

Elektronische Zutrittsorganisation - der neue Standard

Elektronische Schließanlagen entwickeln sich bei Behörden, Industrieunternehmen, Gewerbegebäuden, Krankenhäusern und immer häufiger auch bei Büro- und Wohngebäuden zum Standard. Sie verdrängen damit sowohl die traditionellen mechanischen Schließanlagen (mechanische Profilzylinder) als auch die herkömmlichen Online Zutrittskontrollsysteme (kabelgebunden vom Server mit der Verwaltungssoftware bis zum Leser an der Tür). Dieses Whitepaper ermöglicht Ihnen, bereits im frühen Planungsstadium die für eine elektronische Schließanlage wesentlichen Planungseckpunkte in Ihre Überlegungen einzubeziehen. Für weiterführende Gedanken stehen Ihnen unsere Ansprechpartner im Außendienst und im Produktmanagement gerne zur Verfügung.

1. Die charakteristischen Systemvarianten und deren Funktionsmerkmale sind in der nachfolgenden Tabelle dargestellt und werden im Anschluss erläutert

Ausprägung der Schließsysteme:	Mechanische Schließanlage	Zutrittskontrolle online - klassisch ¹	Elektronische Schließanlage		
			Funkvernetz	Offline - klassisch	Virtuell vernetzt ¹
Anschaffungskosten	😊	😞	😞	😊	😊
Laufende Kosten	😊	😊	😊	😊	😊
Installationsvoraussetzungen System (Kabel/Leitungen)	😊	😊	😊	😊	😊
Installationsvoraussetzungen Tür (E-Öffner, Motorschlösser)	😊	😞	😊	😊	😊
Zusätzliche Systemkomponenten (Router, Aufbuchleser)	😊	😞	😞	😊	😊
Batteriestandzeiten	-	-	😞	😊	😊
Kosten bei Schlüsselverlust	😞	😊	😊	😊	😊
Kosten bei wesentlichen Berechtigungsänderungen	😞	😊	😊	😊	😊
Flexibilität	😞	😊	😊	😊	😊
Komfort	😞	😊	😊	😊	😊

¹ Einige Systeme bieten die Möglichkeit, eine virtuell vernetzte elektronische Schließanlage und eine klassische kabelgebundene Online-Zutrittskontrolle zu kombinieren und somit Bereiche mit höheren Anforderungen an die Sicherheit gemeinsam in einer Zutrittsorganisation abzusichern (Beispiel Serverräume).

2. Erläuterung der Systemvarianten

Mechanische Schließanlage

Traditionelle mechanische Schließanlagen bieten eine einfache und schnelle Montage im Schloss der Tür. Zusätzliche Komponenten werden in diesen Türen nicht benötigt. Diese Schließanlagen unterliegen jedoch starren hierarchischen Strukturen und müssen für eine Anlagenfertigung grundsätzlich anhand eines Schließplanes geplant werden. Bei betrieblichen Organisationsänderungen bietet eine mechanische Schließanlage eine sehr begrenzte Flexibilität. Hinzu kommt, dass bei einem Schlüsselverlust in der Regel eine größere Anzahl von Zylindern und Schlüsseln ersetzt werden muss, um die Sicherheit des Gebäudes wieder herzustellen. Neben den eigentlichen Kosten für die Neuanschaffung sind Sie mit dem meist weit größeren Problem der zwischenzeitlichen Sicherheitslücke konfrontiert. Ggf. sind bis zur Installation einer neuen Schließanlage sogar Wachdienste einzusetzen. Hinzu kommt der meist sehr hohe Handlingaufwand inkl. Schlüsselausgabe im Rahmen des Einbaus einer neuen Schließanlage. Selbstredend kann eine mechanische Schließanlage zielführend sein und bei guter Planung auch gewisse Freiheit bieten. Gegenüber der Flexibilität elektronischer Schließanlagen sind diese mechanischen Schließanlagen allerdings immer im Nachteil.

Zutrittskontrolle - online - klassisch

Die Daten, z.B. Zutrittsberechtigungen und Sperrungen, werden zentral (Server) verwaltet. Über die Kabelinfrastruktur (Ethernet/LAN, KNX/EIB oder seriell per RS485 vernetzt) werden die Daten direkt vom PC-Arbeitsplatz versendet. Die Verkabelung muss bis zum Zutrittsleser an der Tür und in die Tür (Klinke, Riegelschaltkontakt, Zustandssensorik) erfolgen und es werden auch weitere Komponenten an der Tür benötigt (Beispiel E-Öffner, Motorschloss). Die Zutrittsrechte sind direkt nach der Über-

tragung an der Tür wirksam. Bei entsprechender Ausstattung der Türen kann deren Status (offen, geschlossen, verriegelt) permanent überwacht werden. Auch eine Anbindung an die Gebäudeleittechnik ist möglich.

Elektronische Schließanlage – funkvernetzt

Die funkvernetzte Zutrittskontrolle verbindet batteriebetriebene Komponenten wie elektronische Zylinder, Beschläge oder Leser über spezielle Gateways. Diese werden meist für die zentrale Verwaltung der Anlage über eine Kabelinfrastruktur (LAN) oder auch per WLAN angebunden. Vom Gateway aus werden die Zutrittsrechte per Funk an die batteriebetriebenen Komponenten übertragen. Diese Anlagenart erfordert eine intensivere Projektierung, da eine Funkfeldmessung notwendig ist. Im Vergleich zur klassischen verkabelten Online-Zutrittskontrolle ist sie störanfälliger in Bezug auf die Datenübertragung. Bei der Funkvernetzung kommen meist Übertragungsfrequenzen von 868 MHz bis 2,4 GHz zum Einsatz. Gängige Standards sind enOcean, Zigbee, Bluetooth Low Energy und WLAN. Technologiebedingt gibt es Restriktionen bzgl. Reichweiten, gerade im Gebäudeinneren, aber auch bzgl. maximaler Türkomponenten je Gateway. Durch den meist hohen Energieverbrauch für Echtzeitanwendungen im Bereich der Funkvernetzung sind die Batteriestandzeiten funkvernetzter Türkomponenten deutlich geringer als bei offline- oder virtuell vernetzten Türkomponenten. Bei Ortsveränderung von Komponenten ist mitunter ein neues Anlernen an ein anderes Gateway erforderlich.

Elektronische Schließanlage – offline – klassisch

Zutrittsberechtigungen oder -sperrungen (Transaktionen) werden am PC-Arbeitsplatz in der Verwaltungssoftware programmiert und jeweils einzeln vom Verwalter der Schließanlage an die betroffenen Türkomponenten übertragen. Hier wird umgangssprachlich von „Turnschuh“-Programmierung gesprochen. Die Übermittlung der so genannten Transaktionen erfolgt je nach Systemanbieter mit einem zum Schließsystem gehörenden Programmiergerät und/oder Programmierschlüssel. Bei einigen Systemanbietern muss das Programmiergerät auch zum Zeitpunkt der Komponentenprogrammierung mit einem Laptop verbunden sein. Diese Anlagenart empfiehlt sich bei kleinen Schließanlagen und bei solchen Anlagen, bei denen selten Berechtigungsänderungen erforderlich sind. Ansonsten sind durch die Laufwege bei der „Turnschuh“-Programmierung häufige Berechtigungsänderungen aufwändig.

Elektronische Schließanlage – virtuell vernetzt

Zutrittsberechtigungen oder -sperrungen werden am PC-Arbeitsplatz in der Verwaltungssoftware hinterlegt und über ein so genanntes virtuelles Netzwerk an die Türkomponenten übertragen. Als virtuell wird das Netzwerk deshalb bezeichnet, weil keine klassische Datenverbindung zu den Türkomponenten, beispielsweise über ein Bus-System, besteht. Stattdessen wird der Schlüssel als Träger für Daten und Befehle innerhalb einer Schließanlage genutzt. Er dient als Bindeglied zwischen einem oder mehreren online an die Verwaltungssoftware angebundenen Lesern im virtuellen Netzwerk, meist Aufbuchleser genannt, und den Türkomponenten. Der Aufbuchleser ist zuständig für die Übertragung der Informationen von den und auf die Identmedien des Nutzers (z.B. Transponderschlüssel). Aufbuchleser werden typischerweise an neuralgischen Punkten am Gebäude montiert und können direkt auch als Zutrittsleser genutzt werden. Der Nutzer merkt gar nicht, dass im Hintergrund Daten und Befehle ausgetauscht werden. Abhängig vom Hersteller des Schließsystems beinhalten Aufbuchleser auch eine Zutrittskontrollfunktion für eine parallele Türöffnung.

Je nach Systemanbieter können Türkomponenten (z.B. elektronische Zylinder) über die Identmedien auch untereinander Informationen übertragen (viraler Sperrbefehl) und Statusmeldungen wie Batteriewarnmeldungen und die Anzahl der bisher erfolgten Schließungen (Schließungszähler in der Komponente) selbstständig über das virtuelle Netzwerk an die Verwaltungssoftware senden.

Die Anbindung der Aufbuchleser erfolgt meist kabelgebunden mittels eines so genannten COM-Servers, über den die Einbindung in das LAN des Kunden aufgebaut wird. Bei einigen Systemanbietern ist parallel zum virtuellen Netzwerk zusätzlich eine Übermittlung der Transaktionen mit dem Programmiergerät und/oder Programmierschlüssel möglich (Mischbetrieb) oder sogar erforderlich, weil für eine Sperrung Identmedien physikalisch vorliegen müssen. Ein Merkmal ausgereifter virtuell vernetzter Systeme ist die automatische Rückprotokollierung von ausgeführten Transaktionen in die Datenbank der Verwaltungssoftware. Dies ist von hoher Bedeutung, damit die Datenbank konsistent ist. Der große Vorteil einer virtuellen Vernetzung liegt zusammengefasst darin, dass die Mehrzahl aller Türen im Objekt bis auf die Aufbuchleser nicht verkabelt oder über Gateways angebunden werden muss und somit die Flexibilität der Online-Zutrittskontrolle mit dem Komfort von Offline-Schließanlagen zusammenwächst.

3. Systemvarianten und Transpondertypen im Vergleich

Benutzer-Identmedien	Identmedien - kontaktbehaftet ¹		Identmedien - berührungslos ²				
	Transponder-schlüssel aktiv	Transponder-schlüssel passiv	Schlüsselanhänger passiv, RFID	Funktransponder aktiv	Transponderkarte passiv, RFID	Transponder-schlüssel aktiv, RFID	Transponder-schlüssel passiv, RFID
Wartungsfrei	☹️	😊	😊	😐	😊	😐	😊
Ohne Batterie	☹️	😊	😊	☹️	😊	☹️	😊
Kosten	☹️	😐	😐	😐	😊	☹️	😐
Robustheit	😐	😐	😊	😐	☹️	😐	😊
Bedienung von:							
Online-Leser	☹️	😐	😊	😊	😊	😊	😊
Offline-Leser	😐	😐	😊	😊	😊	😊	😊
Aktive Doppelknäufzylinder	☹️	☹️	😊	😊	😊	😊	😊
Passive Doppelknäufzylinder	☹️	☹️	☹️	😊	☹️	😊	☹️
Aktive flächenbündige Zylinder	😊	☹️	☹️	😊	☹️	😊	😊
Passive flächenbündige Zylinder	😊	😊	☹️	☹️	☹️	😊	☹️
Elektronische Türbeschläge	☹️	☹️	😊	😊	😊	😊	😊
Schrank-/Spindschloss	😐	😐	😊	😊	😊	😊	😊

¹ Eine kontaktbehaftete Chip-Karte oder ein kontaktbehafteter mechatronischer Schlüssel benötigt einen elektrischen Kontakt zur Daten- und Energieübertragung zwischen dem Chip im Identmedium und der Türkomponente. Kontaktbehaftete Identmedien lassen nur den Einsatz an einer eingeschränkten elektronischen Komponentenauswahl zu, können jedoch mit mechanischen Profilzylindern kombiniert werden. Um eine komfortable berührungslose Türöffnung über Offline- oder Online-Leser zu ermöglichen, werden mechatronische Schlüssel vielfach zusätzlich mit einem separat zu programmierenden RFID-Transponder im Schlüsselkopf ausgestattet.

² Berührungslose Identmedien übertragen die Daten mittels Radio Frequency Identification (RFID) und stehen für ein automatisches sowie berührungsloses Authentifizieren (Sender-Empfänger-System). Diese Übertragungsart ist kontaktlos und daher nicht verschleißbehaftet. Bei aktiven Identmedien erfolgt nicht nur die Datenübertragung, sondern auch die Energieübertragung an die Türkomponente berührungslos. Aktive Identmedien benötigen jedoch eine eigene Energieversorgung und sind daher nicht wartungsfrei. Passive RFID-Identmedien benötigen keine Spannungsversorgung und sind daher wartungsfrei.

4. Die im Allgemeinen bekannten und gängigen Hardware-/Türkomponenten

Offline-/Online-Leser

- Berührungslose Prüfung der Berechtigung durch das Vorhalten des Identmediums (RFID-Transponderkarte, -anhänger, -schlüssel)
- Berührungslose Prüfung der Berechtigung nach dem Betätigen der Funktionstaste des Identmediums (Funktransponder aktiv)
- Kontaktbehaftete Prüfung der Berechtigung durch Einstecken des Identmediums bis zum Kontaktschluss (Chipkarte, mechatronischer Schlüssel)
- Automatische Öffnung und Zuhaltung durch angeschlossene Türkomponente, beispielsweise mittels E-Öffner
- Systemvoraussetzung für einen versicherungstechnischen Verschluss ist ein Motorschloss

Elektronischer Türbeschlag

- Berührungslose Prüfung der Berechtigung durch das Vorhalten des Identmediums (RFID-Transponderkarte, -anhänger, -schlüssel)
- Berührungslose Prüfung der Berechtigung nach dem Betätigen der Funktionstaste des Identmediums (Funktransponder aktiv)
- Systemvoraussetzung für einen versicherungstechnischen Verschluss ist ein selbstverriegelndes Schloss

Schrank-/Spindschloss

- Berührungslose Prüfung der Berechtigung durch das Vorhalten des Identmediums (RFID-Transponderkarte, -anhänger, -schlüssel)
- Berührungslose Prüfung der Berechtigung nach dem Betätigen der Funktionstaste des Identmediums (Funktransponder aktiv)
- Automatische Öffnung des Schrank-/Spindschlusses

Doppelknäufzylinder

- Berührungslose Prüfung der Berechtigung durch das Vorhalten des Identmediums (RFID-Transponderkarte, -anhänger, -schlüssel)
- Berührungslose Prüfung der Berechtigung nach dem Betätigen der Funktionstaste des Identmediums (Funktransponder aktiv)
- Anschließend Öffnung oder Verschluss der Tür durch Drehen des Zylinderknäufes
- Funktion auf Grund der Knäufgröße nicht an allen Türen gegeben (Beispiel Rohrrahmentür mit geringem Dornmaß – Knäuf blockiert Türöffnung)
- Insbes. bei geringen Dornmaßen gilt es, die Norm (vgl. u.a. DGUV 81, GUV-R 1/494, BGR 232) zu beachten für einen effektiven Schutz vor Einklemmen von Fingern oder Händen
- Ungewohntes Schließverhalten erfordert meist zwei Hände (eine Hand Identmedium, andere Hand Knäufdrehung) und führt zu Irritationen beim Nutzer, vor allem beim Verriegeln der Tür (Ist Zylinder wirklich eingekuppelt?)

Flächenbündige Zylinder

- Berührungslose Prüfung der Berechtigung beim Einstecken des Identmediums (RFID-Transponderschlüssel)
- Kontaktbehaftete Prüfung der Berechtigung durch Einstecken des Identmediums bis zum Kontaktschluss (mechatronischer Schlüssel)
- Öffnung und Verschluss der Tür durch Drehen des Schlüssels (wie von der mechanischen Schließanlage gewohnt)
- Durch die Flächenbündigkeit auch für historische Türen geeignet (Denkmalschutz)
- Geringstmögliche Vandalismusgefahr (z.B. abgetretene Knäufe in Fußballstadien)
- Geringstmögliche Gefahr der Beschädigung im normalen Betriebsablauf (z.B. abgefahrene Knäufe durch Servicewagen oder Krankenhausbetten)

5. Verwaltungssoftware-Lösungen und Hosting-Modelle im Vergleich

Systemsoftware	Hersteller-Cloud - Token	Hersteller-Cloud - Mieten	Lokale Einzelplatz-Installation	Lokale Server-/Client-Installation
Offline - netzwerkunabhängig				
Ohne Netzwerk nutzbar				
Ohne Internet nutzbar				
Daten im eigenen Haus				
Anschaffungskosten				
Folgekosten				
Unabhängig vom Hersteller nutzbar				

6. Software-Installations-Nutzungsvarianten

Hersteller-Cloud-Lösung – Tokens (kostenpflichtige Berechtigungsänderung)

Die Software läuft auf den Servern des Herstellers bzw. auf vom Hersteller angemieteten Servern (Beispiele: AWS, Microsoft Azure, Google Cloud Platform [GCP]). Somit befinden sich die jeweiligen Schließanlagendaten (komplette Berechtigungsstruktur sowie die Nutzerdaten, ggf. auch Bewegungsdaten) auf externen Servern und außerhalb des Unternehmens. Für die Nutzung ist eine aktive Internetverbindung mit ausreichender Übertragungsrate erforderlich. Notwendige Berechtigungsänderungen (Transponderverluste, Zutrittsänderungen, beispielsweise durch Mitarbeiterzu- und -abgänge sowie Versetzungen, oder Organisationsveränderungen) werden vom Anbieter in Form von Tokens in Rechnung gestellt. Je nach Anbieter entstehen unterschiedliche Kosten. Eine Abhängigkeit von geplanten und ungeplanten Wartungszeitfenstern (Downtimes) der Cloud-Services ist in die geplante Verfügbarkeit der Schließanlage einzuberechnen. Bzgl. der EU-Datenschutzgrundverordnung (EU-DSGVO) ist neben anderen Voraussetzungen zwingend darauf zu achten, dass ein Hosting auf innerhalb der EU befindlichen Servern erfolgt.

Hersteller-Cloud-Lösung – Miete/Software as a Service (SaaS)

Der Unterschied zum o.g. Token-Modell ist, dass beim Mieten unabhängig von der Anzahl an Berechtigungsänderungen ein monatliches oder jährliches Nutzungsentgelt mit dem jeweiligen Systemanbieter vereinbart wird. Das Nutzungsentgelt ist wiederum abhängig von der Anzahl der verwalteten Systemkomponenten und/oder der Anzahl der Mitarbeiterstammdatensätze. In diesem Fall sind neben den Preisanpassungen auch die Laufzeiten abzuklären. Eine Abhängigkeit von geplanten und ungeplanten Wartungszeitfenstern (Downtimes) der Cloud-Services ist in die geplante Verfügbarkeit der Schließanlage einzuberechnen.

Lokale Einzelplatz-Installation – Kauf

Eine Einzelplatzlizenz beinhaltet ein zeitlich unbegrenzt Recht zur Nutzung an einer Verwaltungssoftware, die nur auf einem PC-Arbeitsplatz installiert wird und somit an einen Desktop-PC oder Laptop gebunden ist.

Lokale Server-/Client-Installation – Kauf

Eine Client-Server-Lösung beinhaltet ein zeitlich unbegrenzt Recht zur Nutzung an einer Verwaltungssoftware. Die Verwaltungssoftware wird auf dem nutzereigenen Server installiert. Auf den PC-Arbeitsplätzen wird jeweils ein lokaler Software-Client installiert. Eine standortübergreifende Programmierung/Softwarebetreuung mit mehreren Usern wird somit auf derselben Datenbank ermöglicht. Einige Hersteller bieten Web-Clients an. Der Unterschied besteht darin, dass der Anwender die Verwaltungssoftware in einem Web-Browser öffnet. Bei leichten wartungsseitigen Vorteilen gibt es hier mitunter Nachteile bzw. Einschränkungen bzgl. der Kompatibilität mit bestimmten Browsern oder Versionen von Browsern.

7. Schnittstellen zu Drittsystemen

Neben den Softwarevarianten, den Hardwarekomponenten und den Transponderformen sind auch weiterführende Themen und Schnittstellen zu anderen Systemlösungen zu ermitteln. Welche Systeme sollen in die Zutrittskontrolle mit eingebunden werden, um zukünftig z.B. mit einem Identmedium mehrere Systeme bedienen zu können? Es kann sich dabei um zukünftige Fremdsysteme handeln, aber auch um bereits im Bestand befindliche Systeme, wie beispielsweise:

- Mitarbeiterzeiterfassung
- Einbruchmeldeanlage (EMA)
- Fluchtwegsteuerung
- Kantinenabrechnung
- Kleider-Wäscheausgabenautomaten (Krankenhäuser)
- Gebäudeleittechnik
- Drucker-/Kopierer-System
- PC-Anmeldung
- Externes Besprechungsraummanagement

8. Mögliche Türausstattungen mit Auswirkung auf das Schließsystem

Nach einer Systementscheidung sind auch die Schnittmengen zu anderen Gewerken (z.B. Elektriker/Türlieferant/Aufzugsbauer) zu prüfen und zu klären. Welche Verschlusstechnik sollte je nach Sicherheitseinstufung und Komfort an den Außen- und Innentüren zum Einsatz kommen? Sind dafür Kabel/Leitungen erforderlich und ggf. das Setzen von Unterputzdosen? Dazu nachfolgend ein Auszug zu Verschluss-/Türkomponenten.

- Selbstverriegelnde Schlösser (mechanisch oder motorisch)
- Mehrfachverriegelungen, mechanisch oder motorisch
- E-Öffner (Zuhaltung der Tür)
- Türantrieb
- Automatische Schiebetür
- Fluchtwegsteuerung
- Personenvereinzelungsanlage
- Einbruchmeldeanlage (EMA)
- Aufzugssteuerung
- Schranke
- Rolltor
- Anforderungen an erhöhten Einbruchschutz (Angriffswiderstandsklassen bzw. RC-Klassen) unter Beachtung der Normen, wie u.a. der DIN EN 1627, DIN EN 15684, DIN EN 16867
- VdS konforme Ausstattung bzw. Zulassung von Türkomponenten

9. Ein weiteres sehr wichtiges Thema ist der Datenschutz

Besonders zuverlässige elektronische Zutrittsorganisations- und Zutrittskontrollsysteme ermöglichen eine vollständige Überwachung ganzer Liegenschaften und Arbeitsbereiche. Die Rechte der Mitarbeiter und deren Bewegungsdaten sind daher besonders schützenswert. Weiterhin sind DSGVO-konforme Mechanismen wie z.B. die Möglichkeiten zur automatisierten Löschung von Bewegungsdaten oder der Zugriff auf diese nur mittels eines 4- oder gar 6-Augen-Prinzips empfehlenswert. Eine 2-Faktor-Authentifizierung wie beispielsweise durch die zwingende Nutzung einer Programmierkarte und gleichzeitige Abfrage des individuellen Nutzerkennwortes erhöhen den Schutz vor unberechtigtem Zugriff auf die Daten der Schließanlage. Darüber hinaus empfiehlt es sich, frühzeitig den Datenschutzbeauftragten, den Personal- bzw. Betriebsrat und auch die Personalabteilung in die Planung mit einzubinden.

10. Fazit

Sie beabsichtigen den Einsatz einer elektronischen Schließanlage in Ihrem Objekt und sind nach Lektüre unseres Whitepapers mit den wesentlichen Planungseckpunkten vertraut? Zur konkreten Planung, Ausschreibung oder für weiterführende Informationen wenden Sie sich gerne jederzeit an uns unter zutrittsorganisation@winkhaus.de, einen unserer Fachhändler, zu finden unter www.winkhaus.com, oder an unsere Ansprechpartner im Außendienst.

Möglicherweise hatten Sie eine Antwort auf die Frage nach einer grundsätzlichen Empfehlung für die Art der Schließanlage – offline, online oder virtuell vernetzt – gewünscht. Diese ist allerdings letztlich immer von Ihren konkreten Anforderungen in Ihrem Objekt abhängig. Beispielsweise auch von der Fragestellung, ob es sinnvoll ist, die gesamte Schließanlage oder Teile davon mit batterielosen Türkomponenten auszustatten, und welche Restriktionen sich daraus ergeben können. Wir freuen uns auf Ihre Kontaktaufnahme.