Charité Hausstandard

399_Schließanlage

Dieser Hausstandard ist für alle Baumaßnahmen an der Charité - Universitätsmedizin Berlin (kurz Charité) bindend und gilt in allen Liegenschaften der Charité.

Die Festlegungen dieses Hausstandards ergänzen die verbindlichen deutschen und internationalen Normen, Richtlinien und Empfehlungen.

Der Hausstandard ist mit Freigabe durch die Baudienststelle der Charité und der Charité CFM Facility Management GmbH die Grundlage zur Aufstellung der Bedarfsplanung und die sich daraus ergebenden weiteren Planungsschritte.

Abweichungen sind im Einzelfall zulässig, bedürfen jedoch der Einzelfallgenehmigung.

Bezogen auf den Stichtag der Freigabe ist der Einfluss auf laufende Planungen und Bauprojekte im Einzelfall zu prüfen. Eine rückwirkende Gültigkeit für bereits in Betrieb befindliche Anlagen ist nicht vorgesehen und bedarf einer Einzelfallprüfung.

	Funktion	Name	Datum	Unterschrift
Freigegeben	Baumanagement	Bruchmann	18.02.2020	elektronisch erstellt, ohne Unterschrift gültig
Freigegeben	Geschäftsführung	Maßwig	16.03.2020	elektronisch erstellt, ohne Unterschrift gültig
Freigegeben	Baudienststelle	Brinkmann	10.03.2020	elektronisch erstellt, ohne Unterschrift gültig

Inhaltsverzeichnis

1. Allgemeines

Das Schließsystem / Zutrittskontrollsystem ist ein zentrales System im Krankenhaus. Ziel ist es, die Funktionen und die Sicherheit in den Gebäuden zu gewährleisten. Grundsätzlich sind elektronische Schließsysteme einzusetzen. Nur in Außnahmefällen und in Abstimmungen mit den Auftraggeber sind mechanische Schließsysteme in Bestandsgebäuden zulässig.

Das Schließ- / Zutrittskontrollsystem ist zentraler Bestandteil der Planung. Es sind ebenfalls Vorschläge zur Schließhierarchie dem Auftraggeber mit farbigen Funktions- und Übersichtsplänen zu erstellen. Diese sind seitens dem Auftraggeber / Schließverwaltung der Charité CFM und in größeren Projekten mit dem Baumanagement abzustimmen und freigeben zu lassen.

Bei der Erstellung ist das Sicherheitskonzept der Charité (Schutzziele, Zonen usw.) zu beachten!

Den Zugang für Räume erhält der Nutzer über das Schließmedium. Die elektronischen Träger (Transponder, Karten, Telefone) enthalten die Berechtigungen. Grundsätzlich sind die Berechtigungen auf dem Trägermedium räumlich und zeitlich limitiert. Wenn ein Trägermedium unentdeckt entwendet oder verloren wird, ist die Nutzbarkeit damit eingeschränkt. Dies ist ein Eckpfeiler der Sicherheit.

Bei Umbauten einzelner Gebäudebereiche muss untersucht werden, in wie weit das vorhandene System genutzt werden kann.

2. System / Hardware

In der Charité wird für alle Baumaßnahmen ein elektronisches Schließsystem vorgegeben. Ein System besteht neben den Zugängen im Wesentlichen aus dem Managementsystem, Controllern, Updatern, dem Trägermedium und Endgeräten wie elektronische Schließzylinder und Leser (auch in Aufzügen).

Die Zugänge in der Außenhaut sind nach Möglichkeit online und die Zugänge innen offline anzubinden. Aus Sicherheitsgründen kann in Ausnahmefällen auch innen online installiert werden. Für jedes Haus sind ausreichend Updater (inkl. Controller im IKS Raum) zu installieren. Die Verortung ist zwingend abzustimmen und hat das Verkehrskonzept / Logistikkonzept zu unterstützen.

Zurzeit wird das Verwaltungssystem der Firma DATASEC genutzt. Neue Bauprojekte sind zwingen in dieses System zu integrieren. Die Verwaltung des Systems erfolgt in der Schließverwaltung über das Managementsystem ZK 3000. Die Berechtigungen werden über Controller zu den Updatern übertragen. Der Nutzer kann seine Berechtigungen dort auf sein Trägermedium übertragen. Die elektronischen Zylinder und Leser geben den Weg frei oder verhindern den Zutritt.

Dieses System ist weitestgehend herstellerunabhängig, aber gegen ungewollten Zugriff von innen und außen über die gesamte Kette hin geschlossen.

Der Eckpfeiler hier ist der Charité Standard „MIFARE® DESFire EV2 OSS“. Dies ist eine standardisierte Möglichkeit, herstellerübergreifend und sicher, die Komponenten zu verbinden.

3. OSS

Innerhalb der Charité wird „MIFARE® DESFire EV+2 OSS“ verwendet. Nähere Informationen finden sie unter https://www.oss-association.com. Als Verwaltungssystem ist die ZK 3000 verankert.
Alle Komponenten sind zwingend entsprechend kompatibel zu wählen. Endgeräte (Leser, Schließzylinder) müssen zwingend über das CFM Standardtool von DATASEC programmierbar/konfigurierbar sein.

Bezüglich der Kartensegmentierung und Keys gibt es Vorgaben. Diese sind bei der CFM Schließverwaltung abrufbar.

4. Hinweise Schließkonzept Hierarchie und Bezeichnung

Innerhalb des Systems ist es notwendig, bestimmte Hierarchien und Bezeichnungen einzuhalten. Das Konzept ist so zu erarbeite, dass es standortübergreifend funktioniert und enthält mindestens folgende Informationen.

- Einzelberechtigung (einzelner Türen)
- Berechtigung (Zutrittszone: Gruppierung von Türen/Toren)
- Berechtigungsprofil (Zutrittsprofil aus ggf. mehreren Berechtigungen und ggf. mehreren Einzelberechtigungen)

Es werden diverse bau- und nutzerspezifische Berechtigungen, ggf. ebenen- und/oder gebäudeübergreifend gebildet.

Jeder Zutrittspunkt (Tür, Tor etc.) wird mindestens einer Berechtigungszone zugeordnet. Diese Berechtigungen wiederum werden später den Personen als Profil zugewiesen.

Jedem Mitarbeiter wird wenigstens ein Berechtigungsprofil durch die Schlüsselverwaltung nach Freigabe durch den Vorgesetzten zugewiesen. Die sich daraus ergeben baulichen und technischen Notwendigkeiten sind umzusetzen.

Jedes Schließkonzept wird vor Inbetriebnahme des Nutzerbereiches durch die CFM Schlüsselverwaltung geprüft und erst nach Freigabe umgesetzt. Das Sicherheitskonzept der Charité muss befolgt werden.

5. Bauliche Rahmenbedingungen

In Absprache mit dem Bauherrn sind die Endgeräte des Zutrittskontrollsystems (Leser, Updater etc.) geschützt gegen Wettereinflüsse, Sabotage und Vandalismus auszuwählen. Die Verortung soll den Verkehrsfluss unterstützen.

Die Leser müssen zwingend batteriegepuffert sein. Die Mindestdauer der autonomen Stromversorgung durch Batterien beträgt mindestens 5 Minuten bei Anbindung der Leser an die SV oder 30 Minuten bei Anbindung der Leser an die AV. Bei stark frequentierten Türen/Tore ist eine Ausführung mittels Leser verpflichtend. Sollte diese technische Umsetzung unmöglich sein, muss der elektronische Zylinder an die AV angeschlossen sein.

Sämtliche AMC-Controller und Updater müssen an die SV-Stromversorgung angeschlossen sein (Sicherheitsversorgung – max. Ausfall 15 Sek.).

Alle Allarmeinrichtungen (EMA) sind zwingend kompatibel zur vorhandenen Komponenten zu errichten.

Die Aufzugssteuerung durch Schließmedien ist mit transpondergesteuerten Leser umzusetzen. Im Außenruf wird ein Wandleser bündig integriert, ebenso im Aufzugsinneren für die Etagenwahl/Funktionswahl. Beide sind online auszuführen. Hinsichtlich der einwandfreien Kommunikation (Senden/Empfangen) ist die Ausführung/Größe der Leserausschnitte mittels Trägermedium Karte zu prüfen bzw. entsprechend zu errichten.

6. Sonstiges

Für die Erarbeitung von größeren Schließkonzepten finden Sie Hinweise im „Schließ- und Sicherheitskonzept“ des Katastrophenschutzes des Universitätsklinikums Berlin.