Bundesministerium
für Wohnen, Stadtentwicklung
und Bauwesen

Arbeitskreis Maschinen- und Elektrotechnik staatlicher und kommunaler Verwaltungen

Elektronische Zutrittskontrollanlagen eZKA

Planung, Bau und Betrieb von elektronischen Zutrittskontrollanlagen in öffentlichen Gebäuden

Empfehlung Nr. 171

Stand November 2023

AMEV

Arbeitskreis Maschinen- und Elektrotechnik staatlicher und kommunaler Verwaltungen

Planung, Bau und Betrieb von elektronischen Zutrittskontrollanlagen in öffentlichen Gebäuden

(eZKA)

lfd. Nr. 171
Aufgestellt und herausgegeben vom Arbeitskreis
Maschinen- und Elektrotechnik staatlicher
und kommunaler Verwaltungen (AMEV)
Berlin 2023

Geschäftsstelle des AMEV im
Bundesministerium für Wohnen, Stadtentwicklung und Bauwesen (BMWSB)
Krausenstraße 17-18 10117 Berlin

Telefon (030) 18 335 16860
E-Mail: amev@bmwsb.bund.de

Informationen über Neuerscheinungen erhalten Sie unter
www.amev-online.de
oder bei der AMEV-Geschäftsstelle

INHALTSVERZEICHNIS

VORWORT		**5**
1	**GRUNDSÄTZLICHE ÜBERLEGUNGEN ZU SCHLIEßANLAGEN UND ZUTRITTSKONTROLLANLAGEN**	**6**
1.1	**Varianten von Schließanlagen**	**6**
1.1.1	**Mechanische Schließanlagen**	**6**
1.1.2	**Mechatronische Schließanlagen (Hybrid-Systeme)**	**7**
1.1.3	**Elektronische Schließanlagen**	**7**
1.2	**Elektronische Zutrittskontrollanlagen (eZKA)**	**7**
1.2.1	**Offline Zutrittskontrollanlage**	**9**
1.2.2	**Online Zutrittskontrollanlage**	**9**
1.3	**Einstufung der Sicherheitsgrade nach DIN 60839-11**	**10**
2	**AUFBAU UND BESTANDTEILE EINER EZKA**	**12**
2.1	**Zutrittskontrollzentrale**	**12**
2.2	**Erfassungseinheit (Leser)**	**12**
2.3	**Sperrelemente**	**13**
2.4	**Identifikationsmittel**	**13**
2.4.1	**Transponder**	**13**
2.4.2	**PIN-Code**	**14**
2.4.3	**Biometrie**	**14**
2.4.4	**Öffnen mittels einer App im Smartphone**	**15**
2.5	**Externe Systeme**	**15**
2.6	**Administrationseinheit**	**15**
2.7	**Energieversorgung**	**15**
3	**SCHNITTSTELLEN ZU ANDEREN FACHBEREICHEN UND GEWERKEN**	**16**
3.1	**Hochbau**	**16**
3.1.1	**Barrierefreiheit**	**16**
3.1.2	**Schließzylinder**	**16**
3.1.3	**Zugangsvarianten**	**16**
3.2	**Elektrotechnik**	**17**
3.2.1	**Stromversorgung und Notstromversorgung**	**17**
3.2.2	**Blitz- und Überspannungsschutz**	**17**
3.2.3	**Gefahrenmeldeanlagen**	**18**
3.2.4	**Kabelnetz und Vernetzungstechnologien**	**18**
3.3	**Aufzüge**	**19**
3.4	**Zuordnung der Kostengruppe nach DIN 276**	**19**
4	**IT UND NETZWERK**	**21**

4.1 Administration 21
4.2 Sicherheit im Netzwerk 22
4.3 Schließplansoftware 22
5 RECHTLICHE BESTIMMUNGEN UND DATENSCHUTZ 24
6 ABNAHME, ÜBERGABE, BETRIEB UND INSTANDHALTUNG 25
6.1 Abnahme 25
6.2 Übergabe an den Betreiber/Nutzer 25
6.3 Betrieb und Instandhaltung 25
7 ABKÜRZUNGEN UND BEGRIFFE 27
8 VERZEICHNISSE 28
8.1 Auswahl wichtiger Normen, Vorschriften, Regelwerke und Arbeitshilfen 28
8.2 Literaturhinweise 29
8.3 Abbildungen und Tabellen 29
ANLAGE: MUSTER-CHECKLISTE FÜR DIE BEDARFSERMITTLUNG 31

Vorwort

Diese Empfehlung beschäftigt sich mit elektronischen Zutrittskontrollanlagen (eZKA) in öffentlichen Gebäuden, insbesondere Verwaltungs- und Bürogebäuden sowie Bildungs- und Kultureinrichtungen. Eine eZKA zeichnet sich zusätzlich zu herkömmlichen Schließanlagen durch einen automatisierten dokumentierten Zu- und ggf. Austritt zum Gebäude aus. Eine eZKA dient also der Steuerung und Dokumentation des Zugangs einzelner Personen oder Personengruppen zu Gebäuden, Gebäudeteilen oder einzelnen Räumen. Personen können unter anderem Mitarbeiter, Besucher, Handwerker, Schüler oder Studenten sein, welche verschiedene Berechtigungen haben, bestimmte Teile eines Gebäudes betreten zu dürfen. Der Zugang kann durch Türen, mit einem Verkehrsmittel über Schranken, oder durch Vereinzelungsanlagen geschehen. Dabei sind die Belange des Sachschutzes, der Organisation, sowie des Datenschutzes zu beachten. Bisher wurden diese Anforderungen durch eine konventionelle Schließanlage mit verschiedenen Schlüsseln und Schlüsselgruppen für die Türen erfüllt.

Die Forderung nach einer eZKA hat die nutzende Verwaltung anhand eines Sicherheitskonzepts zu stellen. Dieser obliegt es, die sicherheitstechnischen Schutzziele zu definieren und die organisatorischen Voraussetzungen zu schaffen.

Elektronische Zutrittskontrollanlagen bestehen in wesentlichen Teilen aus IT-Technik und unterliegen deshalb dem BSI IT-Grundschutz sowie den Technischen Leitlinien des BSI. Bei der Planung, der Beschaffung und der Einrichtung einer eZKA sind frühzeitig die zuständigen IT-Stellen der nutzenden Verwaltung, sowie der Personalrat einzubinden.

Diese Empfehlung richtet sich in erster Linie an die Baudienststellen öffentlicher Verwaltungen sowie den nutzenden Verwaltungen. Sie soll als Orientierungshilfe für Planung, Projektierung, Ausschreibung, Abnahme, Übergabe sowie Betrieb und Instandhaltung einer eZKA dienen, ersetzt im Einzelnen jedoch nicht die Erfahrungen und Kenntnisse eines Planungsingenieurs.

Für Einrichtungen mit erhöhtem Sicherheitspotential und spezifischem Schutzbedarf oder Geheimschutzanforderungen, für Gebäude in denen Personen festgehalten werden, insbesondere dem Polizeibau sowie dem Justizvollzug und speziellen Verfassungsorganen gilt diese Empfehlung nicht abschließend.

Die neue Empfehlung

Planung, Bau und Betrieb von elektronischen Zutrittskontrollanlagen in öffentlichen Gebäuden

(eZKA)

liegt jetzt vor.

Berlin, 04.12.2023

Walter Arnold	Ronald Gockel	Marius Elsner
Vorsitzender des AMEV	FBL des Fernmeldeausschuss	Obmann

1 Grundsätzliche Überlegungen zu Schließanlagen und Zutrittskontrollanlagen

Grundsätzlich sollen eZKA wie auch konventionelle Schließsysteme den diskreten bzw. personenbezogenen Zugang zu Objekten oder Liegenschaften ermöglichen.

Dabei sind die grundlegenden Funktionskomponenten eines konventionellen mechanischen Systems sowie eines elektronischen Schließsystems vergleichbar. Bei beiden Systemen gibt es die Grundkomponenten: Öffnungselement (Türschloss, Motorschloss bzw. Freigabeelement) sowie Ident-Mittel (Schlüssel bzw. Transponder, Chipkarte).

Der Grundgedanke einer elektronischen Zutrittskontrollanlage wie auch einer konventionellen Schließanlage ist die Kontrolle von Zutrittsberechtigungen und die Selektion von Berechtigungsgruppen. Neben den oben genannten Vorteilen, ermöglicht die eZKA mittels geeigneter Ident-Mittel eine Personenidentifikation. Dabei werden alle Personenbewegungen an definierten Zutritten autorisiert und nach Berechtigten und nicht Berechtigten selektiert.

Für Anforderungen mit erhöhtem Sicherheitsbedarf ist darüber hinaus eine Identifikation unter Verwendung von mehrstufigen Identifikationsmerkmalen, ähnlich wie 2-Faktor-Authentifizierungen bei modernen Sicherheitsanwendungen, notwendig. Dies geschieht in der Regel durch Merkmale wie den Besitz (z. B. ID-Karte bzw. Transponder, Smartphone-App), dem Wissen (z. B. Zahlen-Code bzw. Code-Wort) oder biometrische Eigenschaften der Person (z. B. Irisscanner, Fingerabdruck, stimmakustische Merkmale).

Der Bedarf bzw. das Anforderungsprofil bestimmt in erster Linie die Komplexität einer elektronischen Zutrittskontrolle. Bei einem Objekt mit vielen verschließbaren Türen und Berechtigungsszenarien ist der Einsatz einer vernetzen elektronischen Zutrittskontrollanlage in Erwägung zu ziehen, da die Betriebskosten für Administration, Schließplanänderungen, Schlüsselverlust und Skalierbarkeit gering im Vergleich zu einem konventionellen Schließsystem sind. Bei einer geringen Anzahl von Schließmöglichkeiten ist eventuell ein nicht vernetztes System bei einer Wirtschaftlichkeitsbetrachtung zielführender. In speziellen Bereichen oder bei Kleinstanwendungen werden auch in Zukunft konventionelle mechanische Schließanlagen ihre Berechtigung behalten.

1.1 Varianten von Schließanlagen

Als Schließanlage wird ein Schließsystem mit mehreren Schließzylindern, die funktional in Bezug zu einander stehen, bezeichnet. Innerhalb der Gebäude können unterschiedliche Zutrittsrechte vergeben werden. Die Schlüssel können einzelne oder auch unterschiedliche Türen (Gruppen) öffnen**.**

Es gibt grundsätzlich 3 verschiedene technologische Varianten von Schließanlagen:

1.1.1 Mechanische Schließanlagen

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

1.1.2 Mechatronische Schließanlagen (Hybrid-Systeme)

Bei mechatronischen Schließanlagen wird die mechanische Schließung durch ein elektronisches Sperrelement ergänzt. Der Schlüssel wird wie bisher in den Zylinder eingeführt und gedreht.

Abbildung 1: Schlüssel einer mechatronischen Schließanlage (Hybrider Schlüssel)

Im Zylinder kontrollieren die mechanischen Zuhaltungen und der Chip im Elektronikmodul die entsprechenden Codierungen (mechanische als auch elektronische) des Schlüssels und geben bei Berechtigung den Schließvorgang frei.

1.1.3 Elektronische Schließanlagen

Elektronische Schließanlagen unterscheiden sich grundsätzlich von den mechanischen Lösungen. Der Code ist nicht mehr über die Form des Schlüssels gegeben. Die Freigabe für einen Schließvorgang erfolgt ausschließlich auf elektronischem Wege. Ein Identifikationsmerkmal wird elektronisch abgefragt und der Zugang bei Übereinstimmung freigegeben. Der Übergang zur elektronischen Zutrittskontrollanlage ist dabei fließend.

1.2 Elektronische Zutrittskontrollanlagen (eZKA)

Eine Zutrittskontrollanlage gewährt berechtigten Personen den Zugang zu Gebäuden oder Arealen. Zugleich verwehrt sie unbefugten Personen den Zutritt zu bestimmten Bereichen.

Häufig werden Zutrittskontrollanlagen und Zutrittssteuerungsanlagen synonym zueinander verwendet, wenngleich es marginale Unterscheidungsmerkmale gibt, auf die in dieser Empfehlung nicht weiter eingegangen wird.

Elektronische Zutrittskontrollanlagen haben im Vergleich zu konventionellen Schließanlagen einen höheren Investitionsbedarf, bieten aber nicht nur hinsichtlich einer effizienten Bewirtschaftung und komfortablen Administration einen deutlichen Mehrwert, sondern auch bei komplexeren Anlagen ein erhebliches Einsparpotential bei Anpassungen und Änderungen.

Einer der wesentlichsten Aufgabe einer elektronischen Zutrittskontrollanlage ist das unterscheiden, wem, wo und wann Zutritt in einen definierten Bereich gewährt wird. Die Kategorien „Wo“ und „Wann“ beziehen sich auf örtliche und zeitliche Merkmale, welche in der Regel auf organisatorischen Festlegungen beruhen. Der Kategorie „Wem“ kommt dabei eine besondere Rolle zu. Hier wird zwischen Verifikation des Ident-Mittels bzw. Identifikation der Person unterschieden.

Im Zusammenhang mit dem Begriff „elektronische Zutrittskontrollanlage“ wird auch häufig der Begriff „elektronische Schließanlage“ verwendet. Dabei kommen ebenfalls die Verfahren zur Identifikation und Verifikation von Zutrittsberechtigten sowie die zentrale Administration von Schließberechtigungen und Schlüsselverwaltung zum Einsatz. Das dokumentieren von Zutritten nach den Gesichtspunkten „Wem“, „Wann“ und „Wo“ ist mit elektronischen Schließanlagen nicht möglich.

Der entscheidende Unterschied zwischen einer konventionellen bzw. einer elektronischen Schließanlage und einer elektronischen Zutrittskontrollanlage liegt somit in der Kontroll- und Dokumentationsfunktion. Aus diesem Grund kann es z. B. für Einrichtungen mit erhöhtem Sicherheitspotential sogar zwei parallele Systeme geben - eine elektronische Schließanlage für alle Türen (Mitarbeiter) sowie eine Zutrittskontrollanlage mit Schleusen, Drehkreuzen, Vereinzelungsanlagen teilweise sogar je nach Erfordernis inkl. Videoüberwachung (Kontrolle berechtigte Personen, Besucher, Handwerker etc.).

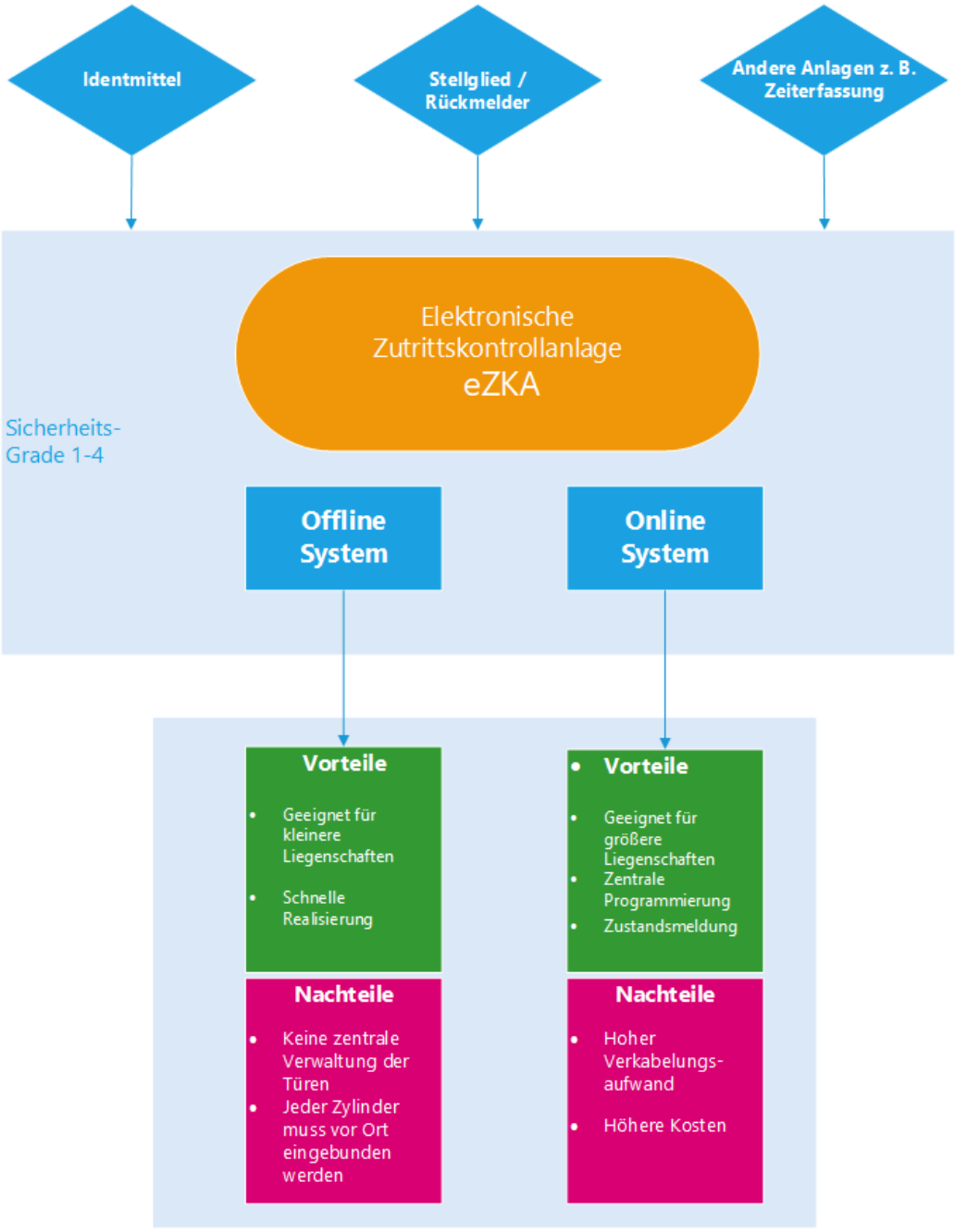

Abbildung 2: Übersicht einer eZKA

1.2.1 Offline Zutrittskontrollanlage

Die offline Zutrittskontrollanlage funktioniert ohne Verkabelung der Schließzylinder bzw. Freigabeelemente untereinander und ist nicht mit einem Datennetz verbunden. Die Nutzungsberechtigungen werden zentral an einem PC in einer Datenbank vorgenommen und mittels eines lokalen Programmiergerätes bzw. Programmierschlüssels übertragen, um anschließend dem einzelnen Zylinder neue Freigabeinformationen zu erteilen. Dafür muss jeder betroffene Zylinder aufgesucht werden (Turnschuhadministration). Für dieses Konzept entfällt die aufwändige Verkabelung in einem Gebäude. Geht ein Ident-Mittel verloren, ist eine Neuadministration der betroffenen Türen notwendig und kann je nach Schließberechtigung eine komplette Gebäudebegehung notwendig machen. Dieser Aufwand kann lediglich vermieden werden, wenn das Ident-Mittel bereits durch eine Zeitbegrenzung nicht mehr gültig ist.
Je nach Gebäudenutzung, betrieblicher Organisation und Anzahl der Türen ist abzuwägen, ob der Administrationsaufwand einer offline Schließanlage noch wirtschaftlich ist. Die Montage und Nachrüstbarkeit bei offline Anlagen sind ohne größeren Aufwand möglich.

1.2.2 Online Zutrittskontrollanlage

Bei der online Zutrittskontrollanlage werden mit Hilfe eines kabelgebundenen oder funkbasierten Netzwerkes die Berechtigungsinformationen der Schließzylinder zentral von einem PC-Arbeitsplatz programmiert und ausgelesen. Es können z. B. Türzustände und der Batteriestatus über das Netzwerk gemeldet werden. Jede Berechtigungsänderung kann ohne Zeitverzögerung an die jeweiligen Zutrittspunkte übertragen werden, ohne dass der entsprechende Zutrittspunkt aufgesucht werden muss.
Bei Neubauten können diese Netzwerke effizient geplant und in das anwendungsneutrale Kommunikationsnetzwerk integriert werden. In bestehenden Gebäuden steigt demgegenüber der Aufwand für die flächendeckende Nachrüstung der Verkabelung. Funkbasierte Lösungen sind insbesondere bei einer Nachrüstung in einem bestehenden Gebäude eine an den Kosten angemessene Alternative zu drahtgebundenen Netzwerken. Das Netzwerk wird durch das Setzen von Accesspoints realisiert. Die genaue Anzahl sollte durch eine Funkfeldausleuchtung festgelegt werden.

Virtuelle Zutrittskontrollanlage

Eine oft erwähnte Funktionalität ist die sogenannte virtuelle Zutrittskontrollanlage**.** Diese wird bei den verschiedenen Herstellern unterschiedlich benannt, beinhaltet aber im Prinzip die Leistungsmerkmale eines online Systems. Auch hier werden die Änderungen in der Datenbank vorgenommen und meist online an einen oder mehrere Ident-Mittel-Leser übertragen. Sobald ein Ident-Mittel an diesem Leser bucht, werden ihm die geänderten Daten übertragen. Bei jeder Nutzung an einer offline Komponente werden dessen Zutrittsdaten durch das Ident-Mittel aktualisiert. Auf gleichem Wege gelangen auch die Ereignisse und der Batteriestatus über die online Leser zurück in die Zentrale.

1.3 Einstufung der Sicherheitsgrade nach DIN 60839-11

Aus einem Sicherheitskonzept der nutzenden Verwaltung muss hervorgehen, welcher Sicherheitsgrad nach DIN EN 60839-11-1 [01] angemessen erscheint. In der DIN EN 60839-11-1 [01] und 2 [02] sind umfangreiche Tabellen enthalten, in denen die notwendigen und optionalen Leistungsmerkmale in Abhängigkeit vom einzuhaltenden Grad einer Zutrittskontrolle dargestellt werden. Mit der nutzenden Verwaltung ist von den Baudienststellen abzustimmen, welche der optionalen Leistungsmerkmale für Sicherheit und Organisation benötigt werden. Hierfür kann die beigefügte Checkliste hilfreich sein.

Für Zutrittskontrollsysteme werden in der DIN EN 60839-11-1 [01] folgende Grade festgelegt:

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

Weiterführende Hinweise zu den Graden finden sich in Tabelle 1 der DIN EN 60839-11-1 [01].

Es ist auch möglich, dass für einzelne Bereiche, wie in Abbildung 3 beispielhaft dargestellt, verschiedene Grade festgelegt werden. Zu beachten ist dabei, dass die zentralen Einrichtungen der eZKA immer in einem Bereich installiert werden, der mit dem höchsten verwendeten Grad gesichert ist.

Ein wesentlicher Punkt bei der Planung einer eZKA ist die Auswahl der zur Identifikation vorzusehenden technischen Einrichtungen. Je nach Sicherheitsbedürfnis kann der Zutritt durch Lesegeräte mit unterschiedlichen Identifikationsmethoden bzw. Kombinationen daraus durch Identifikationsverfahren gewährt werden. In praktischen Anwendungen werden heutzutage zumeist Ausweise bzw. Transponder als Ident-Mittel eingesetzt, jedoch bekommen auch die biometrischen Ident-Mittel vor allem in Kombination bei hohen Sicherheitsanforderungen eine immer größere Bedeutung. Der PIN-Code beispielsweise als ausschließliches Ident-Mittel wird kaum noch eingesetzt.

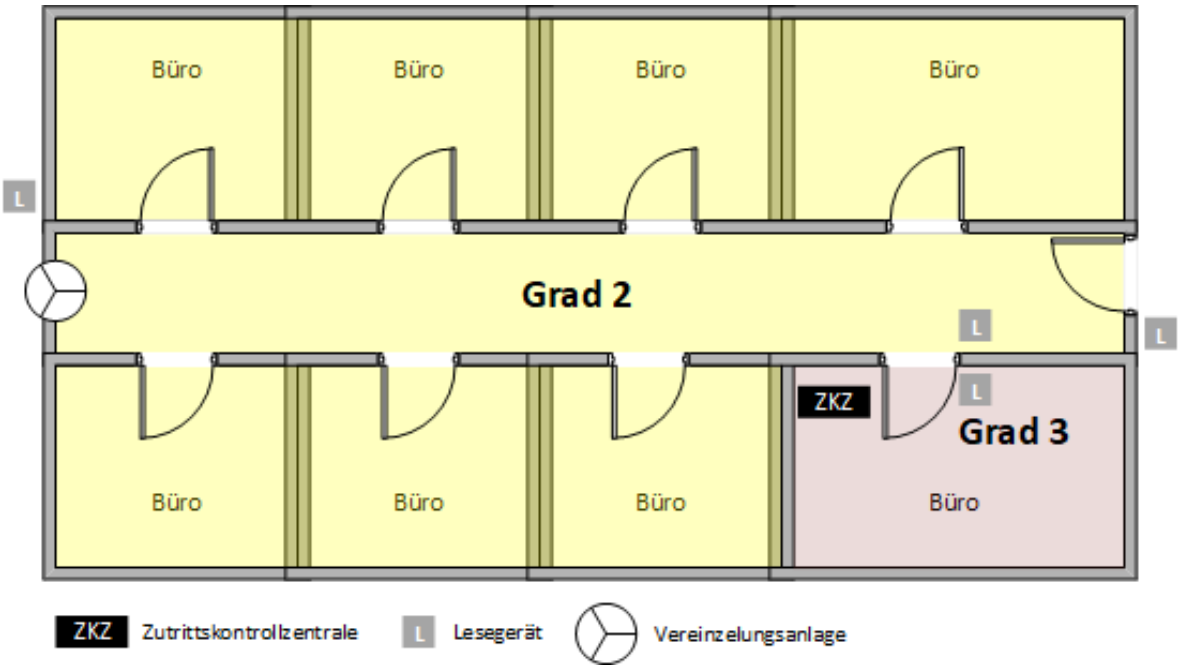

Abbildung 3: Beispielhafte Zutrittskontrollanlage

Die Lesegeräte müssen ab Grad 2 sabotageüberwacht ausgeführt werden. Jeder Zutrittspunkt einer Zutrittskontrollanlage muss nach positiver Identifikation den Zutritt in mindestens einer Richtung gewähren. Ab Grad 2 ist durch Rückmeldung von der zu öffnenden Tür zu überwachen, ob die Tür tatsächlich geöffnet wurde und ob die Tür nach der Öffnung innerhalb einer festzulegenden Zeit wieder geschlossen wurde. Wenn die Zeit für den Verschluss der Tür überschritten wird, muss ein Alarm ausgelöst werden, der eine festzulegende Reaktion (z. B. Alarmierung eines Wachdienstes) veranlasst. Für den Störungsfall (z. B. Stromausfall) ist festzulegen, ob sich die Türen dann automatisch öffnen oder ob sie verschlossen bleiben sollen.

Zusätzlich zur Zutrittskontrolle ist u. U. der Einsatz des Ident-Mittels erforderlich, um den gesicherten Bereich verlassen zu können (Abgangskontrolle).

Es ist somit bei Anlagen ab Grad 2 eine Plausibilitätskontrolle möglich und ab Grad 3 vorgeschrieben, d. h. der Ausgang wird verwehrt, wenn zuvor kein ordnungsgemäßer Zutritt erfolgt ist. Ebenso kann der Zutritt verwehrt werden, wenn der Inhaber des Ident-Mittels sich aus Sicht der Anlage bereits im gesicherten Bereich aufhält. Durch diese Maßnahme kann sichergestellt werden, dass alle Zutritte und Abgänge ordnungsgemäß registriert werden und sich nicht zutrittsberechtigte Personen mit in den gesicherten Bereich einschleusen lassen, ohne dass dies registriert wird. Grundsätzlich können für Zu- und Abgangskontrollen unterschiedliche Identifikationsklassen festgelegt werden. Der Einsatz einer Abgangskontrolle ist mit der nutzenden Verwaltung abzustimmen. Normative Vorgaben hierzu bestehen nicht.

2 Aufbau und Bestandteile einer eZKA

Der grundsätzliche systemtheoretische Aufbau einer elektronischen Zutrittskontrollanlage wird in der DIN EN 60839-11-1 [01] vorgegeben und folgt dabei dem in Abbildung 4 dargestellten schematischen Aufbau. Dabei bildet die Zutrittskontrollzentrale die steuernde und verarbeitende Instanz mit den dazugehörigen Peripherieeinheiten wie Energieversorgung, Sperrelemente, Erfassungseinheiten und externe Schnittstellen.

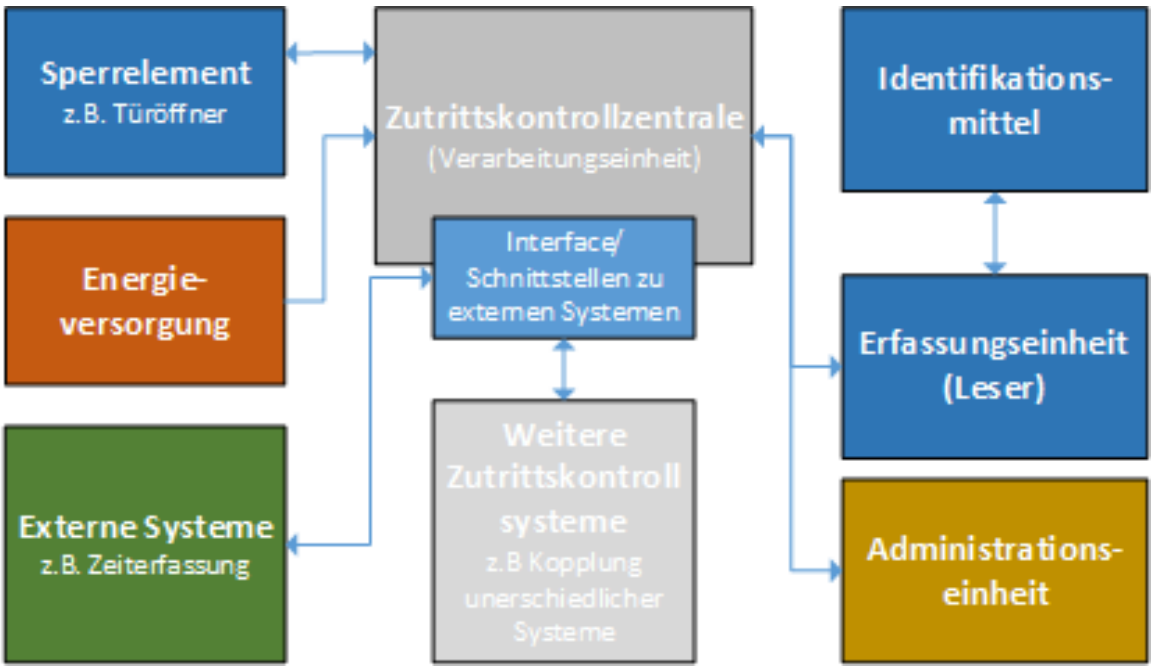

Abbildung 4: Schematischer Aufbau einer Zutrittskontrollanlage

2.1 Zutrittskontrollzentrale

Sie ist das zentrale Element einer online Zutrittskontrollanlage. In ihr werden alle programmierten Berechtigungsdaten gespeichert und verwaltet. Gleichzeitig wird der gewünschte Zutritt nach Berechtigung geprüft und ggf. freigegeben.

2.2 Erfassungseinheit (Leser)

Die Erfassungseinheit ist die Kontaktstation des Systems mit dem Ident-Mittel. Der Leser wandelt die physikalische Codierung des Identifikationsträgers in elektrische Signale um und leitet sie zur Auswertung weiter an die Zutrittskontrollzentrale.

Erfassungseinheiten sind beispielsweise

- RFID Leser,
- Kamera,
- Mikrofon,
- Biometrischer Leser und
- Tastenfeld.

2.3 Sperrelemente

Sperrelemente oder auch Zutrittskontroll-Stellglieder (ZSG) genannt, sind notwendige Bauteile für eine ordnungsgemäße Funktion einer Zutrittskontrollanlage. Der Durchlass an Türen, Tore, Schleusen usw. soll mittels dieser elektromechanischen Bauelemente zuverlässig gesperrt und kontrolliert geöffnet werden können.

Sperrelemente/ Freigabeelemente sind beispielsweise

- Türöffner,
- eine Kombination von selbstverriegelndem Panikschloss mit motorischem Türöffner,
- elektromagnetische Schlösser,
- Motorschlösser, Motorzylinder,
- motorisch betriebene Türriegel,
- elektromagnetische Türverriegelung (Haftmagnete),
- elektromechanische Zargenschlösser,
- Drehkreuze, Drehsperren und
- Schranken.

2.4 Identifikationsmittel

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

Identifikationsmittel sind beispielsweise

- Transponder (aktiv oder passiv) / Karte,
- PIN Code (Persönliche Identifikationsnummer),
- Biometrie (z. B. Auge, Finger, Handvenenscanner),
- Schlüssel mit integriertem Transponder,
- App auf Smartphone,
- Barcode und
- Magnetstreifen.

2.4.1 Transponder

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

Aktive Transponder verfügen über eine eigene Energieversorgung durch eine eingebaute Batterie. Sie haben in der Regel eine größere Kommunikationsreichweite.

Bei passiven Transpondern erhält dieser die Energie über ein magnetisches Feld aus dem Leser.

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

RFID (Radio Frequency Identifikation) bedeutet übersetzt die Identifikation mittels elektromagnetischen Wellen, wodurch eine berührungslose Identifizierung möglich ist.

Ein RFID-System besteht aus einem Transponder, der als Schlüssel dient und einem Lesegerät.

Das Lesegerät erzeugt ein hochfrequentes elektromagnetisches Wechselfeld, in welches der Transponder eingebracht werden muss. Ein Mikrochip im RFID-Transponder wertet die vom Lesegerät gesendeten Befehle aus, generiert eine Antwort und sendet diese zurück an das Lesegerät, welches diese auswertet. Der Transponder erzeugt dazu selbst kein Feld, sondern beeinflusst das elektromagnetische Feld des Lesegeräts.

Abbildung 5*:* Chip-Karte mit nicht sichtbarem RFID Transponder

Abbildung 6: Transponder als Schlüsselanhänger

2.4.2 PIN-Code

Sperrelemente mit PIN-Code benötigen einen gewählten PIN, den man eingeben muss, damit der Zugang gewährt wird.

Gerade für Einzeltüren ist ein Öffnen mittels PIN eine einfache Möglichkeit den Zugang freizugeben. In größeren Zutrittskontrollanlagen findet eine Identifizierung mittels PIN in der Regel keine Anwendung.

2.4.3 Biometrie

Mit geeigneten Lesegeräten können als Ident-Mittel auch Körperteile genutzt werden. Diese Art der Identifizierung wird als biometrische Identifikation bezeichnet, wobei Körpermerkmale wie Fingerabdrücke, Handvenen, Gesichts-, oder Irismuster erfasst und ausgewertet werden.

2.4.4 Öffnen mittels einer App im Smartphone

Eine Identifizierung über ein Smartphone mit passender App ist möglich. Diese Option für das Öffnen eines Zugangs setzt voraus, dass der Benutzer ein dienstliches Smartphone besitzt. Für öffentliche Gebäude wird aus datensicherheitstechnischen Gründen empfohlen diese Technik nicht einzusetzen.

2.5 Externe Systeme

Wird zur Identifizierung ein Transponder oder eine Chipkarte verwendet, so können diese für weitere Anwendungsbereiche und Zusatzdienste Verwendung finden.

Dienstausweis

Eine Chipkarte als Zugangsberechtigung kann beliebig gestaltet werden, so dass die Möglichkeit besteht, diese als Dienstausweis zu bedrucken, um sich innerhalb des Gebäudes jederzeit ausweisen zu können.

Es muss jedoch berücksichtigt werden, dass bei Verlust der Chipkarte für den Finder leicht ersichtlich ist, zu welcher Behörde/Organisationseinheit die Karte gehört und somit Unbefugten leicht Zutritt gewährt werden kann.

Zeiterfassung

Das Ident-Mittel einer eZKA kann in Verbindung mit einer elektronischen Arbeitszeiterfassung genutzt werden, um den Beginn und das Ende der täglichen Arbeitszeit zu erfassen.

Eine Zeiterfassung ist auch automatisiert über den Zutritt zum Gebäude, oder zu bestimmten Einheiten möglich. So kann die Erfassung des Betretens des Gebäudes als Kommen-Buchung und das Verlassen des Gebäudes als Gehen-Buchung gewertet werden.

Kopierer

Viele Kopiergeräte bieten den Modus des „Sicheren Drucks“. Hierbei wird der Druck über den Arbeitsplatz PC ausgelöst und auf den Druckserver geladen. Anschließend muss ein Drucker aufgesucht werden und die druckende Person muss sich am Drucker identifizieren. Erst dann wird der eigentliche Druckvorgang in Anwesenheit der Person gestartet.

Weitere Nutzungsmöglichkeiten

Neben den bereits genannten Nutzungen bieten die Identifikationsmittel weitere Möglichkeiten. So können diese als aufladbare Geldkarte zur Bezahlung in einer Mensa, oder an Kaffee- und Getränkeautomaten genutzt werden. Im Hochschulbereich ist auch die Nutzung als Bibliotheksausweis zur Leihe von Büchern üblich.

2.6 Administrationseinheit

Abhängig vom Hersteller der eZKA wird diese üblicherweise durch eine Computersoftware administriert. Weitere Infos hierzu sind im Abschnitt 4 IT und Netzwerk zu finden.

2.7 Energieversorgung

Der Abschnitt 3.2.1 befasst sich tiefergehend mit dem Thema der Energieversorgung im Normalbetrieb, sowie bei Netzausfall.

3 Schnittstellen zu anderen Fachbereichen und Gewerken

Bei einer eZKA gibt es häufig Schnittstellen zu anderen Gewerken und technischen Anlagen, die im Rahmen der Planung, Projektierung und des Betriebs der eZKA beachtet werden müssen.

3.1 Hochbau

3.1.1 Barrierefreiheit

Die jeweilige Landesbauordnung (LBO) regelt, in welchem Umfang öffentliche Gebäude barrierefrei sein müssen. Zu beachten ist, dass durch den Einbau der eZKA keine weiteren baulichen Barrieren geschaffen werden.

Die DIN 18040-1 [03] als zentrale Norm für Barrierefreies Bauen geht nicht explizit auf Schließanlagen ein. Unter Punkt 4.3.3.2 der Norm findet sich als Angabe für die Höhe von Tastern eines automatischen Türsystems eine mittlere Höhe von 85 cm. Diese Höhe kann sinngemäß auch auf Lesegeräte und Terminale von elektronischen Schließanlagen übertragen werden.

3.1.2 Schließzylinder

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

Die elektronischen Schließzylinder müssen den Anforderungen und Abmessungen uneingeschränkt der DIN 18252 [04] bzw. DIN EN 1303 [05] entsprechen, um diese in dafür vorgerichtete Einsteckschlösser nach DIN 18250 [06] oder DIN 18251 [07] montieren zu können, ohne dass Änderungen an den Türen oder Türbeschlägen und zusätzliche Bohrungen erforderlich sind. Lieferung und Einbau obliegt dem Errichter der eZKA.

Abbildung 7: Beispiel eines elektronischen Schließzylinders

3.1.3 Zugangsvarianten

Elektrische Türantriebe und selbstschließende Türen

Neben den manuell zu öffnenden Türen gibt es eine Vielzahl verschiedener Systeme von automatisch öffnenden Türen, wie beispielsweise Türen mit Unterflurantrieb, Drehflügelantrieb oder automatische Schiebetüren.

Auch bei der Ansteuerung gibt es unterschiedliche Systeme, wie zum Beispiel eine manuelle Ansteuerung oder die Ansteuerung über Näherungssensoren.

Hier muss für jedes Türantriebssystem individuell und herstellerspezifisch geprüft werden, ob und wie eine Einbindung in eine eZKA möglich ist. Allen gemeinsam ist jedoch, dass sichergestellt werden muss, dass sich beide Systeme nicht gegenseitig blockieren. So darf z. B. der Türantrieb nicht gegen eine abgeschlossene Tür arbeiten. Ebenso darf eine offenstehende Tür nicht verriegelt werden.

Bei Brandschutzanforderungen werden selbstschließende Türen mit und ohne Offenhaltung eingesetzt. Bei diesen Türen ist ebenso sicherzustellen, dass sie im geöffneten Zustand nicht abgeschlossen werden können, da ansonsten eine zuverlässige Selbstschließung nicht mehr gewährleistet werden kann.

Fluchttüren

Flucht- und Rettungswege müssen jederzeit frei zugänglich sein, um im Notfall eine zügige Evakuierung des Gebäudes gewährleisten zu können. Diese dürfen nicht durch abgeschlossene Türen versperrt werden, wobei gleichzeitig nicht alle Räume außerhalb eines Notfalls betreten werden dürfen. Um dieses Problem zu lösen, werden dazu Fluchttürsteuerungen eingesetzt. Soll eine eZKA in Flucht- und Rettungswegen eingesetzt werden, sind die Regelungen der Richtlinie über elektrische Verriegelungssysteme von Türen in Rettungswegen (EltVTR) [16] zu beachten.

Sonderformen und weitere Zugangsmöglichkeiten

Neben den bereits genannten Tür-Arten gibt es weitere Zugangsmöglichkeiten zu Gebäuden oder Geländen. Häufig vertreten sind beispielsweise Vereinzelungsanlagen in Form von Drehkreuzen oder Sicherheitsschleusen. Waagen, welche sicherstellen, dass Dinge die in ein Gebäude gebracht werden, auch wieder voll ständig mit herausgenommen werden, finden sich häufig im Bereich der Justiz. Auch solche Anlagen lassen sich in eine Zutrittskontrollanlage integrieren. Solche Anforderungen sind stets auf die Systeme der beteiligten Hersteller anzupassen und mit diesen abzustimmen.

3.2 Elektrotechnik

3.2.1 Stromversorgung und Notstromversorgung

Gemäß DIN EN 60839-11-1 [01] und -2 [02] wird für eine elektronische Zutrittskontrollanlage eine des entsprechenden Sicherheitsgrades zugehörende Notstromversorgung gefordert. Nach dieser Norm müssen eZKA für die Sicherheitsgrade 3 und 4 ihre Funktionsfähigkeit bei Netzspannungsausfall für 2 bis 4 Stunden beibehalten.

Ist eine zentrale Notstromversorgung vorhanden oder aus wirtschaftlichen Gründen geplant, kann die eZKA mit an dieser angeschlossen werden.

Ist keine zentrale Notstromversorgung vorhanden oder geplant, muss eine dezentrale Notstromversorgung aufgebaut werden.

3.2.2 Blitz- und Überspannungsschutz

Für die Integration der Zutrittskontrollanlage in den inneren Blitzschutz sind die aktuell gültigen normativen Vorgaben sowie der Stand der Technik maßgebend. Bei Lesegeräten an Schranken, Drehkreuzen oder Säulen im Außenbereich sind die

Schutzmaßnahmen anhand der jeweiligen Blitzschutzzone des Gebäudes in der die Objekte liegen nach normativer Lage zu definieren.

Weitere Hinweise zum Blitz- und Überspannungsschutz, sowie Erdungssystemen sind der AMEV EltAnlagen *Planung und Bau von elektrischen Anlagen in öffentlichen Gebäuden* [08] zu entnehmen.

3.2.3 Gefahrenmeldeanlagen

Beim Betrieb einer Gefahrenmeldeanlage z. B. Einbruch- und Überfallmeldeanlage (EMA/ÜMA) oder Brandmeldeanlage (BMA) können weitere Schnittstellen zur eZKA zur Umsetzung von Sicherheitskonzepten entstehen.

Bei der Planung einer eZKA in Verbindung mit einer BMA ist eine Abstimmung mit der zuständigen Brandschutzdienststelle bzw. Feuerwehr erforderlich. Beispielsweise muss festgelegt werden, dass sich im Feuerwehrschlüsseldepot -analog zu den geforderten Generalschlüsseln- ein Generalchip befindet, der Zugang zu allen (elektronisch) verriegelten Bereichen gewährt.

Die für eine EMA/ÜMA (siehe AMEV EMA/ÜMA *Planung, Bau und Betrieb von Gefahrenmeldeanlagen für Einbruch, Überfall und Geländeüberwachung in öffentlichen Gebäuden* [09]) gemachten Hinweise bezüglich Gefährdungsbeurteilung und Erstellen eines Sicherungskonzeptes gelten sinngemäß auch für eZKA.

3.2.4 Kabelnetz und Vernetzungstechnologien

Im Zuge der Planung und Festlegung der Art der eZKA wird empfohlen rechtzeitig die Planung der Verkabelung der jeweiligen Komponenten vorzunehmen. In vielen Fällen kann die eZKA in ein vorhandenes Netzwerk eingebunden werden. Hierfür müssen, wie im Abschnitt 4 beschrieben, unbedingt die zuständigen Netzwerkadministratoren rechtzeitig in die Planung mit aufgenommen werden.

Die Verkabelung der einzelnen Komponenten einer eZKA ist über verschiedene Technologien möglich und wird in erster Linie durch den jeweiligen Hersteller und der Art der eZKA festgelegt. Nachfolgend soll nur ein kurzer Überblick über die jeweiligen Möglichkeiten dargestellt werden.

- LAN (Local Area Network): In vielen Fällen können einzelnen Komponenten in ein vorhandenes LAN integriert werden. Hierbei erfolgt die Kommunikation über die Ethernet Technologie. Die Verkabelung wird über spezifizierte Datenkabel realisiert. Einzelne Komponenten können mittels PoE (Power over Ethernet) mit Spannung versorgt werden. Die LAN Verkabelung ist in den meisten Fällen nicht proprietär und somit für verschiedene Hersteller anwendbar.

- RS-485 (oder EIA-485): Hierbei handelt es sich um einen Industriestandard (standardisierter Bus). Die einzelnen Komponenten werden mittels einer Bus-Verkabelung in eine eZKA eingebunden. RS 485 nutzt hierfür ein einfaches Leitungspaar (2-Draht). Die Kommunikation erfolgt in den meisten Fällen durch proprietäre Protokolle. Die 2-Draht Verkabelung ist einfach zu verlegen. Die Spannungsversorgung erfolgt ebenfalls über die Verkabelung.

- Funk: Viele Hersteller können einzelne Komponenten mittels Funkschnittstelle in die eZKA einbinden. Dies erspart oft einen größeren Verkabelungsaufwand. Die einzelnen Funkgateways werden entweder in das LAN oder den Bus eingebunden. Im Falle einer Anbindung über Funk sollte im Vorfeld eine Funkausleuchtung durchgeführt werden.

- Wiegand: Wiegand ist eine unidirektionale Schnittstelle. Diese bietet ebenfalls die Möglichkeit z. B. Kartenleser mit dem Rest einer elektronischen Zutrittskontrollanlage zu verbinden. Viele Hersteller ermöglichen die Anschaltung von sogenannten Drittanbietern auf Basis der Wiegand-Schnittstelle.

- Koax-Schnittstelle: Dies sollte nur bei der Planung der Verkabelung berücksichtigt werden. Eine technische Notwendigkeit stellt diese Schnittstelle nicht dar.

Für alle Technologien gibt es Grenzwerte für Leitungslängen und je nach Leitungslänge Grenzwerte für die Querschnitte. Dies ist in der Planung zu berücksichtigen.

Nach Festlegung der Vernetzungstechnologie ist es sinnvoll ein Kabelschema zu erstellen. Hierfür werden alle Komponenten der eZKA aufgelistet und mit der jeweiligen Anschlussart versehen. Bei der Einbindung von Türen sollte im Vorfeld eine Abstimmung mit dem Objektplaner erfolgen. In vielen Fällen werden die elektrischen Türöffner und andere Türkontakte über die Zentrale der eZKA angesteuert oder die eZKA erhält entsprechende Zustandsmeldungen. Der Übergabepunkt der Gebäudeverkabelung zur Tür sollte im Vorfeld geklärt werden. Dies sollte auch bei Komponenten, welche bei anderen Gewerken eingebunden sind (z. B. Aufzug) rechtzeitig durchgeführt werden.

Für die allgemeine Spannungsversorgung sollte ebenfalls eine Abstimmung erfolgen. Hierbei ist insbesondere die Spannungsversorgung der eZKA-Zentrale von Bedeutung. Ggf. ist eine Einbindung in eine USV (Unterbrechungsfreie Spannungsversorgung) notwendig. Einige Komponenten der eZKA (z. B. Motorschlösser, Drehkreuze, Schleusenanlagen) benötigen ebenfalls einen elektrischen Anschluss, welcher in der Planung zwingend zu berücksichtigen ist.

3.3 Aufzüge

Bereiche außerhalb des Höhenniveaus des Erdgeschosses werden in der Regel durch Treppen und Personenaufzüge erschlossen. Öffnet der Aufzug in Bereiche, welche durch eine eZKA abgetrennt sind, so ist der Aufzug zwingend in die eZKA einzubinden. Dies kann beispielsweise über ein Lesegerät im Bereich des Aufzugbedienfelds, welches dieses freigibt, geschehen.

3.4 Zuordnung der Kostengruppe nach DIN 276

In der Vergangenheit waren konventionelle Schließanlagen, die im Wesentlichen den Ersatz für eine mechanische Schließanlage abdeckten, nach DIN 276 [10] in KG 399 zu veranschlagen.
Da heute in den wenigsten Fällen eine konventionelle mechanische Schließanlage bzw. Zutrittskontrolle zum Einsatz kommt, ist die wesentliche Struktur der Anlage

zumeist von elektronischen Bauteilen bestimmt. Es sind bei der Planung und Auslegung der Anlagen Fachkenntnis der Elektrotechnik bzw. Sicherheitstechnik erforderlich, daher sollten elektronische Schließanlagen bzw. Zutrittskontrollanlagen in der KG 456 veranschlagt werden.

4 IT und Netzwerk

eZKA bestehen aus Anlagenteilen und Komponenten welche untereinander vernetzt sind und in das IT-Netz der Dienststelle eingebunden werden sollen.

In den meisten Fällen ist ein betriebsfertiges Netzwerk schon vorhanden, so dass die neu zu errichtende eZKA hier eingebunden werden kann. Der hierfür verantwortliche Netzwerkadministrator muss frühzeitig in die Planung mit eingebunden werden, damit u. a. die Netzwerkadressen, Verfügbarkeit und Sicherheit geplant und vergeben werden können.

Bei der Einbindung in ein lokales Netzwerk (LAN), was am häufigsten der Fall sein wird, müssen die entsprechenden Voraussetzungen bei den Komponenten und im LAN vorhanden sein.

Hinweise zur Planung von anwendungsneutralen Kommunikationsnetzwerken findet man in der AMEV Empfehlung: *LAN - Planung, Bau und Betrieb von anwendungsneutralen Kommunikationsnetzwerken in öffentlichen Gebäuden* in der jeweils aktuellen Fassung [11].

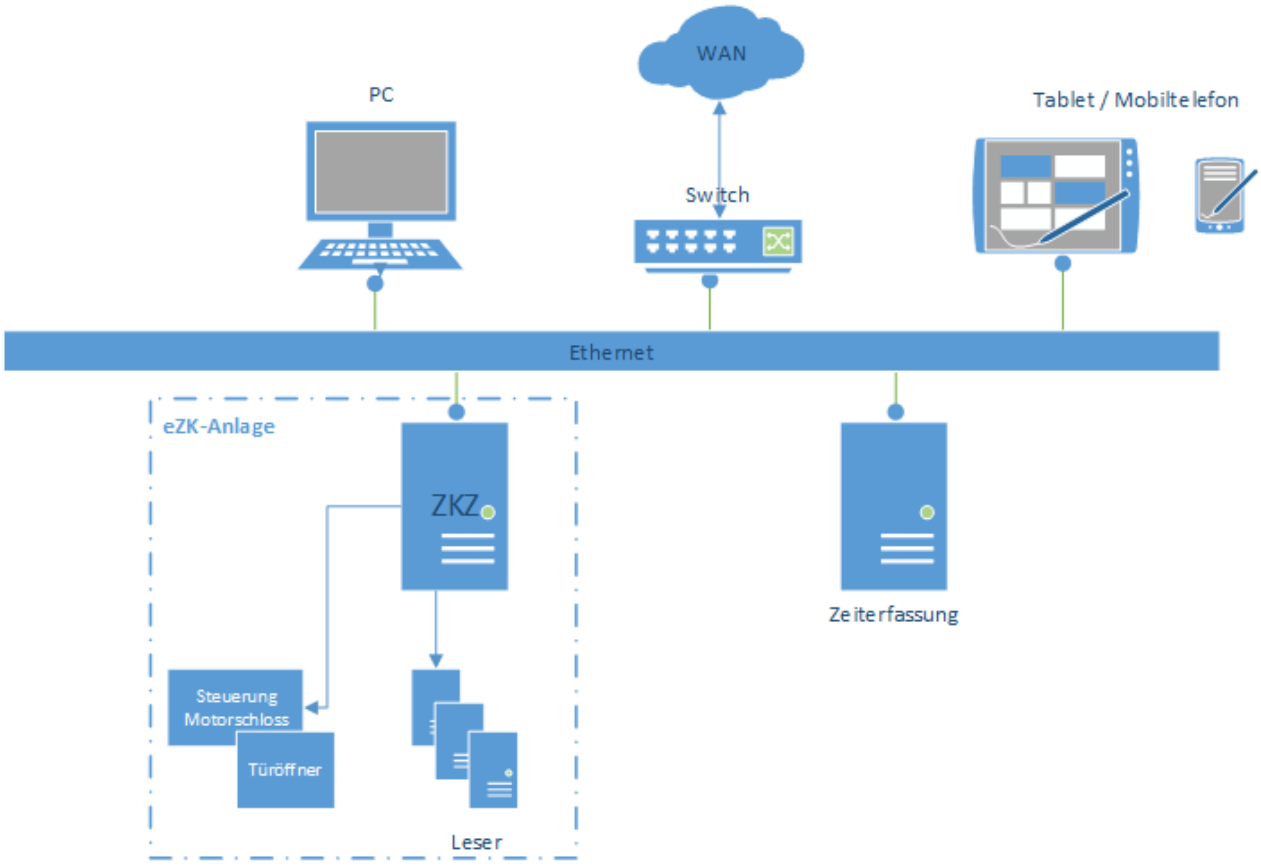

Abbildung 8: Schematische Darstellung der Einbindung einer Zutrittskontrollanlage im LAN

4.1 Administration

Folgende Punkte müssen u. a. bei der Abstimmung mit den zuständigen Netzwerkadministratoren und dem Auftragnehmer präzisiert werden:

- Zur Anbindung an das LAN müssen freie Ports am Switch verfügbar sein. Die Verfügbarkeit und Freigabe der einzelnen Ports erfolgt von der IT.

- Falls zur Versorgung der Komponenten PoE benötigt wird, müssen PoE-fähige Switche oder Powerpanels installiert werden.
- Auflistung der MAC-Adressen der einzelnen Komponenten und Weitergabe an die zuständigen Systembetreuer.
- Vergabe der IP-Adressen. Im LAN hat jeder Netzteilnehmer eine eigene IP-Adresse. Die Vergabe erfolgt von den zuständigen Systembetreuern.

4.2 Sicherheit im Netzwerk

Vereinfacht sprechen wir bei der Einbindung der eZKA in das LAN von einer Anwendung, welche im LAN betrieben wird. Letztendlich sind die zuständigen Systembetreuer für die Sicherheit (abhängig vom IT-Sicherheitskonzept der Liegenschaft) im LAN zuständig. Die hierfür erforderlichen BSI-Richtlinien sind zu beachten.

4.3 Schließplansoftware

Im Schließplan ist die Dokumentation einer Schließanlage dargestellt und die Zutrittsberechtigungen sind hinterlegt. Gleichzeitig stellt die Schließplansoftware die Schnittstelle zwischen Bedienoberfläche und technischen Anlagenkomponenten hinsichtlich ihrer Verwaltung und Administration dar.

Die Schließplansoftware unterstützt den Nutzer bei der Ausgabe und Registrierung der Ident-Mittel, Programmierung der Schließzylinder mit aktuellen Berechtigungen und Sperrung vorhandener Ident-Mittel bei Verlust oder Diebstahl.

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

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

Im Vorfeld der Anlagenplanung ist das Anforderungsprofil an die Software genau zu definieren.

Übliche Leistungsmerkmale einer Schließplansoftware sind beispielsweise

- Client/Server System,
- Datenbank gestützt,
- Import-/Export-Funktionen über Standard Datenformate,
- Offene Systemarchitektur, die sich problemlos in bestehende EDV-Umgebung einbinden lässt,
- Standortverwaltung mit Visualisierung der Gebäudestruktur,
- Visualisierung von Tabellen,
- Integration von verschiedenen Transpondersystemen in einen Stammsatz,
- Systemzugriff über Passwortschutz,
- schnelle Revisionsfähigkeit,
- Hilfe-/ Suchfunktionen,
- Erstellung, Verwaltung und Änderung von Schließplänen,

- Änderungen der Schließberechtigung für vorhandene Schlüssel / Karten und Zylinder,
- Sperrung und Entsperrung von verlorengegangenen Ident-Mittel und
- Programmieren von Ident-Mitteln mit automatischer Kopie der alten Grundeinstellung der Schließberechtigung.

5 Rechtliche Bestimmungen und Datenschutz

Elektronische Zutrittskontrollanlagen bieten vielfältige Möglichkeiten Daten zu erfassen, zu speichern und zu verarbeiten. Idealerweise sollen solche Systeme jedoch keine oder nur notwendige personenbezogene Daten erheben oder verarbeiten.

Ihr Einsatz muss konform mit dem geltenden Datenschutzrecht sein. Die geltende EU-Datenschutzgrundverordnung sowie das Bundesdatenschutzgesetz sind zu beachten. Der Betreiber (in der Regel die hausverwaltende Dienststelle) einer Zutrittskontrollanlage ist für deren Einhaltung verantwortlich.

Für die Einrichtung einer eZKA bei Nutzern mit besonderen Sicherheitsbedürfnissen (z. B. Polizei und Justiz, Militär oder Ministerien) müssen zusätzliche übergeordnete Instanzen wie z. B. BKA, LKA, MAD einbezogen werden. Diese sind dann frühzeitig von der hausverwaltenden Dienststelle zu beteiligen.

Der Einsatz einer eZKA ist in den meisten Fällen mitbestimmungspflichtig. Der Datenschutzbeauftragte sowie ein evtl. vorhandener Personalrat sind von Anfang an vom Nutzer einzubinden. Je nach Personalvertretungsgesetz ist eine Dienstvereinbarung abzuschließen.

Da speziell beim Einsatz der Biometrie als Ident-Mittel sehr persönliche Daten erfasst werden, ist in diesem Fall der Datenschutz in besonderer Weise zu berücksichtigen.

6 Abnahme, Übergabe, Betrieb und Instandhaltung

6.1 Abnahme

Der VOB-Abnahme einer eZKA muss die Inbetriebsetzung vorausgehen. Die Abnahme kann nur erfolgen, wenn der Auftragnehmer gegenüber dem Auftraggeber die Betriebsbereitschaft der Anlage mit Vorlage der Bestandsunterlagen, bestehend aus der Dokumentation, den Betriebsanleitungen sowie den technischen Unterlagen mit Leistungsmerkmalen und individuellen Einstellungen, erklärt.

Der Abnahme soll ein erfolgreicher Probebetrieb vorangehen. Diese Forderung muss jedoch bereits in den Ausschreibungsunterlagen enthalten sein.

Verantwortlich für die Durchführung der Abnahme ist der Auftraggeber.

Die Abnahme sollte im Beisein des Auftraggebers, des Auftragnehmers, des für den Betrieb der Anlage Verantwortlichen (z. B. Betreiber, nutzenden Verwaltung) erfolgen. In bestimmten Fällen können weitere Beteiligte hinzugezogen werden.

Mängel, die bei der VOB-Abnahme festgestellt werden, sind in einem Mängelbericht (VHB-Formblatt 441) [12] unter Angabe eines zeitnahen Termins der Mängelbeseitigung festzuhalten. Die vom Auftragnehmer angezeigte Mängelbeseitigung ist mit einer weiteren Begehung/Prüfung zu kontrollieren.

6.2 Übergabe an den Betreiber/Nutzer

Nach der VOB-Abnahme sollte möglichst kurzfristig die Übergabe an den Nutzer/Betreiber erfolgen. Bei der Übergabe ist der nutzenden Verwaltung eine Anlagenbeschreibung und ein Abnahmeprotokoll einschließlich der technischen Unterlagen sowie weitere Dokumentationsunterlagen (Pläne etc.) auszuhändigen. Bei eingerichteten Schließplänen ist durch die ausführende Firma auch der Software-Stand des Schließplanes zu übermitteln.

Der Betreiber oder die von ihm beauftragten Personen müssen vom Errichter in die Funktion und Bedienung der eZKA nach VOB Teil C DIN 18382 [13] Abschnitt 3.3.4 eingewiesen werden.

6.3 Betrieb und Instandhaltung

Für den Betrieb ist die nutzende Verwaltung zuständig. Sie ist auch für das Management (Administration und Pflege der Schließpläne) sowie der Instandhaltung der eZKA verantwortlich. Um sicherzustellen, dass die eZKA fortlaufend richtig arbeitet, soll diese in zu vereinbarenden Zeitabständen inspiziert und gewartet werden.

Wenn der nutzenden Verwaltung kein ausreichend qualifiziertes Fachpersonal zu Verfügung steht, wird empfohlen einen Instandhaltungsvertrag nach dem aktuellen AMEV Vertragsmuster InstandGMA [14] abzuschließen.

Eine Begehung durch sachkundige Personen ist erforderlich um festzustellen, ob Beeinträchtigungen oder Manipulationen an der eZKA vorliegen, die von der Anlage nicht selbsttätig erkannt werden. Im v. g. Vertragsmuster besteht die Möglichkeit, die Teilnahme des für die Instandhaltung Zuständigen an den Begehungen zu vereinbaren.

Die Bauverwaltung berät den Nutzer im Rahmen der Planung und bereitet bei Bedarf den eventuell von ihm geforderten Instandhaltungsvertrag vor. Das Ergebnis

der Beratung ist zu protokollieren (VHB [12] Formblatt 112 - Instandhaltung – Vereinbarung mit der liegenschaftsverwaltenden Stelle).

Hinweis: Nach VOB/B [15] 13 § Abs. 4 Nr. 2 beträgt die Verjährungsfrist der Mängelansprüche an einer eZKA 4 Jahre, auch wenn dem Auftragnehmer für die Dauer der Verjährungsfrist die Wartung nicht übertragen wird.

Beim Betrieb einer eZKA in Verbindung mit einer BMA ist ein besonderes Augenmerk auf die Funktionsfähigkeit des Ident-Mittels im Feuerwehrschlüsseldepot zu legen. Die Bauverwaltung soll den Nutzer spätestens bei der Übergabe der eZKA darauf hinweisen, dass die Batterien des Ident-Mittels in den Feuerwehrschlüsseldepots regelmäßig vom Nutzer getauscht werden müssen, so dass diese jederzeit funktionsbereit sind.

7 Abkürzungen und Begriffe

AMEV	**A**rbeitskreis **M**aschinen- und **E**lektrotechnik staatlicher und kommunaler **V**erwaltungen
BKA	**B**undes**k**riminal**a**mt
BMA	**B**rand**m**elde**a**nlage
BSI	**B**undesamt für **S**icherheit in der **I**nformationstechnik
DIN	**D**eutsches **I**nstitut für **N**ormung
DSGVO	**D**aten**s**chutz**g**rund**v**er**o**rdnung
EltVTR	Richtlinie über **el**ek**t**rische **V**erriegelungssysteme von **T**üren in **R**ettungswegen
EMA	**E**inbruch**m**elde**a**nlage
EN	**E**uropäische **N**orm
eZKA	**E**lektronische **Z**utritts**k**ontroll**a**nlage
FBL	**F**ach**b**ereichs**l**eiter
IP	**I**nternet **P**rotokoll
IT	**I**nformations**t**echnik
KG	**K**osten**g**ruppe
LAN	(engl. **L**ocal **A**rea **N**etwork) Lokales Datennetz
LBO	**L**andes**b**au**o**rdnung
LKA	**L**andes**k**riminal**a**mt
MAC-Adresse	(engl. **M**edia **A**ccess **C**ode) Identifikationsnummer eines Netzadapters
MAD	**M**ilitärischer **A**bschirm**d**ienst
PC	(engl. **P**ersonal **C**omputer) Einzelarbeitsplatzrechner,
PIN	**P**ersönliche **I**dentifikations**n**ummer
PoE	(engl. **P**ower **o**ver **E**thernet) Stromversorgung von Endgeräten über das Datenübertragungsnetz
RFID	(engl. **r**adio-**f**requency **id**entification) Identifikation über elektromagnetische Wellen
RS-485	(engl. **R**ecommended **S**tandard 485) Industriestandard für Asynchrone serielle Datenübertragung, auch EIA-485
USV	**U**nterbrechungsfreie **S**trom**v**ersorgung
ÜMA	**Ü**berfall**m**elde**a**nlage
VDE	**V**erband **d**er **E**lektrotechnik Elektronik Informationstechnik
VHB	**V**ergabe**h**and**b**uch
VOB	**V**ergabe- und Vertrags**o**rdnung für **B**auleistungen
WAN	(engl. **W**ide **A**rea **N**etwork) Weitverkehrsnetz
WLAN	(engl. **W**ireless **LAN**) Drahtloses lokales Datennetz
ZSG	**Z**utrittskontroll-**S**tell**g**lied

8 Verzeichnisse

8.1 Auswahl wichtiger Normen, Vorschriften, Regelwerke und Arbeitshilfen

01	DIN EN 60839-11-1:2013 (VDE 0830-8-11-1:2013-12)	Alarmanlagen – Teil 11-1: Elektronische Zutrittskontrollanlagen – Anforderungen an Anlagen und Geräte
02	DIN EN 60839-11-2:2015 (VDE 0830-8-11-2:2016-02)	Alarmanlagen – Teil 11-1: Elektronische Zutrittskontrollanlagen – Anwendungsregeln
03	DIN 18040-1:2010-10	Barrierefreies Bauen – Planungsgrundlagen – Teil 1: Öffentlich zugängliche Gebäude
04	DIN 18252:2018-05	Profilzylinder für Türschlösser – Begriffe, Maße Anforderungen Prüfverfahren und Kennzeichnung
05	DIN EN 1303:2015	Schlösser und Baubeschläge – Schließzylinder für Schlösser – Anforderungen und Prüfverfahren
06	DIN 18250:2006-09	Schlösser – Einsteckschlösser für Feuerschutz- und Rauchschutztüren
07	DIN 18251:2020-04	Schlösser – Einsteckschlösser und Mehrfachverriegelungen – Begriffe und Maße
08	AMEV EltAnlagen	Planung und Bau von elektrischen Anlagen in öffentlichen Gebäuden
09	AMEV EMA/ÜMA	Planung, Bau und Betrieb von Gefahrenmeldeanlagen für Einbruch, Überfall und Geländeüberwachung in öffentlichen Gebäuden
10	DIN 276:2018-12	Kosten im Bauwesen
11	AMEV LAN	Planung, Bau und Betrieb von anwendungsneutralen Kommunikationsnetzwerken in öffentlichen Gebäuden
12	VHB 2017 Stand: 2019	Vergabe- und Vertragshandbuch für Baumaßnahmen des Bundes
13	DIN 18382:2019-09 (VOB Teil C)	VOB Vergabe- und Vertragsordnung für Bauleistungen - Teil C: Allgemeine Technische Vertragsbedingungen für Bauleistungen (ATV) - Elektro-, Sicherheits- und Informationstechnische Anlagen
14	AMEV InstandGMA	Vertragsmuster für Instandhaltung von Gefahrenmeldeanlagen (Brand, Einbruch, Überfall und sonstige Alarmanlagen) in öffentlichen Gebäuden
15	DIN 1961:2016-09 (VOB/B)	VOB Vergabe- und Vertragsordnung für Bauleistungen - Teil B: Allgemeine Vertragsbedingungen für die Ausführung von Bauleistungen
16	EltVTR	Richtlinie über elektrische Verriegelungssysteme von Türen in Rettungswegen, DIBt 12/1997

8.2 Literaturhinweise

Die folgenden Publikationen wurden bei der Erstellung dieser Broschüre durchgesehen und gaben Hinweise für Gestaltung und Inhalt.

Praxis Ratgeber Zutrittssteuerung (2018/2019) des Bundesverband Sicherheitstechnik e.V. (BHE)

IT Grundschutz-Kompendium des Bundesamtes für Sicherheit in der Informationstechnik (BSI)

8.3 Abbildungen und Tabellen

Alle Abbildungen, Fotos, Schemen und Tabellen wurden im Rahmen der Erstellung dieser Empfehlung von Mitgliedern des AMEV Fernmeldeausschusses nach bestem Wissen und Gewissen erstellt. Verwendung nur nach ausdrücklicher Genehmigung durch den Obmann.

9 Mitarbeiter

Thomas Augustin	Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr, Koblenz
Marius Elsner, Obmann	Stadt Nürnberg, Nürnberg
Ronald Gockel, FBL	Ministerium der Finanzen Rheinland-Pfalz, Mainz
Martin Heydenbluth	Oberfinanzdirektion Karlsruhe, Bundesbau Baden-Württemberg, Freiburg
Robert Höhl	Bayerisches Staatsministerium für Wohnen, Bau und Verkehr, München
Anne Janssen-Bokämper	Niedersächsisches Landesamt für Bau und Liegenschaften (NLBL), Hannover
René Kaufmann	Bundesamt für Bauwesen und Raumordnung, Berlin
Jens Kochanow	Sächsischer Landtag, Dresden
Karl-Heinz Kranzosch	Bundesamt für Bauwesen und Raumordnung, Bonn
Jürgen Kroll	Ministerium für Heimat, Kommunales, Bau und Digitalisierung des Landes Nordrhein-Westfalen (MHKBD NRW), Düsseldorf
Markus Loer	Landesbaudirektion Bayern, München
Stephan Mackert	Vermögen und Bau Baden-Württemberg, Mannheim
Volker Maurer	Landesverwaltungsamt, Staatliche Hochbaubehörde, Saarbrücken
Wilfried Müller	ehemals Niedersächsisches Landesamt für Bau und Liegenschaften (NLBL), Hannover
David Strzelecki	Gebäudewirtschaft der Stadt Köln, Köln
Dirk Timmsen	Finanzministerium Schleswig-Holstein, Amt für Bundesbau, Kiel

Anlage: Muster-Checkliste für die Bedarfsermittlung

Hinweis: Alle blauen Eintragungen sind als Muster zu verstehen,
sie geben keinen allgemeinen Standard wieder! Es müssen alle Felder neu ausgefüllt werden!

☐ Zutreffendes ist anzukreuzen

Projekt

Baumaßnahme:	***Neubau Amtsgericht Musterstadt***
Liegenschaft:	***Amtsgericht Musterstadt***
Ort:	***Musterstadt***
Straße:	***Musterstraße***
Nutzende Verwaltung:	***Amtsgericht***
Ort	***Musterstadt***
Straße	***Musterstraße***
Telefon:	***0999-9999-0***

Ansprechpartner nutzende Verwaltung

Name:	***Mustermann***
Telefon:	***0999-9999-100***
E-Mail:	***mustermann@amtsgericht.de***

Ansprechpartner Vergabestelle

Vergabestelle:	***Bauamt***
Name:	***Hr. Mustermann***
Telefon:	***0999-8888-200***
E-Mail:	***mustermann@bauamt.de***

A: Grundsätzliche Angaben

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

   2

2. Wie ist die sich daraus ergebene Organisationsstruktur?

   Jede Verwaltung muss die Berechtigungen selbständig vergeben können

3. Gibt es eine begründete Produktbindung?

   Firma X, da bereits im Haupthaus eingesetzt. Vernetzte Struktur.

4. Ist bei erhöhter Sicherheitsanforderung an das Gebäude oder die Liegenschaft eine Abstimmung mit dem LKA / BKA erforderlich?

   ☒Ja / ☐ Nein

   Wenn ja: Hat eine derartige Beratung schon stattgefunden?

   ☒ Ja / ☐ Nein

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

   Grundsätzlich Grad 1, in bestimmten Räumen (Asservatenkammer, Serverraum) Grad 3

5. Welche datenschutzrechtlichen Belange sind zu beachten?

   Keine über die Datenschutz-Grundverordnung (DS-GVO) hinaus

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

   ☐ Ja / ☒ Nein

   Wenn ja: Was muss berücksichtigt werden?

   Klicken oder tippen Sie hier, um Text einzugeben.

B: Planungsgrundlagen

1. Wie viele Türen sind einzubeziehen?

   100

   Mit welchen Funktionen:

   Nur Zugangskontrolle, siehe Tür-Liste

2. Anzahl der benötigten Ident-Mittel?

   300

   Art der Ident-Mittel?

   Transponder passiv

3. Welcher maximale Umfang muss für die eZKA in der Endausbaustufe in etwa möglich sein?

   Anzahl Türen / Zugänge: ***150***

   Anzahl Ident-Mittel: ***500***

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

   Es muss möglich sein den Zugang am Wochenende und Feiertagen zu verhindern

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

5. Können Bereiche mit rein mechanischer Sicherheit ausgerüstet werden?
   ☒Ja / ☐Nein
   Wenn ja: Welche?

   Sanitärräume, Teeküchen, Lager

6. Sind Anlagen mit nutzbaren Ident-Mitteln bereits im Bestand vorhanden?

   ☐Ja / ☒Nein

7. Wenn Ja, sollen diese mit der neuen Anlage in einem Ident-Mittel zusammengefasst werden?

   ☐Ja / ☒Nein

8. Soll die Anlage Schnittstellen zu vorhandenen oder geplanten technischen Anlagen wie z. B. einer Zeiterfassungsanlage haben?

   ☒Ja / ☐Nein

   Wenn ja, zu welcher Anlage oder welcher Schnittstelle?

   Zeiterfassung, Drucker, Schrankenanlage

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

   ☒Ja / ☐Nein

   Wenn ja, welche?

   Schranke Parkplatz

10. Sind spezielle Verschlüsse, wie z. B. Paniktürverschlüsse vorhanden?

    ☒Ja / ☐Nein

    Wenn ja, welche?

    Haupteingang

C: Bemerkungen oder Besonderheiten zum Projekt:

Gibt es besondere Betriebsumgebungen, die bei der Planung und dem Betrieb zu berücksichtigen sind (z. B. Lager für Gefahrstoffe, Ex-Bereiche, Mittelspannungsanlagen, S4-Labore)?

keine

D: Ausführung

1. Auf Grundlage der Angaben unter den Punkten A-C ist die folgende Ausführung der Zutrittskontrolle vorzusehen:

☐ Klassische Schließanlage mit mechanischen Zylindern

☒ eZKA - Offline Anlage

☐ eZKA - Online Anlage

☐ eZKA - Virtuelles System

Datenanbindung: ☐WLAN ☒Kabel

2. Betrieb

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

☐Kein Bedarf / ☒Vorhandener PC / ☐ PC

Falls Bedarf besteht, Anzahl der PC`s?

keine

Welches Betriebssystem wird eingesetzt?

Windows 11

3. Instandhaltung

Welcher Umfang ist für die Instandhaltung der Anlage erforderlich?

☒ Inspektion

☐ Wartung

☐ Instandsetzung

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

Liegt das VHB-Formblatt 112 vor?

☒ Ja / ☐ Nein

Kann der erforderliche Batteriewechsel durch Personal der nutzenden Verwaltung durchgeführt werden?

☒ Ja / ☐ Nein

4. Anlagen

Sind Bestandsunterlagen und Gebäudepläne vorhanden?

☒Ja / ☐Nein

Beigefügte Planunterlagen:

Grundrisspläne

5. Sonstige Bemerkungen:

Nutzende Verwaltung:

keine

Bauverwaltung:

Der Datenschutzbeauftragte sollte nach Bauauftrag beteiligt werden

Aufgestellt

Bauverwaltung	Nutzende Verwaltung
Mainz, den 11.11.2023	
Maurer	*Gockel*
(Maurer)	***(Gockel)***