SHBP



BAULICHE STANDARDS STADT LÜDENSCHEID

Bau-, Qualitäts- und Ausstattungsstandards (BQA)

Stand Oktober 2026 Index 0_ Entwurf

ENTWURF

HEFT 09_
SCHLIEßANLAGEN I ZUTRITTSKONTROLLEN

Allgemeine bauliche Standards für Neu-, Um- und Erweiterungsbauten sowie Generalsanierungen

SHBP

Inhalt

Inhaltsverzeichnis

1.9 Schließanlagen I Zutrittskontrollen 3
1.9.1 Grundlagen 3
Allgemeine Standards 3
Zielsetzung 3
Wirtschaftlichkeit 3
Vorschriften 4
Brandschutz Grundsätze 5
Definition und Wirkungsweise der Schließanlagenarten 5
Systembeschreibung – Digitale Schließanlage 6
Grundsätzlicher Systemaufbau 6
Systembeschreibung Zutrittssoftware 7
Ausweismanagement 8
DSGVO- konform 8
Erweiterbarkeit der Zutrittskontrolle 9
1.9.2.2 Schnittstellenvielfalt 9
Systembeschreibung der Zugangsberechtigungen 10
Geforderte Öffnungs- und Betriebsfunktionen 13
1.9.3.1 Systematik Bezeichnung 15
Schließmedien 16
1.9.4.1 Technische Beschreibung der Komponenten 17
Digitale Schließzylinder 17
Standard Digitalzylinder 17
Digitale Beschlag-Leser 18
Beschreibung digitale Türbeschläge 18
Beschlag-Leser kompakt /Rosettenmontage 18
Wandleser 19
Kompaktleser 19
1.9.5.1 Online-Peripherie für Direktvernetzung 20

ENTWURF

Aufbau der (Online-) Steuerung 20
Zutrittsmanager Hutschiene ((teil-)zentrale Steuerung) 20
Zutrittsmanager (dezentrale Steuerung) 23
Fluchttürterminals 24

Hinweis Anlagen:
alle genannten Anlagen besitzen nicht den Anspruch auf Vollständigkeit.

Hinweis Allgemein: Die Baulichen Standards sind verpflichtend für Neu- und Erweiterungsbauten sowie Generalsanierungen anzuwenden – für alle übrigen Projekte (z.B. Umbauten im Bestand im Rahmen der Bauunterhaltung) dienen die Baulichen Standards als Leitbild und können zur technischen Orientierung herangezogen werden.

Diese BQAs wurden in Anlehnung an die baulichen Standards der Stadt Mainz erstellt.

ENTWURF

1.9 Schließanlagen I Zutrittskontrollen

1.9.1 Grundlagen

Allgemeine Standards

Zielsetzung

Bei der Planung für den Bereich der Schließanlage und Zutrittskontrolle finden dieselben Grundsätze wie für den Bereich Hochbau Anwendung. Alle aufgeführten Anforderungen unter dem Punkt 1.1.1 (Bauliche Standards - Heft 01_Hochbau) sind als allgemeine Zielsetzung zu verstehen und sind entsprechend umzusetzen. Die Hauptaufgabe der Schließtechnik und Zutrittskontrolle ist die Regelung, Steuerung und Kontrolle der betrieblichen Nutzung von Gebäuden und Anlagen zum Zwecke der optimalen Betriebsführung und die sich daraus ergebene Sicherstellung des effizienten Gebäudenutzung. Es ist darauf zu achten, dass die erforderlichen Teilleistungen anderer Gewerke (wie z.B. Andienung von Steuerleitungen, Datenleitungen, Spannungsversorgung, Montagemöglichkeiten von Steuertechnik im Bereich von z.B. Unterverteilungen und Abhangdecken, …) frühzeitig im Planungsprozess zu ermitteln und festzuschreiben sind. Dies ermöglicht eine frühe Planungssicherheit bzgl. der Bedarfe der Schließmedien und Zutrittskontrollen an andere Gewerke und führt so zu einer höheren Kostensicherheit. Ziel ist die Schaffung einer maximalen Gebrauchstauglichkeit bei der Bedienung und Benutzung. Darüber hinaus ist ein Aufwand für die Reinigung, Wartung und Instandhaltung möglichst zu minimieren.

Die Anforderungsprofile und Prioritäten der Schließanlagen und Zutrittskontrollen sind – unter Berücksichtigung der Effizient und des Nutzerbedarfe – für das jeweilige Projekt abzustimmen und umzusetzen.
Bei der Abstimmung sind die Vorgaben der Schließsysteme (Schließpläne, Andienung EDV, etc.) zu beachten.

Schließanlagen I Zutrittskontrollen – Grundlagen Allgemeine Standards - Zielsetzung	
Berücksichtigung der Bedien- und Instandhaltungsfreundlichkeit der entsprechenden Komponenten	☐
Berücksichtigung der erforderlichen Steuerleitung und Andienung EDV	☐

Wirtschaftlichkeit

Wirtschaftlichkeitsbetrachtung

Die erforderliche Wirtschaftlichkeitsbetrachtung ist interdisziplinär umzusetzen. Bereits im Rahmen der Bedarfsplanung ist die Wirtschaftlichkeit, nicht nur isoliert für die Haustechnik, sondern auch für den Bereich des Hochbaus aus fachtechnischer Sicht zu prüfen und bei Bedarf zu ergänzen. Dies gilt als Anforderungsgrundsatz bei jeder Baumaßnahme, unabhängig davon ob, es sich um eine Sanierung oder einen Neubau handelt.

Schließanlagen I Zutrittskontrollen – Grundlagen Allgemeine Standards - Wirtschaftlichkeit - Wirtschaftlichkeitsbetrachtung	
Fachtechnische Überprüfung der Wirtschaftlichkeitsbetrachtung im Bereich Hochbau	☐

Lebenszyklusberechnung

Bei Wirtschaftlichkeits- und Lebenszyklusbetrachtungen ist stets der gesamte Lebenszyklus eines Gebäudes zugrunde zu legen. Dieser umfasst alle Phasen von der Planung über die Errichtung und den Betrieb bis hin zum Rückbau und der Entsorgung. Ziel dieser Betrachtung ist die

ENTWURF

nachhaltige Reduzierung der jährlich anfallenden Gesamtkosten des Gebäudes. In Anlehnung an die Vorgaben des Hochbaus sind für die Schließkomponenten sämtliche Investitionskosten, laufenden Betriebskosten sowie Folgekosten systematisch zu erfassen und in die hochbaulichen Wirtschaftlichkeitsberechnungen zu integrieren. Die hierfür heranzuziehenden Bemessungsgrundlagen sind an die entsprechenden Festlegungen des Hochbaus anzupassen. Zur fundierten Kostenermittlung sind unter anderem Wartungs- und Erneuerungsintervalle und konsequent in allen Planungs- und Berechnungsansätzen zu berücksichtigen.

Schließanlagen I Zutrittskontrollen – Grundlagen **Allgemeine Standards – Wirtschaftlichkeit – Lebenszyklusberechnung**	
Ermittlung der Investitions-, Betriebs- und Folgekosten	☐
Abstimmung und Ergänzung der Kostenermittlung und Festlegungen im Bereich Hochbau	☐

Verfügbarkeit in der Bewirtschaftung

Für mechanische Schließanlagen wird eine Mindestverfügbar- bzw. Nachbestellbarkeit von **10 Jahren** für Zylinder und Schlüssel als Mindestanforderung vorausgesetzt.
Im Zuge der Nachhaltigkeit müssen Schließkomponenten auch in Teilsegmenten (z.B. bei Zylindern die Schließmechanik getrennt vom eigentlichen Zylinder) verfüg- und austauschbar sein.

Für die Erweiterbarkeit und die Ersatzteilversorgung der mechanischen, der mechatronischen und der elektronischen Schließanlage gilt eine Mindestverfügbar- bzw. Nachbestellbarkeit von 10 Jahren.

Schließanlagen I Zutrittskontrollen – Grundlagen **Allgemeine Standards – Wirtschaftlichkeit – Verfügbarkeit der Bewirtschaftung**	
Mindestverfügbar- bzw. Nachbestellbarkeit von **10 Jahren** für Zylinder und Schlüssel	☐
Schließkomponenten auch in Teilsegmenten verfüg- und austauschbar sein.	☐
Erweiterbarkeit und die Ersatzteilversorgung der mechanischen, der mechatronischen und der elektronischen Schließanlage gilt eine Mindestverfügbar- bzw. Nachbestellbarkeit von 10 Jahren.	☐

Vorschriften

Bei der Planung und Ausführung von Gebäuden der Stadt Lüdenscheid sind alle Gesetze, Verordnungen und bauaufsichtlich eingeführte Richtlinien unter Beachtung der Verwaltungsvorschrift technischer Baubestimmungen (VV TB) in der aktuell gültigen Fassung und die allgemein anerkannten Regeln der Technik anzuwenden. Darüber hinaus sind evtl. vorhandene weiterreichende stadtinterne Beschlüsse und Satzungen zu berücksichtigen. Die in der Anlage aufgeführten Ratsbeschlüsse sind als weitere, stadtinterne Vorgaben projektspezifisch zu prüfen und zu beachten (die Anlage besitzt nicht den Anspruch auf Vollständigkeit).

Schließanlagen I Zutrittskontrollen – Grundlagen **Allgemeine Standards –Vorschriften**	
Überprüfen der geltenden, gesetzlichen Vorschriften	☐
Berücksichtigung der aktuellen Regeln der Technik	☐
Berücksichtigung Stadtratsbeschlüsse / stadteigener Satzungen lt. Anlage	☐

Anlagen hierzu:

ENTWURF

Brandschutz Grundsätze

Ziel bei allen städtischen Baumaßnahmen ist eine wirksame, sicherheitstechnisch und rechtlich zulässige, aber dennoch wirtschaftliche Lösung zu finden, den Brandschutz zu gewährleisten und den gesetzlichen Anforderungen zu entsprechen. Die im Titel 1.1.2 (Bauliche Standards – Heft 01_Hochbau) hierzu aufgeführten Vorgaben, Richtlinien und grundlegenden Standards sind entsprechend zu beachten.

Städtische Bauprojekte gelten in der Regel als Sonderbauten gemäß Landesbauordnung NRW. Die Vorlage eines Brandschutzkonzepts ist somit erforderlich. Die Erstellung des Konzepts erfolgt nach den landesrechtlichen Vorgaben. Die Anforderungen sind frühzeitig in der Entwurfsphase zu berücksichtigen und spätestens mit Abschluss der LPH3 mindestens mit der Bauaufsicht, dem Hochbau- bzw. anderen, beteiligten Fachplanern und der Brandschutzdienststelle der Stadt Lüdenscheid abzustimmen
Neben der bereits im Kapitel Hochbau aufgeführten Klärung von Notwendigkeit und Umfang einer ggf. erforderlichen Brandmeldeanlage sind hier insbesondere die Notwendigkeit von anlagentechnischen Brandschutzmaßnahmen zu klären und gemeinsam festzulegen.

Die im Brandschutzkonzept enthaltenen Angaben – besonders die im Kontext von Schließsystemen relevanter Angaben wie z.B. Verläufe von Rettungswegen und Verortungen von Fluchttüren – sind <u>zwingend</u> zu beachten und zu berücksichtigen.

Die Wirkungsweise der Zutrittskontrollen und Schließanlagen ist <u>immer</u> dem Schutzziel unterzuordnen.

Schließanlagen I Zutrittskontrollen – Grundlagen Allgemeine Standards –Brandschutz Grundsätze	
Wurden alle Vorgaben des Brandschutzkonzeptes berücksichtigt	☐
Keine Einschränkungen des Schutzzieles durch Zutrittskontrolle und Schließanlagen	☐

1.9.2.1 Systembeschreibung

Definition und Wirkungsweise der Schließanlagenarten

Mechanische Schließanlage (Zutrittssystem, bei dem mehrere Türen über mechanische Schließzylinder organisiert und mit genau definierten Schlüsseln gesteuert werden).

Mechatronische Schließanlage (Eine mechatronische Schließanlage verbindet mechanische Schließtechnik mit digital gesteuerter Zutrittskontrolle, z.B. über Profilzylinder mit elektronischer Identifizierung).

Elektronische Schließanlage (Eine elektronische Schließanlage steuert den Zugang zu Gebäuden vollständig über digitale Signale – ganz ohne mechanische Schlüssel).

Die Art der verwendeten Schließung bzw. der Schließanlagen ist entsprechend der Anforderungen des Projektes, bei Neubauten und Generalsanierung spätestens bis zum Ende der Leistungsphase 3 festzulegen und die erforderlichen Schnittstellen zur TGA sind zu klären (dies gilt immer bei rein elektronischen Schließanlagen bzw. bei mechatronischen Anlagen, die i.T. oder als gesamte Anlage Online aufgeschaltet werden).

Gerade in weitläufigen Objekten, die eine hohe Deckung der Schließberechtigung haben (z.B. Schulen, Kitas u.ä.) oder bei einem stufenweisen Auf- bzw. Ausbau der Schließanlage ist

ENTWURF

möglichst eine Kombination aus mechanischer (ggf. Bestandsschließanlage) und mechatronischen bzw. elektronischen Schließanlage zu verwenden. In diesem Fall gilt das Schutzzielprinzip; Gebäudehülle hoch, nach innen abnehmend.

Bei Gebäuden, die durch unterschiedliche Nutzergruppen wechselseitig genutzt werden – z.B. Sporthallen mit Nutzung durch Schulen und Vereine – gilt dieselbe Anforderung wie an Schulen. Die Berechtigung der der einzelnen Nutzergruppen kann über die elektromechanische bzw. elektronische Schließung entsprechend gesteuert und genutzt werden.

Systembeschreibung – Digitale Schließanlage

Verwendeter Hersteller: **dormakaba**

Eine digitale Schließanlage ist ein elektronisches Zutrittskontrollsystem, das den Zugang zu Gebäuden und Räumen ohne herkömmliche mechanische Schlüssel ermöglicht. Stattdessen kommen elektronische Identifikationsmedien, hier RFID-Schließmedien - wie Karten, Schlüsselanhänger, Smartphones (Bluetooth/NFC, optional) oder digitale Schlüssel – zum Einsatz. Die Berechtigungen werden zentral oder dezentral verwaltet und können jederzeit (z.T. zentral) geändert oder entzogen werden.
Die Verwaltung der Schließmedien erfolgt über die zuständige Stelle der Gebäudewirtschaft der Stadt Lüdenscheid (Ausnahme bilden hier Gebäude, die in den Zuständigkeitsbereich des Nutzers – u.a. der Feuerwehr der Stadt Lüdenscheid – fallen. Hier erfolgt die Verwaltung der Anlage über den Nutzer).

Grundsätzlicher Systemaufbau

Das System besteht im Wesentlichen aus:

- elektronischen Schließzylindern oder Türbeschlägen,
- Zutrittslesern (in Kombination mit elektrifizierten Türelementen, z.B. elektrischen Schlössern, E-Öffnern),
- Identifikationsmedien (RFID-Karte, Transponder, optional Smartphone),
- Verwaltungssoftware bzw. Cloud-Lösung,
- optionalen Wireless-Gateways zur Vernetzung der Komponenten (wenn keine Andienung über PoE oder Standalone gegeben ist).

Grundlegende Funktionsweise

Durch das Vor- bzw. Anhalten des Zutrittsmediums (RFID- Identifikationsmedium) an den Leser (elektronische Schließung) oder den elektronischen Zylinder/Türschild (mechatronische Schließung) erfolgt die Aktivierung. Das System prüft die hinterlegte Berechtigung anhand der hinterlegten Berechtigungsgruppen. Bei gültiger Berechtigung wird der Schließmechanismus freigegeben und die Tür kann geöffnet werden. Ungültige oder gesperrte Medien erhalten keinen Zutritt. Ereignisse werden im System bzw. bei Stand Alone- Medien im Speicher des Akuprotokolliert und können gelesen werden (es erfolgt keine Dokumentation in Klarnamen sondern es wird die ID-Nummer des Identifikationsmediums registriert – ein Abgleich mit Klarnamen darf nur nach Freigabe im „Vier-Augen- Prinzip“ und unter Beachtung der Datenschutzbestimmungen für Schließmedien erfolgen).

Effizienz der digitalen Schließungen

- Flexible Vergabe und Änderung (Erweiterung und Reduktion) von Zutrittsrechten
- Sofortige Sperrung verlorener Transponder oder Karten

ENTWURF

- Keine Neuanschaffung von Schließzylindern bei Schlüsselverlust
- Zeitlich begrenzte Zutrittsberechtigungen (z.B. bei Handwerkern oder Vereinen in Sporthallen)
- Hohe Sicherheit durch verschlüsselte Kommunikation
- Erweiterbar und für unterschiedliche Gebäudegrößen – stufenweiser Ausbau im Objekt
- Optional Protokollierung von Zutritten und Fernverwaltung u.a. über Cloud-Lösungen.

Einsatzbereiche

- Büro- und Verwaltungsgebäuden
- Kulturgebäuden wie Museen und Veranstaltungsgebäuden
- Schulen und Kindergärten
- Gebäuden der Feuerwehr

Diese Systeme ermöglichen eine sichere, komfortable und wirtschaftliche Zutrittskontrolle und lassen sich bei Bedarf in bestehende Sicherheits- und Gebäudemanagementsysteme integrieren.

Systembeschreibung Zutrittssoftware

Das Zutrittskontrollsystem ist ein webbasiertes Softwaresystem und ermöglicht die zentrale Administration, Überwachung und Steuerung sämtlicher angebundener Zutrittskomponenten. Hierzu zählen insbesondere Controller, Zutrittsleser, Stand- Alone- Komponenten mit Onlineanbindung sowie drahtlose Zutrittseinheiten.

Die Softwarelösung ist skalierbar, mandantenfähig und modular aufgebaut. Die Architektur ermöglicht eine bedarfsgerechte Erweiterung des Systems und unterstützt die Integration zusätzlicher Funktionen sowie weiterer Systemkomponenten.

Die Bedienung des Systems erfolgt über eine benutzerfreundliche und intuitiv nutzbare Benutzeroberfläche. Darüber hinaus ist eine barrierefreie Nutzung entsprechend den jeweils geltenden gesetzlichen Vorgaben, Normen und Richtlinien sicherzustellen.

Berechtigungsverwaltung

Die Zutrittskontrollsoftware erfüllt folgende Funktionen bzw. unterstützt diese:

- Verwaltung von Schließplänen und Zutrittsprofilen (Benutzer Rollen)
- individuelle und gruppenbezogene Vergabe von Zutrittsberechtigungen
- Verwaltung von Raum- und Sicherheitszonen
- zeitgesteuerte Berechtigungen auf Grundlage von Zeitmodellen und Kalendern
- Umsetzung von Zwei-Personen-Zutritten (Vier-Augen-Prinzip)
- Unterstützung einer Wiederholsperre (Anti-Passback)
- zeitlich befristete sowie dauerhaft gültige Zutrittsberechtigungen,
- automatische Aktivierung und Deaktivierung von Berechtigungen entsprechend definierter Zeitmodelle

ENTWURF

Ausweismanagement

Das Ausweismanagement kann in drei aufeinander aufbauenden Ausbaustufen realisiert werden. Die erste Stufe umfasst die Verwaltung und Bereitstellung von Einzelausweisen für einzelne Nutzer. In der zweiten Stufe wird die Verwaltung von Mehrfachausweisen ermöglicht, wodurch eine flexible Zuordnung und Organisation mehrerer Ausweise und Berechtigungen unterstützt wird. Die dritte und umfassendste Stufe beinhaltet eine erweiterte Ausweisverwaltung mit zusätzlichen Funktionen wie der Integration eines Besuchermanagements, der Verwaltung von Fremdfirmen und externen Dienstleistern sowie der Unterstützung von Mobile-Access-Lösungen. Dadurch entsteht eine ganzheitliche Lösung zur effizienten Steuerung und Verwaltung von Zutrittsberechtigungen.

Die Zutrittskontrollsoftware muss ein integriertes Ausweismanagement bereitstellen. Dieses umfasst mindestens:

- Verwaltung von Personen- und Ausweisdaten
- Ausgabe, Aktivierung, Sperrung, Entsperrung und Ersatz von Ausweisen
- Unterstützung unterschiedlicher Identifikationsmedien (z. B. RFID-Karten, Schlüsselanhänger und mobile Zutrittsmedien),
- Zuordnung mehrerer Identifikationsmedien zu einer Person
- Verwaltung von Gültigkeitszeiträumen
- automatische Sperrung ungültiger oder abgelaufener Ausweise (bei online Lesemedien)
- revisionssichere Protokollierung sämtlicher Ausweisvorgänge
- Funktionen zur Massenanlage, Massenänderung und zum Massenaustausch von Ausweisen

Flexible Berechtigungsverwaltung

Die Berechtigungsverwaltung ermöglicht eine individuelle und dynamische Steuerung von Zutrittsrechten mithilfe von Schließplänen, Zutrittsprofilen, Raumzonen, Zeitmodellen, Zwei-Personen-Zutritten sowie Wiederholsperren.

DSGVO- konform

Die Einhaltung der Anforderungen der Datenschutz-Grundverordnung (DSGVO) wird durch ein umfassendes Datenschutz- und Sicherheitskonzept sichergestellt. Dieses umfasst klar definierte Datenhaltungsgrenzen – eine Zuordnung in der Zutrittsverwaltungssoftware mittels Klarnamen erfolgt nicht.
Nutzer bzw. den RFID- Medien werden Rollenprofile zugewiesen, die wiederum in den Berechtigungsgruppen hinterlegt sind.
Bei aktiver Verwendung des Schließmediums wird lediglich die ID-Nummer des RFID-Mediums gespeichert – ein Abrufen der Daten ist nur im Vier-Augenprinzip, Kennwortgeschütz und protokollier - zur lückenlosen Nachvollziehbarkeit sicherheitsrelevanter und datenschutzbezogener Vorgänge - vorgesehen.
Eine Zuordnung der ID-Nummer zu einem Klarnamen kann nur anhand der protokollierten Ausgabelisten des Schließmediums erfolgen (analog zu einer „Schlüsselausgabeliste“).

Darüber hinaus gewährleisten strukturierte Lösch- und Aufbewahrungskonzepte, dass personenbezogene Daten ausschließlich für die vorgesehenen Zwecke und innerhalb der rechtlich zulässigen Fristen verarbeitet und anschließend nachvollziehbar sowie dauerhaft gelöscht werden. Ergänzend wird ein vollständiger Export personenbezogener Daten ermöglicht, sodass betroffene Personen ihre Rechte auf Auskunft und Datenübertragbarkeit gemäß DSGVO wahrnehmen können.

ENTWURF

Durch diese technischen und organisatorischen Maßnahmen wird sichergestellt, dass personenbezogene Daten transparent, zweckgebunden, sicher und rechtskonform verarbeitet werden. Die Prozesse unterstützen eine nachvollziehbare Datenschutzorganisation und schaffen die Grundlage für eine dauerhaft DSGVO-konforme Verarbeitung und Verwaltung sensibler Informationen.

Anlage:
Datenschutz – und Sicherheitskonzept für die stadteigenen Zutrittskontrollsysteme der Stadt Lüdenscheid (n.N.)

Zuverlässiger Systembetrieb

Der zuverlässige und kontinuierliche Betrieb der Systeme wird durch ein Betriebs- und Überwachungskonzept sichergestellt. Ein wesentlicher Bestandteil ist die regelmäßige Durchführung zyklischer Datensicherungen unter Verwendung eines separaten Backup- bzw. Resource-Management-Tools. Dadurch wird gewährleistet, dass kritische System- und Anwendungsdaten im Falle eines Ausfalls oder einer Störung zeitnah wiederhergestellt werden können.
Ergänzend erfolgt eine kontinuierliche Überwachung der Systemkomponenten durch ein Systemmonitoring. Hierbei werden relevante Betriebsparameter, Ressourcenverfügbarkeiten sowie potenzielle Störungen frühzeitig erkannt und bewertet, sodass erforderliche Maßnahmen proaktiv eingeleitet werden können.
Zur Gewährleistung einer lückenlosen Nachvollziehbarkeit und Analyse von Betriebsereignissen werden systemrelevante Aktivitäten, Fehlerzustände und sicherheitsrelevante Ereignisse in Ereignisprotokollen dokumentiert. Diese Protokollierung unterstützt sowohl die Fehleranalyse als auch die kontinuierliche Optimierung der Systemstabilität und Betriebssicherheit.
Darüber hinaus werden regelmäßige Servicereports erstellt, welche den aktuellen Betriebszustand, durchgeführte Wartungsmaßnahmen, erkannte Auffälligkeiten sowie relevante Kennzahlen dokumentieren. Diese Berichte dienen der transparenten Kommunikation, der Qualitätssicherung und der kontinuierlichen Verbesserung des Systembetriebs.
Durch die Kombination aus regelmäßiger Datensicherung, proaktivem Monitoring, revisionsfähiger Protokollierung und standardisierten Serviceberichten wird ein stabiler, sicherer und nachvollziehbarer Systembetrieb gewährleistet.

Erweiterbarkeit der Zutrittskontrolle

Die Lösung bietet eine hohe Erweiterbarkeit und kann bedarfsgerecht um zusätzliche Funktionen und Module ergänzt werden. Hierzu zählen unter anderem die Besucherverwaltung, das Alarmmanagement, die Zeitwirtschaft, die Abbildung und Steuerung von Zutrittsworkflows sowie Funktionen zur Bilanzierung. Darüber hinaus stehen weitere optionale Erweiterungen zur Verfügung, sodass die Lösung flexibel an individuelle Anforderungen und zukünftige Entwicklungen möglich sind.

1.9.2.2 Schnittstellenvielfalt

Schnittstellen, Datenintegration und Dokumentenverarbeitung

Die Systemsoftware unterstützt verschiedene standardisierte und systemübergreifende Verfahren zur Datenübertragung, Integration und Verarbeitung von Personal-, Zutritts- und Dokumentendaten.

ENTWURF

Standardisierter Datenimport und -export im CSV-Format (Comma-Separated Values, z.B. aus MS Excel):
Der strukturierte Import und Export von Daten im CSV-Format stellt einen unkomplizierten und systemübergreifenden Austausch von Informationen sicher. Dadurch können Daten aus unterschiedlichen Vorsystemen übernommen, verarbeitet und für nachgelagerte Systeme bereitgestellt werden.
Die genauen Anforderungen an die CSV-Dateien müssen vor der Umsetzung abgestimmt werden.

Ausweiserstellung und Personalisierung:

Die RFID-Schließmedien im Scheckkartenformat können bedruckt werden. Hierbei können unter anderem personenbezogene Daten (z. B. für Handwerkerkarten), Identifikationsmerkmale, Lichtbilder sowie weitere für den jeweiligen Einsatzzweck relevante Informationen verarbeitet und auf dem RFID-Schließmedium im Scheckkartenformat abgebildet werden.

Tür- und Raumzonensteuerung

Die zentrale Steuerung und Überwachung von Türen und Raumzonen ermöglicht die Konfiguration sowie die Ausführung definierter Steuerungsfunktionen. Hierzu zählen unter anderem die Freigabe zur Daueröffnung, die Sperrung von Türen sowie die PIN-basierte Authentifizierung (bei Wandlesestellen mit Tastenfeldern).

Ergänzt wird der Funktionsumfang durch eine kalenderbasierte Steuerung, die zeit- und ereignisabhängige Schaltvorgänge automatisiert. So können beispielsweise in Schulen Öffnungs- und Schließzeiten auf Basis von Stunden-, Pausen- und Ferienplänen definiert werden, etwa eine automatische Freigabe während der Pausen sowie eine Verriegelung außerhalb der Unterrichtszeiten oder an Wochenenden.

Systemadministration

Das System ermöglicht die zentrale Verwaltung von Benutzerkonten, Rollen sowie den zugehörigen Zugriffs- und Berechtigungsstrukturen. Darüber hinaus unterstützt es die strukturierte Abbildung der Organisationsstruktur durch die Verwaltung organisatorischer Einheiten und ihrer hierarchischen Beziehungen. Zur Administration der technischen Infrastruktur bietet das System Funktionen zur Einrichtung, Parametrierung und Verwaltung von Controllern, Lesegeräten und weiteren digitalen Systemkomponenten. Ergänzend stehen Diagnose- und Analysefunktionen zur Verfügung, die eine kontinuierliche Überwachung des Systemzustands, die Durchführung von Fehleranalysen sowie die Unterstützung eines zuverlässigen und sicheren Systembetriebs ermöglichen.

Systembeschreibung der Zugangsberechtigungen

Funktionsbeschreibung Online-Vernetzung

Bei der Online-Vernetzung werden sämtliche Anlagenkomponenten über ein LAN miteinander verbunden. Das zentrale Verwaltungssystem ist über eine Ethernet-Verkabelung mit den Online-Steuerungen verbunden. An diese Steuerungen werden die einzelnen Zutrittsleser über eine Standardverkabelung angeschlossen (i.d.R. über RS-485 oder Cat.). Änderungen an den Daten werden in Echtzeit über das Netzwerk an alle relevanten Komponenten übertragen. Darüber hinaus können die Online-Steuerungen – bei entsprechender technischer Ausstattung der Tür – auch Türzustände wie „offen“, „geschlossen“ oder „verriegelt“ an das Verwaltungssystem übermitteln.

ENTWURF

Funktionsbeschreibung virtuelles Netzwerk mit AoC-Berechtigung

Bei **Access on Card** werden die persönlichen Zutrittsberechtigungen nicht direkt in jeder Türkomponente gespeichert, sondern auf dem **Zutrittsmedium** des Benutzers (z. B. RFID-Ausweis, Schlüsselanhänger oder elektronischer Schlüssel) hinterlegt.

Beim Öffnen einer **digitalen Standalone-Komponente** (z. B. einer batteriebetriebenen Türgarnitur oder eines elektronischen Zylinders) liest die Komponente die auf dem RFID-Medium gespeicherten Berechtigungsdaten aus und entscheidet anhand dieser Informationen, ob der Zutritt erlaubt ist.

Die Kommunikation funktioniert wechselwirksam in beide Richtungen:

- Der RFID-Chip übermittelt die Zutrittsrechte an die Türkomponente.
- Die Türkomponente kann Informationen zurück auf den RFID-Chip schreiben, beispielsweise den **aktuellen Batteriestatus** oder Ereignisdaten.

Sobald der Benutzer sein Medium an einem **Update-Terminal oder Online-Leser** aktualisiert bzw. validiert, werden diese gesammelten Informationen an das zentrale Zutrittskontrollsystem übertragen und dort verarbeitet.

Zusätzlich können Berechtigungen mit einem **Zeitstempel oder Ablaufdatum** (z.B. bei Handwerkerkarten) versehen werden. Dadurch bleiben Zutrittsrechte nur für einen bestimmten Zeitraum gültig und können über die Online-Infrastruktur regelmäßig erneuert oder verlängert werden.

Funktionsbeschreibung Programmierung mit Whitelist- Berechtigung

Eine **Whitelist-Berechtigung** bedeutet, dass in einem Aktuator (z. B. einem elektronischen Schloss oder einer Schließeinheit) eine feste Liste von **zugelassenen Medien** (z. B. Schlüssel, Transponder, Chipkarten) gespeichert ist. Nur die Medien, die in dieser Liste eingetragen sind, erhalten eine Berechtigung.
Die Berechtigungen werden **direkt im Aktuator programmiert**. Wird ein Schlüsselmedium vor den Aktuator gehalten, prüft dieser, ob das Medium in der gespeicherten Whitelist (Berechtigungsgruppe) enthalten ist. Bei einer Übereinstimmung wird die Sperre aufgehoben und der Aktuator öffnet.
Geht ein Schlüssel verloren oder ändern sich die Zugangsberechtigungen, muss die gespeicherte Liste im Aktuator angepasst werden.

Bei standalone Akuatoren werden **mobile Programmiergeräte** verwendet, mit denen die neuen Berechtigungen eingetragen oder alte Berechtigungen gelöscht werden.
Bei Akuatoren, die online eingebunden sind erfolgt die Anpassung zentral.

Funktionsbeschreibung Wireless- Anbindung

Digitale Standalone-Komponenten, die über eine Wirless- Anbindung verfügen, können mittels vernetzten Gateways per
ZigBee-Funk mit der Verwaltungssoftware verbunden werden. Die zuletzt gespeicherte Zutrittsberechtigung bleibt im Gerätespeicher bestehen. Nur bei Änderung einer Berechtigung o.ä. wird eine Funkverbindung aufgebaut. Über die Verwaltungssoftware sind u.a. auch zeitliche gesteuerte Fernöffnungen zu tätigen. Zudem können auch Firmware-Änderungen auch über das Wireless-System abgebildet werden.

ENTWURF

Aktuatoren

Der Begriff „Aktuator“ bezeichnet die digitale Komponente an einer Tür bzw. einem Verschlusspunkt, welche die kontrollierte Öffnung ausführt oder den hierzu erforderlichen Öffnungsimpuls an die mechanische Verriegelung übermittelt.
Die angebotene Systemlösung muss eine einheitliche Integration der nachfolgend genannten digitalen Offline-Aktuatoren und Zutrittskomponenten in eine übergeordnete Systemlandschaft ermöglichen.
Die Lösung ist so auszulegen, dass eine spätere Erweiterung der eingesetzten Identifikationstechnologien und der mobilen Zutrittsmedien ohne Austausch der installierten Hardware möglich ist.

Geforderte Aktuator- und Komponentenarten

In die Systemlandschaft müssen mindestens folgende Offline-Aktuatoren bzw. digitalen Komponenten integrierbar sein:

- mechatronische Zylindersysteme
- digitale Knaufzylinder in modularer Bauweise
- digitale Hebelzylinder
- digitale Langschild-Beschläge für Vollblatttüren
- digitale Langschild-Beschläge in schmaler Ausführung für Rahmentüren
- digitale Langschild-Schutzbeschläge mit einem Mindeststandard ES1
- digitale Kompaktbeschläge mit Rosettenmontage für Vollblatttüren
- digitale Wandlesegeräte zur Unterputz- oder Aufputzmontage
- digitale Möbelschrankverschlüsse
- eine geeignete Funkanbindung der mechatronischen und digitalen Aktuatoren an ein Funknetzwerk mittels Wireless Gateway

Die verschiedenen Aktuator- und Komponententypen müssen in einer gemeinsamen Systemlandschaft betrieben und administriert werden können.

Technologie und Identifikationsmedien

Multi-RFID-Technologie

Die eingesetzten Aktuatoren müssen dem Technologieansatz **MRD (Multi RFID Device)** entsprechen. Die Aktuator-Hardware muss die Verarbeitung unterschiedlicher RFID- und Transpondertechnologien ermöglichen.
Mindestens die folgenden Transpondertechnologien müssen unterstützt werden:

- MIFARE,
- LEGIC,
- OSS-Transpondermedien.

Die Unterstützung der genannten Transpondertechnologien muss durch die installierte Aktuator-Hardware gewährleistet sein. Die Auswahl, Änderung oder Erweiterung der eingesetzten Transpondertechnologie darf keinen Austausch der installierten Aktuator-Hardware erfordern.

Technologische Erweiterbarkeit

Die Systemarchitektur muss so ausgelegt sein, dass weitere Identifikations- und Zutrittsmedien nachträglich integriert werden können, ohne dass die installierten Aktuatoren

ENTWURF

ausgetauscht werden müssen.
Die nachträgliche Aktivierung oder Nutzung einer BLE-basierten Smartphone-Zutrittsfunktion darf keinen Austausch der installierten Aktuator-Hardware erfordern.

Stromversorgung

Aus Gründen der Nachhaltigkeit werden für die Stromversorgung der **digitalen und mechatronischen** Aktuatoren, die nicht über Leitungsgebundene Spannungsversorung verfügen (z.B. PoE, 12-34V DC), handelsübliche Standardbatterien eingesetzt, die über den öffentlichen Handel bezogen werden können.

Nicht zulässig sind insbesondere:

- speziell konfektionierte Batterieeinheiten (z.B. proprietäre Batterie-Packs), Batterieeinheiten mit fest aufgebrachten Kabeln, sonstige herstellerspezifische Sonderlösungen, die nicht als handelsübliche Standardbatterien erhältlich sind.

Geforderte Öffnungs- und Betriebsfunktionen

Mit den digitalen Aktuatoren sind folgende Öffnungs- und Betriebsfunktionen realisierbar:

Office-Funktion bei digitalen Türbeschlägen (Beschlagslesern)

Durch einmaliges Vorhalten eines berechtigten Zutrittsmediums kann Komponente dauerhaft auf „offen“ geschaltet werden.
Die Rückkehr in den regulären Betriebszustand wird durch eine definierte Bedienhandlung bzw. einen entsprechenden Steuerbefehl umgesetzt.

Wirkungsweise Bürofreigabe

Die Komponente unterscheiden zwischen einer Standardöffnung und einer dauerhaften Freigabe.

- Ein kurzes Vorhalten des berechtigten Mediums führt zu einer Standardöffnung (zeitlich begrenzter und definierbarer Aktivierungszeitraum).
- Ein längeres Vorhalten des berechtigten Mediums aktiviert die dauerhafte Öffnung bzw. Bürofreigabe („Dauer-Auf“).

Die erforderliche Vorhaltezeit ist systemseitig zu definieren.

Programmierung und Parametrierung

Die Programmierung und Parametrierung der Aktuatoren, insbesondere von Zylindern und Beschlagslesern, erfolgt ohne eine Verkabelung der Türen.
Eine kabelgebundene Verbindung zur Tür bzw. zum Aktuator ist für die reguläre Programmierung und Parametrierung nicht erforderlich.
Die Programmierung erfolgt über die vorgesehene Systemlösung bzw. über geeignete drahtlose oder mobile Verbindung (z.B. über Gateway- Komponenten).

Einheitliche Produktfamilie und Herstellerzugehörigkeit

Aus Gründen der Nachhaltigkeit, der Systemkompatibilität und der langfristigen Wartbarkeit sind sämtliche nachfolgend genannten Komponenten aus einer einheitlichen Produktfamilie des Herstellers **dormakaba** zu verwenden:

- digitale Aktuatoren,

ENTWURF

- Zutrittsmedien,
- Transpondermedien,
- mechanische Schließzylinder.

Die Komponenten müssen innerhalb der Systemlandschaft miteinander kompatibel sein.

Zukunftsfähigkeit und Technologiewechsel

Die Systemlösung ermöglicht eine langfristige Nutzung der installierten Hardware.

Ein Wechsel oder eine Erweiterung der Zutrittstechnologie, insbesondere:

Wechsel zwischen unterschiedlichen RFID- bzw. Transpondertechnologien,
Einsatz von MIFARE,
Einsatz von LEGIC,
Einsatz von OSS-Transpondermedien,
spätere Nutzung von Smartphones zur Öffnung mittels BLE,

darf keinen Austausch der bereits installierten Aktuatoren erforderlich machen.

Die technische Lösung ist daher so auszulegen, dass die erforderlichen Funktionen durch Software, Konfiguration, geeignete Medien oder systemseitige Erweiterungen umgesetzt werden können.

Erforderliche Nachweise des Bieters bei Systemerweiterung

Der Bieter hat für die angebotene Systemlösung nachvollziehbar nachzuweisen, dass die vorgenannten Anforderungen erfüllt werden.

Insbesondere sind nachzuweisen:

unterstützte Aktuator- und Komponentenarten,
unterstützte Transpondertechnologien,
MRD-Fähigkeit,
spätere Nutzbarkeit von Smartphones zur Öffnung mittels BLE,
Möglichkeit des Technologiewechsels ohne Hardwaretausch,
verwendete Batterietypen und deren öffentliche Verfügbarkeit,
Eignung der relevanten Komponenten für Feuerschutztüren,
verfügbare Öffnungs- und Betriebsfunktionen,
Programmierung und Parametrierung ohne Verkabelung der Türen,
Möglichkeit der Funkanbindung an ein noch festzulegendes Funknetzwerk,
Zugehörigkeit der Aktuatoren, Medien und mechanischen Schließzylinder zu einer einheitlichen Produktfamilie eines Herstellers.

Abweichungen von den genannten Anforderungen sind vom Anbieter ausdrücklich und nachvollziehbar zu benennen.

ENTWURF

1.9.3.1 Systematik Bezeichnung

Fluchtwegterminal Türnummer		
Fluchtwegterminal	Schließmedium	Beschlagart
Panikschloss	Standalone oder online	Andienung Spannungsversorgung
E- Schloss	E-Antrieb	E-Öffner

Angabe: nicht vorhanden **0**

Türnummer
Angabe: entsprechend der Projektvorgabe bzw. der Projekt-Türliste gem. der Bezeichnungsschlüssel BQA 08_Orientierungs- und Leitsysteme.

Schließmedium
Angabe:
B (digitaler Zylinder)
S (digitales Schild)
L (Wandlesestelle)

Beschlagsart
Angabe:
D/D (Drücker/Drücker)
D/K (Drücker/Knauf)
D/_ (Drücker/kein Beschlag bzw. nur einseitiger Beschlag)

Panikschloss
Angabe: **P** (vorhanden)

Standalone
Angabe: **SA**

Online
Angabe: **OL**

Aktuatoren:
E-Schloss
Angabe: **ES**

E-Antrieb
Angabe: **EA**

E-Öffner
Angabe: **EÖ**

Fluchtwegterminal **FWT**

ENTWURF

Andienung:
Angabe: **12V** (12Volt) **PoE**, **24V DC**, …
Bsp. Tür mit Fluchtwegterminal mit Wandleser, mit Drücker – Knauf Beschlag (Wechselgarnitur), mit Panikschloss, online (über …), ohne Andienung, ohne E-Schloss, ohne E-Antrieb, mit E-Öffner

Bsp. als Schaubild

T0815		
FWT	**L**	**D/K**
P	**OL**	**0**
0	**0**	**EÖ**

Bsp. als Text

T0815_FWT _L_D/K _P_OL_0_0_0_EÖ

Schließmedien

Für das Schließsystem sind ausschließlich passive RFID-Schließmedien (Datenträger ohne eigene Energieversorgung / Batterie) zulässig.

Es sind ausschließlich Schließmedien mit folgender Chiptechnologie einzusetzen:

LEGIC Advant / MIFARE DESFire EV3.

Die Schließmedien sind in den folgenden Ausführungen zu verwenden:

- Standard-DIN-Karte (ISO/IEC 7810 ID-1, EC-Kartenformat)
- Schlüsselanhänger
- passiver Schlüsselclip

Die Kommunikation zwischen Schließmedium und Leseeinheit hat ausschließlich berührungslos innerhalb des Lesefeldes des jeweiligen Lesegerätes zu erfolgen. Die Datenübertragung sowie die Authentifizierung sind nach dem Stand der Technik verschlüsselt auszuführen.

Die angebotenen Schließmedien müssen als unkodierte Standardmedien **frei am Markt** verfügbar und **unabhängig vom Hersteller** des angebotenen Schließsystems (hier **dormakaba**) beschaffbar sein.

Proprietäre, anlagengebundene Schließmedien, die ausschließlich über den Hersteller oder autorisierte Vertriebspartner des angebotenen Systems bezogen werden können, sind <u>nicht</u> zulässig.

Die vollständige Kodierung, Personalisierung und Inbetriebnahme der Schließmedien muss mit der vorhandenen Programmier- und Kodierperipherie eigenständig (durch die Stadt Lüdenscheid) durchgeführt werden können.

ENTWURF

1.9.4.1 Technische Beschreibung der Komponenten

Digitale Schließzylinder

Digitale Schließzylinder in modularer Bauweise für 17-mm-Europrofilzylinder prüfen die elektronische Codierung des verwendeten Identmediums. Die im Chip des RFID-Mediums (z. B. Ausweis, Schlüssel, Schlüsselanhänger oder vergleichbare Transponder) gespeicherten Daten werden kontaktlos über die Antenneneinheit ausgelesen und an die integrierte Steuerelektronik übertragen.
Wird das Medium durch die Steuerelektronik als berechtigt erkannt, koppelt ein Motormechanismus den Außenknauf ein. Eine erteilte bzw. verweigerte Zutrittsberechtigung wird optisch und akustisch signalisiert.
Bei vorhandener Zutrittsberechtigung und Betätigung des Außenknaufs wird über die Kupplung die Sperrnase mechanisch mitgenommen und die Tür kann entriegelt werden. Nach einer standardmäßig eingestellten Kupplungszeit von fünf Sekunden entkoppelt der Motor automatisch. Anschließend lässt sich der Außenknauf ohne Funktion frei drehen. Die Kupplungszeit muss entsprechend den Anforderungen des Anwenders/Nutzers individuell einstellbar sein.
Die digitalen Schließzylinder werden mit handelsüblichen Batterien betrieben und funktionieren unabhängig von externen Spannungsquellen. Eine Verkabelung der Tür ist nicht erforderlich.
Die digitalen Zylinder verfügen über BLE- und/oder NFC-Schnittstellen, um eine mögliche Anbindung an Smartphones zu ermöglichen.
Bei Verwendung mit Antipanikschlössern, die für den Einsatz mit Drehknopfzylindern zugelassen sind, müssen digitale Schließzylinder gemäß EN 1125 und EN 179 eingesetzt werden.

Standard-Digitalzylinder müssen für den Einsatz an Paniktüren mit der Anforderung „Freilauf“ geeignet sein.

Standard Digitalzylinder

Der Standard Digitalzylinder ist entweder als elektronischer Doppel-Knauf-Zylinder mit außenliegender Berechtigungsprüfung und mechanischem Innenknauf für eine komfortable und sichere Zutrittskontrolle, oder als Halbzylinder (z.B. für Schlüsselschalter) zu verwenden.
Die Ausführung erfolgt im Europrofil und unterstützt die Transpondertechnologien **MIFARE** und **LEGIC**. Der Zylinder wird mittels **CR2-Batterie** betrieben und ist für den Einsatz an **Brandschutztüren bis T90** sowie für Anwendungen mit erhöhten Anforderungen durch die **Schutzart IP55** geeignet.
Die verfügbaren (Grund-) Baulängen beginnen bei **30/30 mm** und sind in **5-mm-Schritten** bis zu einer Gesamtlänge von **140 mm** erweiterbar. Die Oberfläche ist in **Edelstahl-Optik** gehalten.
Als Batterieaustauschintervall ist ein jährlicher Zyklus vorzusehen.

ENTWURF

Digitale Beschlag-Leser

Beschreibung digitale Türbeschläge

Der Standalone Beschlagleser ist an beiden Seiten mit Drücker ausgestattet. Er verfügt an der Beschlagaußenseite über die Schutzart IP55.
Der Deckschild- und Drückerbeschlag besteht aus hochwertigem Edelstahl und ist mit einer verdeckten Befestigung ohne sichtbare Schrauben ausgeführt. Der Beschlagleser ist wahlweise mit einem schmalen Schild (40 mm) oder einem breiten Schild (54 mm) - entsprechend der Anforderungen – zu verwenden.
Die Innen- und Außenschilder können individuell in unterschiedlichen Breiten kombiniert werden.
Optional stehen verschiedene Ausführungen mit horizontalen oder vertikalen Rosettenbefestigungspunkten sowie Varianten mit Kurzschild und Panikstangen zur Verfügung.
Die C-Lever pro Beschlagleser können optional mit einer Schnittstelle (S-Modul) zur Anbindung und Übersteuerung durch externe Fremdsysteme sowie mit Anschlüssen für eine externe Stromversorgung ausgestattet werden. Zusätzlich ist eine einbruchhemmende Schutzbeschlagvariante gemäß Widerstandsklasse ES1 erhältlich.
Die Betätigungswirkung wird über die Drückernuss im Schlosskasten ausgeführt. Die Lesetechnik unterstützt die Transpondertechnologien **MIFARE** und **LEGIC**. Der Beschlag ist für den Einsatz an **Brandschutztüren bis T90 geeignet.**
Die Energieversorgung erfolgt über handelsübliche Lithium-AA-Batterien mit 1,5 Volt.
Als Richtwert für den Austausch der Batterien sind etwa 150.000 Betätigungszyklen anzusetzen. Bei einer Nutzung von etwa 250 Betätigungen pro Werktag entspricht dies einer Batterielebensdauer von ca. zwei Jahren (auch wenn ein längerer Zyklus theoretisch erreicht werden kann, sollte der Batterieaustauschintervall von 2 Jahren nicht überschritten werden).

ZERTIFIKATE
Fertigung: DIN ISO 9001
Gesundheit/Sicherheit: EN 60950-1/A12;EN 50364;EN 62479
Elektromagnetische Verträglichkeit: EN 301489-1,
EN 301489-3
Effektive Nutzung Funkspektrum: EN 300220-2
R TTE-Richtlinie Artikel: EN 300330-2
Feuer-/Rauch: DIN EN 1634-1+3
in Verbindung mit DIN EN 1363-1 ; DIN 4102
Dauerfunktionsprüfung: DIN 18273
Flucht- und Rettungsweg: EN179
Schock-/Schwingprüfung: DIN EN 60088-2-27,
DIN EN 60068-2-6
EN 1906 Klassifizierung: 47-B1 1 3 0 U

Beschlag-Leser kompakt /Rosettenmontage

Bei Türen ohne Europrofilzylinderschließung kann ein Drücker-/Rosetten-Leser inklusive Innendrücker verwendet werden. Er verfügt über eine integrierte Drückersteuerung sowie eine 60 mm breite Edelstahlrosette mit wahlweise schwarzen oder weißen Kunststoff-Applikationen.
Die Befestigung erfolgt über eine horizontale Rosettenverschraubung. Der Beschlag ist für Türdicken von 38 bis 50 mm geeignet.
Die Betätigungswirkung wird über die Drückernuss im Schlosskasten ausgeführt. Die Lesetechnik unterstützt die Transpondertechnologien **MIFARE** und **LEGIC**. Der Beschlag ist für den Einsatz an **Brandschutztüren bis T90 geeignet.**

ENTWURF

Die Energieversorgung erfolgt über handelsübliche Lithium-AAA-Batterien mit 1,5 Volt.
Als Richtwert für den Austausch der Batterien sind etwa 150.000 Betätigungszyklen anzusetzen. Der Batteriewechsel muss ohne Demontage des Drückers und ohne Entfernung der Gehäuseabdeckung möglich sein.
Der Beschlag ist für den Einsatz an **Brandschutztüren bis T90 geeignet.**

Wandleser

Kompaktleser

Zutrittsleser zur direkten Aufputzmontage auf vorhandenen Untergründen – ohne erforderliche Aussparungen oder Unterputzdosen.

Das Gerät verfügt über ein integriertes RFID-Lese- und Schreibmodul zur Unterstützung von MIFARE Classic und MIFARE DESFire sowie über den BLE Peripheral Mode für die Nutzung mit iOS- und Android-Smartphones.

Optische und akustische Signale ermöglichen eine eindeutige Rückmeldung bei Zutrittsbuchungen.

Bei der Ausführung mit Tastenfeld kann über die Eingabe eines PIN-Codes die Türöffnung erfolgen. Das Ziffernfeld ist hinerleuchtet, sowie mit Tasten für Korrektur und Bestätigung ausgestattet.

Die Anbindung an den Zutrittsmanager erfolgt über eine Cat.6 - o.glw. Datenleitung mit verschlüsselter Datenübertragung zur sicheren Kommunikation.

Die Anbindung des Kompatlesers bei einer Leitungslänge bis 30m über ein Koax- Kabel.

Für schmale Ausführungen, wie z.B. bei der Direktmontage auf Pfosten-Riegelkonstruktionen oder auf Rahmen von Rohr-Rahmentüren kann die schmale Bauform verwendet werden.

Bei Außentüren wird eine getrennte Erfassungseinheit (außen) mit einem Remotleser (innen) kombiniert – diese Montageart macht eine Fremdmanipulation (durch kurzschließen von Steuerrleitungen) auf der Außenseite unmöglich und dient der Erhöhung des Objektschutzes.

ZERTIFIKATE
EN 301489-1 V2.1.1
EN 301489-3 V2.1.0 Draft
EN 301489-17 V3.1.1
EN 300328 V2.1.1
EN 300330 V2.1.1
EN 50364:2010
EN 62311:2008
EN 62368-1:2014
EN 60529:2014-09
2014/53/EU:2015-01-23
2011/65/EU:2011-06-08
UL 62368-1:2014-12
CAN/CSA-C22.2 No. 62368-1:2014-12

ENTWURF

1.9.5.1 Online-Peripherie für Direktvernetzung

Aufbau der (Online-) Steuerung

Zutrittsmanager Hutschiene ((teil-)zentrale Steuerung)

Für die Zutrittskontrolle wird ein Zutrittsmanager verwendet – bei der Teilzentralen Steuerung kann dies über einen Manager Montageart Hutschiene oder über einen wandhängenden Zutrittsmanager erfolgen.
Die Verortung erfolgt zentral – z.B. im Technik- oder Hausanschlussraum des Objektes.
Diese Art der Steuerung ist die wirtschaftlichste und wartungsfreundlichste Art der bzgl. der Hardware Steuerungskomponente.

Durch die Zentrale Verortung muss für jede Tür bzw. angesteuerte Komponente und Lesestelle eine eigene Leitung von der Steuerung vorgesehen werden.
Sind mehr als vier Funktionen (z.B. 1 Lesestelle + 3 Akteure) am Zielort vorgesehen, muss eine zusätzliche Leitung verwendet werden.
Die Andienung erfolgt i.d.R. mittels Cat.6 Kabel (2*4) oder besser.

Der Manager hat die Funktion, das erfasste Zutrittssignal der Lesestellen an die, der Lesestelle zugehörigen Komponenten (z.B. Türen mit E-Öffner, Schranken, Aufzüge und weitere) nach der Prüfung weiterzuleiten und die hinterlegte Aktion mittels Steuerungsspannung auszulösen.
Darüber hinaus wir über die Schreibfunktion der Lesestelle eine mögliche Änderung der Rollenfunktion des Nutzers aktualisiert, erfasste Daten von Standalone-Komponenten (z.B. Batteriestände von digitalen Zylindern) werden an das übergeordnete Matrixsystem weitergeleitet.
Die Türöffnung bzw. der Steuerungsvorgang wird ausschließlich durch ein berechtigtes RFID-Medium ausgeführt. Die Aktualisierung der AoC-Zutrittsrechte wird über die Lese- und Schreibfunktion gewährleistet.

Der Zutrittsmanager (Ausführung Hutschiene) verfügt über vier überwachte digitale Eingänge für potenzialfreie Kontakte mit einer maximalen Spannung von 5 V DC, einen Sabotagekontakt und drei Relaisausgängen. Die Relais sind für eine Kontaktbelastung von maximal 30 V AC/DC und 2 A ausgelegt.

Werden mehr als drei Relaisausgänge benötigt, kann der Zutrittsmanager mittels Erweiterungsmodul ergänzt werden.

Für den Anschluss von zwei Erfassungseinheiten ist eine entsprechende Koaxial-Schnittstelle vorzusehen. Zusätzlich ermöglicht eine RS-485-Schnittstelle (Andienung mittels Cat.6 o.ä. Leitung) den Anschluss von bis zu 15 Lesern. Durch das Erweiterungsmodul können zusätzliche Steuerungsausgänge ermöglicht werden.

Der Zutrittsmanager unterstützt die RFID-Technologien LEGIC advant und prime sowie MIFARE Classic und DESFire. Die Kompatibilität mit den Standards ISO 14443 und ISO 15693 ist entsprechend den jeweiligen unterstützten Medien sicherzustellen.

ENTWURF

Über die Netzwerkanbindung wird über die Ethernet-Schnittstelle (PoE) mit 10/100 Mbit/s und IPv4 umgesetzt. Die Nutzdatenkommunikation zwischen dem Terminal und dem MATRIX-System ist verschlüsselt wird über HTTPS ausgeführt.
Die Aktualisierung und Übertragung der Zutrittsrechte wird über die Steuerungsmatrix umgesetzt.

Der interne Datenspeicher kann die Verwaltung von mindestens 2.000 Personen und 8.000 Erfassungssätzen ermöglichen.

Die Spannungsversorgung muss im Bereich von 10 bis 34 V DC liegen. Die typische Leistungsaufnahme des Zutrittsmanagers beträgt 3,6 W. Die zusätzliche Leistungsaufnahme der angeschlossenen Erweiterungsmodule ist bei der Dimensionierung der Spannungsversorgung zu berücksichtigen.

Der Zutrittsmanager ist in einem für die Montage auf einer DIN-Hutschiene TS 35 gemäß EN 50022 geeigneten Gehäuse auszuführen. Die Abmessungen betragen ca. 125 × 99 × 45 mm (L × B × H).

Die Schutzart entspricht IP20 gemäß IEC 60529. Bei der Montage ist sicherzustellen, dass die Einbaubedingungen den Anforderungen des Herstellers entsprechen und ein geeigneter Schutz vor unzulässigen Umwelteinflüssen gewährleistet ist (z.B. durch die Montage in einem geeignetem Medienschrank).

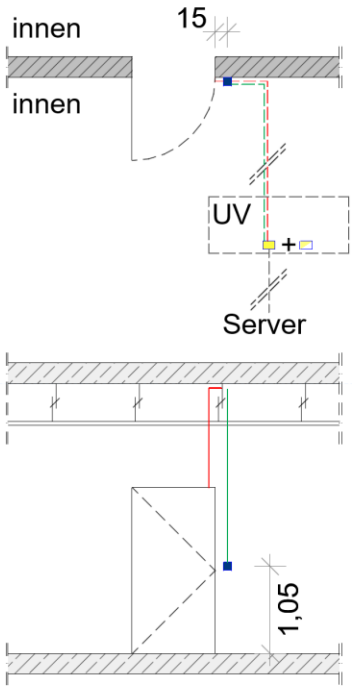
Der zulässige Umgebungstemperaturbereich liegt zwischen 0 °C und +50 °C. Die relative Luftfeuchtigkeit muss zwischen 5 % und 85 % liegen; Kondensation ist auszuschließen.

Die Installation und der elektrische Anschluss sind gemäß den Herstellervorgaben und den geltenden elektrotechnischen Anforderungen durchzuführen. Der Zutrittsmanager ist vollständig in das Zutrittskontrollsystem MATRIX einzubinden. Nach Abschluss der Montage sind die Spannungsversorgung, die Kommunikation, die angeschlossenen Leser und Erweiterungsmodule, die überwachten Eingänge, die Relaisausgänge sowie die Türöffnung mit berechtigten RFID-Medien zu prüfen.

Die ordnungsgemäße Aktualisierung der Zutrittsrechte und die verschlüsselte Kommunikation mit dem MATRIX-System sind im Rahmen der Inbetriebnahme ebenfalls zu überprüfen. Die Anlage ist erst nach erfolgreicher Funktionsprüfung für den regulären Betrieb freizugeben.

ENTWURF

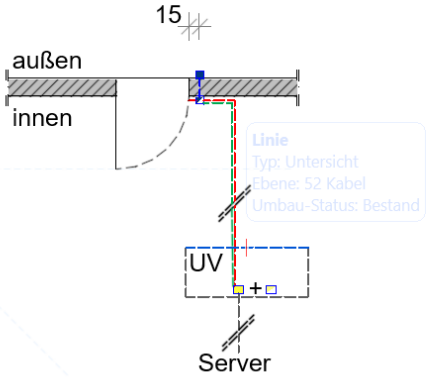
1b. Schema zentrale Steuerung Innentür



- Kompaktleser (Montage AP oder UP dann mit UP Dose)
- RS-485 Leseeinheit
- RS-485 Steuerspannung (über Relaiausgang
- Zutrittssteuerung in UV - wenn mehr als 3 Komponenten ist eine
- Erweiterung erforderlich - muss beim Platzbedarf auf der Hutschiene berücksichtigt werden)
- UV Unterverteilung
- LAN PoE 12-24V

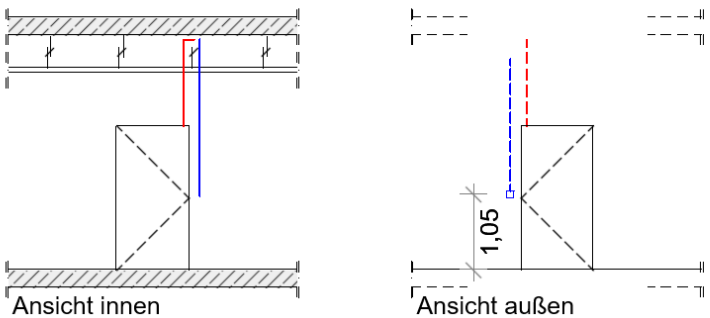
Arbeitsspannung der E-Komponenten Tür erfolgt gesondert und ist nicht Bestandteil der Schließanlage!!!

2b. Schema zentrale Steuerung Außentür



- Erfassungseinheit (außen, Montage AP oder UP dann mit UP Dose)
- Remoteleser
- RS-485 Leseeinheit
- RS-485 Steuerspannung (über Relaiausgang
- Zutrittssteuerung in UV - wenn mehr als 3 Komponenten ist eine
- Erweiterung erforderlich - muss beim Platzbedarf auf der Hutschiene berücksichtigt werden)
- UV Unterverteilung
- Coax
- LAN PoE 12-24V

Arbeitsspannung der E-Komponenten Tür erfolgt gesondert und ist nicht Bestandteil der Schließanlage!!!



Zutrittsmanager (dezentrale Steuerung)

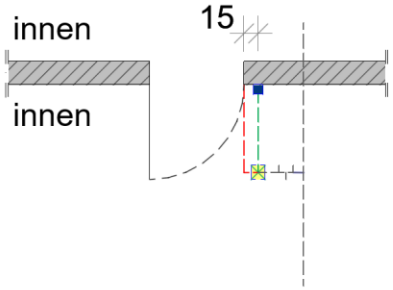
Im Gegensatz zur zentralen Steuerungsform wird bei der dezentralen Variante der entsprechende Manager in der Nähe der Lesestelle bzw. des zu steuernden Objektes verortet.
Durch die dezentrale Verortung ist der Vorteil der zentralen Steuerung hinsichtlich der Kosten und der Wartungsfreundlichkeit nicht mehr gegeben.
Bei Weitläufigen oder komplexen Objekten mit einem geringen Anteil bzw. weit auseinanderliegenden (>30m), anzusteuernden Komponenten oder bei einer Nachrüstung in Bestandsgebäuden kann eine dezentrale Steuerung vorteilhaft sein.
Die dezentrale Steuerung benötigt als Andienung lediglich eine Datenverbindung (PoE) und für die Türkomponenten einen entsprechend dimensionierten Arbeitsstrom, der durch die Relaisteuerung angesteuert werden kann.

Die Montage kann wandhängend (z.B. oberhalb einer Abhangdecke) erfolgen.

Der Zutrittsmanager verfügt über 4 Signal-Eingänge und kann über drei Relais-Ausgänge drei elektrifizierte Akteure ansteuern.

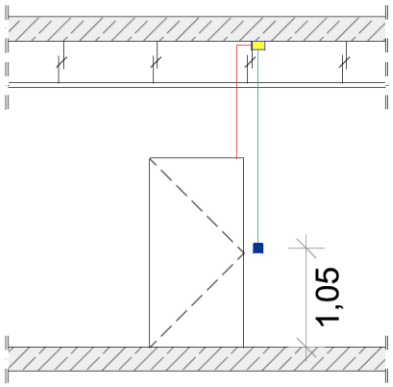
Die Spanungsversorgung für den Manager wird über PoE ermöglicht (15,4W oder 25,5W, 10-35V DC).

1a. Schema dezentrale Steuerung Innentür

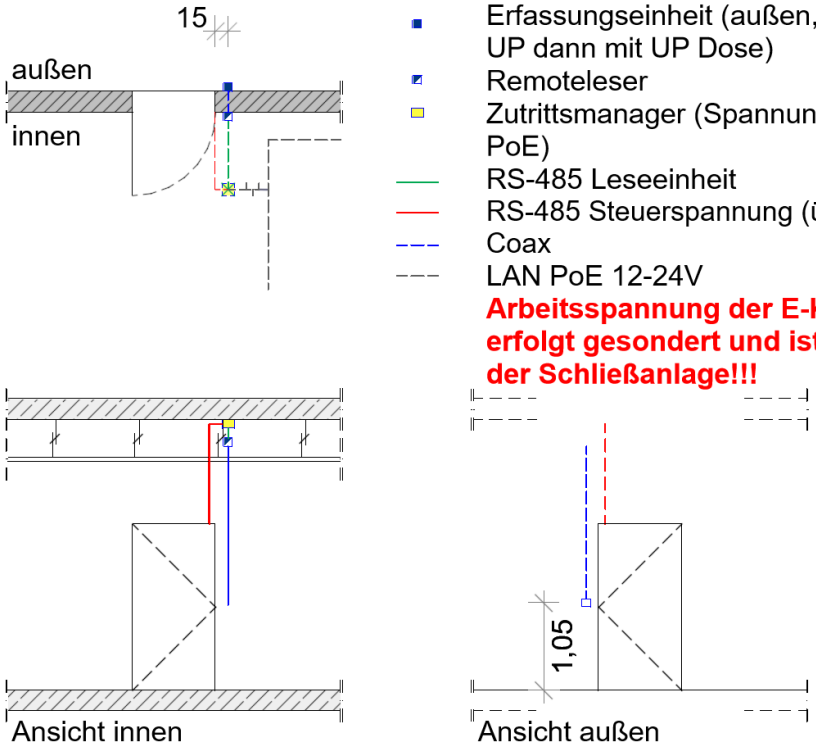


- Kompaktleser (Montage AP oder UP dann mit UP Dose)
- Zutrittsmanager (Spannungsversorgung ü. PoE, 3 Relaiausgänge)
- RS-485 Leseeinheit
- RS-485 Steuerspannung (über Relaiausgang)
- LAN PoE 12-24V

Arbeitsspannung der E-Komponenten Tür erfolgt gesondert und ist nicht Bestandteil der Schließanlage!!!



2a. Schema dezentrale Steuerung Außentür



Fluchttürterminals

Fluchttürterminals sind Steuerungen für Türen in Fluchtwegen. Die Montage erfolgt i.d.R. als Unterputzinstallation. Sollte die Tür über eine elektronische Schließung verfügen, so ist die Lesestelle im (Schalter-) Rahmen des Fluchtwegterminals zu integrieren (dreifach Rahmen).

Die Einheit besteht aus einer Nottaste nebst Steuereinheit, die im Notfall die Türverriegelung oder Türzuhaltung freigibt.
Das Terminal wird entweder als Solitärinstallation betrieben, kann aber auch mit weiteren Terminals vernetzt werden – bei Betätigung erfolgt dann die Freigabe der Fluchtroute.

Zur Aktivierung der Nottaste muss der Schutzdeckel entfernt werden.

Die Funktion und der Status werden durch eindeutige Lichtanzeigen im Bereich der Taste sichtbargemacht.
Die Signale müssen folgende Status anzeigen:

- Busverbindung OK
- Busverbindung unterbrochen
- Hardware Fehler – ohne Funktion
- Normaler Betrieb – Betriebsbereit
- Manipulation (inkl. akustischen Signal)

Versorgungsspannug 24V DC (über PSU 24 AP oder UP)
Stromaufnahme Ruhestrom 65mA – bei Alarm und aktivierung 100 mA
Umgebungstemperatur -10°C bis + 55°C
Relqative Luftfeuchtigkeit bis 93%rH (nicht betauend)

Schutzart IP 30

Die Taste bzw. das Terminal muss gut erkennbar kenntlich gemacht werden und entsprechend der DIN 13637 beschriftet werden. Das Piktogramm ist hinterleuchtet und nachleuchtend auszuführen und in der Schalterserie zu integrieren.



Die Deaktivierung des Alarmtons des Terminals erfolgt über einen Schlüsselschalter.

Soll die Fluchtwegterminalgesicherte Tür auch entgegen der Fluchtrichtung genutzt werden, muss ein Taster zur Entsperrung der Türfalle verbaut werden.

