Zentrale Applikation

Verwaltung und Steuerung verschiedener Schloss-Systeme; Anlegen, Berechtigen, Löschen von Benutzern aus der Ferne.

Codevergabe und Code-Synchronisation

Zentrale Code-Vergabe und automatische Code-Synchronisation an alle berechtigten Schloss-Systeme.

SAFECOR
SICHERHEIT UND AUTOMATION

Access-Management

Die plattform-übergreifende Lösung für ein modernes Access-Management

Die Steuerung und Administration von Öffnungsberechtigungen für Automaten und Tresore von zentraler Stelle ist heute eine entscheidende Anforderung an Verschluss-Konzepte. Unter Einhaltung höchster europäischer Sicherheitsstandards sind so kürzeste Reaktionszeiten und ein geringer Aufwand in der Steuerung der Benutzer und Schloss-Öffnungen garantiert. In wenigen Minuten werden die Berechtigungen vergeben oder gelöscht und einzelne oder mehrfache Öffnungs-Freigaben von zentraler Stelle erteilt. Dabei sind die Schloss-Konzepte multifunktional in einer Online- oder Offlinevariante nutzbar. Unter Sicherstellung der VdS- und IT-Anforderungen, sowie interner Revisions-Vorgaben, bietet die Lösung eine sehr einfache Handhabung für Benutzer und Administratoren, mit vielseitigen Anwendungsoptionen.

Zentrale Steuerung von Benutzern & Rechten

Maximale Transparenz und Kontrollfunktion

Eine fortlaufende und redundante Protokollierung schafft maximale Transparenz und Überwachung bei Manipulation. Alle Schritte sind jederzeit nachvollziehbar.

Integrierte Alarmfunktionen

Überwachung der Schloss-Systeme mit bereits integrierten Alarmfunktionen: Überfallmelder (stiller Alarm), Sperreinrichtung (bei aktiver EMA), Verschlussüberwachung (Zustand).

Höchste Ausfallsicherheit

Eine redundante Datenhaltung mit zentraler und dezentraler Speicherung bietet auch bei Ausfall des Netzwerks volle Funktionsfähigkeit. Die Benutzer öffnen die Tresore wie gewohnt.

Einmalcodes für den externen WTU-Betrieb

Einmalcodes für den sicheren Betrieb mit Wertdienstleistern, inkl. Notfallkonzept (BCM).

Hybridfunktion: Unterstützung mehrerer Betriebsmodi

Schloss-Betrieb online/offline/virtuell: verkabelt und online über Netzwerk, als wirtschaftliche Lösung ohne Verkabelung oder virtuell mit Network-on-Card.

Vielseitig einsetzbar, zertifiziert in allen Sicherheitsklassen

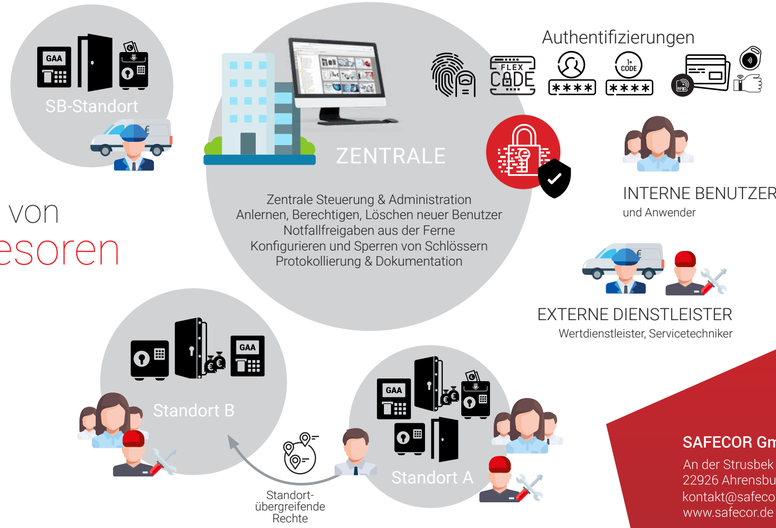
Nachrüstbar in VdS B und VdS C für alle Automaten, sowie Wertschutzschränke und Tresorräume aller Hersteller.

einfach
sicher
effizient

Zentrale Steuerung von Automaten & Tresoren

Sicherheitsbereiche, Automaten und Tresore bedürfen einen größtmöglichen Schutz vor unerlaubten Zugriffen.

Diesen bieten wir mit unserer Access-Management Lösung. Moderne Öffnungs- und Zutrittsverfahren mit lückenloser Dokumentation werden den ständig wachsenden Anforderungen an Sicherheit und Flexibilität in den Prozessen und Abläufen gerecht.



SAFECOR GmbH
An der Strusbek 28
22926 Ahrensburg
kontakt@safecor.de
www.safecor.de

Zentrale Benutzer-Administration:
So einfach und sicher wie nie zuvor!

Mit nur wenigen Maus-Klicks vergeben Verantwortliche von ihrem Arbeitsplatz aus die Öffnungsberechtigungen für die Benutzer vor Ort. Neue Codes lassen sich so - ohne großen Aufwand - jederzeit, schnell und einfach vergeben. Die neue VdS-Richtlinie für „Verteilte Systeme" ermöglicht die Synchronisation der Codes auf alle Schlösser, für die die Benutzer berechtigt sind.

Noch nie war die Benutzer-Administration so einfach und effizient. Die zentrale Applikation stellt sicher, dass die Rechte und Codes automatisch auf die Automaten und Tresore übertragen werden, welche im Berechtigungskonzept definiert wurden. Den Administratoren spart dies Zeit und Arbeit und für die Schloss-Benutzer wird es deutlich einfacher. Wechseln Mitarbeiter von einer in eine andere Filiale, kann innerhalb von Sekunden die Berechtigung zentral erteilt werden und der Mitarbeiter kann mit seinem persönlichen PIN öffnen. Codes müssen nicht ständig neu programmiert werden.

VdS 3841
& EN 17646 konform

Mit der VdS-Norm 3841, Neufassung in 02-2021, und dem Update der europäische Normung für Hochsicherheitsschlösser EN 17646 wird das Sicherheitsniveau definiert und für alle Beteiligten geregelt. Kürzere Innovationszyklen der Elektronik und der IT-Netzwerke garantieren das hohe Sicherheitsniveau und ermöglichen gleichzeitig den Instituten die effiziente und kostensparende Organisation der Prozesse. Die neue VdS-Richtlinie für „Verteilte Systeme" definiert das digitale Öffnen von Wertbehältnissen. Dies sichert den Instituten vereinfachte Abläufe, verpflichtet Hersteller zur Einhaltung von Sicherheitsstandards und macht so die Risiken der modernen Technik für Versicherer bewertbar. Darunter fällt beispielsweise der Einsatz aktueller Kryptoverfahren bei der Erzeugung von Signaturen und Schlüsseln, sowie beim Pairing von Komponenten im Netzwerk.

Volle Transparenz für die
Benutzer-Rezertifizierung

Die Identity & Access Management Lösung unterstützt die Verantwortlichen bei diesen automatischen Datenabgleich erheblich. Administratoren können den Automatisierungsgrad zudem flexibel definieren. Ob nur ein Stammdaten-Abgleich stattfinden soll und die Rechte eigenständig in der zentralen Applikation gepflegt werden oder ob auch die Berechtigungsgruppen aus dem zentralen Verzeichnis übernommen werden sollen, so oder so – durch den zentralen Abgleich der standardisierten Daten und einer automatisierten Bereitstellung dieser wird der Rezertifizierungsprozess im hohen Maß automatisiert.

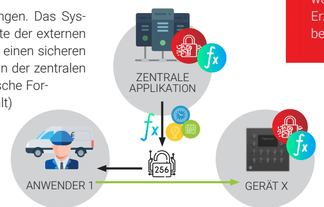
Wie werden
PIN-Codes
vergeben?

PIN-Codes müssen nur einmal programmiert werden. Anschließend erfolgt die automatische Synchronisation auf alle berechtigten Systeme. Die Neu-Programmierung auf weiteren Tresorschlössern entfällt. Wechselt ein Benutzer den Standort oder kommen neue Tresore und Automaten hinzu, so muss der verantwortliche Administrator je nach Berechtigungskonzept nichts weiter machen oder maximal weitere „Haken" setzen.

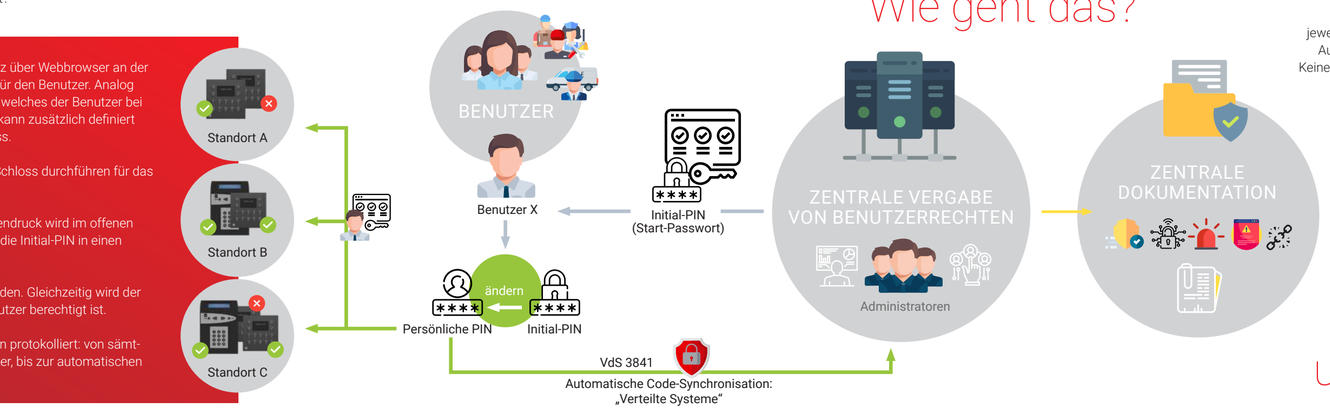
Wie läuft die initiale PIN-Vergabe ab, wenn ein neuer Benutzer hinzukommt
oder ein bestehender Benutzer seinen persönlichen PIN-Code vergessen hat?

1. Der Administrator meldet sich zentral an einem beliebigen Arbeitsplatz über Webbrowser an der Applikation mit Benutzer und Kennwort an und vergibt die Initial-PIN für den Benutzer. Analog zur Passwort-Vergabe handelt es sich hierbei um ein Start-Kennwort, welches der Benutzer bei der Programmierung in ein persönliches, geheimes ändern muss. Es kann zusätzlich definiert werden, dass dieser Prozess im 4- oder 6-Augen-Prinzip erfolgen muss.
2. Die persönliche Code-Programmierung kann der Benutzer an jedem Schloss durchführen für das der Administrator Berechtigungen erteilt hat.
3. Die eigentliche Programmierung ist „kinderleicht". Mit nur einem Tastendruck wird im offenen oder geschlossenen Zustand des Tresors, der Vorgang gestartet und die Initial-PIN in einen persönlichen Code geändert.
4. Die persönliche PIN ist sofort aktiv und kann zur Öffnung genutzt werden. Gleichzeitig wird der Code des Benutzers an alle Schlösser übertragen, für welche der Benutzer berechtigt ist.
5. Der Vorgang wird transparent und nachvollziehbar mit allen Aktivitäten protokolliert: von sämtlichen administrativen Tätigkeiten, der Code-Anlage durch den Benutzer, bis zur automatischen Synchronisation auf alle berechtigten Schlösser.

Mit Einmalcodes kabellos vernetzt oder als Online-System über IP-Datenleitungen. Das System steuert die Berechtigungen der internen Mitarbeiter genauso, wie die Rechte der externen Dienstleister. Doch wie kommt der Anwender - intern oder extern - eigentlich an einen sicheren Code, wenn kein Netzwerk vorhanden ist? Die Lösung liegt in der Kryptografie. In der zentralen Datenbank und dem zu öffnenden Schloss wird eine Art individuelle kryptografische Formel hinterlegt. Dieser Algorithmus enthält diverse Parameter und Variablen (Salt) wie zum Beispiel Zeit, Gerätedefinition, Datum, Uhrzeit, Benutzer-ID und Berechtigungsgrade. Die zentrale Datenbank und das lokale Offline-Gerät werden also im Vorfeld einmalig „gepaired" und laufen dann mit dieser Formel synchron. Mit diesem gemeinsamen, geheimen Schlüssel (Hashkey) lässt sich dann eine zentrale Codevergabe realisieren, ohne die Notwendigkeit des Netzwerkzugriffs oder die Online-Anbindung von Endgeräten.



Mit oder ohne Netzwerk
Wie geht das?



Verschlüsselt
Sicherheit der Daten und Schutz vor unbefugter Verarbeitung oder Daten-Verlust.

Präzise
Definieren Sie einen spezifischen Zugriff für den jeweiligen Benutzer und dessen Aufgaben. Keine Ausnahmen. Keine Umgehungsmöglichkeiten.

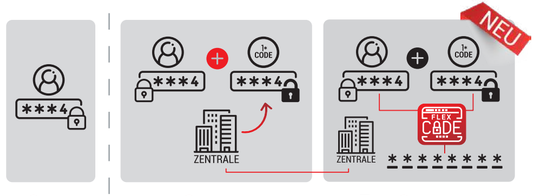
Revisionssicher
Nachvollziehbarkeit der Daten-Änderungen

Integrität & Vertraulichkeit
DSGVO und Revision erfordern sachlich richtige Daten und deren Schutz

Wer hat welche Rechte und werden diese noch benötigt? Die Einrichtung, Änderung, Deaktivierung sowie Löschung von Berechtigungen und die Rezertifizierung müssen nachvollziehbar und auswertbar dokumentiert werden. Die zyklische Überprüfung, ob die eingeräumten Berechtigungen weiterhin benötigt werden und ob diese den Vorgaben des Berechtigungskonzeptes entsprechen (Rezertifizierung), ist mit hohem organisatorischen Aufwand verbunden. Die Lösung für diesen Prozess bringt der optionale Active Directory/LDAP-Connector mit sich. Hierüber gleicht sich die zentrale Datenbank automatisch mit dem Verzeichnisdienst ab, in welchem die digitalen Identitäten der Mitarbeiter bereits in einem definierten Prozess gepflegt werden. Scheidet ein Mitarbeiter aus, wird dies über die einschlägigen Tools für die Benutzer-Verwaltung (OSP, DAW im Fi-Umfeld und Admin-Gui im ATRUVIA-Umfeld) im Verzeichnisdienst der IT vermerkt und der Benutzer verliert automatisch die Schloss-Berechtigungen. Zeitgleich werden die Codes aus allen Tresoren gelöscht.

Die Lösung für den Rezertifizierungsprozess:
unser Identity & Access Management

Unterschiede von statischen & dynamischen Codes



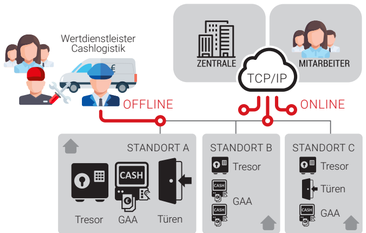
Code
Fest und persönlich

Code + Einmalcode
2-Faktor-Prinzip

FlexCode
Einmalcodes ohne jegliche Administration vor Ort

Was sind Einmalcodes?

Ein entscheidender Vorteil von dynamischen Codes liegt darin begründet, dass diese nicht dauerhaft gültig, sondern flüchtig sind. Einmalcodes können also nur einmal und nur in einem definierten Zeitfenster benutzt werden. Dynamischen Codes können zentral beim Wertdienstleister (z.B. in dessen Leitstand, Disposition oder Touren-Programm) „erzeugt" und an die Fahrer (Tour) übermittelt werden.



Einmalcode-Verfahren benötigen keine Netzwerkverbindung. Ein Zugriff vom Wertdienstleister auf das Banknetzwerk ist daher nicht erforderlich.

WICHTIG

Inbetriebnahme

Der Prozess der Automaten-Inbetriebnahme ist effizienter.

Sicherheit

Einmalcodes erhöhen die Sicherheit, da Skimming und Manipulation bei der Öffnung verhindert wird. Es lässt sich zudem optional der Verschluss der Automaten zentral im Leitstand überwachen. So ist eine lückenlose Dokumentation jeder Öffnung und Schließung gegeben.

Verfügbarkeit

Die Störungsbehebung kann je nach Vereinbarung durch den Wertdienstleister, das Institut selbst oder auch in Kombination mit Service-Dienstleistern erfolgen.

Flexibilität

Einmalcodes verbessern die Reaktionsgeschwindigkeit und Flexibilität bei Störungen und tragen somit zu einer höheren Verfügbarkeit bei.
Im Fall einer Störung werden Einmalcodes direkt an das Interventions-Team übermittelt. Es entstehen keine Wartezeiten durch bereits ausgegebene (bestehende) Einmalcodes eines Befüllungsteams.

Sicherheit & Flexibilität für den WTU Handlungsfähigkeit für das Institut

Business Continuity Management (BCM)

Notfallkonzepte ermöglichen die Fortführung des zeitkritischen Geschäftsprozesses „Bargeldversorgung" nach einer Unterbrechung im Sinne des Business Continuity Management (BCM) nach MaRisk. Das Konzept sichert die Handlungsfähigkeit des Instituts. Es muss Geschäftsfortführungs- sowie Wiederherstellungspläne umfassen. Dem Institut werden für das Risiko- oder Notfallmanagement Möglichkeiten der Steuerung (im Fall von Pandemie, Cyberattacke,...) ermöglicht.

Die Applikation wurde für verschiedene spezifische organisatorische Anforderungen und Prozesse entwickelt. Durch einen modularen Aufbau sind unterschiedliche Anwendungs- und Nutzungs-Szenarien möglich. Das mandantenfähige und modular aufgebaute System steuert das gesamte Benutzer, Rechte-, Daten- und Freigabemanagement von verschiedenen physikalischen Endgeräten. Als LocksManagement System werden alle Schloss-Systeme und Wertgelasse verwaltet. Als umfassende Zutrittskontrolle lassen sich standortübergreifend sämtliche Tür-Zugänge und ohne mechanische Schlüssel steuern. Tagestresoren, Personenschleusen und weitere Endgeräten sind ebenfalls in die Access-Lösung integrierbar.

Automaten, Tresore und andere Wertgelasse mit netzwerkbasierten, elektronischen IP-Schloss-Systemen und Offline Schloss-Systeme kabellos über Einmalcode.

Tür-Zugänge mit Multi-Terminals (TCP/IP), Digitalen Schließsysteme (kabellos, offline)

MultiSafes (Tagestresore, CashSafes), Personenschleusen, Vereinzelungsschleusen Virtuelle Vereinzelung & Bilanzierung

Breite Hardware-Unterstützung und verschiedene Authentifizierungen

Die Lösung unterstützt verschiedne Authentifizierungs-Arten. Anwender können sich mit dem persönlichen Fingerabdruck identifizieren. Dies ist nicht nur für den Anwender praktisch, sondern bietet mehr Sicherheit, da die Echtheit des Anwenders verifiziert wird.

Mit & ohne Biometrie

Mit dem Einmalcode lassen sich temporäre und einmalige Öffnungscodes (OTC/OTP) erzeugen. Benutzer können in einem definierten Zeitraum für einen bestimmten Zugang berechtigt werden. Einmalcodes werden nach dem Gebrauch oder einer bestimmten Zeit ungültig.

Mit Einmalcode

Anwender öffnen mit persönlichen PIN-Codes. Für Tresorschlösser ist dies eine etablierte Öffnungsvariante, aber auch für den Zutritt stellt dies eine schnelle und flexible Möglichkeit dar, temporäre Berechtigungen an Externe zu vergeben.

Mit & ohne festen PIN

Anwender authentifizieren sich mit Ausweiskarten, Transpondern, Tags oder auch Armbändern. RFID-Medien können auch die Berechtigungen für Offline-Türen enthalten und lassen sich so – ganz ohne Kabel - zu einem virtuellen Netzwerk erweitern.
Karte, Transponder, Armband, TAGs & Keyfobs

Mit & ohne RFID-Technik

Bank-Betrieb intern

externer Cash-Logistik-Betrieb

Mit und ohne Netzwerk

Mit FlexCode

mit Hybrid-Funktionen

Für eine sichere Daten-Verschlüsselung wird ein manipulationsgeschütztes Sicherheitselement (Secure Element) verwendet, welches die kryptografischen Verfahren absichert und vor unberechtigtem Zugriff schützt. Das Element wurde nach Common Criteria (CC) EAL 6+ zertifiziert und entspricht somit höchsten Sicherheitsanforderungen. Die ISO Norm 15408 ist ein internationaler Standard zur Prüfung und Bewertung der Sicherheit von IT-Produkten. Sämtliche Daten werden nach kombinierten kryptographischen Verfahren, basierend auf symmetrischer Verschlüsselung nach dem Advanced Encryption Standard (AES) 256 bit und mit asymmetrischen Schlüssel mit RSA 2048 bit Optimal Asymmetric Encryption Padding (OAEP) verschlüsselt. Gemäß BSI Empfehlung „TR-02102-1" wird zusätzlich ein physikalischer Zufallszahlengenerator (TRNG) verwendet.

Höchste Datensicherheit

Professionelle Schlüsselverwaltung ISO 15408 zertifiziert

Optional können auch kundenseitige Schlüsselspeicher genutzt werden. Die Applikation unterstützt zur Anbindung externer HSM (Hardware Security Module) den Public Key Cryptography Standard (Cryptographic Token Interface Standard).

COMMON CRITERIA CERTIFIED ISO 15408

Zuverlässige & flexible IT-Architektur

Als IT-Architektur besteht die Wahl zwischen einer klassischen Client-Server-Lösung, einem SAAS-Modell oder einer dedizierten Hardware als embedded System. In der letztgenannten Variante kommt der Systemaufbau ohne zusätzliche Software-Installationen aus. Datensicherheit wird durch ein redundantes Backup erreicht. Zudem existieren Konzepte zur Sicherstellung der Verfügbarkeit und Wiederherstellung, sowie zyklischen Software-Pflege.

Die Administration und Verwaltung des System erfolgt bequem per Browser. Die Systemarchitektur ist Multi-User-fähig und ermöglicht die Verwaltung und Steuerung von verschiedenen Arbeitsplätzen durch unterschiedliche Verantwortliche. Software-Funktionen lassen sich differenziert unterschiedlichen Berechtigungsgruppen zuweisen.