

Empfehlungen für elektronische Zutrittssteuerung

Stadt Nürnberg
Hochbauamt
Abteilung Elektrotechnik
Marientorgraben 11
90402 Nürnberg

Inhalt

1	Empfehlungen für elektronische Zutrittssteuerung	3
1.1	Allgemein	3
1.2	Zentrale für die Zutrittssteuerung	4
1.2.1	Anbindung an das städtische Datennetz	5
1.2.2	Installation Hinweise	5
1.2.3	Besonderheit bei der Beschaffung der Basisplatine und Lizenzen	6
1.3	Türperipherie.....	6
1.3.1	Grundlegende Türbeschreibung	6
1.3.2	Unterschied Online- / Offline-System	13
1.3.3	Empfehlung für städtische Liegenschaften	13
1.3.4	Kabelgebundene Türperipherie	13
1.3.5	Kabellose Türperipherie	14
1.3.6	Drahtloses Türsystem Aperio	14
1.4	Leser.....	17
1.5	ID-Träger	18
1.5.1	Multifunktionskarten	18
1.5.2	Token	19
1.6	Zentrale Verwaltungssoftware zur Zutrittssteuerung.....	20
1.6.1	Benutzerverwaltung	20
1.6.2	Lokationen	21
1.6.3	Raum- / Zeitzone	21
1.6.4	Makros	22
1.6.5	Mandantenfähigkeit.....	22
1.7	Grundlegende Bestandteile der Zutrittssteuerung	23
1.7.1	Spannungsversorgung der Komponenten	23
1.7.2	Modul-Bus RS-485.....	23

Vorwort

Diese Empfehlungen für elektronische Zutrittssteuerung basieren auf dem einheitlichen Einsatz einer bestimmten Zugangskontrolle. Sie sind als Handlungsempfehlung zu verstehen und ergänzen die gültigen DIN-, VDE-Normen sowie sonstige Vorschriften und Verordnungen in ihrer jeweils aktuellen Fassung.

Für Rückfragen steht Ihnen gerne der Fachbereich Elektrotechnik zur Verfügung.

Änderungen

Verfasser:	Thema:	Seiten:	Datum:

Stadt Nürnberg

Hochbauamt

Abteilung Elektrotechnik

Marientorgraben 11

90402 Nürnberg

Tel.: 0911/231-4302

0911/231-4310

Kontakt zu Fragen, Prozessen und Störungen:

H-E-Werkstatt@stadt.nuernberg.de

oder

H/E@stadt.nuernberg.de

1 Empfehlungen für elektronische Zutrittssteuerung

1.1 Allgemein

Die Zutrittssteuerung dient zur Organisation und zum Steuern der Zugänglichkeit von städtischen Gebäuden. Es soll verhindert werden, dass unbefugte Personen in das Gebäude gelangen oder dass berechtigte Personen nur zu vorbestimmten Zeiten das Gebäude betreten können. Sie ersetzt ein aufwendiges mechanisches Schließsystem und dessen Schlüsselmanagement. Auch das Tauschen der mechanischen Schließanlage bei einem unbekannten Verbleib eines Schlüssels lässt sich mit einer Zutrittssteuerung einfach softwaretechnisch lösen. Zugangsberechtigungen können schnell online vergeben und geändert werden, auch können Zugangsberechtigungsprofile angelegt werden und diese dann einzelnen Mitarbeitern zugewiesen werden.

Bei der Stadt Nürnberg sind unterschiedliche Zutrittssteuerungssysteme und -fabrikate im Einsatz, daher kann in dieser Richtlinie kein Fabrikat zwingend vorgeschrieben werden. Durch langjährige Erfahrung in der Sicherung der Gebäude der Stadt Nürnberg haben sich Systemkomponenten des Herstellers Honeywell bewährt. Sie bieten vielfältige Einsatzmöglichkeiten sowie eine zentrale Zutrittssystemverwaltung.

Die vorliegende Ausarbeitung dient dazu, ein einheitliches Konzept der Zutrittssteuerung in den Gebäuden der Stadt Nürnberg zu gewährleisten. Aus ihr können die standardmäßige Peripherie, sowie die Möglichkeiten dieser abgeleitet werden.

Die Zutrittssteuerung besteht aus zwei Einheiten.

Die Zutrittssteuerung besteht aus zwei Einheiten, zum einen aus Geräten und Materialien, welche fest mit dem Gebäude verbunden sind (Zentrale, Schlösser, Leser und Verkabelung) und zum anderen aus beweglichen Bauteilen z.B. den ID-Trägern, (Multifunktionskarten und Transpondern) die eine Personalisierung ermöglichen.



1.2 Zentrale für die Zutrittssteuerung

MB-Secure Pro

Die MB-Secure Pro besteht hardwaretechnisch aus vier Teilen:

aus einer Rechnerplatine, einem Gehäuse, einem Netzteil und einer Notstromvorrichtung. Diese Teile sind separat bestellbar und individuell auf die Lokation anpassbar.

Die Rechnerplatine kann als Basisplatine bestellt werden, diese beinhaltet, aber keinerlei Lizenzen.

Lizenzen können individuell nachbestellt werden, z. B. für Türen, Benutzer, Makros oder Raum- / Zeitzonen.

Dies stellt sich oft als nicht wirtschaftlichste Lösung heraus.

Wirtschaftlicher ist es, ein Lizenzpaket zu erwerben und dieses dann nach Bedarf individuell zu erweitern.

Zur Beschaffung von Basisplatine und Lizenzen ist der Hinweis im Abschnitt „Besonderheiten bei der Beschaffung der Basisplatine und Lizenzen“ zu beachten.

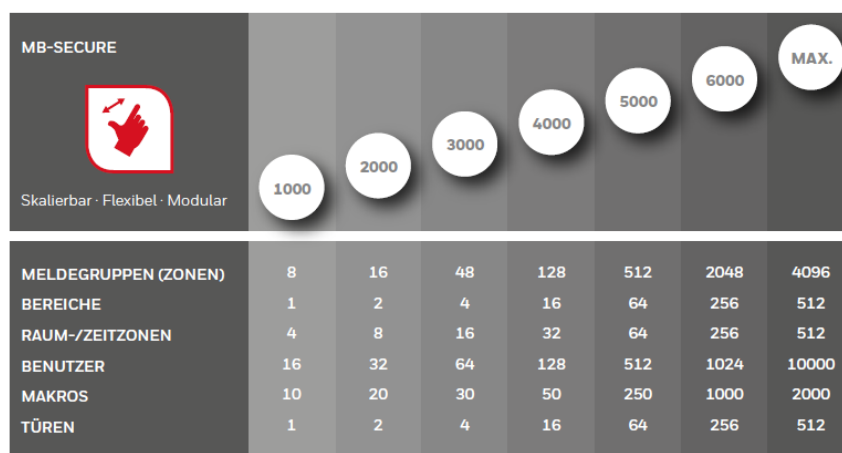


Abbildung Erweiterungsmöglichkeiten für die MB-Secure

Gehäuse sind in verschiedenen Größen vorhanden. Jedes bietet Platz für die Rechnerplatine und ein Netzteil. Unterschiede gibt es in der Einbaumöglichkeit von Erweiterungsmodulen wie etwa Bus-Erweiterungen, I/O-Erweiterungen oder Relaismodule.



Abbildung Gehäuse Beispiel einer MB-Secure Pro

Die Rechnerplatine hat eine Versorgungsspannung von 12 V DC. Um die MB-Secure Pro in die Spannungsversorgung des Hausnetzes zu integrieren, wird ein Netz- / Lade-teil benötigt. Dieses hat zwei Funktionen, zum einen die Spannungsversorgung der MB-Secure Pro und zum anderen die Ladung der Akkumulatoren für die Notstromversorgung bei Spannungsausfall. Das Netzteil muss an die Größe der zu versorgenden Akkumulatoren angepasst werden. Des Weiteren muss der Spannungswandler so ausgelegt werden, dass er die benötigte Leistungsaufnahme der MB-Secure Pro abdecken kann. Diese kann je nach nachgeschalteter Peripherie (z. B. Motorschlösser) unterschiedlich sein.

Eine Notstromversorgung muss für 30 Stunden gewährleistet sein, die Akkumulatoren sind dementsprechend auszulegen.

1.2.1 Anbindung an das städtische Datennetz

Die Zentralen sind über das städtische Datennetzwerk mittels Datenkabel angeschlossen und im ständigen Austausch mit der zentralen, durch die Stadt Nürnberg betriebenen Datenbank- und Serverinfrastruktur. Änderungen der Benutzerkonfiguration können somit direkt auf dem aktuellen Stand gehalten werden. Diese Konfiguration bleibt in den Zentralen lokal gespeichert. Das hat den Vorteil, dass wenn die Verbindung zum Server kurzzeitig unterbrochen ist, die Zugangsberechtigungen aller an dem vom Ausfall betroffenen Zentralen erhalten bleiben und diese die Zutrittssteuerung im "Offlinebetrieb" mit den zuletzt gespeicherten Berechtigungen aufrechterhalten können.

1.2.2 Installation Hinweise

Die Gehäusegrößen für die MB-Secure Pro ist bei Anlagen mit wenigen Modulen bei 500 x 300 x 210 mm bei mehreren bei 580 x 640 x 300 mm und wird an der Wand montiert. Der Montageort sollte sich in einem Bereich im Gebäude befinden der nicht für jedermann zugänglich ist, wie etwa in Elektrounterverteileräumen oder EDV-Verteileräumen.

Am Installationsort der MB-Secure Pro ist eine Doppeldatendose und ein Stromanschluss (Verteilerdose; 230 V; 10 A) vorzusehen. Der Stromanschluss ist in der (Unter-) Verteilung separat abzusichern.



1.2.3 Besonderheit bei der Beschaffung der Basisplatine und Lizenzen

Die Auslieferung von Erweiterungslizenzen erfolgt über das Lizenzierungsportal mb-secure.honeywell.com. Dort werden die erworbenen Lizenzen den jeweiligen Rechnerplatinen anhand ihrer Seriennummern zugeordnet. Auf dieser Grundlage wird ein Lizenzschlüssel erzeugt, der heruntergeladen oder per E-Mail versandt werden kann. Die Übergabe der erworbenen Lizenzschlüssel an die Stadt Nürnberg erfolgt an die Abteilung H/E, Sachgebiet H/E-Servicebetrieb, nach Abstimmung und gemäß dem vorgesehenen Lizenzierungsprozess.

1.3 Türperipherie

Als Türperipherie werden Türdrücker, -beschläge und -zylinder bezeichnet, die an der Tür angebracht werden und den Schließ- bzw. Öffnungsvorgang abwickeln. Sie kann unterschieden werden in kabelgebundene und drahtlose Peripherie, sowie in ein Online- oder Offline-System.

1.3.1 Grundlegende Türbeschreibung

Die nachfolgenden Bezeichnungen und Empfehlungen dienen während der Planungsphase als Orientierung für Fachplaner*innen und Architekt*innen. Sie sollen dazu beitragen, die Planung der Zugangskontrolle zu vereinheitlichen und die jeweiligen Anforderungen eindeutig zu definieren. Die Bezeichnungen können direkt in den Plänen an den zugehörigen Türen, beispielsweise in Form von A1, vermerkt werden. Dadurch ist für alle Beteiligten unmittelbar erkennbar, welche Anforderungen an die jeweilige Tür gestellt werden. Die Bezeichnungen ersetzen keine direkte Abstimmung mit den Fachplanerinnen oder Architektinnen, sondern sollen den Planungsprozess sinnvoll unterstützen.





A0 – Allgemeine Außentür mit mechanischer Schließung (ohne Zugangskontrolle)

- Die Tür ist mit einer mechanischen Verriegelung in Abstimmung mit dem Bauherrn bzw. der Liegenschaft auszuführen.
- Der Schließplan für die verwendeten Schließzylinder wird von der jeweils verantwortlichen Liegenschaft festgelegt und dokumentiert.
- Die Schließzylinder und Komponenten sind so auszuwählen und einzubauen, dass sie den Vorgaben der Liegenschaft entsprechen und eine sichere sowie nutzerfreundliche Bedienung gewährleistet ist.
- **Hinweis:** Diese Türen sind nicht Teil der elektronischen Zutrittskontrolle und werden beispielsweise für Technikräume benötigt, die von außen zugänglich sind, aber keinen Zugang zum Gebäudeinneren ermöglichen.

A1 – Allgemeine Außentür mit Zugangskontrolle

- Die Außentür ist mit einem elektromechanischen Sicherheitsschloss auszustatten, welches mit einer Betriebsspannung und Steuerspannung von 12 V Gleichspannung und einer Einschaltdauer von 100% zu betreiben ist.
- Der gesamte Strombedarf der Türperipherie ist im Rahmen der Elektroplanung aufzuführen und zu bemessen. Die Spannungsversorgung hat ausschließlich aus dem Zugangskontrollsystem zu erfolgen.
- Zur Zutrittskontrolle sind kabelgebundene Leser- und Auswerteeinheiten einzubauen.
- Die elektronischen Sicherheitsschlösser müssen gewährleisten, dass die Tür im Gefahrenfall jederzeit von innen leicht geöffnet werden kann und die Fluchtwegsicherheit sowie Panikfunktion entsprechend den anerkannten sicherheitstechnischen Anforderungen erfüllt wird.
- An den Türen sind keine Bohrungen für Profilzylinder im Türblatt vorzusehen.
- Alle Zutrittskontrollvarianten (A1 bis A6) sind grundsätzlich an das zentrale Online-Zugangskontrollsystem anzubinden. Ausnahmen hiervon sind nur dann zulässig, wenn sie in der jeweiligen Variante explizit und eindeutig beschrieben werden. Variante A1 bildet die verbindliche Grundlage für die Anbindung aller Türperipherien an das zentrale online System. Dadurch ist sichergestellt, dass sämtliche Türen im Regelfall zentral überwacht, gesteuert und protokolliert werden.
- Die eingesetzten Systeme sind gemäß den Allgemeinen Richtlinien der Stadt Nürnberg für elektrotechnische Anlagen auszuwählen und zu installieren.
- Beispiele für diese Türen sind insbesondere Treppenhaustüren und Nebentüren.

A2 – Außentür mit Zugangskontrolle und Feuerwehrschießzylinder

- Soweit nachstehend nicht anders beschrieben, gelten die Anforderungen aus Version A1 sinngemäß als Grundlage für diese Spezifikation.
- Zusätzlich ist ein mechanischer Schließzylinder einzubauen, der gemäß dem für die Liegenschaft gültigen Schließplan festgelegt wird. Die zugehörigen Schlüssel sind im Feuerwehr-Schlüsseldepot (FSD) zu hinterlegen, um den zerstörungsfreien Zugang für die Einsatzkräfte jederzeit sicherzustellen. Die Anzahl der Schlüssel für diese Tür ist in der Regel auf fünf Stück zu begrenzen: zwei Schlüssel im FSD, ein Schlüssel im Tresor der jeweiligen Liegenschaft, ein Schlüssel im Tresor des Nutzers (z. B. Nutzerleitung) sowie ein Schlüssel bei der beauftragten Wach- und Schließgesellschaft.
- Es ist sicherzustellen, dass zwei zusätzliche Datenträger (z. B. Multifunktionskarten oder Token) mit den entsprechenden Zugriffsrechten für die Feuerwehr im Feuerwehr-Schlüsseldepot hinterlegt werden, um den Zugang über die elektronische Zutrittskontrolle im Einsatzfall jederzeit zu ermöglichen.

A3 – Außentür mit Zeitsteuerung, numerischer Leser optional

- Soweit nachstehend nicht anders beschrieben, gelten die Anforderungen aus Version A1 sinngemäß als Grundlage für diese Spezifikation.
- Die Außentür für den Publikumsverkehr (z. B. Haupteingang, Zugang zum Pausenhof) wird zur Gewährleistung des öffentlichen Gebäudezutritts über eine Zeitzonenschaltung betrieben. Innerhalb der von der Liegenschaft definierten Zeitfenster (z. B. Publikumszeiten, Pausenzeiten) kann die Tür ohne elektronische Berechtigung manuell geöffnet werden.
- Sollen berechtigte Personen außerhalb dieser Zeitfenster das Gebäude über diese Tür betreten können, sind zusätzliche kabelgebundene Kartenleser mit numerischer Tastatur vorzusehen.
- Die Ansteuerung des elektronischen Sicherheitsschlosses erfolgt durch die Zutrittskontrollanlage. Das System ist so auszulegen, dass der Betrieb des elektronischen Sicherheitsschlosses unabhängig von der Installation eines elektronischen Lesers sichergestellt ist.

A4 – Außentür Barrierefrei mit drei Zutrittsmöglichkeiten

- Soweit nachstehend nicht anders beschrieben, gelten die Anforderungen aus Version A1 sinngemäß als Grundlage für diese Spezifikation.
- Die barrierefreie Außentür ist mit drei unterschiedlichen Zutrittsmöglichkeiten auszustatten.
 - Die erste Zutrittsmöglichkeit ist für den regulären Gebrauch berechtigter Personen vorgesehen. Diese öffnen die Tür manuell, nachdem das Schloss über einen Datenträger an der Leseinheit freigegeben wurde (wie Grundfunktion A1).
 - Die zweite Zutrittsmöglichkeit richtet sich an Personen mit Mobilitätseinschränkungen, insbesondere Rollstuhlfahrer. Diese erhalten über einen speziell mit einem Makro programmierten Datenträger die Freigabe des Türschlosses und Antrieb durch die Zutrittskontrolle. Daraufhin öffnet die Tür automatisch im Automatikbetrieb. Die Leseinheit ist außerhalb des Schwenkbereichs der Tür zu installieren und in barrierefreier Höhe anzubringen, um eine uneingeschränkte Zugänglichkeit und Bedienbarkeit sicherzustellen.
 - Die dritte Zugangsmöglichkeit dient Personen ohne Datenträger oder Token. Über eine barrierefreie Sprechanlage haben diese die Möglichkeit, das Personal zur Türfreigabe zu kontaktieren. Die Tür öffnet anschließend ebenfalls automatisch.
- Die barrierefreien Zugänge sind unter Wahrung der elektrotechnischen und sicherheitstechnischen Vorschriften zu realisieren.
- Die nötigen Anpassungen der Steuerung, der Tür und der Schließung, insbesondere für die Umsetzung der unterschiedlichen Zugriffsmöglichkeiten und der automatischen Türöffnung, sind vorzusehen und im Vorfeld durch die jeweils beteiligten Fachfirmen und Planer vor Ort abzustimmen.

A5 – Außentür mit Fluchtwegsteuerung und Zutrittskontrolle

- Soweit nachstehend nicht anders beschrieben, gelten die Anforderungen aus Version A1 sinngemäß als Grundlage für diese Spezifikation.
- Die elektrische Verriegelung ist so auszuführen, dass im Gefahrenfall (z. B. Betätigung des Fluchtwegdrückers oder Notöffnungselements) die Tür unverzüglich freigegeben wird und gleichzeitig eine akustische Alarmierung erfolgt.
- Der Regelbetrieb der Tür und die entsprechenden Freigabezeiten werden von der jeweils verantwortlichen Liegenschaft festgelegt und über die Zutrittskontrollanlage gesteuert.
- Zusätzlich ist im Innenbereich ein Kartenleser (Innenleser) vorzusehen, über den die berechtigten Personen die Tür regulär entriegeln können, ohne einen Alarm auszulösen.



A6 – Außentür mit Fluchtwegsteuerung, Zutrittskontrollintegration und Innentaster

(z.B. Kindertagesstätte)

Hinweis:

Der Nutzer bestätigt damit, wissentlich in das Fluchtwegkonzept einzugreifen und übernimmt die Verantwortung für diese Entscheidung. Die technische und rechtliche Abstimmung (z. B. mit Brandschutzplaner, Elektroplaner oder Bauaufsicht) kann durch die Fachplaner erfolgen. Eine schriftliche Bestätigung des Nutzers ist erforderlich, um die Umsetzung freizugeben.

Die genannten Lösungsvorschläge dienen ausschließlich zur Orientierung und erheben keinen Anspruch auf Vollständigkeit oder allgemeine Gültigkeit. Jede Umsetzung muss individuell mit allen Beteiligten abgestimmt werden, da die Anforderungen je nach Projekt, Gebäude und lokalen Vorgaben variieren können.

- Es gelten die Grundvoraussetzungen aus Version A2 und Version A3, inklusive numerischem Leser.
- Die Zutrittskontrollanlage steuert die elektrische Verriegelung. Ist eine Fluchtwegsicherung erforderlich, so ist diese so auszuführen, dass die Tür im Gefahrenfall über die Fluchtwegsteuerung unverzüglich und unabhängig von der Zutrittskontrollanlage freigegeben wird und gleichzeitig eine akustische Alarmierung erfolgt. Die Freigabe ist in kindgerechter Höhe anzuordnen, sodass sie auch von Kindern betätigt werden kann.
- Der Regelbetrieb der Tür sowie die entsprechenden Freigabezeiten werden von der jeweils verantwortlichen Liegenschaft festgelegt und können über die Zutrittskontrollanlage gesteuert werden.
- Ein Innentaster ist so zu montieren, dass er ein Öffnen der Tür ohne akustische Alarmierung ermöglicht (z. B. für Eltern in einer Kindertagesstätte). Die Montagehöhe ist in der Planungsphase unter Berücksichtigung der jeweiligen Nutzungseinheit festzulegen, um beispielsweise eine Bedienung durch Kinder zu verhindern und somit ein unbemerktes Verlassen des Gebäudes auszuschließen.
- Eine zusätzliche Türfreigabe ohne akustische Alarmierung kann über die Gegensprechanlage erfolgen. Der Standort der Gegensprechanlage ist in der Planungsphase eindeutig festzulegen. Die Steuerung der Türfreigabe erfolgt dabei über die Zutrittskontrollanlage.
- An der Eingangstüre sind zwei unterschiedliche Verriegelungssysteme vorzusehen. Der Fluchttüröffner für die Fluchtwegsicherung ist mit dem Errichter der Fluchttürsteuerung abzustimmen. Für die Zutrittskontrolle ist ein elektronisches Panikschloss mit 12 V Betriebsspannung und 100% Einschaltdauer vorzusehen.
- Die nötigen Anpassungen der Steuerung, der Tür und der Schließung, insbesondere für die Umsetzung der unterschiedlichen Zugriffsmöglichkeiten, sind vorzusehen und im Vorfeld durch die jeweils beteiligten Fachfirmen und Planer vor Ort abzustimmen.

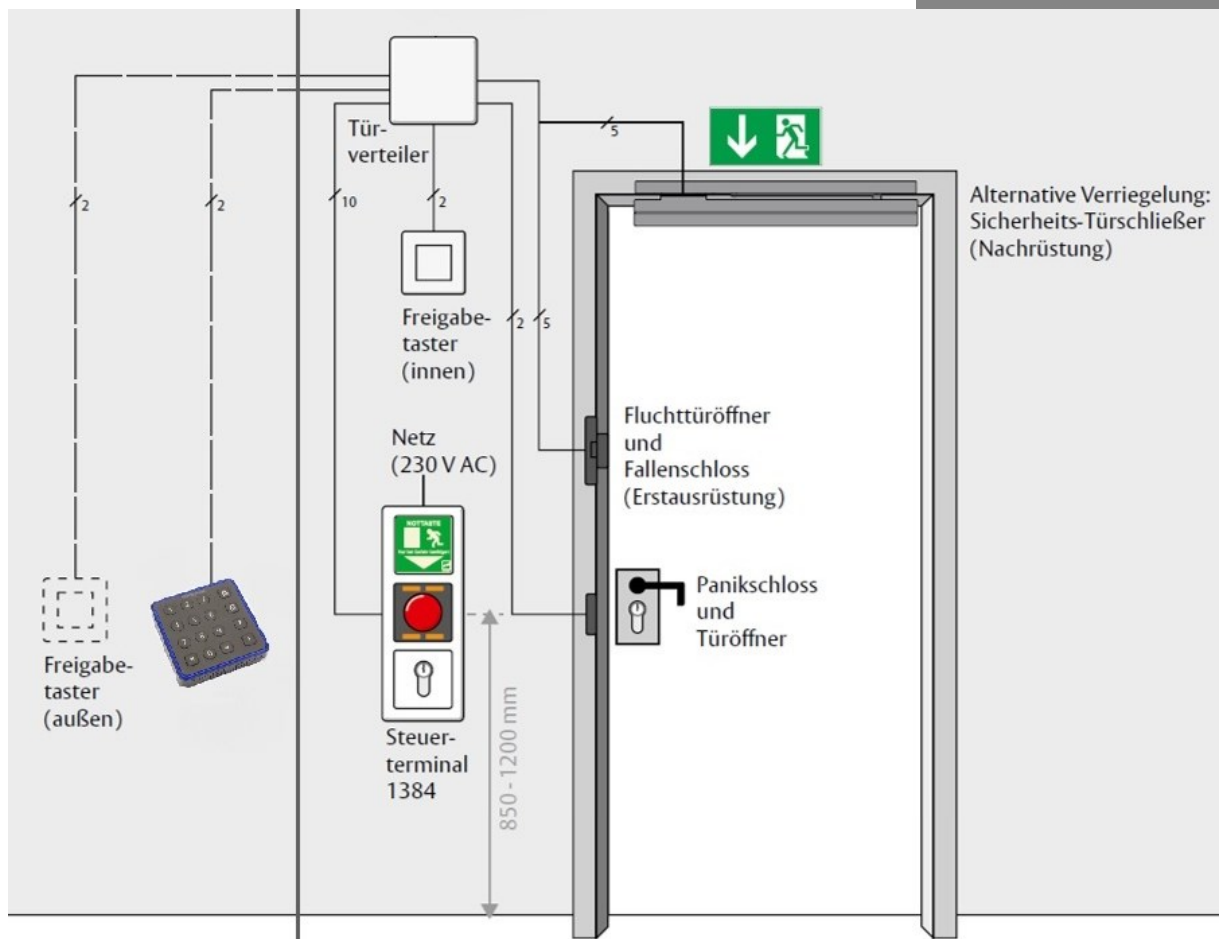


Abbildung Beispiel Zutrittsregelung und gesicherter Rettungsweg

10 – Allgemein Innentür mit mechanischen Profilzylinder (ohne Zugangskontrolle)

- Die Innentür ist mit einer herkömmlichen mechanischen Schließung auszurüsten.
- Der Schließplan und die Vergabe der Schlüssel erfolgen gemäß den Bestimmungen der zuständigen Liegenschaft.
- Die eingebauten Schließzylinder sind auf Kompatibilität mit dem Schließplan zu prüfen und entsprechend zu installieren, um eine konsistente Sicherheitsverwaltung sicherzustellen.
- **Hinweis:** Diese Türen sind nicht Teil der elektronischen Zutrittskontrolle und werden beispielsweise für Klassenzimmer oder Fachunterrichtsräume in Abstimmung mit dem Bauherrn bzw. der Liegenschaft benötigt.

I1 – Innentür mit batteriebetriebener Zutrittskontrolle und Bedarfsbegründung

- Dieses System ist nur an Innentüren anzuwenden, die von der jeweiligen Liegenschaft als notwendig definiert wurden.
- Die Innentüren sind mit dem elektronischen, batteriebetriebenen Schließsystem Aperio der Firma ASSA ABLOY auszustatten.
- Die Installation ist so auszuführen, dass ein sicherer und zuverlässiger Betrieb gewährleistet ist und das System in das zentrale Zutrittskontrollsystem integriert wird.
- Der Aperio RS-485 Online-Hub ist als Schnittstelle zwischen dem MB-Secure Pro - System und den Aperio-Türkomponenten für I1-Innentüren zu verwenden. Er verwaltet bis zu acht Aperio-Komponenten und stellt die Datenkommunikation über den RS-485-Bus sicher. Die Einhaltung der maximal zulässigen Teilnehmerzahl, Leitungslänge und Adressierung ist entsprechend den „Allgemeinen Richtlinien für elektrotechnische Anlagen der Stadt Nürnberg“ sowie den jeweils gültigen Herstellerunterlagen sicherzustellen.

I2 – Innentür mit kabelgebundener Türschließung, Leserintegration, Fallenfreigabe und Bedarfsbegründung

- Dieses System ist nur an Innentüren einzusetzen, die von der jeweiligen Liegenschaft als erforderlich definiert wurden.
- Die Türschließung und Versorgung erfolgt kabelgebunden, um eine stabile und dauerhafte Anbindung an die Zutrittskontrollanlage sicherzustellen und einen Batteriewechsel zu vermeiden.
- Die Tür wird ausschließlich durch die Falle gehalten; eine zusätzliche Verriegelung, z. B. über einen Riegel, ist nicht vorgesehen. Die Außenseite der Tür ist mit einem Türknauf auszuführen, sodass ein Öffnen von außen nur bei geöffneter Falle möglich ist. Die Tür muss jederzeit von innen leicht zu öffnen sein (z. B. über einen Türdrücker), um den Fluchtweg sicherzustellen.

I3 – Innentür mit kabelgebundener Türschließung, Leserintegration, Riegelfreigabe und Bedarfsbegründung

- Dieses System ist nur an Innentüren einzusetzen, die von der jeweiligen Liegenschaft als erforderlich definiert wurden.
- Die Türschließung und Versorgung erfolgt kabelgebunden, um eine stabile und dauerhafte Anbindung an die Zutrittskontrollanlage sicherzustellen und einen Batteriewechsel zu vermeiden.
- Die Tür ist mit einem mechanischen, selbstverriegelnden Antipanikschloss auszustatten. Nach jedem Schließvorgang fährt der Riegel mechanisch aus und verriegelt die Tür automatisch, sodass diese versicherungstechnisch ordnungsgemäß verschlossen ist.



1.3.2 Unterschied Online- / Offline-System

Ein Online-System steht im ständigen Austausch mit dem zentralen Server und es können somit unverzüglich aktuelle Änderung von Zugangsberechtigungen beeinflusst werden. Sollte eine kurzfristige Änderung nötig sein z. B. ein neuer Mitarbeiter oder ein unbekannter Verbleib eines ID-Trägers, so kann dies in der Software unmittelbar und in Echtzeit bearbeitet werden. Die Türperipherie fragt bei jeder Aktion online die Berechtigung(en) ab und wertet diese aus. Online-Systeme bestehen in der Regel aus kabelgebundener Türperipherie oder aus Komponenten des nachfolgend beschriebenen Aperio-Systems.

Bei einem Offline-System besteht kein direkter Informationsaustausch zwischen Server und Türperipherie, die aktuellen Zugangsberechtigungen müssen immer manuell oder durch einen Informationsträger vor Ort an die Zugangskomponenten übermittelt werden. Dieser Prozess ist organisatorisch und personell sehr aufwendig und wird nicht empfohlen.

1.3.3 Empfehlung für städtische Liegenschaften

Die Sicherung der Außentüren erfolgt in der Regel über kabelgebundene Türperipherie. Für die Innentüren können sowohl kabelgebundenen wie auch kabellose Funksysteme in Form von Türbeschlägen oder Zylindern eingesetzt werden.

Bei der Zutrittssteuerung der Außenhaut ist darauf zu achten, dass die gewählte Türperipherie ein versicherungstechnisches Abschließen sicherstellt. Auch sind diese Komponenten stärkeren Witterungsbedingungen ausgesetzt als Türen im Innenbereich. Dies hat zur Folge, dass an die Peripherie spezielle Anforderung an Robustheit und Zuverlässigkeit gestellt werden. Batteriebetriebene Systeme sind weniger für den Einsatz im Außenbereich geeignet, da eine geringere Nutzungsdauer aufgrund der niedrigen winterlichen Temperaturen zu erwarten ist. Außentüren sind bevorzugt kabelgebunden auszuführen. Drahtlose Systeme können in begründeten Ausnahmefällen eingesetzt werden.

Für die Zutrittssteuerung in Innenräumen kann ein Online-System, kabelgebunden oder drahtlos, installiert werden. Eine wirtschaftliche Abwägung zum Einsatz eines kabelgebundenen Systems, welches zunächst höhere Installationskosten erzeugt, und einem drahtlosen System mit nachfolgenden laufenden Kosten für ständigen Batteriewechsel, ist aufzustellen.

1.3.4 Kabelgebundene Türperipherie

Die Türperipherie ist kabelgebunden, wenn die Stromversorgung und Kommunikation mit der MB Secure Pro über eine feste Leitungsführung erfolgt. Somit entfällt das Tauschen der Versorgungsbatterie, wie es bei drahtlosen Systemen laufend notwendig ist. Der Vorteil bei einer kabelgebundenen Türperipherie ist der geringere Organisations- und Wartungsaufwand. Im Außenbereich ist diese Einsatzart zu bevorzugen, da diese Peripherie ein versicherungstechnisches Abschließen der Außenhaut gewährleisten kann.

1.3.5 Kabellose Türperipherie

Zur Sicherung von Innenräumen in Gebäuden sind standardmäßig batteriebetriebene Online-Funkzylindern oder Funkbeschläge ist eine MB-Secure Pro von Honeywell einzusetzen. Die Türen können entweder mit einem kabelgeführten System ausgelegt werden oder mit dem drahtlosen online Türsystem Aperio von ASSA Abloy.

1.3.6 Drahtloses Türsystem Aperio

In bestehenden Gebäuden kann wegen der einfacheren Nachrüstbarkeit ein drahtloses Schließsystem mit Beschlägen und Zylindern installiert werden. Das drahtlose online Türsystem Aperio von ASSA Abloy ist innerhalb der bereits eingesetzten Honeywell IQ-Multi Access-Software integriert und bietet sich dafür an. Nachfolgend werden die einzelnen Komponenten des Türsystems vorgestellt.

1.3.6.1 Aperio RS-485 HUB

Die Übertragung der Daten von der MB-Secure Pro zu den Türen erfolgt mittels eines Aperio RS-485 HUB. Dieser bekommt die Daten über den Modul-Bus / RS-485 von der MB-Secure Pro. Je HUB können 8 Türkomponenten angesprochen werden. Seine Reichweite beträgt 15 m bis 25 m, je nach baulichen Gegebenheiten (hier ist eine individuelle Planung notwendig). Seine Schutzart ist die IP 20 und seine Betriebstemperatur ist zwischen 5°C und 35°C, was für einen Einsatz innerhalb von Gebäuden spricht. Der HUB steht im Austausch mit der MB-Secure Pro in der alle Zugangsberechtigungen für die Lokation zwischengespeichert sind.



Abbildung Aperio RS-485 HUB



1.3.6.2 Zylinder

Die Aperio Schließzylinder kommunizieren verschlüsselt mit dem HUB, der wiederum die Zutrittsanfrage an die MB-Secure Pro übermittelt. Darüber hinaus können im Zylinder dauerhaft 10 Ausweise (ID-Karten) gespeichert werden. Das hat den Vorteil, dass bei einem Ausfall der gesamten Anlage mit diesen ID-Karten immer noch ein Zugang gewährleistet werden kann z. B. für die Feuerwehr oder Berechtigte als „Generalschlüssel“.

Diese „Generalschlüssel“-ID-Karten werden mittels der PAP-Tool-Software vor Ort und für jeden Zylinder einzeln konfiguriert. Bei einem Verlust eines solchen Trägers müssen an allen Zylindern die Notberechtigungen aktualisiert werden. Bei diesen Trägern sollte es sich um räumlich gesicherte Notfalloptionen handeln und nicht um ID-Träger für die tägliche Zugangssteuerung.

Die Zylinder werden über eine Lithium CR2 Batterie versorgt, die bei etwa 10 Öffnungen pro Tag für 27 Monate ausreicht. Werden mehr Öffnungen pro Tag durchgeführt, verringert sich entsprechend die Versorgungszeit. Mit der Schutzart IP 65 und dem Betriebstemperaturbereich zwischen -20°C bis zu 55°C ist der Schließmechanismus auch für Außenbereiche geeignet. Der Einsatz sollte aber nur, wenn nötig, im Außenbereich erfolgen, da durch die niedrigen Temperaturen die Batterien eine deutlich geringere Haltbarkeit aufweisen. Im Außenbereich bzw. zur Sicherung der Außenhaut sollte das System in Kapitel A0 verwendet werden.



Abbildung Aperio Standard- und Halbzylinder

Die Zylinder werden einmal in der Variante Standardzylinder AP-0010 und Halbzylinder AP-0020 ausgeliefert. Die Standardvariante hat außen eine Leseelektronik und innen einen mechanischen Knauf ohne Lesefunktion. Wenn nötig können auch zwei Knaufe mit Lesefunktion angebracht werden. Die richtigen Abmaße sind für jede Tür individuell zu bestimmen. Diese können von 30 mm bis 60 mm in 5 mm-Schritten gewählt werden. Um eine mechanische Abnutzung des Beschlags zu vermeiden, ist bei Zwischenmaßen auf das nächstgrößere aufzurunden.

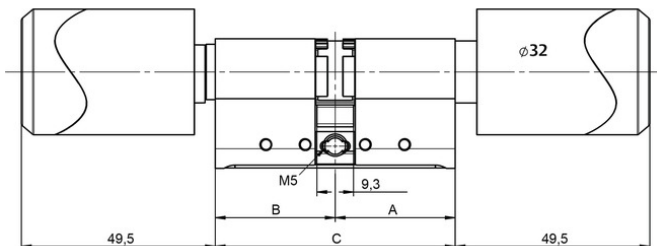


Abbildung Abmaße des Standardzylinders in mm

1.3.6.3 Türbeschläge

Die Aperio Türbeschläge kommunizieren verschlüsselt über den HUB, der wiederum die Zutrittsanfragen an die MB-Secure Pro übermittelt. Darüber hinaus können auch hier im Beschlag dauerhaft 10 Ausweise (ID-Karten) gespeichert werden, um bei einem Ausfall der Kommunikation zur zentralen Servereinheit den Zugang zu gewähren.

1.3.6.4 Basisbeschlag

Die Beschläge werden über eine Lithium CR123A Batterie versorgt, die etwa für 40 000 Öffnungszyklen oder maximal 3 Jahre ausreicht. Mit der Schutzart IP 52 und Betriebstemperaturen zwischen 0°C bis zu 60°C ist der Schließmechanismus für den Innenbereich geeignet.

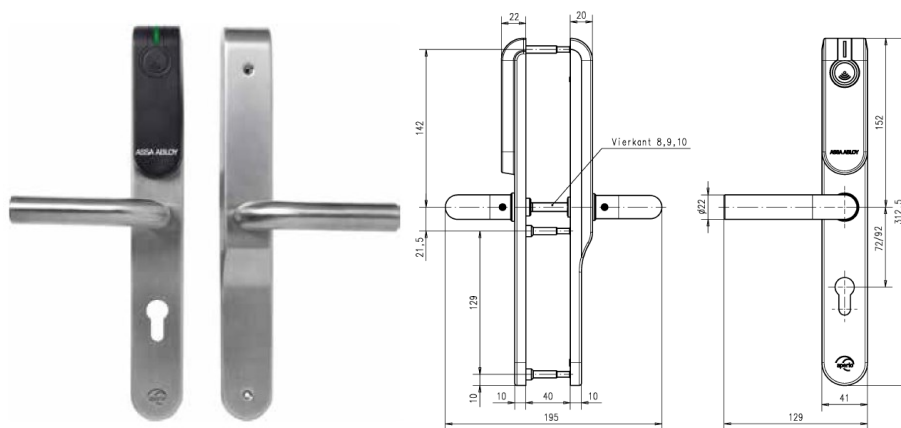


Abbildung Aperio Standardbeschlag

Der Standardbeschlag ist auf einer Seite mit einer Leseinheit ausgerüstet und die andere mit einem mechanischen Drücker. Er ist für eine Türstärke für 40 mm bis 100 mm ausgelegt. Optional kann eine PIN-Tastatur auf dem Beschlag angebracht werden.

Eine robustere und mit höheren Schutzart (IP 54) versehene Variante des Beschlags ist der Aperio Premiumbeschlag mifare. Dieser erfüllt die Auflagen der DIN EN 179 (Notausgangsschließungen mit Drücker oder Stoßplatte für Türen in Rettungswegen) und sollte dort eingebaut werden, wo mit hohem Benutzer-Aufkommen zu rechnen ist.

1.3.6.5 Türdrücker

Der Türdrücker H100 ist in der Ausführung Links und Rechts erhältlich. Er wird über eine Lithium CR123A Batterie versorgt, verfügt über die Schutzart IP 42 (0 bis 50°C) und ist somit für den Einsatz nur im Innenbereich geeignet.



Abbildung Aperio Türdrücker

1.4 Leser

Mit den Lesern werden an kabelgebundenen Türen die ID-Träger überprüft und so festgestellt, ob eine Zugangsberechtigung vorliegt. Liegt diese vor wird die Türe freigegeben. Die Leser sollten in der Nähe der zu öffnenden Türe angebracht werden.

luminAXS

Als Standardleser soll der luminAXS mifare DESFire EV2 Leser mit 16 Tasten eingesetzt werden. Bei z. B. Schrankenanlagen zur Zufahrtsregelung kann auch der der luminAXS Leser mit 2 Tasten oder keiner Tastatur eingesetzt werden.

Über die Tasten ist es möglich programmierte Makros abzurufen oder eine PIN abzufragen.



Abbildung Leser luminAXS mit 16 Tasten

1.5 ID-Träger

Die ID-Träger dienen der Identifikation der Person, die eine Zutritts- oder Schließberechtigung anfragt. Jeder ID-Träger ist gewöhnlich auf eine Person personalisiert. Es kann sich um eine Multifunktionskarte oder um einen Token handeln. Der Standard für die städtischen Mitarbeiter ist die Multifunktionskarte.

Es sind ID-Träger und Leser mit Unterstützung von MIFARE DESFire EV3 einzusetzen. Bestehende EV1-/EV2-Systeme dürfen aus Gründen der Abwärtskompatibilität weiterbetrieben werden, sind jedoch nicht mehr für Neuausgaben oder Erweiterungen vorzusehen

1.5.1 Multifunktionskarten

Die meisten städtischen Mitarbeiter besitzen eine Multifunktionskarte mit der sie unter Anderem ihre Berechtigung für das Drucken, Kopieren oder ihre elektronische Zeiterfassung nachweisen können. Ist eine solche Karte vorhanden, ist diese standardmäßig für die Zutrittssteuerung zu verwenden. Gibt es spezielle Anforderungen an Robustheit oder ähnliches wie dies z. B. im Feuerwehrdienst ist, ist ein Token zu verwenden.

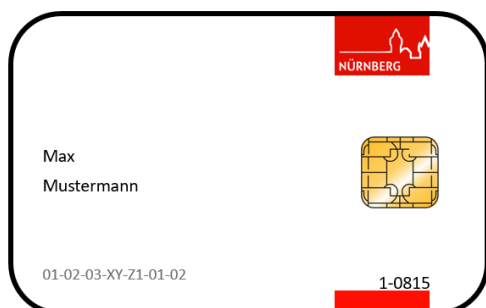


Abbildung Multifunktionskarte für städtische Mitarbeiter

1.5.2 Token

Token sind immer dann einzusetzen, wenn ein städtischer Mitarbeiter mit Multifunktionskarte besondere Anforderungen an den ID-Träger hat. Dies kann z. B. eine besondere Robustheit oder einfachere Handhabung sein.

Es könnte z. B. bei städtischen Mitarbeitern im Feuerwehrdienst notwendig sein, da diese die ID-Träger z.B. mit Handschuhen handhaben müssen.

Ein weiterer Beschaffungsgrund für Token, können externe Mitarbeiter sein die ebenfalls Zutritt zu den Gebäuden erhalten sollen. Dieses kann von personenbezogenem Token für z. B. Reinigungskräften oder nicht Personen zugeordneten Token, z. B. eingeschränkte temporär arbeitende Handwerker, der Fall sein.

Zu beschaffen sind nur Token mit Metallaufhänger so wie in Abbildung dargestellt, auf die Ausführung mit Plastikaufhänger ist auf Grund der Haltbarkeit zu verzichten.



Abbildung Token

1.5.2.1 Kombi-Token für MIFARE DESFire und proX

Soll die Kompatibilität zu einer Bestands- / Altanlagen möglich sein bei denen noch proX-Lesertechnik eingesetzt wird, so sind Token zu verwenden die beide Technologien unterstützen. Dies ist mit dem MIFARE DESFire / EM4200 Kombi-Schlüsselanhänger möglich.

1.6 Zentrale Verwaltungssoftware zur Zutrittssteuerung

Die Verwaltungssoftware zur Zutrittssteuerungen bei der Stadt Nürnberg ist die IQ-MultiAccess von Honeywell. Diese ermöglicht eine zentrale und dezentrale Verwaltung aller Funktionen wie Benutzergruppen und Zugangsberechtigungen, sowie weitere Sonderfunktionen des Systems. Auch bietet die Software die Möglichkeit, die Schließsysteme der Fabrikate Honeywell und ASSA Abloy gemeinsam in einem User-Interface zu managen. Die beiden Fabrikate decken die Zutrittssteuerung bei der Außenhaut und im Innenraum ab. Mit der IQ-MultiAccess ist deshalb eine zentrale Verwaltung der gesamten angebundenen Gebäude auf einer Benutzeroberfläche möglich.

1.6.1 Benutzerverwaltung

Eine zentrale Benutzerverwaltung wird innerhalb der Stadt Nürnberg betrieben und auf stadteigenen Servern zentral gesichert. Die Abteilung H/E-S verwaltet diese Server als Superuser und legt zentral neue Benutzer an. Aus diesem Grund müssen auch alle neuen Datenträger vor Ausgabe an den / die Nutzer von einem Superuser angelegt werden. Diese Datenträger werden im Zutrittskontrollsystem global registriert und können von den entsprechenden Lokationsmanagern mit Zutrittsrechten versehen werden.

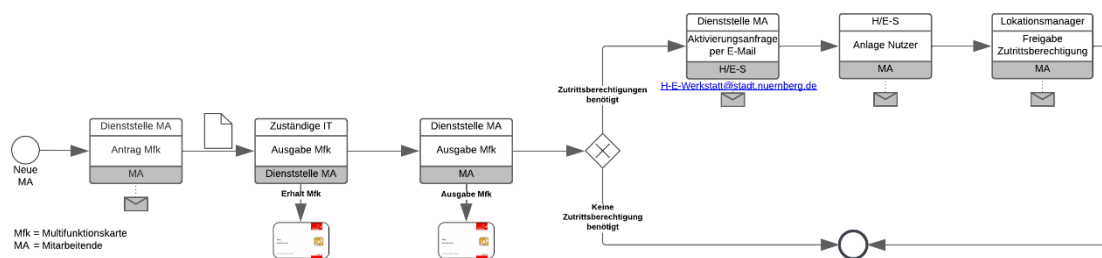


Abbildung Multifunktionskarte mit Zutrittssteuerungsfunktion für neue Mitarbeitende

Das Auslesen bzw. die Einsichtnahme von persönlichen Parametern und Log-Vorgängen wie z. B. Zutrittszeiten kann aus datenrechtlichen Gründen nur gemeinsam mit Personalrat und dem jeweiligen Vorgesetzten nach dem Vier-Augen-Prinzip erfolgen.

1.6.1.1 Datenschutz

Die Verarbeitung personenbezogener Zutrittsdaten hat gemäß DSGVO und den gültigen Datenschutzrichtlinien der Stadt Nürnberg zu erfolgen.

Protokollierungen sind auf das notwendige Maß zu beschränken und regelmäßigen Löschfristen zu unterwerfen.

1.6.2 Lokationen

Bei einer Lokation handelt es sich um eine separate Verwaltungseinheit. Eine Lokation kann z.B. ein Gebäudekomplex, ein Gebäude oder mehrere separate Einheiten (z. B. Ämter) innerhalb eines Gebäudes sein.

Jede Lokation wird einzeln durch einen Lokationsmanager verwaltet, der die Berechtigungen, Raum- / Zeitzonen und Makros innerhalb der Lokation zuweisen oder verändern kann. Der Lokationsmanager hat nur eine Zugriffsberechtigung auf die Daten seiner Lokation, nicht auf andere.

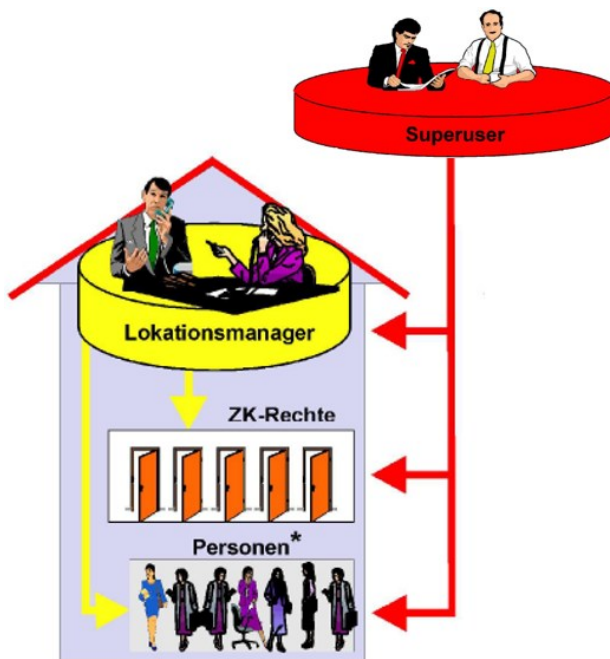


Abbildung Zusammenhang Superuser und Lokationsmanager

Jeder Lokation können softwaremäßig maximal 65 000 Ausweise, 999 Türen und 512 Raum- / Zeitzonen zugewiesen werden.

1.6.3 Raum- / Zeitzonen

Über Raum- / Zeitzonen wird definiert, an welchen Türen zu welchen Tagen und Uhrzeiten ein berechtigter Ausweis (Datenträger) eine Freigabebuchung erhalten soll. So kann separat für jeden Mitarbeiter und jede Tür ein individuelles Profil definiert werden. Die Berücksichtigung einzelner Wochentage oder Sonn- und Feiertagen ist ebenso möglich.

1.6.4 Makros

Mit Makros können Funktionen, z.B. durch Eingabe einer bestimmten Tastenkombination, an dafür vorgesehenen Lesern abgerufen werden. Diese Makros müssen individuell programmiert werden. So kann zum Beispiel bei Aktivierung, eine Türe, nach berechtigter Öffnung für eine bestimmte Zeit geöffnet bleiben.

1.6.5 Mandantenfähigkeit

Die Mandantenfähigkeit beschreibt die Möglichkeit, auf einem Software-System mehrere sogenannte Mandanten, also Personen- oder Benutzergruppen, anzulegen, ohne dass diese einen gegenseitigen Einblick auf ihre Daten (z. B. Zugangs- oder Anwesenheitszeiten) haben. Es können z. B. bei Schulturnhallen für Sportvereine Berechtigungen vergeben werden, die tatsächlichen Zutrittszeiten oder Personendaten können aus datenrechtlichen Gründen aber nicht eingesehen werden.

Jeder Mandant kann beliebig vielen Lokationen zugeordnet werden. Das bietet den Vorteil einer zentralen Verwaltung und einen geringeren Speicherbedarf für die Daten, da mandantenübergreifende Daten und Objekte nur einmal im städtischen Zutrittssystem und nicht einmal pro Mandanten und Lokation gespeichert werden müssen. Nur eine Benutzerlizenz muss pro Mandanten vorgehalten werden, was wiederum die Lizenzkosten senkt.

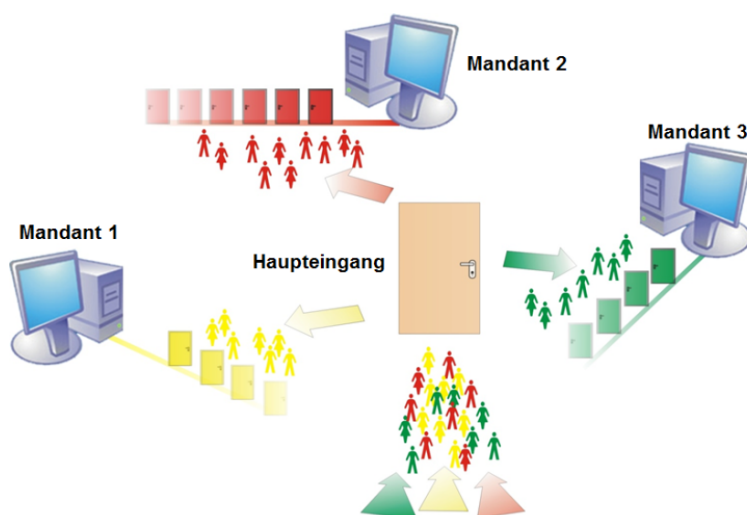


Abbildung Beispielhafte Mandantenfunktion

Ein Mandant kann auch über eigene gesteuerte Türen verfügen. Dies kann dann der Fall sein, wenn in einem städtischen Gebäude mehrere Dienststellen untergebracht sind. Über die Mandantenfunktion können mehrere Mandanten z. B. gesteuerte Türen einer MB-Secure/AXS4-Secure benutzen. Mandant A könnte die Türen 1 bis 3 und Mandant B die Türen 4 bis 8 verwalten, obwohl alle 8 Türen über selbe MB-Secure Pro gesteuert werden.



1.7 Grundlegende Bestandteile der Zutrittssteuerung

Für jede Zutrittsanlage ist ein Wartung- und Lebenszykluskonzept vorzusehen. Dieses umfasst regelmäßige Funktionsprüfungen, Batteriewechsel, Software-Updates, Ersatzteilstrategien sowie die Bewertung des Produktlebenszyklus.

1.7.1 Spannungsversorgung der Komponenten

Geräte-Komponenten, welche für eine Netzspannung von 230 V ausgelegt sind, werden über die allgemeine Stromversorgung der Liegenschaft gespeist. Es ist dafür mindestens ein Leitungstyp NYM 3 x 1,5 mm² zu verwenden.

1.7.2 Modul-Bus RS-485

Um die Hardware des Zugangskontrollsystems miteinander zu verbinden und einen Datenaustausch zu ermöglichen wird ein Modul-Bus mit der RS-485-Schnittstelle verwendet.

Der Modul-Bus wird über eine Bus-Topologie aufgebaut, eine sternenförmige Verkabelung ist unzulässig. Als Verbindung dient eine busfähige, bidirektionale Schnittstelle. Es lassen sich bis zu 32 Teilnehmer verbinden, die sowohl Sender als auch Empfänger sein können.

Bei dem RS-485 Bussystem handelt es sich um eine 5-Draht Schnittstelle. Zum Anschluss sollte mindestens ein Leitungstyp J-Y(St)Y 4 x 2 x 0,6 mm² verwendet werden.

Abhängig von dem eingesetzten Controller, können auch IP-basierte Modul- und Türanbindungen zum Einsatz kommen. Die jeweilige Systemarchitektur ist projektbezogen festzulegen.

Kontakt zu Fragen, Prozessen und Störungen:

H-E-Werkstatt@stadt.nuernberg.de

oder

H/E@stadt.nuernberg.de