STAATLICHES BAUMANAGEMENT
NIEDERSACHSEN

LANDESKRIMINALAMT NIEDERSACHSEN

Technische Information
Schließanlagen
in den Dienststellen des Landes Niedersachsen

TI-Schließanlagen-2016

Niedersachsen

1 Vorwort/Veranlassung

Diese technische Information wendet sich an alle, die mit der Planung, dem Bau und dem Betrieb von Schließanlagen befasst sind.

In großen Gebäuden oder Liegenschaften, in denen viele Menschen arbeiten, stoßen mechanische Schließanlagen in der heutigen Arbeitswelt häufig an ihre Grenzen. Allein schon ihre Verwaltung verursacht einen erheblichen Kostenaufwand für das Ausgeben und das Einziehen von Schlüsseln bei wechselnden Zugangsrechten und ggf. bei Verlust der Schlüssel. Die Schließberechtigungen von mechanischen Schlüsseln können zeitlich nicht eingeschränkt werden. Der jeweilige Schlüsselbesitzer kann jederzeit ohne Kontrollmöglichkeiten die zugehörigen Türen benutzen.

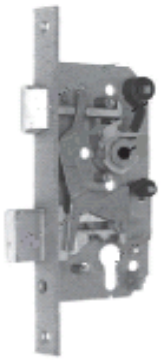
Elektronische Schließanlagen ermöglichen das kurzfristige Sperren verlorener Schlüssel, eine flexible Vergabe und eine zeitliche Begrenzung der Schließberechtigung. Darüber hinaus gewährleisten sie die gestiegenen Sicherheitsanforderungen der nutzenden Verwaltung.

Mit dieser technischen Information sollen die mechanischen und elektronischen (digitalen) Schließanlagen erläutert werden. Der Aufbau einer elektronischen Schließanlage, die dazugehörige Software und deren Bedienung werden aufgezeigt. Weitere Einsatzmöglichkeiten z. B. als Zutrittskontrollanlage werden betrachtet. Der Kostenverlauf mechanischer und elektronischer Schließanlagen wird über einen bestimmten Nutzungszeitraum gegenüber gestellt.

Ein wesentlicher Punkt vor Beginn der Planung ist die Prüfung der datenschutzrechtlichen Zulässigkeit der Leistungsmerkmale einer elektronischen Schließanlage und deren damit verbundener Zutrittskontrolle am jeweiligen Standort. Die rechtlichen Rahmenbedingungen für eine Zutrittskontrolle sind zu beachten. Entsprechende Informationen hierzu befinden sich auf der Homepage des Landesbeauftragten für den Datenschutz Niedersachsen (LfD) unter http://www.lfd.niedersachsen.de.

Die gemeinsam mit dem Landeskriminalamt (LKA) Niedersachsen und dem LfD erarbeitete Broschüre „TI-Schließanlagen 2016“ soll für die Mitarbeiter der Bauverwaltung und ihren Fachplanern als Beratungs- und Planungsgrundlage zur Erstellung von Leistungsbeschreibungen behilflich sein. Sie dient gleichzeitig aber auch der nutzenden Verwaltung als Entscheidungshilfe. Bereits in den ersten Beratungsgesprächen kann sie dabei helfen, den optimalen Lösungsansatz bei der Anlagenauswahl für das Gebäude oder die Liegenschaft zu finden.

2 Funktion einer Schließanlage



Ein Schließzylinder ermöglicht es mit Hilfe eines passenden Schlüssels das Türschloss zu bedienen. Durch die Drehung eines Hebels im Schließzylinder wird die Mechanik des Türschlosses bewegt, wobei der Riegel und die Falle zurückgezogen werden, sodass die Tür geöffnet werden kann.

Das Einsteckschloss ist ein Türschloss mit Falle und Riegel nach DIN 18251 [4]. Diese DIN legt Begriffe, Maße, Anforderungen, Prüfungen und die Kennzeichnung von Einsteckschlössern mit Falle und/oder Riegel einschließlich Einsteckschlösser mit Selbstverriegelung fest.

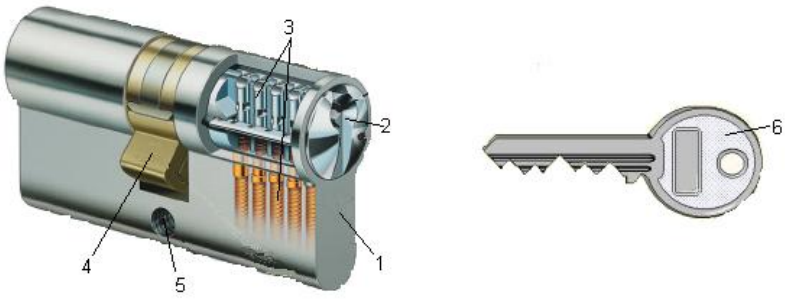
Für Einsteckschlösser in Feuerschutz- und Rauchschutztüren gilt die DIN 18250 [3].

Abbildung 1: Einsteckschloss zum Einbau eines Schließzylinders

Schließzylinder, ob konventionell mechanisch, oder bis hin zum Einsatz von elektronischen Medien müssen immer in Maßen und Anforderungen der DIN 18252 [5] entsprechen. Diese Norm stellt sicher, dass der Schließzylinder in Einsteckschlössern nach DIN 18250, bzw. DIN 18251 passt.

2.1 Mechanische Schließanlagen

Mechanische Schließanlagen bestehen aus Schließzylinder und Schlüssel. Die Schließberechtigungen werden durch den Schlüssel und die mechanischen Zuhaltungen im Schließzylinder bestimmt. Die Sicherheit wird durch mechanische Elemente definiert.



- 1 Zylindergehäuse
- 2 drehbar gelagerte Zylinderkern mit dem Schlüsselkanal
- 3 Kern- und Gehäusestifte, Stiftfedern
- 4 Schließbart
- 5 Bohrung für die Stulpschraube
- 6 Profilschlüssel

Abbildung 2: Mechanische Schließanlage

Die Codierung der mechanischen Schließanlage ist durch das Profil des Schlüssels und der Profilierung des Schlüsselkanals gegeben.

Stimmt das Profil des Schlüssels mit der Profilierung überein, werden die Stifte im Schließzylinder in eine Position gebracht, die es ermöglicht, den Zylinderkern und damit den Schließbart zu drehen. Der Schließbart bewegt die Mechanik des Einsteckschlosses, Falle und Riegel werden zurückgezogen, die Tür öffnet sich.

Mechanische Sicherungselemente beim Schlüssel beziehen sich im Wesentlichen auf die „Profilierung“, die „Sperrwelle“ oder dem „Undercut“ (Hinterschnitt im Schlüsselprofil).

Die DIN EN 1303 „Schließzylinder für Schlösser“ [8] legt Anforderungen und Prüfverfahren für die Schließzylinder fest. Geprüft werden Eigenschaften wie Festigkeit, Dauerhaftigkeit (Anzahl von Schließzyklen, die ein Schließzylinder erbringen muss), Korrosionsbeständigkeit und Verschlusssicherheit.

Die Maße, Anforderungen und Kennzeichnungen für Profilzylinder für Türschlösser werden in der DIN 18252 „Profilzylinder für Türschlösser“ [5] festgelegt.

Es können je nach Hersteller und Anlage sehr komplexe Schließhierarchien aufgebaut werden. Dabei ist immer ein Schließplan zu erstellen in dem festgelegt wird welche Schlüssel welche Zylinder schließen dürfen. Die Ausführungsarten einer mechanischen Schließanlage sind:

- **Zentralschlüsselanlage (ZGS)**
- **Hauptschlüsselanlage (HGS)**
- **Generalhauptschlüsselanlage (GHS)**

Bei einer Zentralschlüsselanlage schließen mehrere unterschiedliche Schlüssel einen oder mehrere Zentralschließzylinder. Beispielsweise wird in einer gemeinsam genutzten Eingangstür ein gleichschließender Schließzylinder eingebaut.

Eine Hauptschlüsselanlage ist eine Schließanlage, bei der ein Hauptschlüssel alle vorhandenen Schließzylinder in der Schließanlage, die eine Gruppe bilden, schließen kann.

Eine Generalhauptschlüsselanlage ist eine Schließanlage mit hierarchischem Aufbau mehrerer Schließebenen. Der Generalhauptschlüssel ist der ranghöchste Schlüssel schließt in jeder Gruppe jeden Zylinder der Schließanlage.

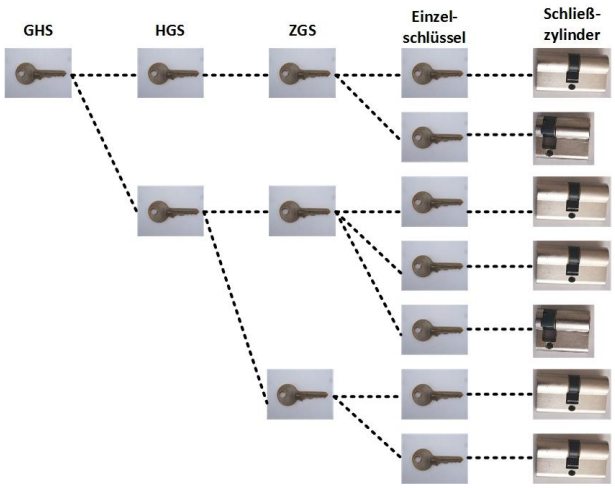


Abbildung 3: Schema einer Generalhauptschlüsselanlage

Eine mechanische Schließanlage bleibt aber eine unflexible Anlage, die nachträgliche Änderungen in den Schließberechtigungen nur durch Austausch von Schlüsseln und/ oder Zylindern möglich macht. Bei einem Schlüsselverlust (z. B. des Generalschlüssels) kann ein Austausch aller Schließzylinder und Schlüssel notwendig werden. Es sollten nur Anlagen mit Sicherungskarte (Legitimation zum Fräsen eines identischen Schlüssels) verwendet werden, um das unberechtigte Kopieren von Schlüsseln zu verhindern.

2.2 Mechatronische Schließanlagen

Bei einem mechatronischen Schließzylinder wird die mechanische Schließung durch ein elektronisches Sperrelement ergänzt.

Der Schlüssel wird wie bisher in den Zylinder eingeführt und gedreht. Im Zylinder kontrollieren die mechanischen Zuhaltungen und der Chip im Elektronikmodul die entsprechenden Codierungen (mechanische als auch elektronische) des Schlüssels und geben bei Berechtigung den Schließvorgang frei. Der Schließzylinder benötigt keine Verkabelung. Eine Batterie im Schlüssel versorgt auch den Schließzylinder während der Bedienung mit Energie. Die Lebensdauer einer Batterie sollte mindestens zwei Jahre betragen.

Durch die zusätzliche Prüfung der Schließberechtigung über den Schlüssel (elektronisches Identifikationsmittel wie RFID-Transponder, Chip-Karte) kann der Zutritt (wer – wann – wohin) ausgelesen und protokolliert werden.

Eine Schließplansoftware und ein Programmiergerät sind weitere Komponenten für eine mechatronische Schließanlage. Das Programmiergerät dient der Datenübertragung zwischen der Verwaltungssoftware und dem Programmierschlüssel. Durch Einstecken des Programmierschlüssels in den Zylinder, sowie die Programmierung der Nutzerschlüssel, erhält dieser die Daten der Zutrittsberechtigungen, die dem jeweiligen Schlüsselinhaber zugeordnet sind.

Ein Vorteil dieses Systems ist, dass der Schlüsselinhaber keine andere Anwendung für das neue Schlüsselsystem lernen muss. Bei einer Nachfertigung eines Schlüssels müssen nicht nur Profile und Einschnitte des Schlüssels, sondern auch die Elektronik kopiert werden.

Mechatronische Schließsysteme können in Kombination mit einer mechanischen Schließanlage betrieben werden. Aus sicherungstechnischer Sicht ist es möglich, nur sensible Bereiche mit mechatronischen Schließsystemen auszurüsten.

Die Schließhierarchien werden flexibler, weil sie sich in Teilen anpassen lassen, soweit es sich um die Modifizierung der elektronischen Eigenschaften handelt. Dementsprechend lassen sich Schließberechtigungen flexibler gestalten. Schlüsselverluste führen nicht zwangsläufig zum Kompletttausch von Schlüssel und Zylinder. Es ist ausreichend einen verloren gegangenen Schlüssel im System zu sperren.

Durch die Entwicklungen bei den nachfolgend beschriebenen elektronischen Schließanlagen werden mechatronische Schließanlagen nur noch in Ausnahmefällen eingesetzt. Eine Veranschlagung nach DIN 276-1 [18] erfolgt in Kostengruppe (KG) 334 (Außentüren) und KG 344 (Innentüren) oder kombiniert in KG 399.

2.3 Elektronische Schließanlagen

Elektronische Schließzylinder unterscheiden sich grundsätzlich von den mechanischen Lösungen. Der Code ist nicht mehr über die Form des Schlüssels gegeben. Die Freigabe für einen Schließvorgang erfolgt ausschließlich auf elektronischem Wege über eine Funkstrecke. Ein elektronisches Identifikationsmerkmal wird abgefragt und der Zylinderkern bei Übereinstimmung elektromechanisch eingekuppelt. Der Schließbart kann dann mit dem Knauf bzw. Schlüssel gedreht und so das Türschloss betätigt werden.

Elektronische Schließanlagen entsprechen grundsätzlich den Anforderungen die die DIN EN 60839-11-1 bzw. -2 [9, 10] an eine Zutrittskontrollanlage mit dem Grad 1 stellt. Derartige Zutrittskontrollanlagen, die im Wesentlichen den Ersatz für eine mechanisches Schließanlage darstellen, sind nach DIN 276-1 [18] in KG 399 zu veranschlagen, unabhängig davon welcher Fachplaner mit der Aufgabe betraut wird. Höherwertige Zutrittskontrollanlagen der Grade 2 bis 4 werden als Gefahrenmeldeanla-

gen betrachtet und entsprechend in KG 456 veranschlagt. Weitere Informationen zu Zutrittskontrollanlagen finden Sie in Abschnitt 3.

Eine elektronische Schließanlage besteht aus einzelnen elektronischen Komponenten, die sie flexibler, komfortabler und sicherer als eine mechanische Anlage machen. Die Anlage wird modular aufgebaut. Es kann eine einfache Schließanlage für einzelne Türen oder eine komplexe PC-gesteuerte Zutrittskontrollanlage sein.

Die einzelnen Komponenten werden nachfolgend beschrieben.

2.3.1 Schließzylinder

Elektronische Schließzylinder sind verkabelungsfrei und haben eine batteriebetriebene Steuereinheit, sowie ein Lesegerät (Reader) für Identmittel als komplette Einheit im Zylinder bzw. in dessen Knauf.

Die elektronischen Schließzylinder müssen in den Anforderungen und Abmessungen uneingeschränkt der DIN 18252 [5] bzw. DIN EN 1303 [8] entsprechen, um diese in dafür vorgerichtete Einsteckschlösser nach DIN 18250 [3] oder DIN 18251 [4] montieren zu können, ohne dass Änderungen an den Türen oder Türbeschlägen und zusätzliche Bohrungen erforderlich sind.

Abbildung 4: Beispiel eines elektronischen Schließzylinders

Beispiele für die verschiedenen Ausführungen:

- Elektronischer Schließzylinder mit Batterie im Innenknauf. Bedienung mit einem Aktivtransponder (batteriebetrieben).
- Elektronischer Schließzylinder mit Batterie im Innenknauf. Bedienung mit einem Passivtransponder.
- Elektronischer Schließzylinder mit Batterie im Profilzylinder. Bedienung mit einem Passivtransponder (als Schlüssel zum Einführen in den Zylinder).
- Elektronischer Schließzylinder sowie elektronischer Schlüssel ohne Batterie, mit interner Energieerzeugung (Energie zur Durchführung des Schließvorganges wird durch Einführen des Schlüssels gewonnen).
- Beschlag mit integrierter Elektronik (Elektronischer Beschlagleser)
  Das Lesegerät (Reader) für das Identmittel (Aktiv- oder Passivtransponder) ist im äußeren Türschild integriert. Die Elektronik und die Batterien sind im Innenschild untergebracht. Bei Beschlägen die nur auf die Drückernuss[1)] wirken, lässt sich die Sicherheit durch Sperrfallenschlösser[2)] oder selbstverriegelnde Panikschlösser erhöhen. Einige Anlagen erlauben einen mechanischen Notzylinder, der über das Identmittel hinweg schließt.

[1] Teil des Einsteckschlosses: in der Drückernuss ist eine Vierkantöffnung integriert, durch die eine Türklinke oder ein Türknauf eingesteckt wird. Durch eine Drehbewegung wird mittels eines Hebels die Türfalle zurückgezogen, wodurch sich die Tür öffnen lässt. Ein weiterer Hebel mit eingehängter Feder sorgt dafür, dass die Türfalle selbständig zuschnappt.

[2] Ein Sperrfallenschloss ist mit einer Sperrfalle ausgestattet, welche durch eine besondere Funktion bei geschlossener Tür automatisch verriegelt, also gegen Hereindrücken gesperrt ist.

2.3.2 Identmittel

Je nach Hersteller und Anforderungsprofil der Schließanlage, werden unterschiedliche Arten bzw. Methoden der Identifikationsmittel angeboten. Die Auswahl eines für die jeweilige Aufgabe geeigneten Identifikationsmittels richtet sich an verschiedenen Kriterien aus, wie Wirtschaftlichkeit, dem erforderlichen Sicherheitsniveau, der notwendigen Flexibilität und der maximalen Ausbaustufe. Folgende Identmittel werden hier beschrieben:

- Transponder aktiv
- Transponder passiv
- Chipkarte
- Zahlencode als „geistiges“ Identifikationsmittel
- Biometrischer Schlüssel

Ein Transponder ist ein Funk-Kommunikationsgerät, das eingehende Signale aufnimmt und automatisch beantwortet (*siehe* **RFID**). Der Begriff Transponder ist zusammengesetzt aus den Begriffen Transmitter (Sender) und Responder (Antworter).

Aktive Transponder verfügen über eine eigene Energieversorgung durch eine eingebaute Batterie. Sie haben größere Kommunikationsreichweiten und die Speicherkapazität der Mikrochips kann bis zu einem Megabyte groß sein.

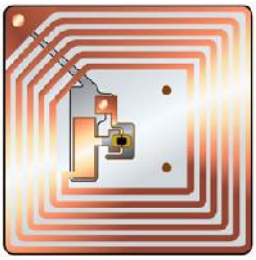
Bei passiven Transpondern gibt der Computerchip (Mikrochip) über seine Antenne die Informationen an das Schreib-/Lesegerät im Schließzylinder. Das Schreib-/Lesegerät sendet Funkwellen und erstellt so ein magnetisches Feld. Die Energie für die Schaltungen in dem Mikrochip erhält der passive Transponder aus diesem Magnetfeld.

Passive Transponder können in verschiedenen Bauformen auftreten. Sie können in Schlüsselanhänger oder in Plastikkarten als Chip-Karte (Smartcard) verklebt werden.

Abbildung 5: Transponder als Schlüsselanhänger

Abbildung 6*:* Chip-Karte

RFID



Der Transponder ist das Kernstück der RFID-Technologie.

RFID ‚Radio frequency identifikation' bedeutet übersetzt die Identifizierung mit Hilfe von elektromagnetischen Wellen, also eine Funkerkennung. Es ist ein technisches System, das Daten lesen kann, ohne diese Daten berühren oder direkt sehen zu müssen, im Gegensatz zur Barcode-Technologie.

Ein RFID-System besteht aus einem Transponder, der an dem Objekt, das identifiziert werden soll, angebracht ist (Identmittel), einem Schreib-/Lesegerät (Reader), den Funkfrequenzen selbst und einem IT-System. Die Energieversorgung des Transponders erfolgt im Normalfall berührungslos vom Reader.

Funktionsweise: Das Lesegerät erzeugt ein hochfrequentes elektromagnetisches Wechselfeld, dem der RFID-Transponder ausgesetzt wird. Der so aktivierte Mikrochip im RFID-Transponder decodiert die vom Lesegerät gesendeten Befehle. Die Antwort codiert und moduliert dieser „Reader" in das eingestrahlte elektromagnetische Feld durch Feldschwächung im kontaktfreien Kurzschluss oder gegenphasige Reflexion des vom Lesegerät ausgesendeten Feldes. Damit überträgt der Transponder seine eigene unveränderliche Seriennummer, weitere Daten des gekennzeichneten Objekts oder andere vom Lesegerät abgefragte Informationen. Der Transponder erzeugt also selbst kein Feld, sondern beeinflusst das elektromagnetische Sendefeld des Readers.

Dieses sichere Authentifizierungsverfahren nennt sich auch „Challenge und Response-Verfahren": Ein Teilnehmer stellt eine Aufgabe (challenge), die der andere lösen muss (response), um zu beweisen, dass er die bestimmte Information kennt. Der Transponder sendet ein Signal zum Schließzylinder und erhält eine Antwort, aus der er einen neuen Code berechnet und erneut sendet. Wichtig dabei ist, dass der Inhalt der Verschlüsselung nicht entschlüsselt wird, sondern nur ein Gleichheitstest stattfindet.

2.3.3 Schließplansoftware

Ein Schließplan ist die Dokumentation einer Schließanlage und ihrer Verwaltung. Die Schließplansoftware ist das vereinende Element der intelligenten Komponenten einer elektronischen Schließanlage, um alle Aufgaben durchzuführen. Es müssen Identmittel an Nutzer ausgegeben werden, Schließzylinder mit aktuellen Berechtigungen programmiert werden und Identmittel bei Schlüsselverlust gesperrt werden.

Die Schließplansoftware stellt das „tägliche" Arbeitsmittel für den Systemadministrator der Schließanlage dar. Daher ist im Vorfeld der Anlagenplanung das Anforderungsprofil an die Software genau zu definieren.

Die Software muss sich in bestehende IT-Strukturen integrieren lassen. Alle Daten wie Türen und Identmittel werden in einer Datenbank erfasst und in einer Matrix dargestellt.

In der Regel bieten die Hersteller Im- und Exportfunktionen unter Nutzung von standardisierten Datenformaten zu anderen Anwendungen an (Zutrittskontrollanlage, Einbruchmeldeanlage, Parkplatzmanagement oder andere Anlagen). Im Zuge der Anlagenplanung sind die Schnittstellen zu erfassen und in die Anlagenplanung aufzunehmen.

Übliche Leistungsmerkmale einer Schließplansoftware sind:

- Client/Server System
- Datenbank gestützt
- Import-/Export-Funktionen über Standard Datenformate
- Offene Systemarchitektur, die sich problemlos in bestehende EDV-Umgebung einbinden lässt
- Standortverwaltung mit Visualisierung der Gebäudestruktur
- Visualisierung von Tabellen
- Integration von verschiedenen Transpondersystemen in einen Stammsatz
- Systemzugriff über Passwortschutz
- schnelle Revisionsfähigkeit
- Hilfe-/ Suchfunktionen
- Erstellung, Verwaltung und Änderung von Schließplänen
- Änderungen der Schließberechtigung für vorhandene Schlüssel / Karten und Zylinder
- Sperrung und Entsperrung von verlorengegangenen Identmittel
- Programmieren von Identmitteln mit automatischer Kopie der alten Grundeinstellung der Schließberechtigung

Zur Übertragung der Informationen aus dem Schließplan stehen verschiedene Wege zur Verfügung, die nachfolgend beschrieben werden. Die für die jeweilige Anlage sinnvollste Variante ist im Rahmen der Planung zu ermitteln.

2.4 Typen von Schließanlagen

2.4.1 Offline-Schließanlagen

Die Schließanlage funktioniert ohne Anbindung an das Gebäude-Datennetz. Die Nutzungsberechtigungen werden zentral am PC in der Datenbank vorgenommen und mittels des Programmiergerätes oder Programmierschlüssels in die einzelnen Zylinder übertragen. Dafür muss jeder betroffene Zylinder aufgesucht werden.

Für diese Anlage ist keine aufwändige Verkabelung in einem Gebäude notwendig. Ebenfalls ist die Montage und Nachrüstbarkeit bei Offline-Anlagen ohne großen Aufwand möglich.

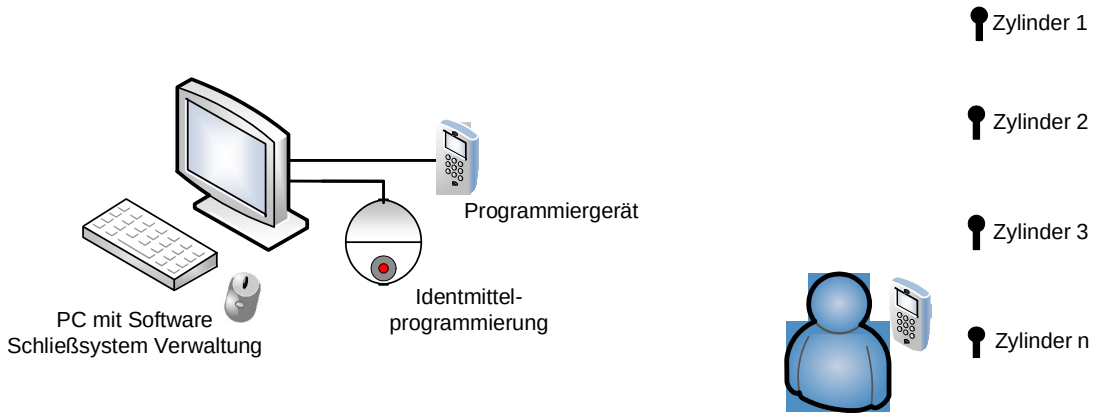


Abbildung 7: Offline-Schließanlage

Geht ein Identmittel verloren, ist eine Gebäudebegehung mit der Umprogrammierung der betroffenen Türen notwendig. Dieser Aufwand kann lediglich vermieden werden, wenn das Identmittel bereits durch eine Zeitbegrenzung nicht mehr gültig ist. Aus baulicher Sicht ist dieses, auch als „Turnschuhnetzwerk“ bezeichnet, die einfachste Lösung. Je nach Gebäudenutzung und Anzahl der Türen ist abzuwägen, ob eine Offline-Schließanlage zu bewältigen ist.

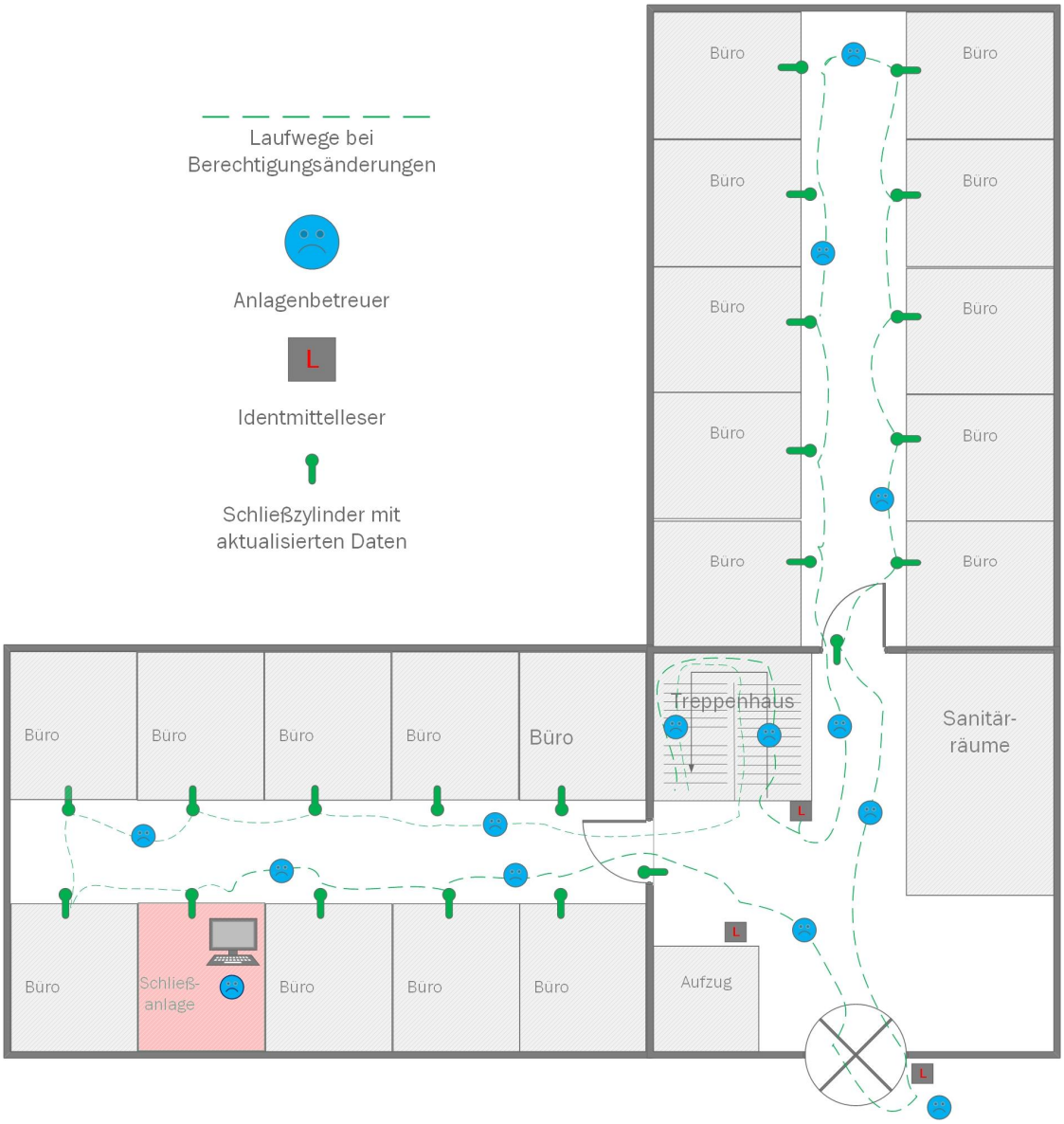


Abbildung 8: Laufwege bei einer beispielhaften Offline-Schließanlage

2.4.2 Online-Schließanlagen

Mit Hilfe eines kabelgebundenen Netzwerkes sind die Schließzylinder zentral von einem PC-Arbeitsplatz programmier- und auslesbar. Es können z. B. Türzustände und der Batteriestatus über das Netzwerk gemeldet werden. Hier werden Berechtigungen, die der einzelne Schließzylinder erhält, zentral von einem PC aus verwaltet. Bei großen Schließanlagen ist eine zentrale Programmierung von Zylindern von Vorteil. Jede Berechtigungsänderung kann ohne Zeitverzögerung an die jeweiligen Türen übertragen werden, ohne dass der entsprechende Zylinder aufgesucht werden muss.

Bei Neubauten können diese Netzwerke relativ gut bautechnisch geplant und realisiert werden. In bestehenden Gebäuden steigt demgegenüber der Aufwand für die flächendeckende Nachrüstung der Verkabelung.

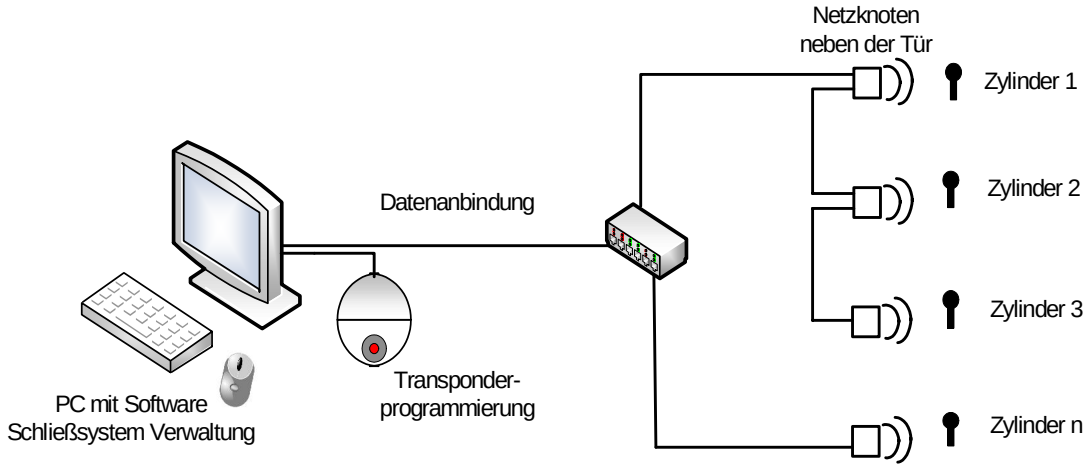


Abbildung 9: Online-Schließanlage

Über eine Unterverteilung mit aktiven Netzwerkkomponenten werden die Netzwerkknoten für die Vernetzung der einzelnen Türen in der Nähe des Schließzylinders installiert. Diese kommunizieren drahtlos mit dem elektronischen Schließzylinder. Die im Schließplan auf dem zentralen PC eingegebenen Daten werden auf alle Schließzylinder übertragen.

2.4.3 Funkvernetzte elektronische Schließanlage

Funkvernetzte Lösungen sind insbesondere bei einer Nachrüstung in einem bestehenden Gebäude eine an den Kosten angemessene Alternative zu drahtgebundenen Netzwerken. Das Netzwerk wird durch das Setzen von Accesspoints realisiert. Der Accesspoint stellt eine Funkverbindung zu den Schließzylindern bis zu einer Reichweite von ca. 30 Metern her. Die genaue Anzahl sollte durch eine Funkfeldausleuchtung festgelegt werden.

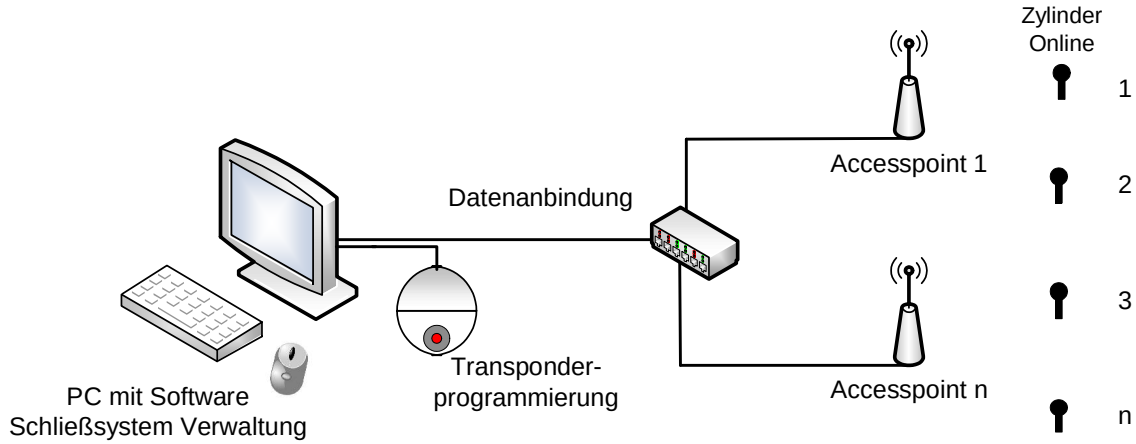


Abbildung 10: Funkvernetzte elektronische Schließanlage

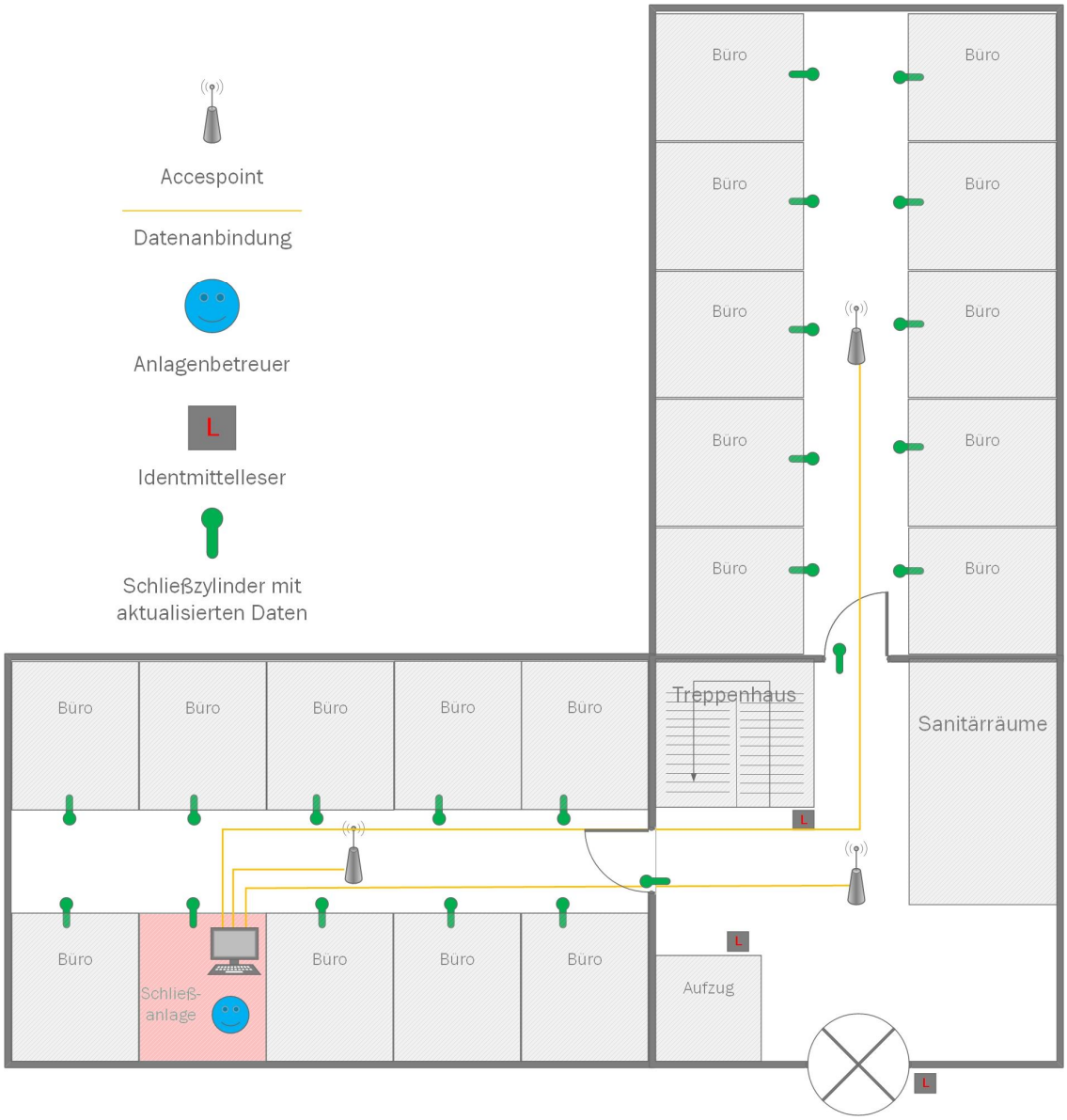


Abbildung 11: Beispielhafte Funkvernetzte Schließanlage

2.4.4 Virtuelles Netzwerk / Netzwerk on Card

Diese Funktionalität wird bei den verschiedenen Herstellern unterschiedlich benannt. Auch hier werden die Änderungen in der Datenbank vorgenommen und – meist online – an einen oder mehrere Identmittelleser übertragen.

Sobald ein Identmittel an diesem Leser bucht, werden ihm die geänderten Daten mit auf den Weg gegeben. Bei jeder Nutzung an einer Offline-Komponente werden dessen Zutrittsdaten durch den Schlüssel (Identmittel) aktualisiert. Auf gleichem Wege gelangen auch die Ereignisse und der Batteriestatus an die Online-Leser und damit zurück in die Datenbank.

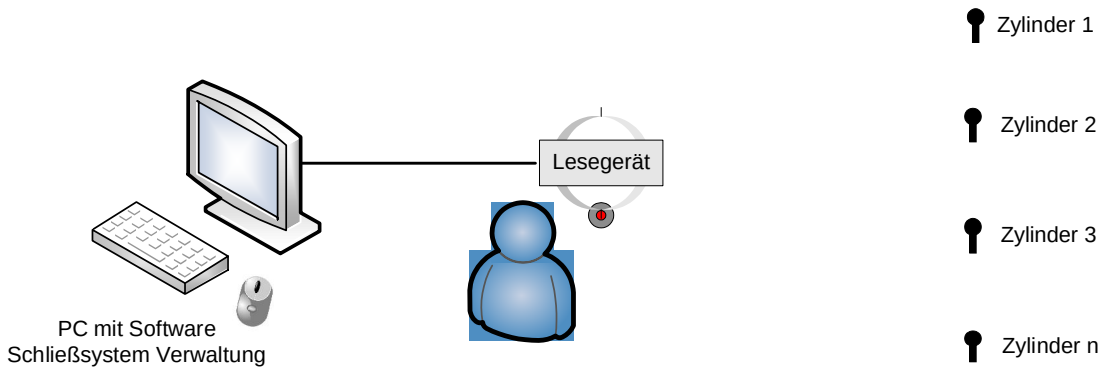


Abbildung 12: Virtuelles Netzwerk

Diese Form des Netzwerkes bietet das beste Verhältnis von Preis/Leistung zur Schnelligkeit der Übertragung. Es eignet sich auch für die Ergänzung von Online-Zutrittskontrollanlagen mit Offline-Komponenten.

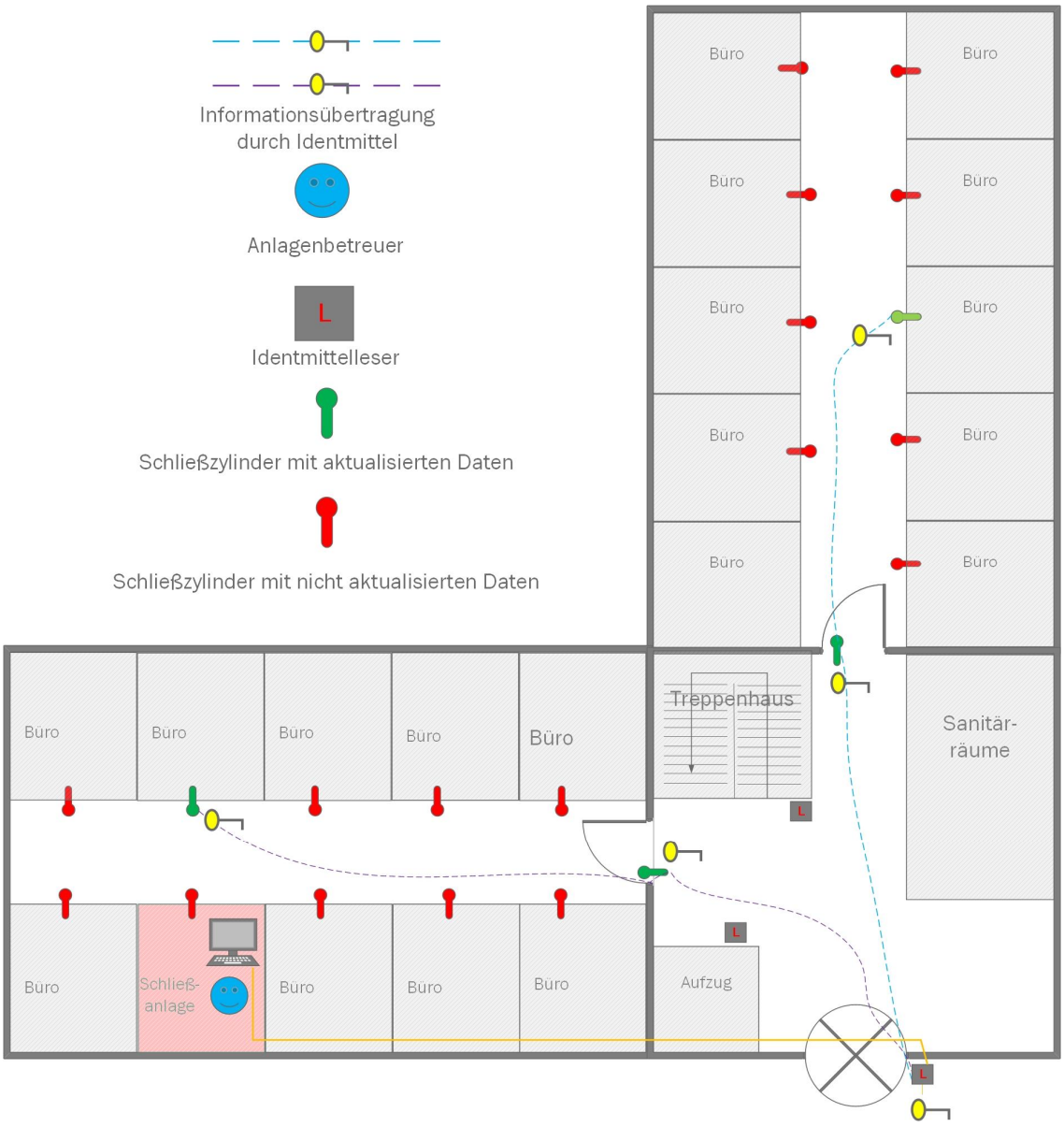


Abbildung 13: Beispielhaftes virtuelles Netzwerk

2.5 Geistige/biometrische Verfahren

2.5.1 PIN-Codierung

Ein Nachteil aller bislang betrachteten Schließanlagen ist, dass die Nutzer dieser Anlagen das Identmittel (Transponder) ständig bei sich tragen müssen, um bestimmte Türen öffnen zu können.

Eine Alternative dazu wäre das Eingeben eines Zahlencodes als geistiges Verfahren.

Abbildung 14: PinCode-Tastatur

Die PinCode-Tastatur ermöglicht das Öffnen eines Schließzylinders über Eingabe eines Zahlencodes. Die Tastatur wird verkabelungsfrei in Türnähe angebracht. Bei richtiger Eingabe des Codes wird durch die Einheit ein Signal ausgelöst, welches ein einmaliges Öffnen der Tür ermöglicht und per Funk übertragen. Anschließend fährt die Tür wieder in die geschlossene Position und verriegelt. Für die Sicherheit ist es entscheidend, wie lang der einzugebende Code ist (Anzahl Ziffern) und wie oft er gewechselt wird.

2.5.2 Biometrie

Biometrische Anlagen lassen den Zutritt zu einem Gebäude über biometrische Identifizierungsmerkmale zu. Biometrische Verfahren sind nur dann einsetzbar, wenn von den betreffenden Personen vorher die Prüffaktoren aufgenommen, analysiert und abgespeichert werden.

Abbildung 15: Augeniris als Identmittel

Biometrischen Identifikationsverfahren sind:

- Stimmerkennung
- Unterschriftenvergleich
- Handgeometrieerkennung
- Augeniris
- Fingerabdruck
- Optische Erkennung (automatischer Bildvergleich)

Nachteile:

- geringe Akzeptanz der Benutzer
- hygienische Bedenken
- Kosten

Ein biometrisches Erkennungssystem setzt sich im Wesentlichen aus den Komponenten Sensor (Messwertaufnehmer), Merkmalsextraktion und Merkmalsvergleich zusammen. Welche Arten von Sensoren zum Einsatz kommen, hängt stark vom biometrischen Charakteristikum ab.

2.5.3 Fingerprint

Die häufigste Methode der biometrischen Verfahren ist die Nutzung des Fingerabdrucks. Die biometrische Leseeinheit erstellt ein digitales Bild eines Fingerabdrucks. Dieses sogenannten Fingertemplate wird mit einem komplexen mathematischen Algorithmus erstellt und als Referenz gespeichert.

Abbildung 16: Fingerabdruck als Identmittel

Nun liefert eine Sensorkomponente ein biometrisches Sample (Abtastwert). Die Merkmalsextraktion entfernt alle vom Sensor gelieferten Informationen, die nicht die geforderten Merkmalseigenschaften erfüllen und liefert als Ergebnis die biometrischen Merkmale. Der Merkmalsvergleicher errechnet einen Vergleichswert (Score) zwischen der in der Einlernphase gespeicherten biometrischen Vorlage und dem aktuellen, von der Merkmalsextraktion gelieferten Datensatz.

Über einen Schließplan wird die biometrische Erkennung integriert. Die Terminals mit den Biometrielesern werden an den betreffenden Standorten installiert. Daneben gibt es mobile Biometrieleser, deren Fingerprintsensor in einem Transponder-Taster enthalten ist.

3 Zutrittskontrolle

Für Zutrittskontrollsysteme werden in DIN EN 60839-11-1 [9] folgende Grade festgelegt:

- Grad 1 Risikograd niedrig
- Grad 2 Risikograd niedrig bis mittel
- Grad 3 Risikograd mittel bis hoch
- Grad 4 Risikograd hoch

Weitere Hinweise zu den Graden finden sich in Tabelle 1 der v. g. Norm.

Eine Anlage mit elektronischen Schließzylindern stellt bereits eine einfache Form einer Zutrittskontrollanlage (Grad 1) dar. Sie kann Anforderungen wie z. B. der Sicherung eines Serverraums genügen. Um der Funktion einer Zutrittskontrollanlage für Sicherheitsanwendungen zu genügen, sind jedoch ergänzend die Anforderungen der Normenreihe DIN EN 60839-11 [9, 10] zu beachten. Weitere Hinweise zu Zutrittskontrollanlagen können der AMEV-Veröffentlichung EMA/ÜMA 2012 [1] entnommen werden.

Wenn der Einsatz einer Zutrittskontrollanlage (ZKA) aus sicherheitstechnischen Gründen in Betracht gezogen wird, sollte sich die nutzende Verwaltung zunächst von einer fachkundigen Stelle (z. B. LKA, MAD, BSI) beraten lassen. Aus dem Beratungsergebnis muss hervor gehen, welcher Grad nach DIN EN 60839-11-1 angemessen erscheint. In der DIN EN 60839-11-1 und 2 sind umfangreiche Tabellen enthalten, in denen die notwendigen und optionalen Leistungsmerkmale einer Zutrittskontrollanlage dargestellt werden. Mit der nutzenden Verwaltung ist abzustimmen, welche der optionalen Leistungsmerkmale benötigt werden. Es ist dabei auch möglich, dass für einzelne Bereiche, wie in Abbildung 17 beispielhaft dargestellt, verschiedene Grade festgelegt werden. Zu beachten ist dabei, dass die zentralen Einrichtungen der Anlage (ZKA) immer in einem Bereich installiert werden, der mit dem höchsten verwendeten Grad gesichert ist.

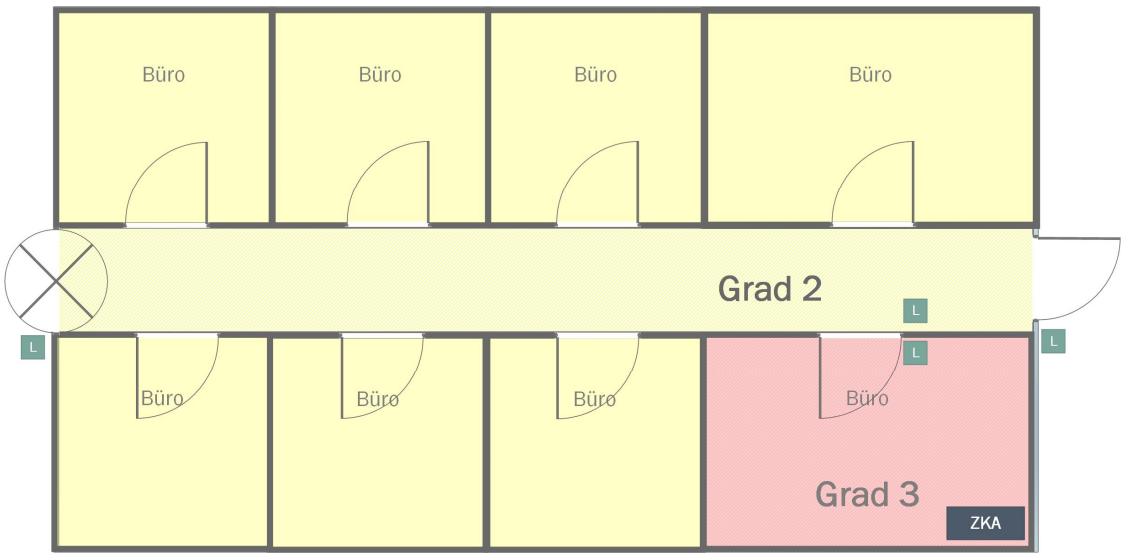


Abbildung 17: Beispielhafte Zutrittskontrollanlage

Die bisherigen Klassifizierungen zum Einsatz von Identmitteln sind normativ nicht mehr gegeben. Die Klassen können jedoch weiter als Anhalt bei der Auswahl der Identmittel verwendet werden:

- Identifikationsklasse 1 Einsatz eines geistigen Identifikationsmerkmals (z. B. Türcodegerät)

  Hier wird die Sicherheit durch längere Zahlenkombinationen und häufigere Wechsel erhöht. Es besteht auch die Möglichkeit einen Überfallcode festzulegen, den ein Benutzer verwenden kann, wenn er gezwungen wird den Türcode einzugeben. Durch den Überfallcode wird dann ein stiller Alarm ausgelöst, der es ermöglicht weitere Maßnahmen (z. B. Alarmierung der Polizei) einzuleiten.

- Identifikationsklasse 2 Identmittel (z. B. Transponder)
  oder biometrische Erkennung

  Wenn ein geistiger Verschluss nicht ausreicht, um das erforderliche Sicherheitsniveau zu erreichen, können auch biometrische Erkennungsverfahren eingesetzt werden. Es kann sich dabei z. B. um ein Fingerabdrucklesesystem handeln. Es sind Identmittel auf dem Markt erhältlich, bei denen dies bereits integriert ist.

- Identifikationsklasse 3 Identmittel
  oder biometrisches- (z. B. Fingerabdruckleser)
  sowie geistiges Identifikationsmerkmal

Die wesentlichen Merkmale einer Zutrittskontrollanlage werden im Folgenden beschrieben.

Lokale Anzeige

- Optische und/oder akustische Anzeige dass Zutritt gewährt oder verweigert wird (ab Grad 1).
- Optische und/oder akustische Anzeige dass die zulässige Öffnungszeit in Kürze endet (ab Grad 3)

Erkennung und Meldung (ab Grad 2)

- Sabotage
- Aufbruch
- Tür zu lange offen

Leistungsmerkmale (ab Grad 2)

- Eindeutige Erkennung jeden Nutzers (damit scheidet Identifikationsklasse I aus)
- Möglichkeit Uhrzeit- (Stunde, Minute) und Tagesabhängige Berechtigungen zu vergeben
  Der Zugang ist dann nur zu bestimmten Zeiten erlaubt. Die v. g. Leistungsmerkmale lassen sich üblicher Weise schon mit elektronischen Schließzylindern realisieren.
- Zeitweiliges Sperren von gültigem Identmittel, wenn eine ungültige geistige Erkennung verwendet wurde.

Signalisierungen am Bedienplatz

- Protokoll dass Zutritt gewährt oder verweigert wurde (ab Grad 3, siehe auch die Ausführungen unter Ziffer 5 zum datenschutzrechtlichen Erforderlichkeitsgrundsatz).

  Es wird protokolliert, wann mit welchem Identmittel der Zugang erreicht wurde. Ebenso abgewiesene Versuche, wenn z. B. der Zugang zu einem Zeitpunkt versucht wurde zu dem keine Berechtigung bestand. Insbesondere bei einer Proto-

kollierung von Zu- und Ausgängen ist die Personalvertretung der nutzenden Verwaltung im Vorfeld zu beteiligen.

- Optische Meldung, Alarm und Protokollierung bei (ab Grad 4)
  - Bedrohungsalarm
  - ungültigem Identmittel
  - gültigem Identmittel und ungültigem geistigen Erkennungsmittel
  - Zutrittspunkt bleibt offen (ab Grad 3)
    Es wird überwacht, dass eine geöffnete Tür in einer festzulegenden Zeit wieder verschlossen wird. Hierzu ist eine zentrale Überwachungseinrichtung erforderlich. Wird die Zeit überschritten, werden festzulegende Maßnahmen (z. B. Alarmierung eines Wachdienstes) automatisch ausgelöst.
- Zustandsmeldungen der Energieversorgung (ab Grad 3)

Abgangskontrolle

Zusätzlich zur Eingangskontrolle ist u. U. der Einsatz des Identmittels erforderlich, um den gesicherten Bereich verlassen zu können. Es ist dann eine Plausibilitätskontrolle möglich, d. h. der Ausgang wird verwehrt, wenn zuvor kein ordnungsgemäßer Zutritt erfolgt ist. Ebenso kann der Zutritt verwehrt werden, wenn der Inhaber des Identmittels sich aus Sicht der Anlage noch im gesicherten Bereich aufhält. Durch diese Maßnahme kann sichergestellt werden, dass alle Zutritte und Abgänge ordnungsgemäß registriert werden und sich nicht zutrittsberechtigte Mitarbeiter mit in den gesicherten Bereich einschleusen lassen, ohne dass dies registriert wird. Grundsätzlich können für Zu- und Abgangskontrollen unterschiedliche Identifikationsklassen festgelegt werden. Der Einsatz einer Abgangskontrolle ist mit der nutzenden Verwaltung abzustimmen. Normative Vorgaben bestehen nicht.

4 Bauliche Anforderungen

4.1 Grundlagen

Alle Anforderungen an Türen, wie sie sich aus planerischen, funktionalen, nutzerspezifischen wie auch bauordnungsrechtlichen oder sicherheitstechnischen Betrachtungen heraus ergeben, führen zu baulichen Anforderungen, die unabhängig von der Schließanlage zu beachten sind. Dies wird hier nicht gesondert abgehandelt. Insbesondere eine brandschutztechnische Anforderung an eine Türanlage ist unabhängig von der Schließanlage zu beachten.

Entscheidend ist jedoch, dass v. g. Anforderungen die Wahl der entsprechenden Schließanlage beeinflussen (z. B. besondere Sicherheitsanforderungen).

Hilfreich ist es, wenn alle Ausstattungsmerkmale der Türen, beziehungsweise die entsprechenden Türapplikationen, in einer gemeinsamen Matrix (Türliste) gelistet werden.

4.2 Einsteckschloss

Die baulichen Anforderungen für den Einsatz mechanischer Schließanlagen reduzieren sich auf die Planung der jeweiligen Schlösser mit geeigneten Zylindern. Dabei sind die Dorn-/ Achsmaße zu beachten.

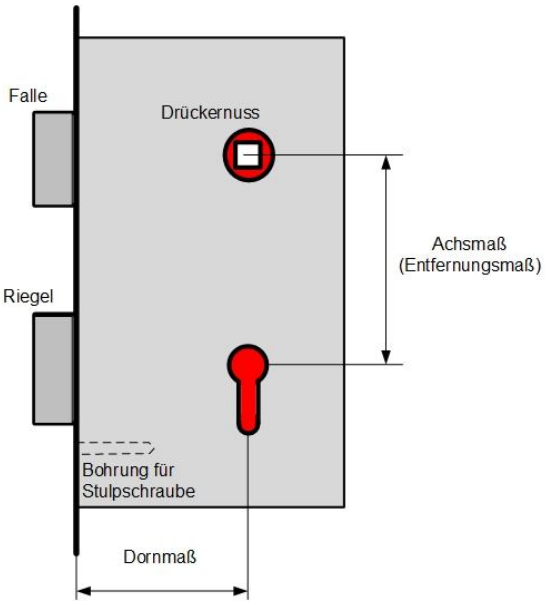


Abbildung 18: Dorn- und Achsmaß

Ein überstehender Zylinder birgt sicherheitstechnische Gefahren bei Angriffen mit Werkzeugen, ein zu kurzer Zylinder behindert den Schlüssel im Schließvorgang. Notwendige Zylinderverlängerungen müssen daher berücksichtigt werden (Abbildung 18).

4.3 Länge Profilzylinder

Gemessen wird ein Profilzylinder ausgehend von der Mitte des Gewindeloches für die Befestigungsschraube (unter dem Schließbart);

Die Grundlänge einer Seite beträgt je nach Hersteller ca. 30 mm.

Zylinderverlängerungen sind in **5 mm - Schritten** erhältlich.

Beispiel: Standard-Falztüren mit 40 mm starkem Türblatt;

Zylinder 30/35, also außen 30 mm und Innen 35 mm:

Türbeschlag Außenschildstärke 15 mm, um den Zylinder am Außenbeschlag bündig abschließen zu lassen.

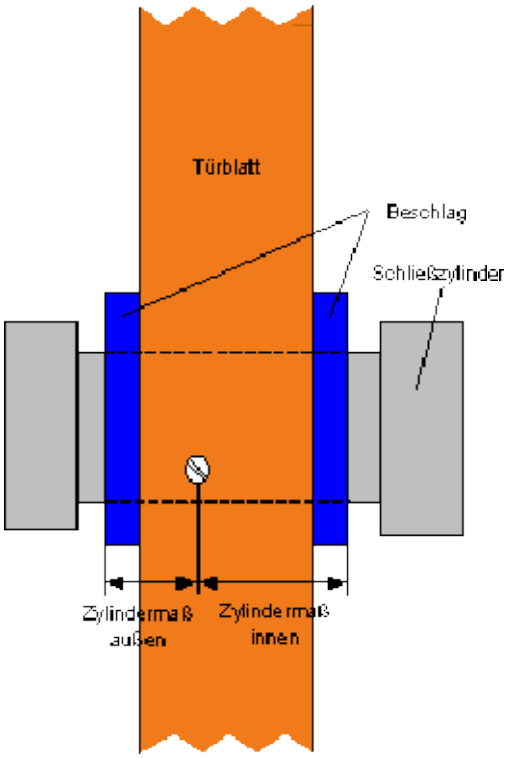
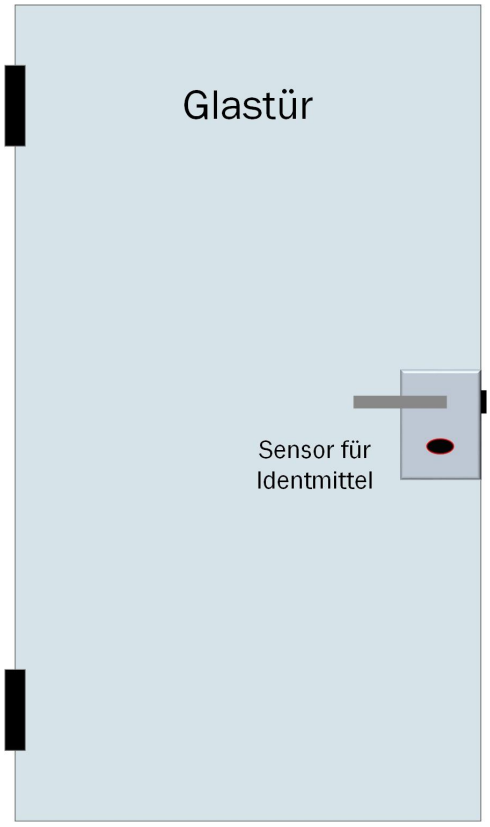


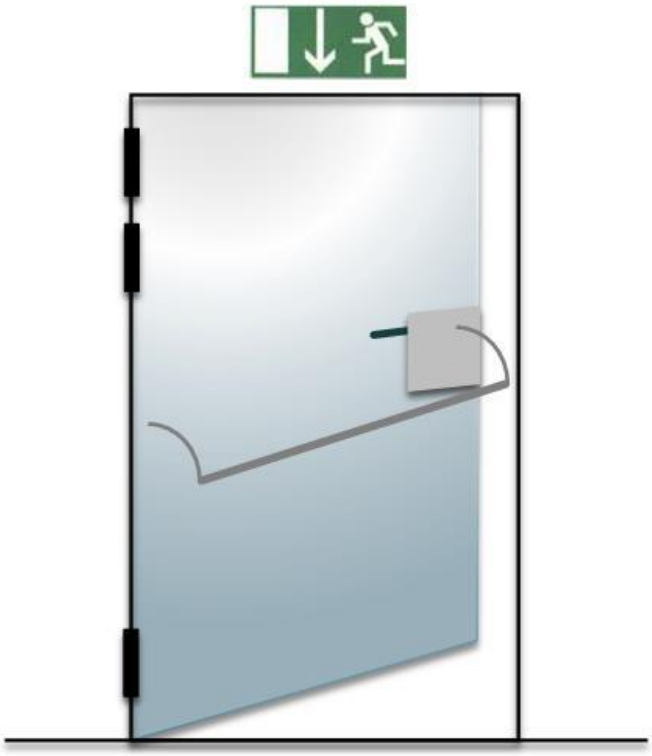
Abbildung 19: Türschnitt zur Darstellung der Ermittlung der Zylindermaße

4.4 Besondere Türen: Fluchttüren, Glastüren



Für Türen in die der Einbau von Normzylindern (z. B. Glas-, Schranktüren) nicht möglich ist, stehen Sonderlösungen zur Verfügung. So gibt es z. B. wie in Abbildung 20 dargestellt vollständige Türbeschläge mit integriertem Sensor für das Identmittel (z. B. RFID-Chip).

Abbildung 20: Glastür mit integrierten Identmittelleser



Bei Türbeschlägen mit einseitigem Zutritt für Paniktüren gibt es speziell für Fluchttüren geeignete Panik-Austrittelemente. Diese Beschläge müssen sich für die Kombination mit Stangengriffen (Panikverschlüsse mit horizontaler Betätigungsstange) nach EN 1125 [7] eignen.

Abbildung 21: Fluchttür mit Panik-Verschluss

Bei Schiebetüren, Drehkreuzen oder auch für die Ansteuerung von Motorzylindern können Wandleser eingesetzt werden, die die unterschiedlichen Verschlusselemente ansteuern. Dieses System besteht meist aus dem Wandleser für den Benutzer und einer Steuereinheit, für die elektronischen Verschlusselemente.

5 Rechtliches

Ziel des Einsatzes von elektronischen Schließanlagen ist grundsätzlich die Erhöhung der Sicherheit für Personen, Anlagen und Gegenständen in Gebäuden und beim Zugang zu den Gebäuden, somit der Flexibilität und Wirtschaftlichkeit im Betrieb.

Datenschutz- und personalvertretungsrechtliche Hinweise:[3)]

Aus datenschutzrechtlicher Sicht ist bei der der Einführung neuer Schließanlagen grundsätzlich folgendes zu beachten:

Die auf dem Markt verfügbaren elektronischen Zugangs- bzw. Schließanlagen sind oft modular aufgebaut und bieten – wie beschrieben - vielfältige Möglichkeiten der Datenverarbeitung, wie z. B. eine Zugangskontrolle mittels Transponder oder die Erfassung und Auswertung von Arbeitszeiten.

Gestaltung und Auswahl dieser Datenverarbeitungssysteme haben sich an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu verarbeiten (datenschutzrechtliches Gebot der Datenvermeidung und -sparsamkeit, s. § 7 Abs. 5 des Niedersächsischen Datenschutzgesetzes - NDSG – [13]).

Die oder der behördliche Datenschutzbeauftragte (behDSB) ist nach § 8 a Abs. 2 Satz 4 NDSG über die geplante Beschaffung und Einführung von automatisierten Zugangsanlagen zu unterrichten. Sofern in diesem Verfahren personenbezogene Daten verarbeitet werden sollen, ist eine datenschutzrechtliche Bewertung durchzuführen. Dabei ist u. a. die Erforderlichkeit der erhobenen Daten, deren Zweckbindung (z. B. Nachverfolgung von Diebstählen, Einbruch, Vandalismus oder Verhaltens- und Leistungskontrolle der Beschäftigten), die Frage der Zugriffsberechtigung, der Auswertung sowie die Speicherdauer bzw. die Löschungsfrist zu prüfen. Für die Durchführung der Datenverarbeitung sind die erforderlichen, geeigneten und angemessenen technisch - organisatorischen Sicherungsmaßnahmen auszuwählen (§ 7 Abs. 1 NDSG). Je nach Art der personenbezogenen Daten oder bei der Verwendung neuer Technologien muss dies im Rahmen einer Vorabkontrolle dokumentiert werden (§ 7 Abs. 3 NDSG; s. hierzu auch www.lfd.niedersachsen.de à Technik und Organisation à Vorabkontrolle). Dafür ist der oder dem behDSB nach § 8 a Abs. 2 Satz 5 NDSG die gemäß § 8 Satz 1 NDSG zu erstellende Verfahrensbeschreibung über die automatisierten Datenverarbeitungen vor der Beschaffung und Einführung des Verfahrens von dem zuständigen Fachbereich zur Verfügung zu stellen.

Viele der aufgeführten (technischen) Schließanlagen sind geeignet, das Verhalten oder die Leistung der Beschäftigten zu überwachen und unterliegen daher der Mitbestimmungspflicht der Personalvertretung nach § 67 Abs. 1 Nr. 2 des Niedersächsischen Personalvertretungsgesetzes (NPersVG [14]). Nicht nur die technische Erhebung, sondern auch die technische Auswertung manuell erhobener Daten unterliegt dem Mitbestimmungsrecht des Personalrats (s. z. B. Bundesarbeitsgericht, Beschluss vom 15. Dezember 1992 - 1 ABR 24/92 -). In diesen Fällen wird der Abschluss einer Dienstvereinbarung mit der Personalvertretung empfohlen, in der insbesondere festgelegt werden sollte:

- wie lange die aufgezeichneten Daten gespeichert werden,
- welche Personen Zugriff auf die gespeicherten Daten haben und
- wer welche Auswertungen und Berichte wann veranlassen kann (z. B. ob und ggf. wie die Personalvertretung über die sich aus der Software ergebenden Berichte und Auswertungen zu unterrichten ist).

[3] Zuarbeit vom Niedersächsischen Beauftragten für den Datenschutz

6 Wirtschaftlichkeitsbetrachtung

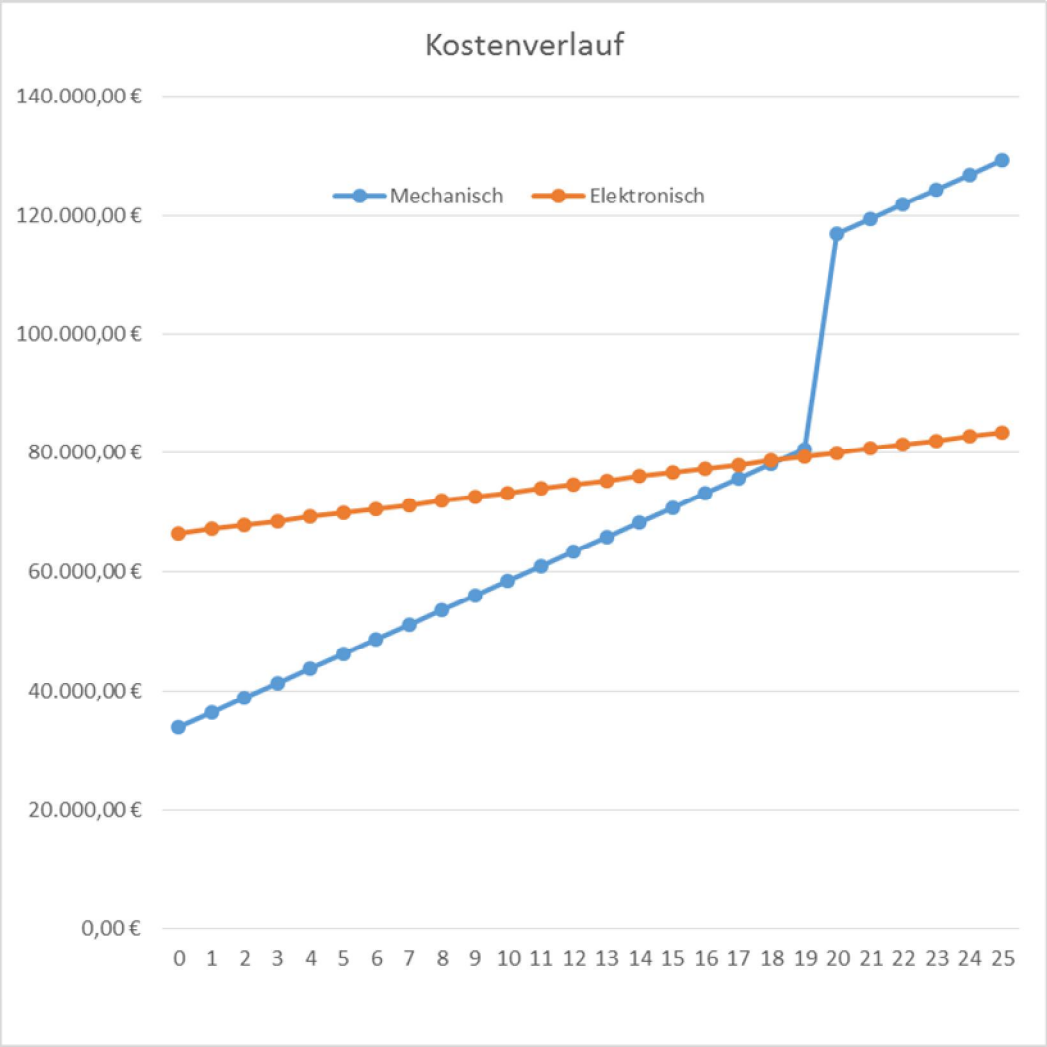


Abbildung 22: Schematische Kostenentwicklung bei Schließanlagen

Die Kostenanschläge für die verschiedenen Anlagen unterliegen immer einer Betrachtung innerhalb der gestellten Ausgangssituation. Angaben über Art und Umfang von Schlüsselverlusten beruhen häufig auf Erfahrungswerten und weichen von Fall zu Fall voneinander ab. Der Zeitaufwand für eine Schlüsselbestellung und die Ausgabe der Schlüssel hängt immer von den örtlichen organisatorischen Voraussetzungen ab.

Die Anschaffungskosten beinhalten die Kosten für die Lieferung einer Schließanlage (Zylinder, Schlüssel / Identmittel, Software und Hardware), einschließlich Montage, Inbetriebnahme und Nebenkosten für die Anpassung von Türschlössern etc.

Folgekosten aus Organisationsänderungen müssen bei der Betrachtung der Betriebskosten berücksichtigt werden, da bei Zentralschließanlagen eine Anpassung an betriebliche Umstrukturierungen in der Regel nur durch einen kostenintensiven Austausch der kompletten Anlage oder eines Anlagenteils möglich ist.

Kosten für temporäre Ersatzschließanlagen, Bewachung während der Neubeschaffung einer Ersatzanlage und für den internen Schlüsseltausch der Mitarbeiter bleiben oft unberücksichtigt.

Die Instandhaltung (Instandsetzung, Inspektion oder Wartung) muss kostenmäßig bei der Wirtschaftlichkeitsbetrachtung berücksichtigt werden.

6.1 Mechanische Schließanlagen

6.1.1 Anschaffungskosten

Im Anschaffungspreis ist eine mechanische Schließanlage günstiger als eine elektronische Anlage.

6.1.2 Folgekosten

Die Folgekosten beinhalten die Kosten für Einzelschlüssel und Schließzylinder oder auch den Gesamtaustausch der Anlage, z. B. bei Verlust von übergeordneten Schlüsseln.

Aufgrund von Schlüsselverlusten oder Umnutzungen mit veränderten Gruppenschließungen entstehen Kosten bei Nachbestellungen von Schließzylindern und Schlüsseln. Häufig jedoch mit Mindermengen- oder Altanlagenzuschlägen.

6.2 Elektronische Schließanlagen

6.3.1 Anschaffungskosten

Die Anschaffungskosten einer elektronischen Schließanlage sind, bedingt durch teure Zylinder, verhältnismäßig hoch. Daneben fallen die Kosten für die Hard- und Software an.

6.3.2 Folgekosten

Es können Zylinder und Transponder in geringen Stückzahlen bevorratet werden. Da die Schlüssel und Zylinder im unprogrammierten Zustand nicht nutzbar sind, können diese auch ungesichert aufbewahrt werden.

Bei einer elektronischen Anlage sind lediglich in Zeitabständen von mehreren Jahren Batterien zu wechseln und verlorene elektronische Schlüssel (Identmittel) zu ersetzen. Alle weiteren Aufwendungen liegen in der Neuprogrammierung der Anlage.

6.3 Kostenvergleich, Beispiel

Wenn aus funktionalen Gründen mehrere Lösungen möglich sind, ist die Wirtschaftlichkeit zu untersuchen. Um die Abhängigkeit der Investitions- und Folgekosten (Instandhaltung, Verlust von Schlüsseln, bzw. Identmitteln) darzustellen wurde eine Musterrechnung (siehe Anlage 2) erstellt[4)].

Die Investitionskosten für die Ersteinrichtung wurden dabei ermittelt = (Anzahl Schließzylinder x EP) + (Anzahl Schlüssel/Identmittel x EP), bei elektronischen Anlagen außerdem die Kosten für Schulung und Schließplansoftware.

Die Kosten für die Ersatzschlüssel = Anzahl Schlüssel x EP x Betrachtungszeitraum x Verlustquote.

Die Kosten für die Instandhaltung wurden pauschal angenommen und in der graphischen Darstellung linear auf den Betrachtungszeitraum verteilt.

Bei mechanischen Schließanlagen wurde außerdem noch ein Totalaustausch berücksichtigt, wenn die genannte Verlustquote erreicht wird = Investitionskosten x Betrachtungszeitraum / (Verlustquote / Austausch bei Verlust).

[4] Die Berechnung steht auch im Intranet als Blanco-Tabelle zur Verfügung unter: http://intra.sbn.ads.niedersachsen.de/fileadmin/daten/ofd/Bibliothek/BL_22/FeMeBau/Teil8/Wirtschaftlichkeit_Elektronische_Schliesssysteme_01.xls

7 Planung und Installation

7.1 Technische Anforderungen an Schließanlagen

Ein Vergleich von Produkten mit den unter Praxisbedingungen relevanten Anforderungskriterien, ist im Einzelfall sehr schwierig und aufwändig.

Vor der Planung ist es erforderlich die technischen Anforderungen zu klären. Unter Berücksichtigung der Gütekriterien sind die entsprechenden Zylinder bzw. die Anlage für die Aufgabenstellung auszuwählen.

Vor der Erstellung der Leistungsbeschreibung ist das Leistungsbild klar und eindeutig zu definieren. Das Einfordern von speziellen herstellerspezifischen Zertifikaten kann schnell zum Widerspruch oder gar Ausschluss anderer für den Anwendungsfall geeigneter Fabrikate führen.

7.2 Beratung der nutzenden Verwaltung

Eine Planungsvoraussetzung zu einer Schließanlage ist die Klärung der Anforderungen an die Anlage im Rahmen der Beratung der nutzenden Verwaltung.

Nachfolgend sind Fragen aufgeführt, die Bestandteil der Beratung der nutzenden Verwaltung sein sollten. Ein Fragenkatalog ist immer projektspezifisch aufzustellen, daher sind die nachfolgenden Fragen als Hilfestellung zur Erarbeitung eines projektspezifischen Fragenkataloges anzusehen.

- Wie wird das Gebäude genutzt?
- Wie viele unterschiedliche nutzende Verwaltungen sind in dem Gebäude oder der Liegenschaft?
- Wie ist die sich daraus ergebene Organisationsstruktur?
- Welche Sicherheitsanforderungen bestehen an das Gebäude? Welche Anforderungen ergeben sich daraus an die Schließanlage? Ist bei erhöhter Sicherheitsanforderung an das Gebäude oder an die Liegenschaft eine Abstimmung mit dem LKA / BKA / MAD erforderlich?
- Wird durch die Schließanlage ggf. ein bestehendes Sicherheitskonzept für das Gebäude / die Liegenschaft verändert (Zugänglichkeit von Gebäudeteilen, Fluchtwege aus dem Brandschutzkonzept / der Baugenehmigung)?
- Wie viele Türen mit welchen Funktionen sind zu berücksichtigen?
- Art und Anzahl der benötigten Identmittel?
- Welcher maximale Umfang muss für die Schließanlage in der Endausbaustufe möglich sein?
- Welche Anforderungen der nutzenden Verwaltung müssen für die Funktion der Schließanlage erfüllt werden, um den uneingeschränkten Betriebsablauf zu gewährleisten (Zeitzonen)?
- Können Teilbereiche mit rein mechanischen Schließzylindern ausgerüstet werden?
- Sind Anlagen mit Identmittel bereits vorhanden? Wenn Ja, sollen diese mit der neuen Anlage in einem Identmittel zusammengefasst werden?
- Soll das Identmittel auch für andere Zwecke verwendet werden (z. B. als Ausweis für die Bibliothek, Zahlungsmittel in der Kantine)

- Soll die Anlage Schnittstellen zu vorhandenen oder geplanten technischen Anlagen wie z. B. einer Zeiterfassungsanlage haben? Wenn ja, zu welcher Anlage oder zu welcher Schnittstelle?
- Ist der Einsatz von speziellen Verschlüssen, wie z.B. Paniktürverschlüssen, erforderlich?
- Sind für eine ggf. anzuschaffende Schließplansoftware separate PC`s für die Verwaltung der Schließanlage vorhanden oder sind zusätzliche Geräte erforderlich?
- In welchem Umfang ist eine Instandhaltung der Anlage erforderlich? Ist z. B. der erforderliche Batteriewechsel durch Personal der nutzenden Verwaltung durchzuführen?
- In welchen Zeiträumen ist eine Ersatzbeschaffung, für Identmittel und Schließzylinder erforderlich?
- Wie hoch ist die Verlustquote von Identmitteln / Schlüsseln pro Jahr?
- Wann ist ein Austausch einer kompletten mechanischen Schließanlage notwendig?
- Soll die Schließanlage als elektronische Zutrittskontrollanlage nach DIN EN 60839-11 [9, 19] eingesetzt werden?
- Welche datenschutzrechtlichen Anforderungen sind zu beachten? [Þ Abschnitt 5]

Der Abschluss der Bedarfsanalyse kann als Grundlage der Anlagenplanung zur Grobstruktur der Schließanlage betrachtet werden. Nun kann die Anlagenauswahl (mechanisch, elektronisch) in technischer Hinsicht definiert werden. Die Anlagenplanung stellt einen iterativen Prozess dar. Um eine optimale Lösung für die jeweilige Aufgabenstellung zu erreichen, ist es erforderlich, die Planung mit der nutzenden Verwaltung und dem SBN vor Erstellung der Ausschreibungsunterlagen nochmals abzustimmen gemäß_Anlage 1 zur TI-Schließanlagen 2016: Checkliste[5)]. Hierzu gehören auch der abgestimmte Ausführungszeitraum und ggf. erforderliche Interimsmaßnahmen.

7.3 Planung und Veranschlagung nach DIN 276-1

Auf Grund der speziellen Anforderungen an elektronische Schließanlagen sollte die Planung federführend von der Betriebstechnik betreut werden. Für die Themen: Schließplan, Anforderungen an Türen und Zylinder etc. ist die Beteiligung des Hochbaus erforderlich.

Soweit es sich um eine Zutrittskontrollanlage Grad 1 handelt, erfolgt eine Veranschlagung nach DIN 276-1 [18] in Kostengruppe (KG) 390 und dort, innerhalb der KG 390, in der Untergruppe 399 "Sonstige Maßnahmen für Baukonstruktionen, Sonstiges", auch wenn z. B. die Betriebstechnik mit der Planung beauftragt wird. Eine Veranschlagung in KG 334 für Zylinder in Außentüren und KG 344 für Innentüren ist nicht sinnvoll, da auch immer zentrale Einrichtungen benötigt werden, die keiner der beiden Kostengruppen zuzuordnen sind.

Wenn es sich um eine Zutrittskontrollanlage handelt, die zumindest partiell einem höheren Grad als eins entspricht, erfolgt die Veranschlagung in KG 456 – Gefahrenmeldeanlagen.

[5] Eine editierbare Fassung der Checkliste finden Sie im Intranet des SBN unter: http://intra.sbn.ads.niedersachsen.de/fileadmin/daten/ofd/Bibliothek/BL_22/FeMeBau/Teil8/Checkliste_Bedarfsermittlung.docx

7.4 Ausschreibung

Bauliche, sicherheitstechnische und technische Anforderungen dienen wie zuvor unter Abschnitt 4 und Abschnitt 7.2 als Auswahlkriterien bei der Anlagenwahl und der Beschreibung der Anforderungen in den zusätzlichen technischen Vorbemerkungen zum Leistungsverzeichnis.

Um ein wirtschaftliches Ergebnis zu erreichen, ist die Leistungsbeschreibung herstellerneutral abzufassen. Basis einer herstellerneutralen Leistungsbeschreibung, bilden die in den Planungsphasen festgelegten Randbedingungen. In der Leistungsbeschreibung sind mindestens zu verankern:

- Zusätzliche technische Vorbemerkung mit der konkreten objektspezifischen Ausführungsbeschreibung der Schließanlage. Eine Objektbeschreibung mit den spezifischen sicherheitstechnischen Anforderungen der nutzenden Verwaltung. Siehe hierzu auch VOB / A in der gültigen Fassung.
- Beschreibung der Programmierungsanforderungen des Schließplans; Anforderungen zur Ausführung der Hard- und Software.
- Art, Menge und Ausführungsmerkmale der Identmittel (Transponder / Schlüssel).
- Art, Menge und Ausführungsmerkmale der Schließzylinder (auch Paniktürverschlüsse).
- Maße der Schließzylinder (siehe Abbildung 18) auf Basis der für das Objekt ermittelten Türen.
- Erforderliche Integrationen vorhandener Motorschlösser (z. B. Schranken, Rolltore, Aufzüge).
- Ist eine Einbeziehung einer Gefahrenmeldeanlage (Scharfschalteinheiten einzelner Schließzylinder) erforderlich?
- Dienstleistungen, die über die geforderten Nebenleistungen nach VOB / C DIN 18357 [17] hinausgehen.
- Instandhaltungsvertrag (entsprechend dem in VHB Formblatt 112 abgestimmten Umfang) mit den Vorgaben der Instandhaltung zur angefragten Schließanlage (Arbeitskarte).
- Eventuell erforderliche Ausbaureserven für spätere Anlagenerweiterung, soweit bekannt.

8 Schulung und Einweisung

Die Einweisung in die vor Ort errichtete Schließanlage ist als Nebenleistung nach VOB Teil C durch den Auftragnehmer ohne gesonderte Vergütung zu erbringen.

Um eine elektronische Schließanlage aber optimal nutzen zu können, sollten die Mitarbeiter, die die Anlage bedienen, geschult werden.

Die Schulung stellt keine Nebenleistung nach VOB Teil C dar. Diese Leistung ist separat in der Leistungsbeschreibung darzustellen und gesondert zu vergüten.

Für die anlagengebundene Schulung ist der Umfang der Schulung in der Leistungsbeschreibung zu definieren. Im Vorfeld ist dazu vom zukünftigen Nutzer der Anlage der einzuweisende Personenkreis festzulegen. Je nach Umfang und Größe der Schließanlage kann es erforderlich werden, neben einer Erstschulung auch Folgeschulungen vorzusehen.

Für den Schulungsinhalt sollten neben den projektspezifischen Anforderungen mindestens folgende Punkte definiert werden:

- Anzahl der zu schulenden Personen.
- Ort der durchzuführenden Schulung.
- Zeitpunkt der Schulung.
- Mindestumfang der Schulung.
- Aufbau und Funktionen der Hardwarebestandteile.
- Umfang und Bedienung der Schließplansoftware (bei Anlagen mit PC).
- Anlegen, Ändern und Löschen von Personen und Zutrittsprofilen.
- Geplantes Bestellwesen für den Ersatzbedarf.
- Zeitumfang der Schulung.

Über die Einweisung und über die anlagengebundene Schulung sind Protokolle zu fertigen, welche Bestandteil der Abnahme und Übergabe der Dokumentation werden.

9 Betrieb und Instandhaltung

9.1 Betrieb

Die nutzende Verwaltung muss den Datenbestand der Anlage jederzeit aktuell halten. Dies betrifft die Daten der ausgegebenen Identmittel und die in die einzelnen Schließzylinder übertragenen Informationen[6)]. Dies setzt eine Schulung [Þ Abschnitt 8] voraus. Es sind mindestens zwei geschulte Personen erforderlich, um eine Vertretung sicherstellen zu können.

Es ist sicher zu stellen das jederzeit eine ausreichende Instandhaltung [Þ Abschnitt 9.2] gewährleistet ist.

9.2 Instandhaltung

Im Rahmen der Planung ist mit der nutzenden Verwaltung abzustimmen, wie die Instandhaltung der Anlage erfolgen soll. Das Ergebnis ist auf dem VHB-Formblatt 112 festzuhalten. Wenn von der nutzenden Verwaltung ein Instandhaltungsvertrag gewünscht wird, kommt hierfür das AMEV Vertragsmuster InstandGMA 2012 [2], Variante „sonstige Alarmanlage“ in Frage. Welche Phasen der Instandhaltung abgeschlossen werden sollen, ist auf Basis der nachfolgend beschriebenen Kriterien abzustimmen. Es werden dabei die Begriffe der Instandhaltung nach DIN 31051 [7] verwendet, wie sie auch im Formblatt 112 erläutert werden. Wenn die Anlage auch die Funktion einer Zutrittskontrollanlage für Sicherheitsanwendungen (Grad 2 oder höher) erfüllen soll, ist nach DIN EN 60839-11-2 Pkt. 10.2 [10] der Abschluss eines Instandhaltungsvertrages erforderlich, soweit die nutzende Verwaltung nicht selbst über ausreichend qualifiziertes Personal verfügt.

Inspektion

Im Rahmen einer Inspektion könnte z. B. überprüft werden, ob einzelne Komponenten (elektronische Schließzylinder) einen niedrigen Batteriestatus signalisieren.

Wartung

Zu den zu berücksichtigen Wartungsarbeiten gehört der Austausch von Batterien in elektronischen Schließzylindern oder Identmitteln (z. B. Transpondern). Es ist zu klären, ob die nutzende Verwaltung diese Leistung selbst erbringen kann oder ob diese mit ausgeschrieben und vergeben werden soll. Auf Grund der langen Lebensdauer der Batterien wird empfohlen, bei externer Vergabe die Ausführung der Leistung nur auf besondere Anforderung zu vereinbaren. Dies bedeutet für die nutzende Verwaltung, dass nur Leistungen zu vergüten sind, wenn tatsächlicher Leistungsbedarf besteht.

Instandsetzung

Da Instandsetzungsarbeiten nur in Ausnahmefällen abzusehen sind, sollte auch hier die Leistung nur auf besonderen Auftrag erteilt werden. Der Abschluss eines Instandsetzungsvertrages nach dem o. g. Muster hat den Vorteil, dass damit auch die Lieferverpflichtung für Ersatzteile für die Vertragslaufzeit verbunden ist. Es wird also das Risiko gemindert, dass eine Instandsetzung nicht mehr möglich ist, weil keine Ersatzteile mehr angeboten werden.

Verbesserung

Von Verbesserungen durch Änderungen bei der Bediensoftware bei elektronischen Schließanlagen ist abzusehen. Bei Bedarf kann das Angebot fortgeschriebener Programmversionen mit dem o. g. Vertragsmuster im Rahmen der dort optional vorgesehenen Anlagenbetreuung vereinbart werden.

[6] Wer hat wann wo Zutrittsberechtigung

10 Verzeichnis der verwendeten Normen und Richtlinien

1	AMEV-Empfehlung EMA/ÜMA 2012	Gefahrenmeldeanlagen für Einbruch, Überfall und Geländeüberwachung
2	AMEV-Vertragsmuster Instand GMA 2012	Vertragsmuster für Instandhaltung von Gefahrenmeldeanlagen (Brand, Einbruch, Überfall und Geländeüberwachung) in öffentlichen Gebäuden
3	DIN 18250:2006-09	Schlösser - Einsteckschlösser für Feuerschutz- und Rauchschutztüren
4	DIN 18251-1:2002-07	Schlösser - Einsteckschlösser - Teil 1: Einsteckschlösser für gefälzte Türen
5	DIN 18252:2006-12	Profilzylinder für Türschlösser - Begriffe, Maße, Anforderungen, Kennzeichnung
6	DIN 31051:2012-09	Grundlagen der Instandhaltung
7	DIN EN 1125:2008-04	Schlösser und Baubeschläge - Paniktürverschlüsse mit horizontaler Betätigungsstange für Türen in Rettungswegen - Anforderungen und Prüfverfahren
8	DIN EN 1303:2015-08	Baubeschläge - Schließzylinder für Schlösser - Anforderungen und Prüfverfahren
9	DIN EN 60839-11-1: 2013-12 (VDE 0830-8-11-1)	Elektronische Zutrittskontrollanlagen - Anforderungen an Anlagen und Geräte
10	DIN EN 60839-11-2: 2016-02 (VDE 0830-8-11-2)	Elektronische Zutrittskontrollanlagen - Anwendungsregeln
11	DIN EN179:2008-04-12	Schlösser und Baubeschläge - Notausgangsverschlüsse mit Drücker oder Stoßplatte für Türen in Rettungswegen - Anforderungen und Prüfverfahren
12	EltVTR:1997-12	Richtlinie über elektrische Verriegelungssysteme von Türen in Rettungswegen
13	NDSG	Niedersächsisches Datenschutzgesetz vom 29. Januar 2002 - VORIS 20600 02 - zuletzt geändert 12. Dezember 2012
14	NPerVG	Niedersächsische Personalvertretungsgesetz
15	VdS Richtlinie 2156-1: 2016-01	Profilzylinder für Türschlösser; Begriffe, Maße, Anforderungen, Kennzeichnung
16	VdS Richtlinie 2156-2: 2013-06	Schließzylinder mit Einzelsperrschließung – Anforderungen und Prüfmethoden Teil 2: Elektronische Schießzylinder
17	DIN 18357:2012-09	VOB C Beschlagsarbeiten
18	DIN 276-1: 2008-12	Kosten im Bauwesen - Teil 1: Hochbau

11 Fundstellen

Zur weiterführenden Information können folgende Unterlagen dienen:

- VdS Schadenverhütung GmbH

  VdS-Richtlinie 2156-2

  http://www.vds.de
- Bundesamt für Sicherheit in der Informationstechnik (BSI)

  http://www.bsi.bund.de
- Einige Abbildungen wurden bei Wikipedia entnommen.
- Bayrische Landeskriminalamt: à Schützen und Vorbeugen à Beratung à Technische Beratung.

  www.polizei.bayern.de

12 Glossar /Abkürzungsverzeichnis

Accesspoint	Funkzugangsschnittstelle zum Datennetz
AMEV	Arbeitskreis Maschinen- und Elektrotechnik staatlicher und kommunaler Verwaltungen
behDSB	behördlicher Datenschutzbeauftragter
BKA	Bundeskriminalamt
BSI	Bundesamt für Sicherheit in der Informationstechnik
LfD	Landesbeauftragter für Datenschutz
LKA	Landeskriminalamt
MAD	Militärischer Abschirmdienst
RFID	Radio frequency identifikation à Funkerkennung
Validierung	oder Validation (von lateinisch *validus:* stark, wirksam, gesund); Prüfen auf Plausibilität (Nachvollziehbarkeit), für gültig erklären; In der Informatik Beweisführung, dass eine Anlage die Anforderungen in der Praxis erfüllt.
VdS	VdS Schadensverhütung GmbH
VHB	Vergabehandbuch
VOB	Verdingungsordnung für Bauleistungen
VOL	Verdingungsordnung für Lieferleistungen
NDSG	Niedersächsischen Datenschutzgesetz
NPersVG	Niedersächsisches Personalvertretungsgesetz
ZKA	Zutrittskontrollanlage

13 Mitarbeiter

Frau Anne Janssen-Bokämper	Oberfinanzdirektion Niedersachsen Bau und Liegenschaften
Herr Dieter Feldschnieders	Landesbeauftragte für den Datenschutz Niedersachsen Referat 1.11
Herr Gerald Lomp	Landeskriminalamt Niedersachsen, Hannover
Herr Holger Dittrich	Oberfinanzdirektion Niedersachsen Bau und Liegenschaften
Herr Wilfried Müller	Oberfinanzdirektion Niedersachsen Bau und Liegenschaften

Anlage 1 : Checkliste für die Bedarfsermittlung

Hinweis: Alle blauen Eintragungen sind als Muster zu verstehen, sie geben keinen allgemeinen Standard wieder!

1 Zutreffendes ist anzukreuzen

Baumaßnahme: Neubau Landgericht Neustadt .....

.....

Liegenschaft: Landgericht Neustadt .....

Ort: Neustadt .....

Straße: Gerichtsstraße .....

Nutzende Verwaltung: Landgericht Neustadt .....

Ort Neustadt .....

Straße Gerichtsstraße .....

Telefon: 0999/9999-0 .....

Ansprechpartner nutzende Verwaltung

Name: Janssen ..... Telefon: 0999/9999-100 .....

E-Mail: Janssen@Landgericht-Neustadt.de .....

Ansprechpartner SBN

Bauamt: SBN Neustadt .....

Name: Müller ..... Telefon: 0999/8888-200 .....

E-Mail: Mueller@Bauamt-Neustadt.de .....

Bemerkungen zum Projekt

Es handelt sich um ein Behördenhaus für Landgericht und Staatanwaltschaft Neustadt .....

.....

.....

Art und Nutzung des Gebäudes? Bürogebäude .....

.....

Wie viele nutzende Verwaltungen in dem Gebäude
oder der Liegenschaft sollen die Schließanlage nutzen? 2

Wie ist die sich daraus ergebene Organisationsstruktur? Jede Verwaltung muss die Berechtigungen selbstständig vergeben können. .....

Ist bei erhöhter Sicherheitsanforderung an das Gebäude oder die Liegenschaft eine Abstimmung mit dem LKA / BKA erforderlich? T Ja / 1 Nein

Wenn ja: Hat eine derartige Beratung schon stattgefunden? T Ja / 1 Nein

Wenn ja: Welche Anforderungen (z. B. erforderlicher Grad) wurden festgelegt? .....

Grundsätzlich Grad 1, ausgewählte Räume (Asservatenkammer, Serverräume,) Grad 3.....

.....

Welche datenschutzrechtlichen Belange sind zu beachten?.....

Keine über das NDSG hinaus. .....

Beachten: Ab Mai 2018 gelten unmittelbar die Regelungen der Datenschutz-Grundverordnung (DS-GVO 2016/679).

Wird durch die Schließanlage ggf. ein bestehendes Sicherheitskonzept für das Gebäude / die Liegenschaft verändert? (Zugänglichkeit von Gebäudeteilen, Fluchtwege aus dem Brandschutzkonzept / der Baugenehmigung.) 1 Ja / T Nein

Wenn ja: Was muss berücksichtigt werden? .....

.....

Umfang

Wie viele Türen sind einzubeziehen? 250

mit welchen Funktionen: nur Zugangskontrolle.....

.....

Anzahl der benötigten Identmittel? 300

Art: Transponder .....

Welcher maximale Umfang muss für die Schließanlage in der Endausbaustufe möglich sein?

Zylinder: ..... 300 Identmittel: 500

Leistungsmerkmale

Welche Anforderungen der nutzenden Verwaltung müssen für die Funktion der Schließanlage erfüllt werden, um den uneingeschränkten Betriebsablauf zu gewährleisten? (Zeitzonen):

Es muss möglich sein für ausgewählte Mitarbeiter den Zugang an Wochenenden, Feiertagen und außerhalb der Kernzeit zu verhindern.....

Bei den Grad 3 gesicherten Zugängen muss protokolliert werden wer wann Zugang erlangt hat. Bei den Grad 1 gesicherten Zugängen darf keine Protokollierung erfolgen.....

Können Bereiche mit rein mechanischer Sicherheit ausgerüstet werden? T Ja / 1 Nein

Wenn ja: Welche? Sanitärräume, Teeküchen, Lager.....

.....

Bestand

Sind Anlagen mit nutzbaren Identmitteln bereits vorhanden? 1 Ja / T Nein

Wenn Ja, sollen diese mit der neuen Anlage in einem Identmittel zusammengefasst werden?

.....

.....

Schnittstellen, Sonderlösungen

Soll die Anlage Schnittstellen zu vorhandenen oder geplanten technischen Anlage wie z. B. einer Zeiterfassungsanlage haben? T Ja / 1 Nein

Wenn ja, zur welcher Anlage oder welcher Schnittstelle?.....

Zeiterfassung, Schranke Parkplatz, Drucker.....

Sind andere elektrische oder elektronische Komponenten von der Schließanlage anzusteuern (z. B. Motorschlösser, automatische Torantriebe, Schranken, Aufzüge)?.....

Schranke Parkplatz .....

Ist der Einsatz von speziellen Verschlüssen, wie z.B. Paniktürverschlüssen erforderlich? nein

.....

Ausführung

Als Ergebnis der Beratung ist vorzusehen:

1 Klassische Schließanlage mit mechanischen Zylindern (in Teilbereichen)

1 Offline-Schließanlage

T Schließanlage mit virtuellem Netzwerk (Grundsätzlich)

1 Online-Schließanlagen

Datenanbindung 1 WLAN 1 Kabelverbindung

Betrieb

Sind für eine ggf. anzuschaffende Schließplansoftware separate PC`s für die Verwaltung der Schließanlage vorhanden oder sind zusätzliche Geräte erforderlich?

1 Kein Bedarf / 1 Vorhandener PC / T PC (1 x je Nutzer) muss mit beschafft werden

Welches Betriebssystem wird eingesetzt? Windows 10.....

Instandhaltung

Welcher Umfang ist für die Instandhaltung der Anlage erforderlich?

T Inspektion

1 Wartung

T Instandsetzung

Ergänzend ist für die Fragen der Instandhaltung das VHB-Formblatt 112 zu verwenden und beizufügen.

Kann der erforderliche Batteriewechsel durch Personal der nutzenden Verwaltung durchgeführt werden? 1 Ja / T Nein

In welchen Zeiträumen ist eine Ersatzbeschaffung für Identmittel und Schließzylinder erforderlich? .....15 Jahre

Wie hoch ist die Verlustquote von Identmitteln / Schlüsseln pro Jahr? 5%

Wann ist ein Austausch der kompletten mechanischen Schließanlage notwendig?.....25%

Anlagen

Sind Bestandsunterlagen vorhanden 1 Ja / T Nein

Beigefügte Planunterlagen:
Grundrisse.....
.....

T VHB-Formblatt 112

Bemerkungen

Nutzende Verwaltung
.....
.....
.....

SBN
Die Datenschutzbeauftragten sollten nach Bestellung beteiligt werden .....
.....
.....

Aufgestellt

SBN nutzende Verwaltung

Neustadt., den 4.10.2016

....
(Müller) (Janssen)

Anlage 2: Musterberechnung zum Anlagenvergleich

[Projektspezifisch anzupassen]

Die Tabelle steht im Intranet zum Download zur Verfügung unter:

http://intra.sbn.ads.niedersachsen.de/fileadmin/daten/ofd/Bibliothek/BL_22/FeMeBau/Teil8/Wirtschaftlichkeit_Elektronische_Schliesssysteme_01.xls

Eingaben sind lediglich in den gelb oder grün hinterlegten Feldern erforderlich.

Wirtschaftlichkeitsvergleich Schließsysteme

Projekt	**Landgericht Neustadt**	
Kosten für	Elektronisches Schließsystem	Mechanisches Schließsystem
Schließzylinder (EP)	250,00 €	100,00 €
Schlüssel (EP)	5,00 €	30,00 €
Instandhaltungskosten	sind individuell zu ermitteln	
Betriebsdaten		
Schließzylinder [St]	250	
Schlüssel [St]	3000	
Verlustquote [/Jahr %]	5%	
Austausch bei Verlust [%]	100%	
(Nur bei mechanisch)		
Betrachtungszeitraum [Jahre]	25	
Wertungskosten Mechanisch		
Ersteinrichtung	34.000,00 €	
Ersatzschlüssel	11.250,00 €	
Austauschkosten	25.000,00 €	
Instandhaltungskosten	50.000,00 €	
Gesamt	120.250,00 €	
Wertungskosten Elektronisch		
Ersteinrichtung	64.000,00 €	
Schließplansoftware	500,00 €	
Schulung	2.000,00 €	
Ersatzschlüssel	1.875,00 €	
Instandhaltungskosten	15.000,00 €	
Gesamt	83,375,00 €	

Hinweise

Angaben für gelb hinterlegte Felder sind vom SBN zu machen

Angaben für grün hinterlegte Felder sind vom Nutzer zu machen

Instandhaltungskosten werden auf den Betrachtungszeitraum verteilt