WHITEPAPER

Mai 2025

Zusammenfassung

Wiegand ist zwar nach wie vor eine gängige Schnittstelle für Anwendungen in der Zutrittskontrolle, wird aber aufgrund seiner Sicherheitsmängel immer mehr zum Auslaufmodell. Unternehmen, die Wert auf Sicherheit legen, sollten auf OSDP umsteigen, um besser gegen Angriffe geschützt zu sein. OSDP bietet verschlüsselte, überwachte Kommunikation und ist damit die beste Wahl für sichere Umgebungen. Die Aufrüstung Ihres Systems für die Zutrittskontrolle mit OSDP bietet nicht nur mehr Sicherheit, sondern schützt Ihre Organisation auch vor neuen Bedrohungen.

Inhalt

1 Einführung 4
2 Zutrittskontrolle bei Lösungen für physische Sicherheit 4
3 Kommunikationsprotokolle Kartenleser-zu-Controller 4
3.1 Die alte Norm: Wiegand 5
3.2 Die sichere Alternative: OSDP 5
3.2.1 OSDP Verified 5
4 Wiegand- und OSDP-Kartenleser im Vergleich 5
4.1 Wiegand-Kartenleser 5
4.2 OSDP-Kartenleser 6
4.3 Nutzbarkeit 7
4.4 Sicherheit 7
5 Empfehlungen 8
6 Migration zu Wiegand OSDP 8
6.1 Option 1: Ersetzen der Wiegand-Kartenleser durch OSDP-Kartenleser 9
6.2 Option 2: Einsatz eines Konverters Wiegand-zu-OSDP 9

1 Einführung

Ein wichtiger Aspekt von Systemen zur Zutrittskontrolle sind die verwendeten Kommunikationsprotokolle.

In diesem Whitepaper werden die beiden wichtigsten Kommunikationsprotokolle zwischen Kartenleser und Tür-Controller in Zutrittskontrollsystemen vorgestellt. Wir werfen einen Blick auf ihre Vor- und Nachteile aus der Sicherheitsperspektive und erörtern, wie Sie mit der Migration zur sichereren Option beginnen können.

2 Zutrittskontrolle bei Lösungen für physische Sicherheit

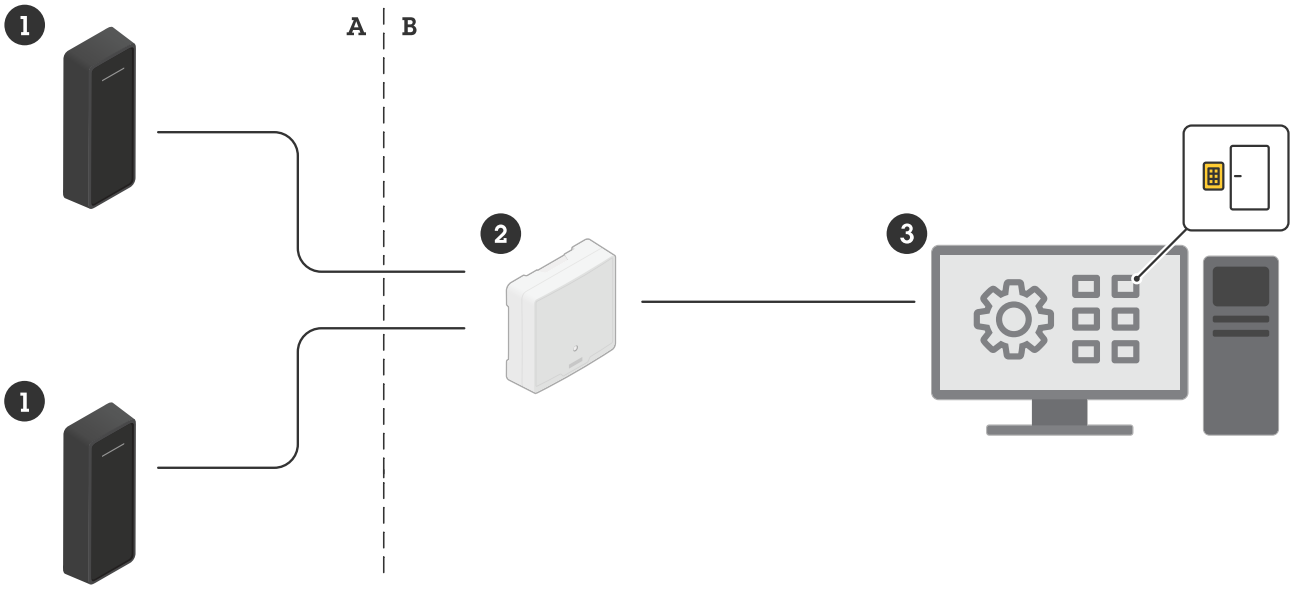
Zutrittskontrollsysteme sind für den Schutz von Gebäuden, Vermögenswerten und Menschen unerlässlich. Sie sorgen dafür, dass nur befugte Personen gesicherte Bereiche betreten können, was die Sicherheitsrisiken verringert und die Effizienz des Betriebs erhöht. Diese Systeme sind in verschiedenen Sektoren weit verbreitet, unter anderem in Unternehmensniederlassungen, Rechenzentren, Einrichtungen des Gesundheitswesens und Verwaltungsbehörden.

Ein typisches System zur Zutrittskontrolle besteht aus drei Hauptkomponenten.

1 Kartenleser für die Zutrittskontrolle: Geräte, die Benutzerausweise lesen und die Ausweisdaten an ein Kontrollgerät übertragen. Zu den typischen Benutzerzugangsdaten gehören Schlüsselkarten, mobile Zugangsdaten, PINs und biometrische Daten.

2 Tür-Controller: die Geräte, die Zugangsdaten verarbeiten und entscheiden, ob der Zugang gewährt oder verweigert wird.

3 Verwaltungssoftware: die Schnittstelle, über die Sicherheitsadministratoren Zugangsrichtlinien konfigurieren, Aktivitäten überwachen und Benutzer verwalten.



Bei der Zutrittskontrolle werden Kartenleser (1) außerhalb der Tür installiert (nicht gesicherter Bereich, A) und kommunizieren mit einem Tür-Controller (2), der auf der Innenseite installiert ist (gesicherter Bereich, B).

3 Kommunikationsprotokolle Kartenleser-zu-Controller

Im Laufe der Zeit haben sich die Protokolle für die Zutrittskontrolle weiterentwickelt und die Sicherheit, Funktionalität und Integrationsfähigkeit verbessert. Sehen wir uns die beiden Hauptprotokolle genauer an.

3.1 Die alte Norm: Wiegand

Wiegand überträgt die Ausweisdaten vom Kartenleser zum Steuergerät über zwei Datenleitungen. Wiegand ist seit Jahrzehnten bekannt und wird nach wie oft genutzt, hauptsächlich wegen seiner Einfachheit und der Kompatibilität mit älteren Systemen.

Der größte Nachteil von Wiegand ist die geringe Sicherheit. Vor allem fehlt es an Verschlüsselung. Die Daten werden im Klartext übertragen, was sie anfällig für Abhör- und Klonangriffe macht.

3.2 Die sichere Alternative: OSDP

Das Open Supervised Device Protocol (OSDP) wurde von der Security Industry Association (SIA) entwickelt, um die Interoperabilität zwischen Zutrittskontroll- und Sicherheitsprodukten zu verbessern. OSDP wurde von der Internationalen Elektrotechnischen Kommission als internationaler Standard zugelassen und führt AES-128-Verschlüsselung, bidirektionale Kommunikation und Geräteüberwachung in Echtzeit ein. Da der Controller mit OSDP Befehle an den Kartenleser zurücksenden kann, werden auch Funktionen wie LED-Steuerung, Aktivierung des Summers und Manipulationserkennung aktiviert.

Ein Hauptmerkmal von OSDP ist der Modus "Secure Channel", der die sichere Übertragung von Zulassungsrohdaten zwischen Smart Card-Lesern und Controllern ermöglicht. Dies ist besonders nützlich für fortgeschrittene Authentifizierungsmethoden, wie z. B. die Validierung biometrischer und mobiler Zugangsdaten.

3.2.1 OSDP Verified

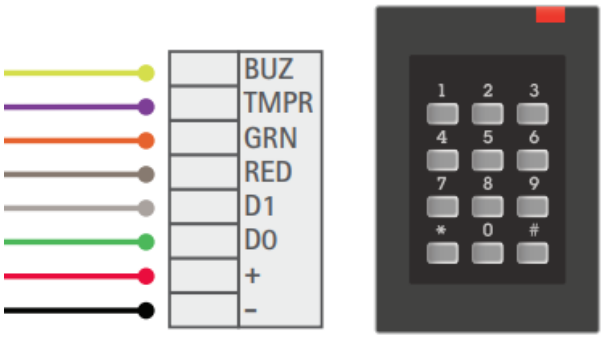
Das SIA OSDP Verified-Programm ist ein umfassendes Prüfprogramm, das die Konformität eines Geräts mit dem OSDP-Standard und den zugehörigen Leistungsprofilen bestätigt. SIA führt eine Liste verifizierter Geräte, die getestet wurden und die Kriterien des Standards und der in der Liste angegebenen Profile erfüllt haben. Die in der Liste aufgeführten Geräte können das OSDP-Prüfzeichen in Marketingmaterialien verwenden.

Das OSDP-Prüfzeichen gibt Integratoren, Planern und Anwendern die Gewissheit, dass OSDP-Geräte für verschiedene Schutzziele der Zutrittskontrolle wie vorgesehen funktionieren.

4 Wiegand- und OSDP-Kartenleser im Vergleich

Kartenleser haben unterschiedliche Stärken und Schwächen, je nachdem, welches Kommunikationsprotokoll sie verwenden.

4.1 Wiegand-Kartenleser



Ein Wiegand-Kartenleser und seine Verkabelung, einschließlich zusätzlicher Kabel für Summer, Melder zur Manipulationserfassung und LEDs.

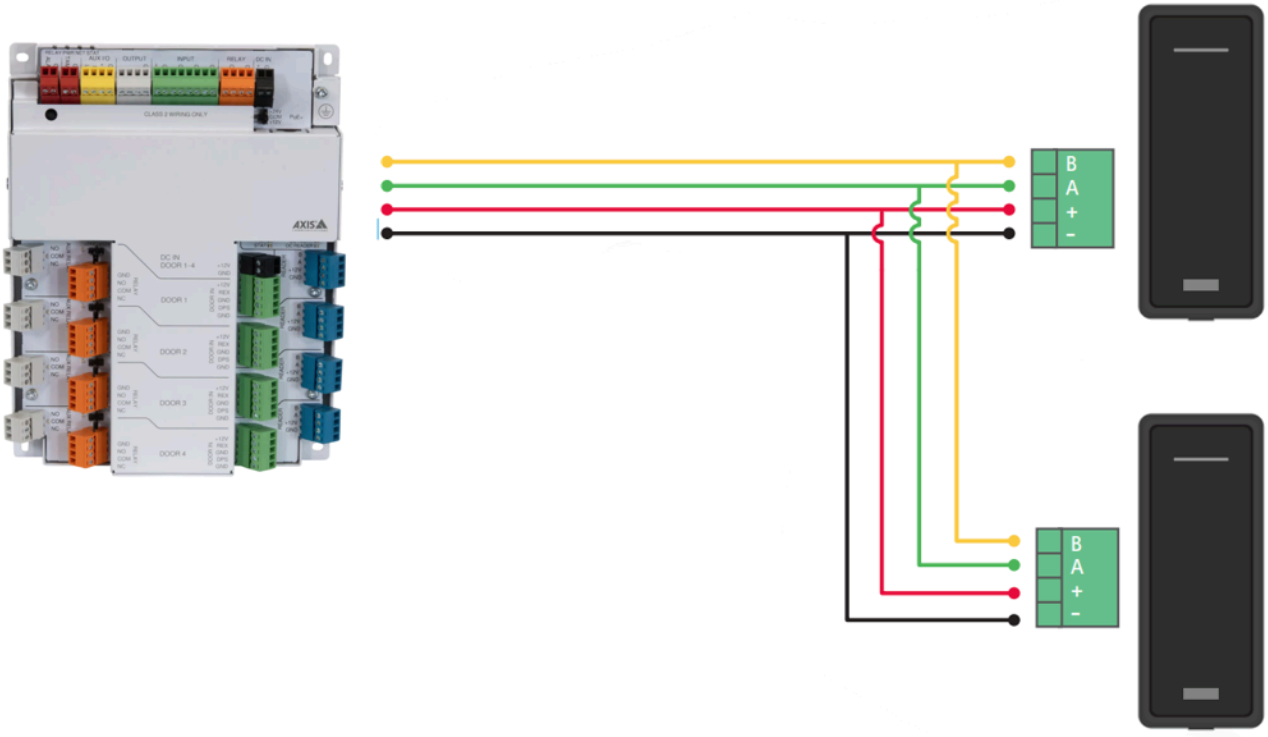
Vorteile:

- Einfach und weitgehend kompatibel mit älteren Systemen.

Nachteile:

- Keine Verschlüsselung. Die Daten werden im Klartext übertragen und können so leicht abgefangen werden.
- Einseitige Kommunikation. Der Controller kann keine Befehle an den Kartenleser zurücksenden. Das bedeutet, dass es keine Möglichkeit gibt zu erkennen, ob ein Kartenleser manipuliert oder ausgetauscht wurde - der Kartenleser ist unbeaufsichtigt.
- Komplexe Verkabelung. Ein Kartenleser, der die Wiegand-Protokolle nutzt, benötigt zusätzliche Kabel für den Summer des Kartenlesers, den Melder zur Manipulationserkennung und die LEDs.
- Die maximale Kabeldistanz beträgt 150 Meter (500 Fuß).

4.2 OSDP-Kartenleser



OSDP-Kartenleser (rechts) und ihre Verkabelung mit einem Tür-Controller (links). Funktionen wie LED-Steuerung, Summeraktivierung und Überwachung der Kartenleser erfordern keine zusätzlichen Kabel.

OSDP nutzt eine RS-485-Verkabelung. Dies ist ein serieller Kommunikationsstandard zur Datenübertragung über große Entfernungen mit Hilfe von Twisted-Pair-Kabeln. Es wird üblicherweise in Systemen eingesetzt, die eine zuverlässige Mehrpunktkommunikation erfordern. Zu den wichtigsten Merkmalen gehören die Fernübertragung und die Multidrop-Fähigkeit.

Vorteile:

- Verschlüsselte Kommunikation verhindert das Abfangen von Zugangsdaten.
- Mit OSDP kann der Controller Befehle an den Leser zurücksenden. Dieser bidirektionale Datenaustausch ermöglicht Überwachung und Fernkonfiguration. Außerdem wird dadurch die Verkabelung vereinfacht.
- Die RS-485-Verkabelung lässt eine längere maximale Kabelstrecke zu.
- Multidrop aktiviert mehrere Leser, die sich eine einzige Verbindung teilen.

4.3 Nutzbarkeit

Tabelle 4.1 *Vergleich der Nutzbarkeit von Wiegand- und OSDP-Kartenlesern.*

	Wiegand	OSDP
Sicherheit	Keine Verschlüsselung, anfällig für Hackerangriffe	AES-128-Verschlüsselung, Manipulationserfassung
Kommunikation	Einweg (Kartenleser zu Controller)	Zwei-Wege
Kabeldistanz	bis zu 150 Metern (ca. 500 Fuß)	bis zu 1.200 Metern (ca. 4.000 Fuß)
Multidrop	Nein, ein Gerät ein Bus	Ja, Unterstützung mehrerer Geräte an einem Bus
Manipulationserkennung	Nein, zusätzliche Verkabelung erforderlich	Ja
Überwachung	Nein, zusätzliche Verkabelung erforderlich	Ja
Datenintegrität	Anfällig für Replay-Angriffe auf Zugangsdaten	Verschlüsselte, sichere Übertragung
Komplexität der Installation	Komplexe Verdrahtung (D0/D1 und LEDs, Melder zur Manipulationserkennung, Summer)	Einfach (RS-485, A und B)
Skalierbarkeit	Begrenzt durch Verdrahtungszwänge	Kann mehrere Kartenleser in einer Daisy-Chain verbinden
Bestes Schutzziel	Ältere Systeme, geringer Sicherheitsbedarf	Moderne sichere Installationen in Ämtern und Behörden oder Unternehmen

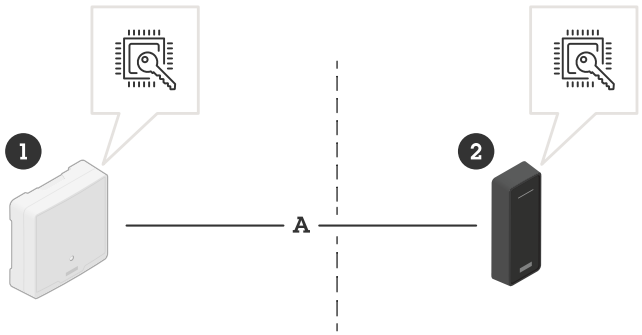
4.4 Sicherheit

Bei der Wahl eines Protokolls für die Zutrittskontrolle sollte die Sicherheit an erster Stelle stehen. Die fehlende Verschlüsselung von Wiegand führt zur Anfälligkeit für verschiedene Arten von Angriffen.

- Abfangen von Zugangsdaten. Angreifer können Datenleitungen abhören und Zugangsdaten erfassen.
- Replay-Angriffe. Einmal aufgezeichnet, können dieselben Zugangsdaten erneut wiedergegeben werden, um unbefugten Zutritt zu erhalten.
- Sabotage. Das System kann nicht erkennen, ob ein Kartenleser entfernt oder ersetzt wurde.

Im Kontrast dazu mildert OSDP diese Risiken durch Datenverschlüsselung mit AES-128 (Secure Channel) und Geräteüberwachung. So ist gewährleistet, dass der Controller die Erfassung von Manipulationen an einem Kartenleser detektieren kann und somit unbefugten Zutritt verhindert.

Durch die Verschlüsselung sind die Daten sicher, aber durch den Schutz der Schlüssel ist auch die Verschlüsselung sicher. Ohne starken Schlüsselschutz kann das gesamte System gefährdet sein. Deshalb sollten die Schlüssel für Secure Channel in einem speziellen Hardware-Chip an beiden Enden - Controller und Kartenleser - gesichert sein. Diese sicheren Hardwarebereiche, wie z. B. sichere Elemente, sind so konstruiert, dass Angreifer nicht an die Schlüssel gelangen können, selbst wenn sie physischen Zugriff auf das Gerät erhalten.



End-to-End-Sicherheit mit einem sicheren Schlüsselspeicher bei der Zutrittskontrolle. Der Master Key und der individuelle Secure Channel Base Key (SCBK) werden beide in sicheren Schlüsselspeichern in Geräten auf beiden Seiten der Tür aufbewahrt.

1 *Tür-Steuerung, installiert auf der sicheren Seite der Tür*
2 *Installation des Kartenlesers an der nicht gesicherten Seite der Tür*
3 *A: OSDP Secure Channel-Kommunikation*

Tabelle 4.2 *Vergleich der Sicherheitsaspekte von Wiegand- und OSDP-Kartenlesern.*

	Wiegand	**OSDP**
Verschlüsselung	Keine, Klartextdaten	AES-128-Verschlüsselung
Abfangen von Daten	Leicht abzufangende Zugangsdaten	Verschlüsselt, um Abhören zu verhindern
Replay-Angriffe	Zugangsdaten können kopiert/ wiedergegeben werden	Verhindert durch Verschlüsselung
Manipulationserkennung	Nein, kann manipulierte Kartenleser nicht detektieren	Ja, der Controller überwacht den Status des Kartenlesers
Überwachung	Nein, der Controller kann den Status des Kartenlesers nicht überprüfen	Ja, Überwachung in Echtzeit
Compliance	Nicht empfohlen für sichere Umgebungen	Erfüllt moderne Sicherheitsstandards

5 Empfehlungen

In der heutigen Sicherheitslandschaft ist Wiegand für neue Installationen keine gangbare Lösung mehr. Organisationen sollten auf OSDP-Kartenleser umsteigen, um mehr Sicherheit, Zuverlässigkeit und zukünftige Skalierbarkeit zu gewährleisten.

- Bewerten Sie Ihre derzeitige Infrastruktur für die Zutrittskontrolle. Wenn Sie derzeit Wiegand nutzen, sollten Sie eine Strategie für die Migration zu Wiegand planen. Bestimmen Sie, ob eine vollständige OSDP-Migration oder ein Konverter Wiegand-zu-OSDP die beste Option ist.
- Wählen Sie bei neuen Installationen nach Möglichkeit OSDP-Kartenleser, um eine verschlüsselte, manipulationssichere Kommunikation zu gewährleisten.
- Arbeiten Sie mit Sicherheitsexperten zusammen, um ein sicheres, modernes System zur Zutrittskontrolle zu implementieren, das vor Bedrohungen schützt.

6 Migration zu Wiegand OSDP

Viele Organisationen setzen nach wie vor auf Wiegand-Kartenleser, wollen aber die Sicherheit erhöhen, ohne ihr gesamtes System auszutauschen. Es gibt zwei praktische Migrationspfade. Beide Optionen verbessern die

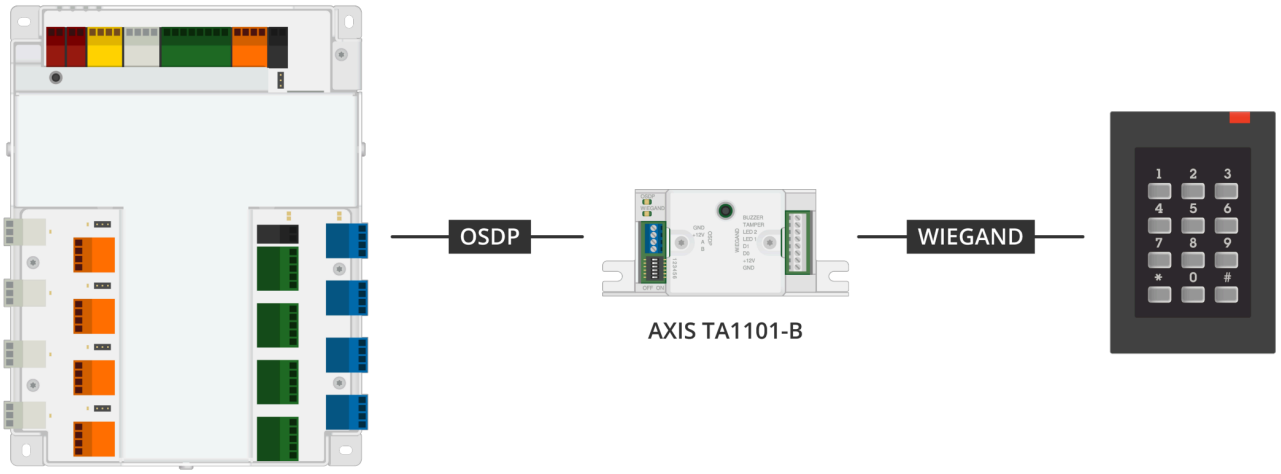
Sicherheit, aber die direkte OSDP-Implementierung ist die beste langfristige Investition für Organisationen, die ihre Systeme für die Zutrittskontrolle zukunftssicher machen wollen.

6.1 Option 1: Ersetzen der Wiegand-Kartenleser durch OSDP-Kartenleser

Dies ist die beste langfristige Lösung. Durch den Ersatz veralteter Wiegand-Kartenleser durch OSDP-kompatible Modelle können Organisationen von Verschlüsselung, Zwei-Wege-Kommunikation und Leserüberwachung profitieren. Dazu muss jedoch sichergestellt sein, dass die Zutrittskontrolle OSDP unterstützt.

6.2 Option 2: Einsatz eines Konverters Wiegand-zu-OSDP

Für Unternehmen, die nicht in der Lage sind, alle Kartenleser sofort zu ersetzen, ist ein Konverter Wiegand-zu-OSDP eine kostengünstige Alternative. Dieses Gerät verschlüsselt Wiegand-Daten, bevor sie an einen OSDP-kompatiblen Controller gesendet werden, und erhöht so die Sicherheit, ohne dass eine komplette Überholung der Hardware erforderlich ist.



Sie können die Sicherheit verbessern, indem Sie einen Konverter Wiegand-zu-OSDP einsetzen (Mitte).

T10227329_DE/DE/M1.7/2505

Über Axis Communications

Axis ermöglicht eine smartere und sichere Welt durch die Verbesserung von Sicherheit, Schutz, betrieblicher Effizienz und Geschäftsanalytik. Als Technologieführer im Bereich Netzwerk-Video bietet Axis Videosicherheits-, Zutrittskontroll-, Intercom- und Audiolösungen. Die branchenweit anerkannten Schulungen der Axis Communications Academy vermitteln fundiertes Expertenwissen zu den neuesten Technologien.

Das 1984 gegründete schwedische Unternehmen beschäftigt etwa 5.000 engagierte MitarbeiterInnen in über 50 Ländern und bietet mit Technologie- und Systemintegrationspartnern auf der ganzen Welt kundenspezifische Lösungen an. Der Hauptsitz ist in Lund, Schweden.

© 2025 — Axis Communications AB. AXIS COMMUNICATIONS, AXIS, ARTPEC und VAPIX sind in verschiedenen Jurisdiktionen eingetragene Marken von Axis AB. Alle anderen Marken sind Eigentum ihrer jeweiligen Inhaber.Wir behalten uns das Recht auf Änderungen ohne Vorankündigung vor.