

smartlox

Sicher. Intelligent. **Digitales LOTO.**



SMARTLOX PTY LTD

www.smartlox.io

hello@smartlox.io

Die Smartlox Lösung.

smartlox

Hardware

Mobile App



Digitales Schloss



Sichere Cloud



LOTO HD-Schloss

Das LOTO HD-Schloss ist der ideale Ersatz für Ihre persönlichen LOTO-Schlösser und Gruppenverschlusskästen. Es ist robust konstruiert und für den Einsatz in jeder Umgebung geeignet.



Körper aus Aluminium • Stahlbügel



IP67 und ATEX-B-zertifiziert



-20 °C bis 74 °C



Bis zu 3 Jahre
Batterielebensdauer



Bluetooth
Konnektivität

Software



Digitales Schloss



Mobile App



Sichere Cloud



Mobile App

Die Smartlox Nyckel-App bietet ein umfassendes digitales LOTO Management mit wichtigen Funktionen wie individuelle und gruppenbezogene Lockout Strukturen, Fernsteuerung der Sperren und vielem mehr.



Herunterladen und registrieren – in weniger als einer Minute



Einfach und benutzerfreundlich



Vollständige Transparenz und Kontrolle – immer griffbereit



Sichere Cloud

Bei Smartlox hat die Sicherheit höchste Priorität. Unsere leistungsstarke Cloud-Infrastruktur gewährleistet den Schutz, die Zuverlässigkeit und die Einhaltung der Vorschriften Ihrer Sicherheitsdaten. Dadurch werden Ihre Betriebsabläufe von Natur aus sicherer, und Ihre Aussperrungen lassen sich einfacher und souveräner verwalten.



Sicher konzipiert gemäß den Anforderungen der Norm ISO 27001



Robuste Architektur für abgelegene Umgebungen



Kann an Ihren IT-Richtlinien angepasst werden (SSO, MFA)

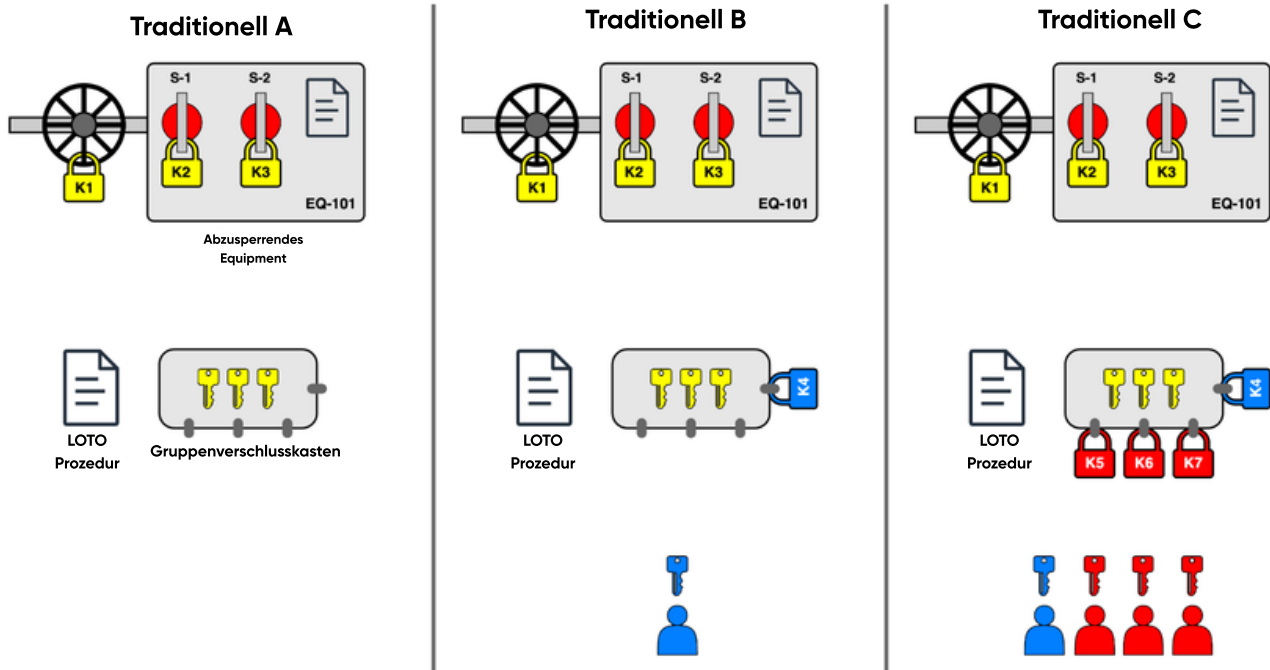


API-Integration in externe Systeme



Google Cloud Firebase

Traditioneller Lockout

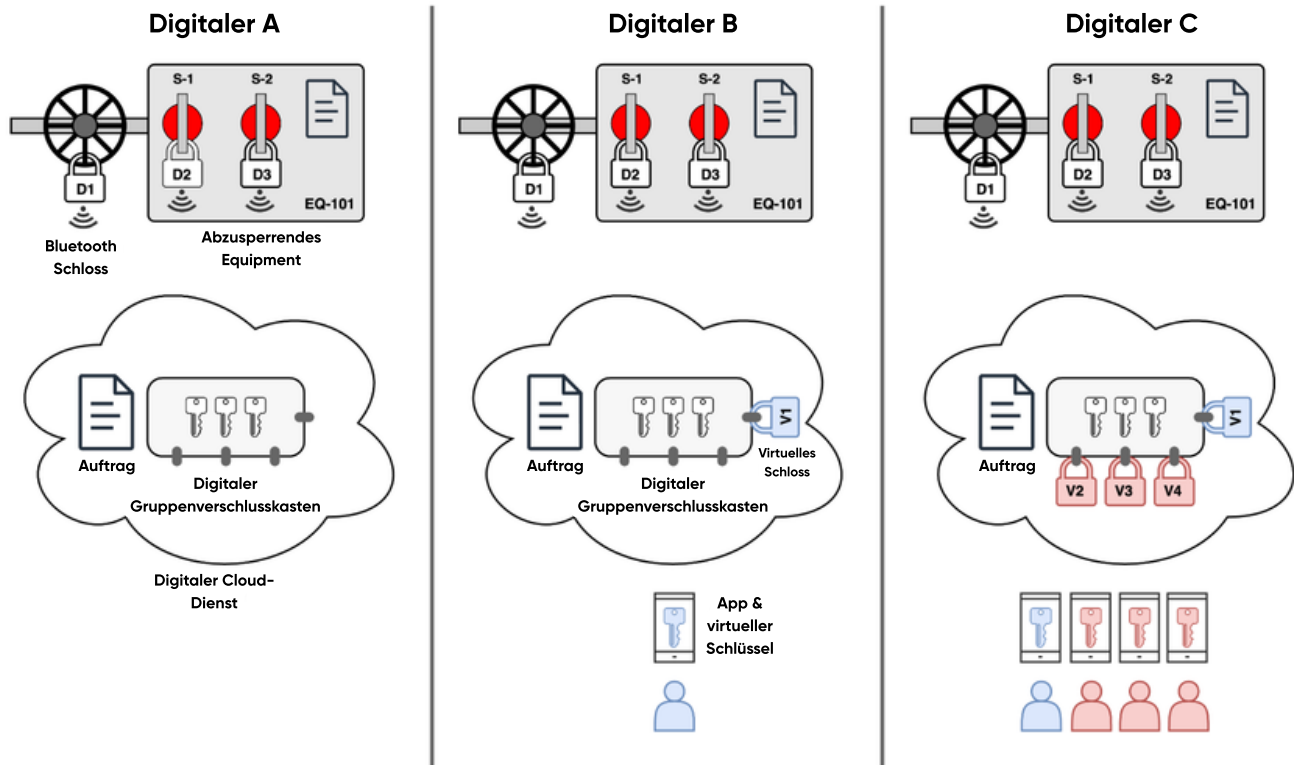


Schauen wir uns zunächst einmal die Schritte zur herkömmlichen Isolierung von Geräten an.

1. Die mechanischen Schlösser K1, K2 und K3 werden gemäß der LOTO-Prozedur an den Energiekontrollpunkten angebracht. Die Schlüssel dieser Schlösser werden in einem Gruppenverschlusskasten aufbewahrt.
2. Die für die Verriegelung zuständige Person bringt ein persönliches Schloss K4 an den Gruppenverschlusskasten an, der verhindert, dass die Schlüssel für K1–K3 entnommen werden können.
3. Autorisierte Mitarbeiter können dann ihre persönlichen Schlösser nach Bedarf an dem Gruppenverschlusskasten anbringen und wieder entfernen.

Zwar sind an dem Gruppenverschlusskasten persönliche Schlösser angebracht, doch darf das Schloss K4 der für den Lockout verantwortlichen Person nicht entfernt werden, und die Absperrschlösser K1–K3 sind gegen Entfernung gesichert.

Digitaler Lockout

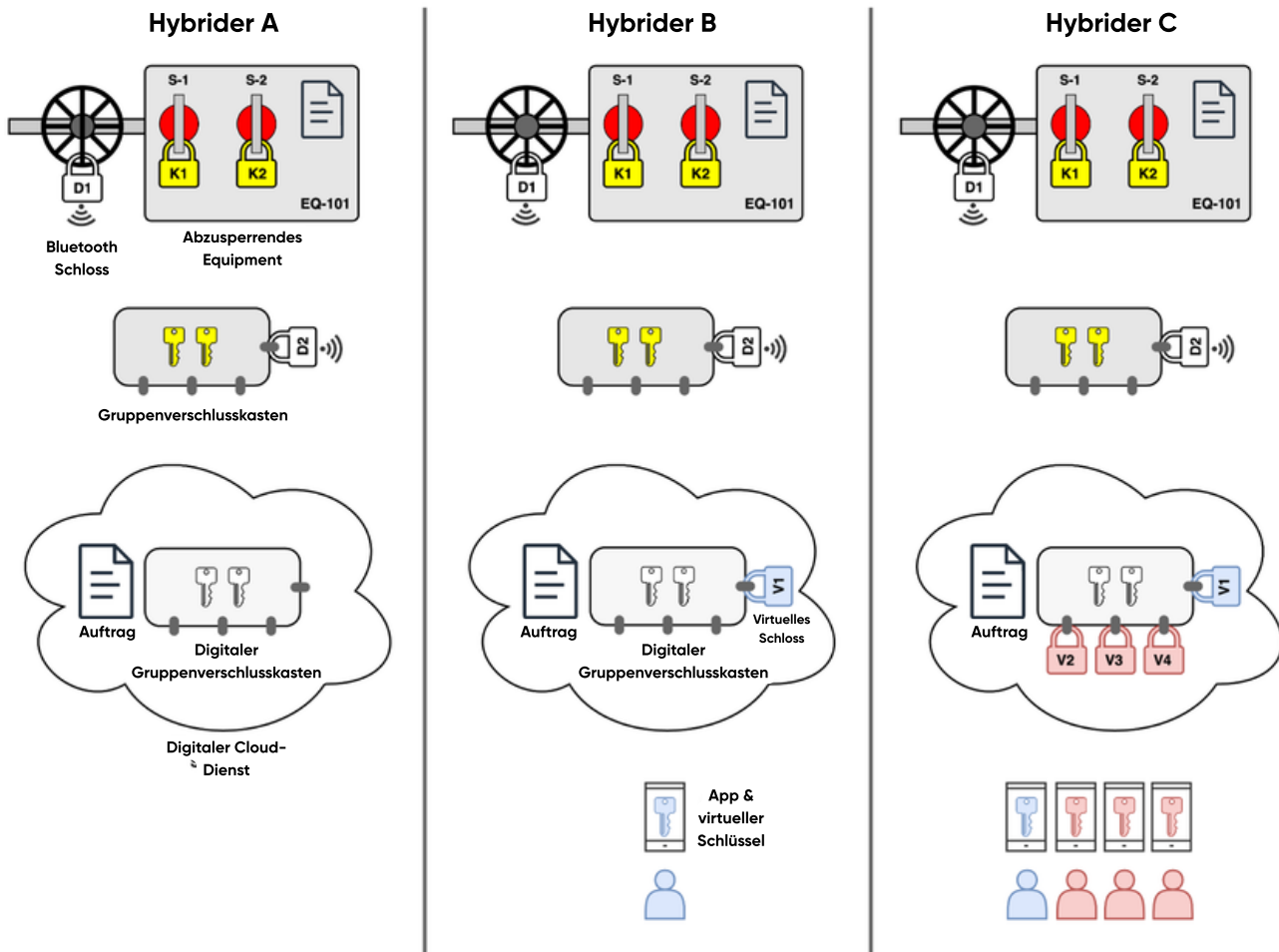


Schauen wir uns nun an, wie ein digitaler Lockout durchgeführt wird – um das gleiche Schutzniveau zu erreichen.

1. Die digitalen Schlösser D1, D2 und D3 werden an den Energiekontrollpunkt angebracht. Die dazugehörigen virtuellen Schlüssel werden anschließend in einem virtuellen Gruppenverschlusskasten im digitalen Cloud-Dienst abgelegt.
2. Die zum lockout berechnigte Person versieht den virtuellen Gruppenverschlusskasten daraufhin mit einem virtuellen Schloss V1, dass das Öffnen der digitalen Schlösser D1–D3 verhindert.
3. Autorisierte Mitarbeiter können dann je nach Bedarf persönliche virtuelle Schlösser V2–V4 am virtuellen Gruppenverschlusskasten anbringen und wieder entfernen.

Obwohl persönliche virtuelle Sperren vorhanden sind, kann die virtuelle Sperre V1 der zum Lockout berechtigten Person nicht entfernt werden, und die Schlösser D1–D3 sind vor einer Entfernung geschützt.

Hybrider digitaler Lockout



Betrachten wir abschließend ein Szenario, bei dem es zu einer kombinierten digitalen und herkömmlichen Sperrung kommt.

1. An den Energiekontrollpunkten wird eine Kombination aus digitalen und mechanischen Schlössern angebracht.
 - Das digitale Schloss D1 wird an einem Energiekontrollpunkt angebracht und sein virtueller Schlüssel wird in einem virtuellen Gruppenverschlusskasten im digitalen Cloud-Dienst gespeichert.
 - Die mechanischen Schlösser K1–K2 werden an den Energiekontrollpunkten angebracht und die Schlüssel in einem Gruppenverschlusskasten aufbewahrt.
 - Das digitale Schloss D2 wird an dem Gruppenverschlusskasten angebracht, und sein virtueller Schlüssel wird im virtuellen Gruppenverschlusskasten gespeichert.
2. Der zum Lockout berechtigte Mitarbeiter bringt ein virtuelles Schloss V1 am virtuellen Gruppenverschlusskasten an, wodurch verhindert wird, dass die digitalen Schlösser D1–D2 geöffnet werden können.
3. Autorisierte Mitarbeiter bringen je nach Bedarf persönliche virtuelle Schlösser V2–V4 am virtuellen Gruppenverschlusskasten an und entfernen sie wieder.

Solange persönliche virtuelle Schlösser vorhanden sind, kann das virtuelle Schloss V1 des für den Lockout autorisierten Mitarbeiters nicht entfernt werden, und die Schlösser D1, K1 und K2 sind vor einer Entfernung geschützt.

Digitales LOTO für Nutzer ohne Gerät.

Trotz der fortschreitenden Digitalisierung in globalen Branchen bleibt die Nutzung von Smartphones in einigen Unternehmen weiterhin untersagt. Diese Einschränkungen können unterschiedliche Ursachen haben, darunter:

- Gefährliche Umgebungen – Anforderungen an die Explosionssicherheit, die den Einsatz elektronischer Geräte untersagen
- Sicherheitsrichtlinien – Sensible oder klassifizierte Bereiche mit strengen Kommunikationsprotokollen
- Arbeitsschutzrichtlinien oder Tarifverträge – Regelungen, die die Verwendung von Mobiltelefonen erschweren oder untersagen.
- Technologische Lücke – Unzugänglichkeit von Smartphones oder mangelnde Verbreitung dieser in einigen Regionen dieser Welt.

Wir bei Smartlox sind der Überzeugung, dass diese Herausforderungen weder die Sicherheit, die Einhaltung gesetzlicher Anforderungen noch die betriebliche Effizienz beeinträchtigen dürfen. Daher bietet unser System flexible Alternativen, welche die Leistungsfähigkeit des digitalen LOTOs erweitern – selbst wenn ein Benutzer kein eigenes Mobilgerät mit sich führt.

Smartlox hat verschiedene alternative Sperrmethoden entwickelt, um auch Nutzern ohne Mobilgerät gerecht zu werden:

Variante 1: Gemeinsam genutztes Gerät

Häufig findet dieses System Anwendung in Gefahrenbereichen, in denen die Nutzung von Smartphones eingeschränkt ist und nur bestimmte Geräte im Arbeitsumfeld zugelassen sind. Ein spezielles Gerät (in der Regel ein Tablet) wird von der für die Sperrung verantwortlichen Person verwendet. Alle Sperrfunktionen für sämtliche beteiligten Benutzer werden über dasselbe Gerät ausgeführt.

So einfach funktioniert es:

- Die Nutzer authentifizieren sich auf dem gemeinsam genutzten Tablet mit ihren persönlichen Anmeldedaten und führen anschließend ihre digitalen Sperrvorgänge durch. Alle regulären Sperrfunktionen stehen den Nutzern zur Verfügung, während sie mit ihrem eigenen Konto angemeldet sind.
- Sobald der Benutzer seine Arbeit beendet hat, muss er sich abmelden, bevor er das Gerät an eine andere Person übergibt.



Digitales LOTO für Nutzer ohne Gerät.

Variante 2: ID-Nutzer – Sperrung aktivieren:

Nutzer, die keinen Zugriff auf ihr eigenes Gerät oder die Nyckel-App haben, können an Sperrungen teilnehmen, indem sie eine systemgenerierte ID-Karte (QR-Code) scannen. Diese Teilnehmer präsentieren ihre ID-Karte einem autorisierten Nutzer, der sie scannt und den Nutzer somit als aktiven Teilnehmer zur Sperrung hinzufügt. Die Sperrung kann durch erneutes Scannen der ID-Karte aufgehoben werden. ID-Karteninhaber genießen während einer Sperrung den gleichen Schutz wie reguläre Nutzer.

So funktioniert es:

- Bei der Einarbeitung in eine Arbeitsstelle erhält der Benutzer einen Ausweis, der über Nyckel erstellt wird.
- Der Benutzer ist verpflichtet, seinen ID-Karte einem autorisierten Benutzer zur Überprüfung durch Nyckel vorzulegen, damit dieser ihn scannen kann, sobald eine persönliche Sperre aktiviert ist.
- Sobald der Benutzer seine Arbeit abgeschlossen hat, muss er einem autorisierten Benutzer seinen ID-Karte zur Überprüfung durch Nyckel vorlegen, um die persönliche Sperre aufzuheben.

Hinweis: ID-Benutzer sind nicht berechtigt, einen Lockout durchzuführen, zu besitzen oder zu entfernen. Sie dürfen lediglich mit einem virtuellen, persönlichem Schloss an einem bereits vorhandenen Lockout teilnehmen.



Das Sperren der ID-Karte führt dazu, dass der Benutzer ein digitales, persönliches Schloss zu einem bereits vorhandenen Lockout hinzufügt.