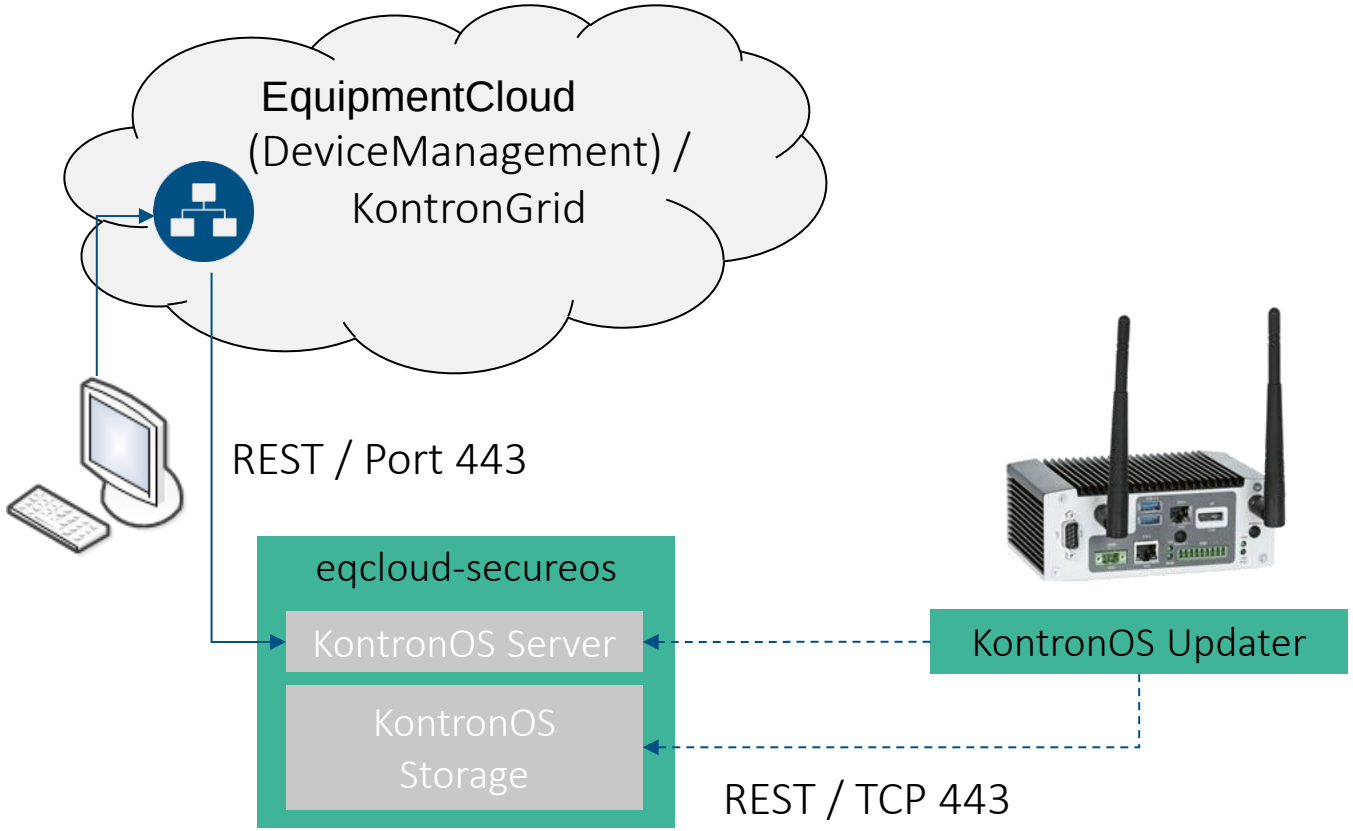
- Basierend auf Wireguard
  - State-of-the-Art Kryptographie (Curve25519, ChaCha20, Poly1305, BLAKE2, SipHash24, HKDF)
  - Befehle zum Auf- und Abbau der Verbindung werden indirekt über den Agent Server und den eqcloud-Agent ausgeführt
  - Benutzer benötigt Zugriff auf Gerät im DeviceManagement-Modul + VPN-Verbindung-Herstellen-Recht
  - Strikte Trennung der einzelnen Geräte
- Optionales Tunneling ins Kundennetzwerk
- Automatisches Beenden von ungenutzten Verbindungen
- Unterstützung von gleichzeitigen Multi-Client Verbindungen auf ein Gerät



06 KontronGrid Dienste

KontronOS Update Server

- Zyklische passive Prüfung auf Updates durch das Gerät
  - SSL geschützt
  - Authentifzierung des Zugriffs
- Zielversion wird vom Benutzer festgelegt
  - Benutzer benötigt Zugriff auf Gerät im DeviceManagement Modul + KontronOS-Managen-Recht
- Verwaltung der verfügbaren KontronOS Images durch Kontron AIS
- Freigabe einer Version kann kundenindividuell gesteuert werden
- Roadmap-Funktion:
  - Aktive Auslösung und Überwachung eines Updates durch den eqcloud-Agenten

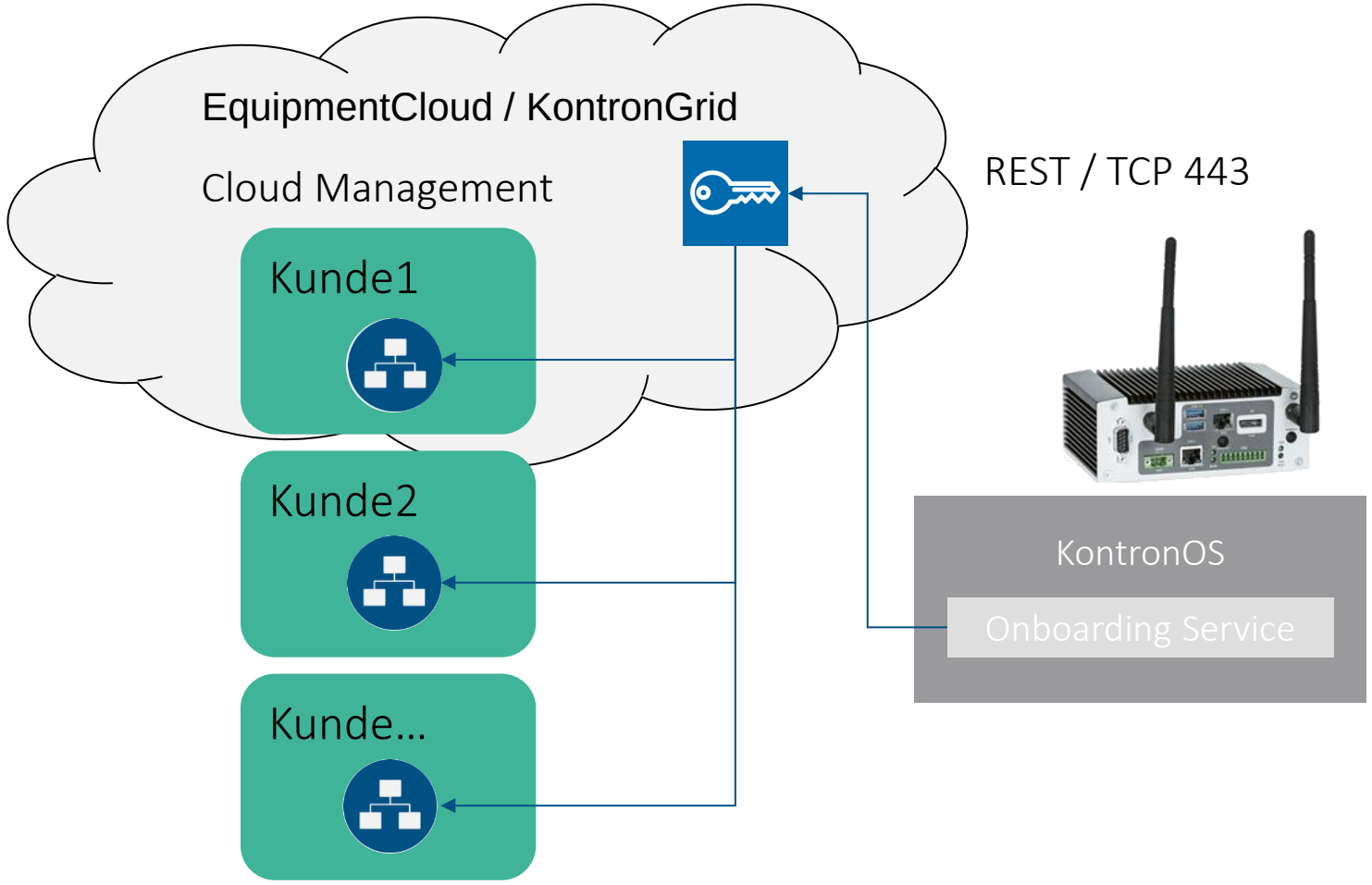


06 KontronGrid Dienste

Onboarding – Aktuelle Lösung mit KontronOS

kontron
The Power of IoT
Kontron AIS GmbH

- In der Regel Vorinstallation durch Kontron AIS Mitarbeiter
  - Gerät erstellt neuen Schlüssel (RSA 2048bit)
  - Gerät sendet Schlüssel an Cloud Management Service (CMS)
- Anmeldeinformationen zur Authentifizierung
  - CMS entscheidet anhand Profilinformationen, welchem Kunden das Gerät zugewiesen wird
- Varianten
  - Standard-Image: Gerät ist einem Sammelcontainer zugeordnet und wird von Kontron AIS Mitarbeitern manuell zum richtigen Kunden verschoben
  - Kundenspezifisches Image: Individuelle Profilinformation identifiziert den Kunden eindeutig

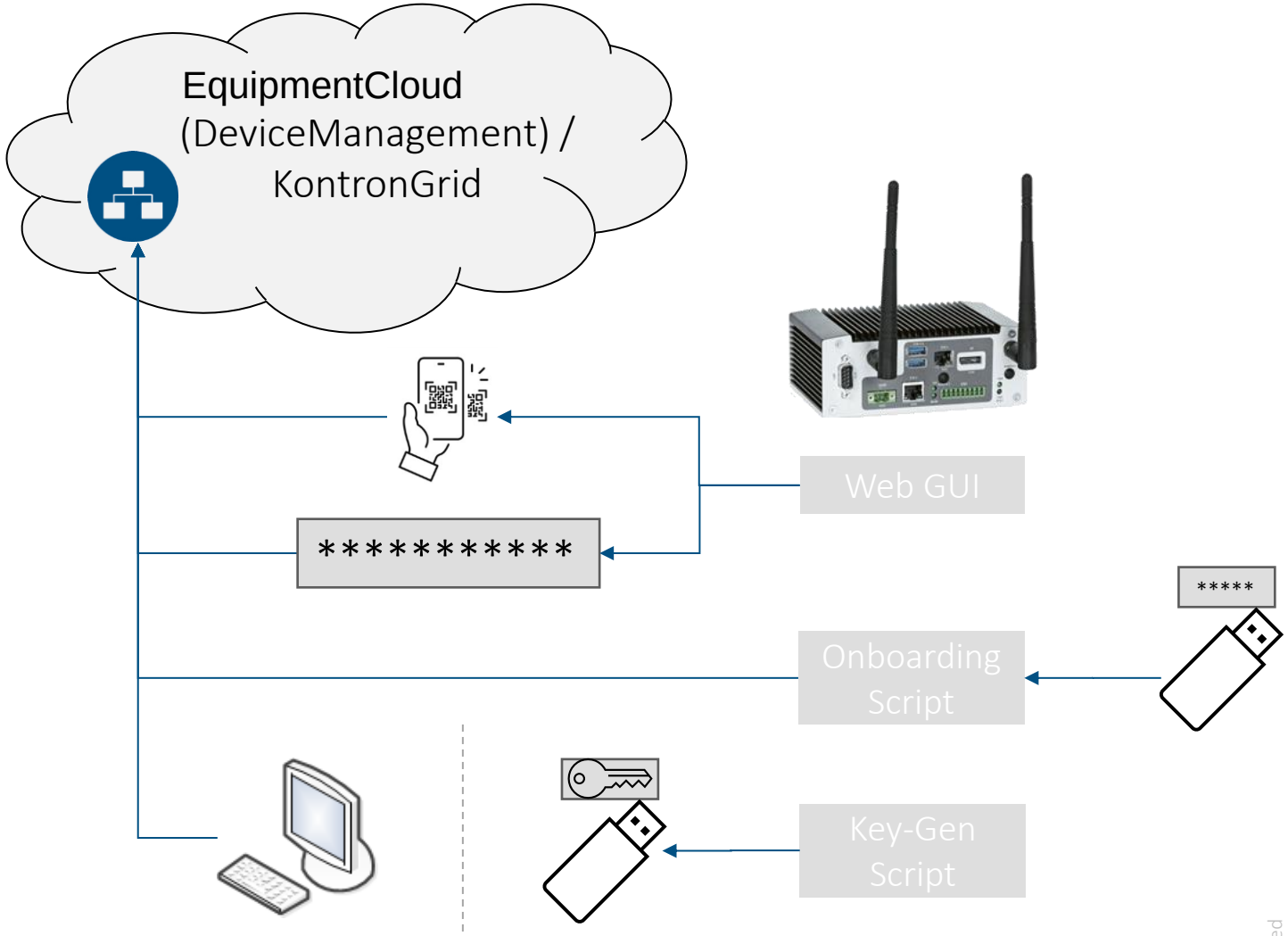


06 KontronGrid Dienste

Roadmap Funktion - Onboarding vom Kunden

Kontron AIS GmbH

- Geräte, die einem Kunden vor der Auslieferung nicht zugewiesen werden können
- Benutzer benötigt Zugriff im DeviceManagement-Modul + Onboarding-Durchführen-Recht
- Mögliche Varianten
  - Erweiterung der Web GUI des KontronOS
    1. Benutzerauthentifizierung mit Kundennummer
    2. QR-Code mit der mobilen App von EquipmentCloud scannen
  - Per USB Stick (automatische Ausführung eines Skripts wenn angesteckt)
    3. Online: Auf einem USB-Stick gespeicherte Benutzeranmeldeinformationen werden von einem Onboarding-Skript verwendet
    4. Offline: Generierter Schlüssel wird auf einem USB-Stick gespeichert, der dann vom Benutzer in DeviceManagement importiert werden kann



kontron
The Power of IoT
Kontron AIS GmbH

Contact

Martin Falsner | Sales Manager
Martin.Falsner@kontron-ais.com

Kontron AIS GmbH
Otto-Mohr-Straße 6
01237 Dresden
www.kontron-ais.com

kontron

The Power of IoT

Kontron AIS GmbH