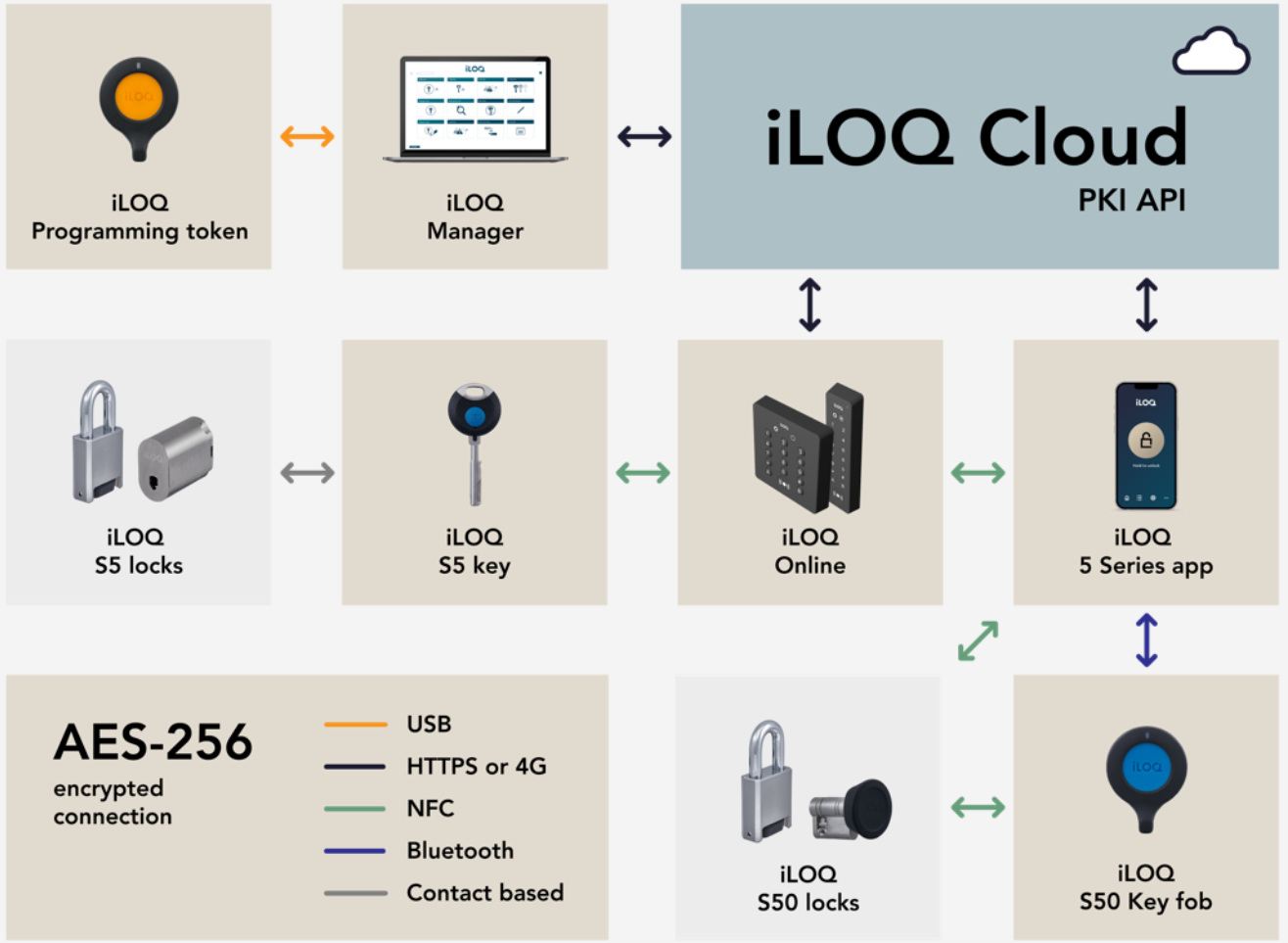
iLOQ

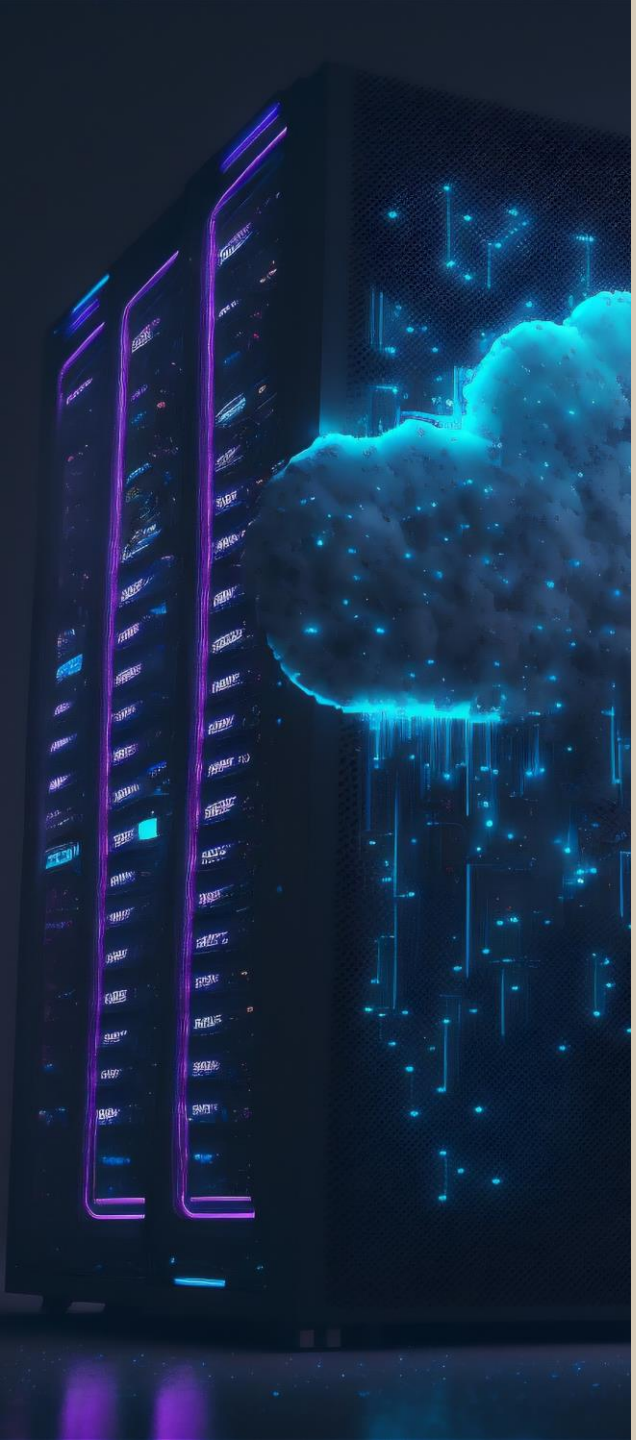
Life made limitless.

Sicherheit & Zertifikate

State-of-the-art Sicherheit/ Systemübersicht

- **AES-256 Verschlüsselung** über alle Komponenten und Kommunikationswege hinweg
- Komponenten **sicher** mittels Programmier-Token programmiert
- Zugangsrechte **immer auf dem neuesten Stand**
- Zugänge von verlorenen oder gestohlenen Schlüsseln **schnell und einfach gesperrt**
- Abgelaufene Schlüssel erhalten erneuten Zugang **nur mittels manuellem Eingriff** des Administrators



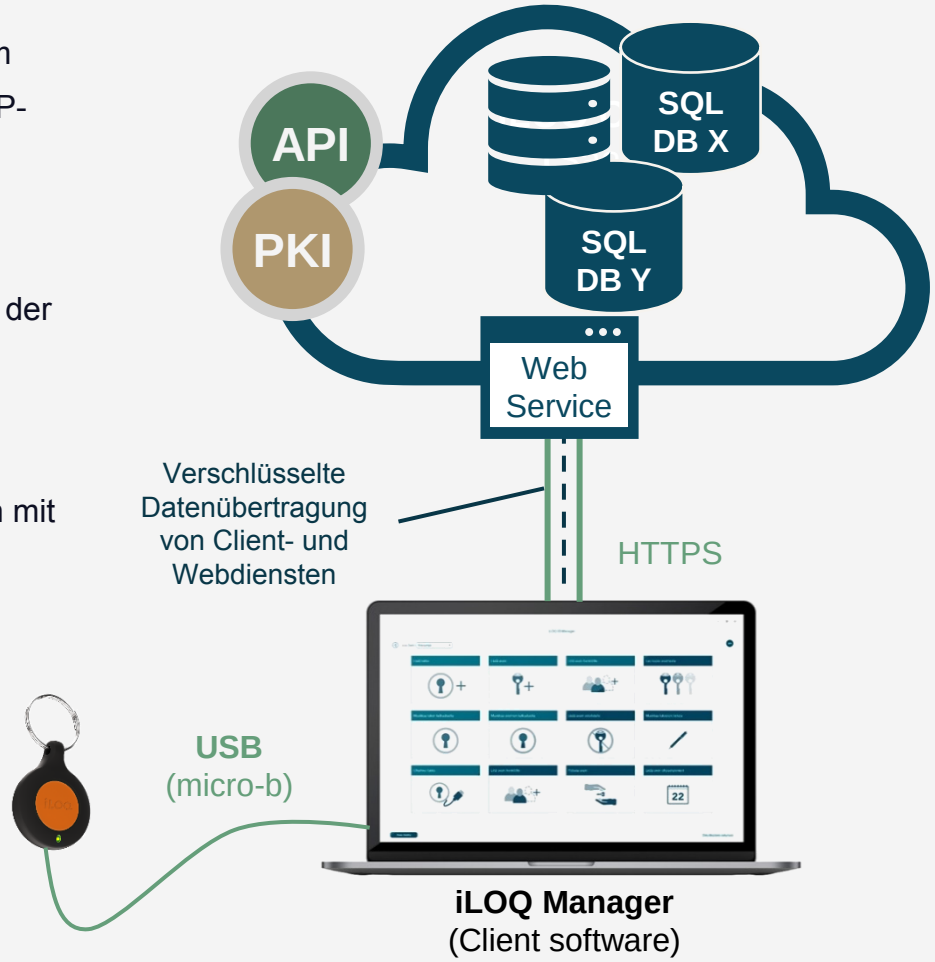


Zertifizierte iLOQ Cloud - C5 nach BSI

- iLOQ verwendet AWS in mehreren Ländern, um den SaaS-Dienst zu hosten/betreiben. **Deutsche Kunden** werden ausschließlich in **DE-Frankfurt** gehostet.
- Der Cloud-Dienst ist nach verschiedenen Standards zertifiziert
  AWS Zertifikate AWS Programme
- C5 Testat vom - Bundesamt für Sicherheit in der Informationstechnik (BSI) LINK
- Jeder Kunde betreibt seine eigene SQL-Server-Datenbank, die vollständig von anderen Datenbanken isoliert ist. Die einzige Möglichkeit zur Kommunikation besteht über den iLOQ-Webserver, der spezifische und vordefinierte Verfahren zur Datenvalidierung verwendet.
- Es werden regelmäßig Aktualisierungen der Betriebssystemsicherheit und des Virenschutzes durchgeführt. Zusätzlich werden jährlich **Backup & Restore** Szenarien durchgespielt.

iLOQ 5 Series Verteilte Sicherheit

- **Standard-PC** für Client-Software-Hosting, ausgestattet mit Microsoft Windows-Betriebssystem
  - ClickOnce-Anwendung vom Webserver heruntergeladen, installiert und aktualisiert – HTTP-Verbindung
  - Benutzeroberfläche
  - Verschlüsselte USB-Verbindung zum iLOQ P55-Programmiertoken
  - Zweite Verschlüsselungsschicht vom Client-Prozess zum Web-Service-Prozess innerhalb der SSL-Schicht
- **Webdienst** = Windows Server und hostet Webdienstprozesse
  - Der Webdienstprozess kommuniziert mit der Kundendatenbank
  - Keine direkte Kommunikation mit der Datenbank – nur definierte gespeicherte Prozeduren mit Datenvalidierung (Schutz vor Hackerangriffen)
  - Sitzungsbasierte SSL-verschlüsselte Webservice-Kommunikation mit Client-PC
- **Daten werden im SQL Server auf einem separaten DB-Server gespeichert**
  - Vom anderen Netzwerk isoliert, kommuniziert nur mit dem Webserver
  - Jeder Kunde betreibt eine eigene Datenbank
  - Die Datenbank enthält Informationen zu Zylindern, Schlüsseln, Zugriffsrechten usw
  - Benutzer werden auch in SQL Server verwaltet
- HTTPS-Verbindung zwischen **Client-PC** und iLOQ-Cloud
- Aufgrund der sitzungsbasierten Kommunikation ist kein Proxy zulässig (einstellbar im Client)
- Für den Systemzugriff sind Anmeldeinformationen und eine physische Identifikation erforderlich →**verteilte Sicherheit 2FA**



Verschlüsselungen der Programmierpakete erfolgen lokal über den Programmier-Token 2FA

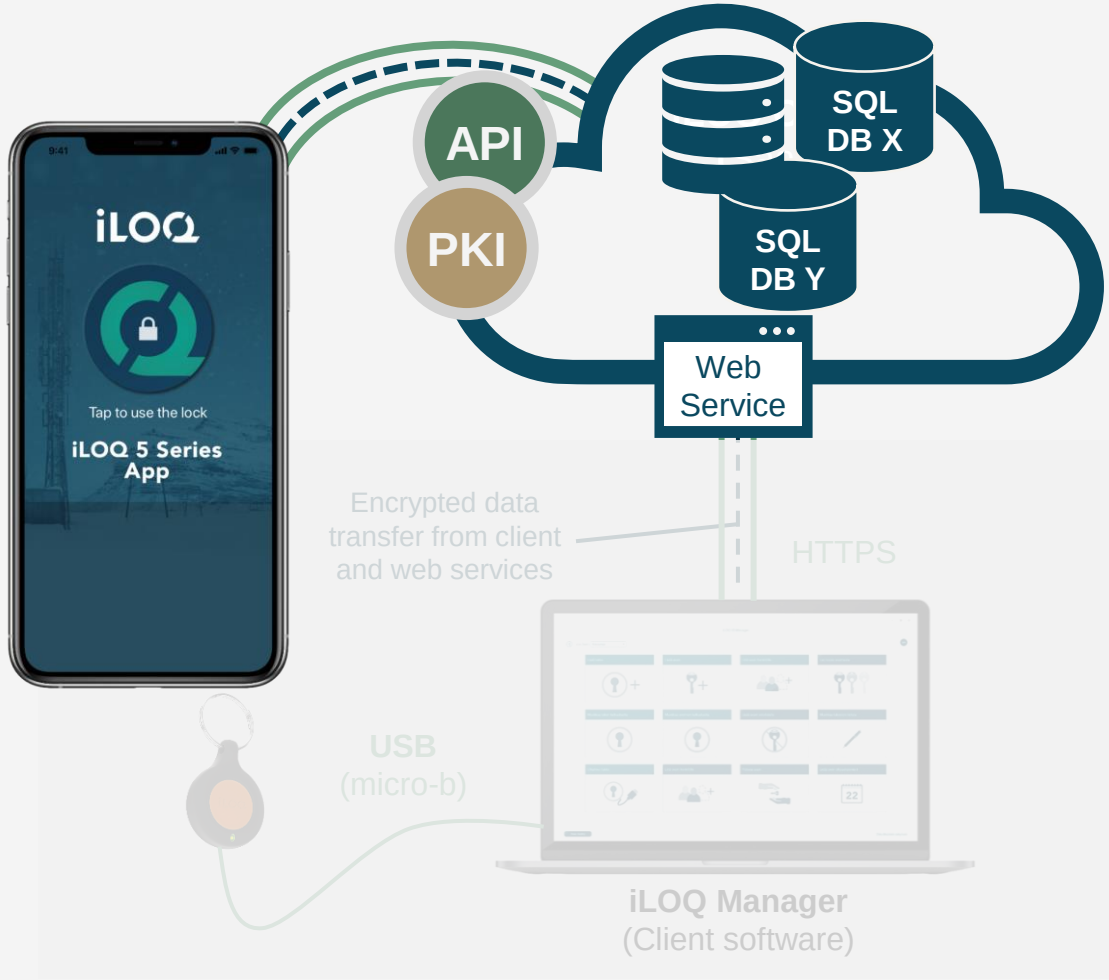
Mobile Zugangsrechte sicher über Mobilfunk

- Die Zugriffsrechte werden verschlüsselt und **drahtlos weitergegeben** zu einem Smartphone, über einen **HTTPS Tunnel**
- Für Smartphones ist die iLOQ App S50 erforderlich

Google Play

App Store

- Der Cloud-Server überprüft die Authentizität mobiler Geräte mit starker Sicherheit -**PKI-basierte Authentifizierung**
- Die iLOQ-App läuft in einer isolierten Anwendungssandbox und speichert Zugriffsrechte in einer verschlüsselten Datenbank. Die App-Daten werden durch mehrere Anwendungsschutzebenen geschützt, die von Betriebssystemen (iOS und Android) bereitgestellt werden.
- Die App funktioniert nicht auf Geräten, die gerootet/gejailbreakt wurden, da diese Aktionen gegen die grundlegenden Sicherheitsprinzipien des Betriebssystems verstoßen und die Systemsicherheit gefährden können
- Zusätzlich zu den im Betriebssystem bereitgestellten Plattformsicherheitsfunktionen bietet die iLOQ-App. außerdem modernste InApp-Schutzmechanismen an, die die App vor Malware und Angriffen schützen.
- Zugriffsrechte können im iLOQ Manager einfach widerrufen werden
- Das Schloss kann so konfiguriert werden, dass beim Öffnen eine Online-Zugriffsvalidierung vom Server erforderlich ist
- Nach jedem Öffnungsversuch wird ein einzelnes Protokoll vom Schließvorgang an den Server gesendet (berechtigt/unberechtigt) **wenn vom Admin aktiviert-optional.**



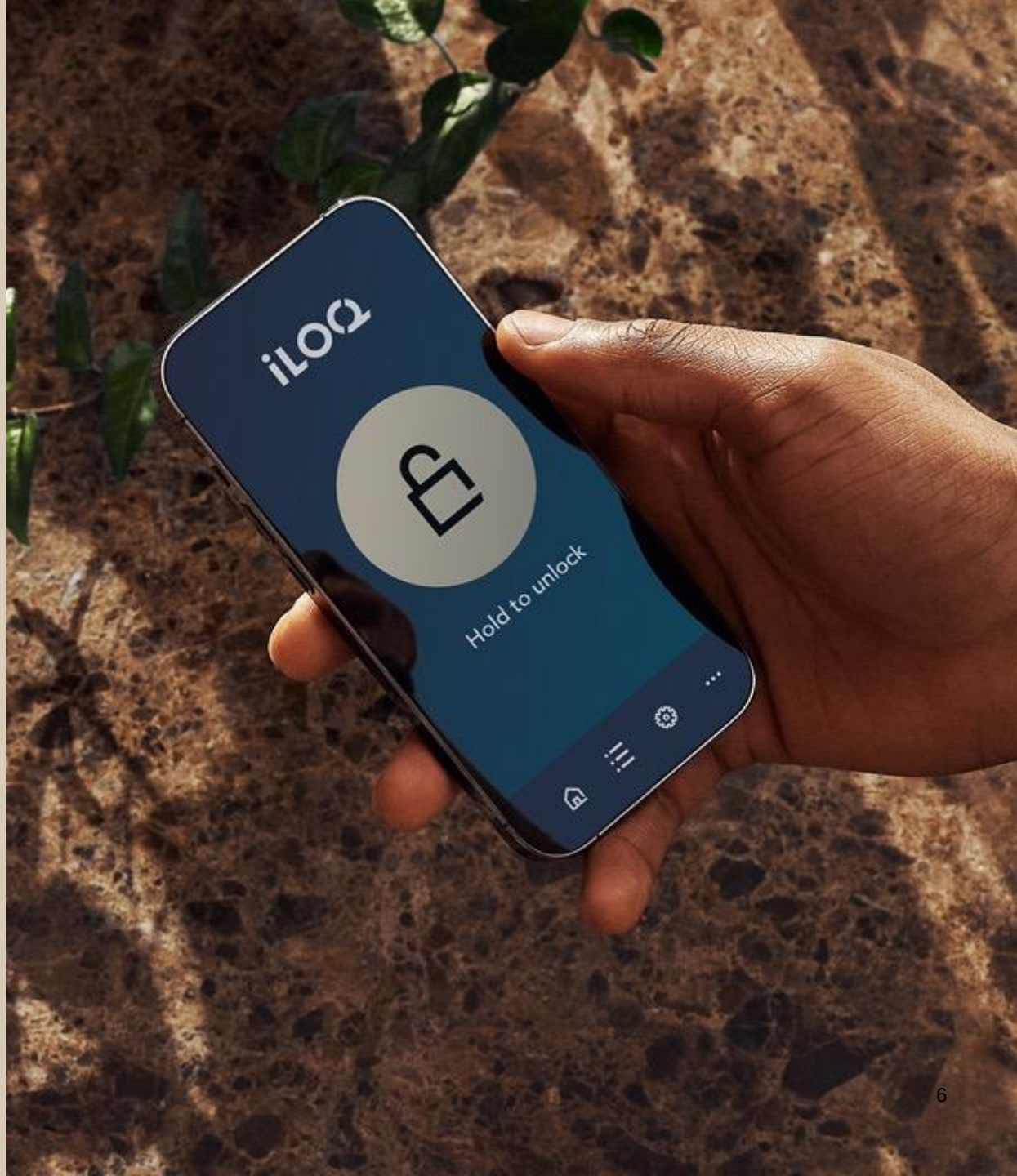
Offline Funktion immer gewährleistet bei
(Keller, kein Mobilfunk-Empfang oder bei einem **Blackout** über Tage hinweg)

Tipps zur sicheren mobilen Nutzung

Um eine hohe mobile Sicherheit zu gewährleisten, beachten Sie bitte die folgenden Hinweise:

- Ermöglichen Sie regelmäßige und automatisierte System- und Anwendungsaktualisierungen
- Verwenden Sie eine Bildschirmsperre mit automatischer Sperre (kurze Leerlaufzeit)
- Verwenden Sie sichere PIN-Codes, Muster, biometrische Daten oder Passwörter (obligatorisch).
- Laden Sie Apps nur von vertrauenswürdigen Quellen herunter (Google Play oder Apple App Store)
- Verwenden Sie aktualisierte Antivirensoftware
- Gerootete/jailbreakte Geräte funktionieren nicht
- Sicherstellen einer kontrollierten Geräteübergabe/ Entsorgung/Recycling

- Eine zentrale Verwaltung mobiler Geräte in Ihrem Unternehmen wird empfohlen "MDM" (IT-Abteilung + Remote-Verwaltungstools).



Sicherheit in Bezug auf die Zylinder und das Öffnen dieser mittels Smartphone

- Symmetrisch (256 Bit) verschlüsselte Zugriffsrechte werden für die Dauer einer Übertragungssitzung vom Schlüssel zum Zylinder **doppelt verschlüsselt**, wodurch **jede** Kommunikationssitzung **einzigartig** ist. In der Praxis würde ein theoretisches Abhören der Session keinen Zylinder beim Versuch öffnen, da der Schlüssel immer unterschiedlich ist. Dasselbe gilt für alle iLOQ-Schlüsseltypen
- Im iLOQ S50-System kann ein Zylinder so konfiguriert werden, dass beim Öffnen eine Online-Authentifizierung vom Server erforderlich ist. (High Level Security)
- Auf Wunsch wird jeder Schließvorgang (Ereignisprotokoll) in Echtzeit vom Smartphone an den Server gesendet. Dieser Schließvorgang wird ebenfalls im Zylinder gespeichert und kann bei Bedarf abgerufen werden. (Optional und kann deaktiviert werden)


iLOQ
Life made
limitless.