Freie Universität Berlin

Freie Universität Berlin

IT-Verfahrensbeschreibung eSa

elektronische Schließanlage

Nur für den internen Dienstgebrauch!

29.01.2009

1 Vorbemerkung

Die zentrale Aufgabe der Freien Universität ist die Durchführung von Forschung und Lehre. Umgesetzt wird diese Aufgabe in den verteilten Liegenschaften der Freien Universität. Zur Sicherstellung der Umsetzung werden alle Liegenschaften mit Schlössern gesichert. Aktuell sind dies nahezu ausnahmslos mechanische Schlösser.
Das folgende IT-Verfahren beschreibt den Betrieb einer elektronischen Schließanlage an der Freien Universität.
Zur Vereinfachung wird hier nicht zwischen Zylindern und Türen unterschieden, sondern allgemein der Passus Schloss verwendet.
Betrachtet werden hierbei die geltenden Datenschutzgesetzte als auch die internen IT-Richtlinien der Freien Universität.

2 Gesetzliche Grundlagen

Die gesetzlichen Grundlagen für den Einsatz einer elektronischen Schließanlage innerhalb der Freien Universität Berlin gliedern sich in Gesetze und Organisationsrichtlinen.

2.1 Gesetze

Entsprechend Artikel 33 der Verfassung von Berlin [VvB] [1] steht jedem Berliner Bürger das Recht auf Schutz seiner Daten zu. Der Datenschutz für Privatpersonen und Bundeseinrichtungen wird im Bundesdatenschutzgesetz [BDSG][2] geregelt. Zusätzlich gibt es noch das Berliner Datenschutzgesetz [BlnDSG][3]. Das BlnDSG regelt den Datenschutz in Landes- und Kommunalbehörden.
Insofern bilden das BDSG und das BlnDSG die gesetzliche Grundlage für den Umgang mit Daten innerhalb des Projektes eSa.
Zusätzlich kommt das Berliner Hochschulgesetz zur Anwendung in welchem die Freie Universität den Auftrag für Forschung und Lehre erhalten hat. Zur Sicherstellung dieser Aufgabe ist es unabdingbar, dass die für Forschung und Lehre notwendigen Objekte entsprechend gesichert werden, sowohl vor unbefugtem Zutritt als auch Diebstahl und/oder Vandalismus.

2.2 Organisationsrichtlinien

Zusätzlich gelten innerhalb der Freien Universität eigene organisatorische Richtlinien, z.B.:

- IT-Sicherheitsrichtlinie[4]
- IT-Grundsatzdienstvereinbarung[5]

[1] *http://www.parlament-berlin.de/pari/web/wdefault.nsf/vFiles/D14/$FILE/Verfassung von Berlin_Times14.pdf*
[2] *http://bundesrecht.juris.de/bdsg_1990/*
[3] *http://www.datenschutz-berlin.de/attachments/346/BlnDSG2008.pdf?1200651252*
[4] *http://www.fu-berlin.de/service/zuvdocs/fu-rundschreiben/2008/it-sicherheitsrichtlinie.pdf*
[5] *http://web.fu-berlin.de/prd/dienst/DV_IT_Grundsatz.pdf*

3 IT-Verfahren

3.1 Definitionen

Im Folgenden sind die innerhalb des IT-Verfahrens genutzten Begriffe definiert.

Begriff	Definition
Alarm	Aufforderung für menschliches Eingreifen nach der Aktivierung eines Signalgebers
Betreiber gesamte eSa	die innerhalb der Freien Universität für den Betrieb des elektronischen Schließsystems verantwortliche Abteilung
Betreiber Teilbereiche eSa	die innerhalb der Freien Universität für den Betrieb des elektronischen Schließsystems eines Fachbereichs verantwortliche Abteilung
Benutzer	Person, die den Durchgang an einem Zutrittspunkt fordert
Berechtigungsgruppe	Gruppe von Benutzern, die die gleiche Zutrittsberechtigung besitzen
Elektronische Schließanlage [eSa]	Anlage, die alle baulichen, apparativen und organisatorischen Gegebenheiten umfasst, um den Zutritt zu steuern
Energieversorgung	Teil einer Zutrittskontrollanlage, der die Energie für den Betrieb der Anlage oder für Teile davon zur Verfügung stellt
Ereignis	Änderung, die in einer Zutrittskontrollanlage auftritt
Freigabe	Signal an das ZSGR, dass Zutritt gewährt worden ist
Geistiges Identifikationsmerkmal	Information, die der Benutzer kennt (z.B. PIN)
Identifikationsmerkmal	Information, die vom Benutzer direkt oder über ein Identifikationsmittel der Identifikationsmerkmalerfassungseinheit eingegeben wird
Identifikationsmerkmalerfassungseinheit (IDEE)	Einrichtung, um Identifikationsmerkmale von einem Identifikationsmerkmalträger zu erfassen - die Einrichtung kann zur Eingabe geistiger Identifikationsmerkmale über eine zusätzliche Tastatur verfügen
Identifikationsmittel	Identifikationsmerkmale, die auf Ausweisen, Schlüsseln und Gegenständen usw. zur Verfügung gestellt werden

Normalzustand	Zutrittskontrollanlage ist vollständig funktionsfähig und kann alle Ereignisse nach den eingestellten Parametern verarbeiten
Offline	Austausch von Daten nicht in Echtzeit möglich, sondern gebunden an die Nutzung des elektronischen Schließsystems durch Anwender oder an individuell durchgeführte Datentransfers
Online	Austausch von Daten (Erteilung / Entzug von Zutrittsberechtigungen) in Echtzeit möglich
Parametrierbarkeit	Fähigkeit, Parametereinstellungen zu empfangen und zu speichern
Rückweisungsfehler	Zutrittsverweigerung für berechtigte Benutzer
Sabotageschutz	Maßnahmen, die angewendet werden, um Zutrittskontrollanlagen oder Teile davon gegen vorsätzliche Eingriffe zu schützen
Signalisierung	Ausgabe von Informationen für den Betreiber oder für andere Systeme
Standort	Einzelgebäude oder räumlich unmittelbar zusammenhängender Gebäudekomplex einer Universitätseinrichtung (Fachbereich, Zentraleinrichtung / Zentralinstitut) - eine Universitätseinrichtung kann mehrere Standorte haben
Störungszustand	Wenn der Gebrauch der Zutrittskontrollanlage zu dem Zwecke, zu dem sie angeschafft wurde, oder zum gewöhnlichen Zwecke nicht unerheblich beeinträchtigt wird
Transaktion	Vorgang, der in Zusammenhang mit der Freigabe eines Zutrittspunktes nach Identifikation des Identifikationsmerkmals steht
Verarbeitung	Vergleich der Informationen mit den eingestellten Parametern, um zu entscheiden, ob Zutritt für die Benutzer gewährt oder verweigert wird und/oder der Vergleich von Ereignissen mit den eingestellten Parametern, um entsprechende Maßnahmen durchzuführen
Zeitbereich	ein oder mehrere Zeitfenster, die mit Kalenderdaten verknüpft sind
Zeitfenster	Zeit, die den Anfang und das Ende einer gültigen Periode innerhalb eines Zeitbereiches anzeigt

Zeitzonen	ein oder mehrere Zeitbereiche, die einer Zutrittsberechtigung zugeordnet sind
ZSGR	Zutrittskontrollstellglied mit Rückmelder Beispiele für Zutrittskontrollstellglieder: - elektrische Türöffner - Schlösser - Drehkreuze - Sperren Beispiele für Rückmelder sind: - Kontakte - Schalter - Druckgeber - Türschalter
ZSGR-Geöffnet	ZSGR ist geöffnet, wenn am Zutrittspunkt der Zutritt möglich ist
ZSGR-Geschlossen	ZSGR ist geschlossen, wenn am Zutrittspunkt kein Zutritt möglich ist
ZSGR-Verletzung	unzulässige Nutzung eines Zutrittspunktes
Zutritt	Vorgang des Betretens oder Verlassens eines Sicherungsbereiches
Zutrittsberechtigung	Berechtigung zum Zutritt zu bestimmten Sicherungsbereichen, ggf. mit dazu-gehörigen Zeitzonen
Zutrittskontrollzentrale (ZKZ)	Einrichtung, die entscheidet, einen oder mehrere Zutrittskontrollpunkte freizugeben und den dazugehörigen Ablauf überwacht und steuert
Zutrittspunkt	Ort, an dem der Zutritt mit einer Tür oder anderen Sperren zur Sicherung gesteuert werden kann

3.2 Zweck & Ziele

Aktuell werden nahezu alle Gebäude der Freien Universität mit mechanischen Schlössern vor unbefugtem Betreten gesichert. Zur Vereinfachung der Nutzung sind mehrere Schlösser mit ein und demselben Schlüssel zu öffnen und zu schließen. Diese Schlösser verfügen dann über eine sogen. Gruppenschließung. Wird jedoch ein passender Schlüssel verloren, so sind aus Sicherheitsgründen alle in der Schließgruppe vorhandenen Schlösser auszutauschen. Bei Verlust eines Schlüssels für mehrere Gruppen – einem Haupt- oder Generalschlüssel – ist die gesamte Schließanlage auszutauschen. Es entstehen hier durchaus Kosten im 6-stelligen Bereich.
Vor diesem Hintergrund setzen sich immer mehr elektronische Schließanlagen [eSa] durch. Hier wird das Öffnen und Schließen der Türen über einen Transponder ermöglicht. Dieser kann flexibel mit neuen Schließrechten versehen werden und zudem bei Verlust einfach an den Schlössern gesperrt werden. Somit ist ein Austausch des Schlosses bzw. der Schließanlage nicht notwendig.
Auch an der Freien Universität soll eine elektronische Schließanlage installiert werden. Ziel dieses Wechsels ist die Erhöhung der Sicherheit, der Flexibilität in der Administration und letztendlich damit Senkung der Kosten zum Betrieb der Schließanlage

3.3 Beschreibung des IT-Verfahrens

Im Folgenden wird das System der elektronischen Schließanlage dargestellt. Die Darstellung erfolgt anhand der verwendeten Architektur, der entstehenden und verwendeten Daten sowie den genutzten Rollen und Workflows.

3.3.1 Architektur

Die elektronische Schließanlage besteht aus mehreren Komponenten. Die Komponenten werden hier aus Sicht des Nutzers gegenüber dem System dargestellt. Grundsätzlich ist bei der eSa zwischen dem Offline- und dem OnlineTeil zu unterscheiden. Die Entscheidung ob Offline oder Online ist abhängig vom jeweiligen Einbauort, Einbauzweck und Sicherheitsbedarf des durch das Schloss zu schützenden Raumes oder Objektes.

3.3.1.1 Transponder | Identifikationsmittel

Der Transponder ist der elektronische Schlüssel des Systems. Dieser Transponder wird dem Nutzer daher ausgehändigt. Mittels dieses Transponders ist es dem Nutzer möglich, Türen zu öffnen und/oder zu schließen.
Das genutzte Verfahren für den Transponder ist RFID – Radio Frequency Identification.[6] RFID ist im Falle der eSa die Identifikation des Transponders per Funk an der Tür bzw. der den Zutritt verhindernden Geräte.
Der Transponder ist in zwei Bauformen verfügbar. Die „klassische Form“ der ISO-Karte[7] entspricht dem gewohnten Bild einer EC-Karte, lediglich mit der Funktion der Schließung. Diese Karte ist entsprechend ISO 7816 ID-1 standardisiert. Sie hat eine Größe von maximal 85,60 × 53,98 mm und darf maximal 0,86 mm dick sein.
Die andere Form ist ein Schlüsselanhänger. Dessen Form ist nicht standardisiert.

[6] *http://de.wikipedia.org/wiki/Radio_Frequency_Identification*
[7] *http://de.wikipedia.org/wiki/ISO_7816*

Beide haben jeweils die fortlaufend nummerierte Kartenummer aufgedruckt – der Schlüsselanhänger frontseitig, die Karte rückseitig. Auf der ISO-Karte ist zudem vorderseitig das Logo der Freien Universität aufgedruckt.

Abbildung 1 | Bild 1 ISO-Karte

Abbildung 2 | Bild 2 Schlüsselanhänger

Der zum Einsatz kommende Transponder ist ein Mifare-Classic-Transponder. Mifare-Transponder sind milliardenfach im Einsatz - weltweit. Dieses System ist seit 1990 auf dem Markt und wird durch die Firma NXP Semiconductors [ehemals Philips][8] vertrieben. Die Lesereichweite des Transponders, also der Abstand zwischen Transponder und Leser, beträgt 1-3 cm.

[8] *http://www.nxp.com/products/identification/mifare/index.html*

Der Hersteller hat bei diesem Transpondertyp eine proprietäre Verschlüsselung [Crypto-1] mit einer Verschlüsselungstiefe von 48 Bit implementiert bzw. umgesetzt.
Da Mifare Classic seit Jahresbeginn 2008 aber sicherheitstechnisch als gefallen – weil Ende 2007 gehackt - betrachtet werden muss[9], verfügt der in der Freien Universität verwendete Transponder über eine wesentlich höhere Verschlüsselung als vom Hersteller vorgesehen.
Bei den Transpondern der Freien Universität kommt eine zusätzliche – wesentlich höhere - Verschlüsselung zum Einsatz. Diese hat eine Verschlüsselungstiefe von 128 Bit und basiert auf AES[10]. Die gleiche Verschlüsselungstiefe wird für nahezu jegliches private und geschäftliche OnlineBanking genutzt. Zudem wird es durch das National Institute of Standards and Technology [NIST/USA] als über das Jahr 2030 hinaus sicher angesehen[11] und für den Einsatz in staatlichen Einrichtungen empfohlen.
Hinweis: Die innerhalb vieler Berliner Mensen genutzte MensaKarte basiert auf Mifare-Classic mit nur 48 Bit Verschlüsselungstiefe.

Im Rahmen der eSa gibt es neben den Transpondern für die Nutzer auch Transponder mit besonderen Rechten bzw. Funktionen für administrative Tätigkeiten. Diese sind wie folgt:

1. Batteriewechselkarte
   Jedem Fachbereich steht eine Batteriewechselkarte zu. Hiermit ist es dem Fachbereich möglich, die Batterien in den OfflineZylindern zu wechseln.
   [Nach vorhalten dieser Karte werden die Arretierungen der Abdeckung des OfflineZylinders freigegeben, so dass die Abdeckung entfernt werden kann und die Batterien zugängig sind.]

2. ServiceKarte
   Sollte an einem OfflineZylinder versucht werden diesen zu manipulieren, so wird dieses erkannt. Der OfflineZylinder nimmt dann aus Sicherheitsgründen keine weiteren Transponder entgegen und muss mittels der ServiceKarte wieder frei gegeben werden. Auch diese Karte ist je Fachbereich 1x vorhanden.

3. Demontagekarte
   Ist es notwendig einen OfflineZylinder auszubauen, so ist hierfür eine Demontagekarte notwendig. Wird eine solche Karte vor den OfflineZylinder gehalten, kann der Zylinderkopf entfernt und der Rest ausgebaut werden.
   Diese Karte steht jedem Fachbereich 1x zur Verfügung.

4. Buchungstransferkarte
   Die blaue Transferbuchungskarte ist für das Auslesen und Übertragen der Buchungen im OfflineZylinder zum Server notwendig. Diese Karte ist lediglich einmal in der gesamten eSa vorhanden. Zum Einsatz kommt diese Karte nur auf Verlangen der Zutrittskontrolleure [vgl. 3.3.3 Rollen]. Diese Karte ist im Tresor der technischen Abteilung hinterlegt.

[9] *http://events.ccc.de/congress/2007/Fahrplan/events/2378.en.html*
[10] *http://de.wikipedia.org/wiki/Advanced_Encryption_Standard*
[11] *http://csrc.nist.gov/publications/PubsSPs.html*

3.3.1.2 OfflineZylinder

Der OfflineZylinder ist ein mechanischer Zylinder mit elektronischer Kontrolle der Schließung. Das bedeutet, dass der OfflineZylinder den bisherigen Zylinder ersetzt und in die entsprechende Tür eingebaut wird. Offline deshalb, weil es keine Kabel zu einem anderen Teil der elektronischen Schließanlage gibt. Das Entriegeln des Schlosses mit OfflineZylinder erfolgt durch die den Zutritt wünschende Person. Eingesetzt wird der OfflineZylinder hauptsächlich innerhalb von Gebäuden, also bspw. Bürotüren und Schlüsselschaltern in Aufzügen. Der OfflineZylinder ist modular aufgebaut und besteht aus 3 Teilen. So ist bspw. beim Wechsel des Schlosses in eine andere Tür nur der Zylinderadapter der jeweiligen Tür anzupassen oder aber bei mutwilliger Zerstörung nur der Elektronikknauf zu tauschen.

Abbildung 3 | OfflineZylinder

3.3.1.2.1 Elektronik-Knauf

Der Elektronik-Knauf ist der Teil des OfflineZylinders der von außen sichtbar ist. In diesem Knauf ist die gesamte Elektronik nebst Batterien untergebracht. Der Knauf verfügt über eine mehrfarbige LED und einen Summer. Die LED zeigt zum einen die Bereitschaft des Zylinders an, einen Transponder zu lesen [grün] und zum anderen, ob ein gültiger Transponder gelesen wurde [grün/rot]. Wurde ein ungültiger Transponder gelesen und damit der Zutritt verwehrt, so ertönt auf Wunsch zusätzlich ein Hinweiston.
Zur Spannungsversorgung verfügt der Zylinder über zwei eingebaute StandardBatterien vom Typ CR-2. Sollten diese – unabhängig aus welchen Gründen - Ihre Spannung nicht mehr an den Zylinder liefern können, so kann der OfflineZylinder mit einem Notbestromungsgerät wieder geöffnet werden. Hierzu verfügt der Zylinder an der Frontseite über zwei Kontakte, die im Falle eines Spannungsverlusts die Notbestromung ermöglichen. Bei vorhandener Batteriespannung sind diese Kontakte zum Schutz vor Sabotage durch bspw. Überspannung deaktiviert.

Abbildung 4 | Elektronik-Knauf

3.3.1.2.2 Zylinderadapter

Der Zylinderadapter ist der in der Tür steckende Teil des gesamten Offlinezylinders. Die Form dieses Adapters entspricht der von Profilzylindern – also dem ggf. bisherig eingebauten Zylinder. Daher sind für den Einbau eines OfflineZylinders keine Umbauarbeiten an der Tür notwendig. Die Länge des Zylinders richtet sich nach der Stärke des Türblattes.

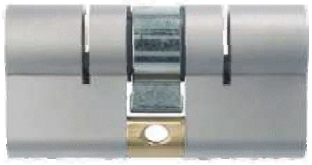

Abbildung 5 | Zylinderadapter

3.3.1.2.3 Innenknauf

Der Innenknauf ermöglicht das Verschließen und Öffnen der Tür von der Innenseite des Raumes ohne Nutzung eines Transponders.

Abbildung 6 | Innenknauf

3.3.1.3 OnlineSchloss/OnlineLeser

Das Onlineschloss ist - wie es der Name nahe legt - online mittels Kabeln mit dem Server verbunden. Die Rechte werden daher nicht im Schloss gespeichert, sondern lediglich bei Zutrittswunsch vom Server abgerufen.
Das OnlineSchloss ist eine Kombination aus Kartenleser und elektronischem Schloss. Der an der Wand montierte Kartenleser zeigt ebenfalls wie das OfflineSchloss durch 2 LEDs den jeweiligen Status an. Grün „Zutritt gewährt“ – Rot „Zutritt untersagt, da keine gültige Berechtigung“. Das elektronische Schloss – ein sogen. Motorschloss – entriegelt bei gültiger Berechtigung das Schloss und ggf. sogar die Tür. Beide sind an eine ZutrittsKontrollZentrale [ZKZ][12] angeschlossen. Diese versorgt zum einen den Kartenleser und das Motorschloss mit der notwendigen Spannung und zum anderen stellt sie den physikalischen Zugang zum Server her.
Der Einsatzort des OnlineSchlosses ist hauptsächlich der jeweilige Eingangsbereich eines Gebäudes oder Räume innerhalb eines Gebäudes mit hohem Schutzbedarf wie bspw. Serverräume. Es können je Gebäude mehrere OnlineSchlösser zum Einsatz kommen.

Abbildung 7 | Kartenleser für OnlineSchloss

[12] *Details siehe 3.3.1.5 ZutrittsKontrollZentrale [ZKZ]*

3.3.1.4 MasterLeser

Der MasterLeser ist äußerlich baulich identisch mit dem Kartenleser des OnlineSchlosses. Jedoch gibt es einen großen Unterschied. Der Masterleser kann nicht nur die Rechte eines Transponders auslesen, sondern diesen Transponder auch neu beschreiben – also Rechte zum Öffnen oder Schließen von Türen hinzufügen oder entfernen. Auch der Masterleser ist an die ZKZ angeschlossen. Der Einsatzort des Masterlesers ist meist ein zentraler Punkt innerhalb des jeweiligen Gebäudes. An diesem Masterleser können sich Nutzer ggf. neue Rechte „abholen“. Dies ist bspw. dann notwendig, wenn der Nutzer Zugang zu weiteren Räumen benötigt und diese Rechte vom für die eSa des Fachbereichs Verantwortlichen durch die ClientSoftware zugewiesen bekommen hat.

3.3.1.5 ZutrittsKontrollZentrale [ZKZ]

Je Gebäude wird eine ZutrittsKontrollZentrale eingesetzt. Die Zutrittskontrollzentrale ist der Übergabepunkt aller OnlineSchlösser und Masterleser eines Gebäudes an den Server. Je nach Gebäude gibt es unterschiedlich große ZKZs. Die größte Ausbaustufe ermöglicht es 32 OnlineSchlösser anzubinden.
Die ZKZ wird oft in das WiringCenter des Gebäudes eingebaut. Das WiringCenter ist der Ort, an dem alle Netzwerkkabel eines Gebäudes zusammen laufen und die Anbindung an das Internet bzw. Netzwerk der Freien Universität erfolgt. Da diese Vernetzung auch für die eSa genutzt wird, ist dies der ideale Ort. Sofern die WiringCenter – bspw. aufgrund Ihrer Nutzung als Kopiererraum – jedermann offen stehen, verfügen die entsprechenden Datenschränke über eine gesonderte Schließung.

Die ZKZ hat folgende Aufgaben:

- Vermittlung zwischen Server und OnlineSchlössern / MasterLesern
- Stromversorgung der Kartenleser – gleich ob OnlineSchloss oder Masterleser
- Stromversorgung der Motorschlösser [installiert in Außentüren, Räumen in Gebäuden mit hohem Schutzbedarf wie Serverräume]
- Zwischenspeicherung der Zutrittsrechte bei Ausfall der Servers resp. der Verbindung zum Server
- Im Falle eines Stromausfalls, die Stromversorgung aller angeschlossenen Komponenten sicher zu stellen [Die Dauer ist abhängig von der Zahl der angeschlossenen Komponenten, beträgt aber mindestens 1 Stunde]

Abbildung 8 | ZKZ

3.3.1.6 Server [Software/Datenbank]

Der Server ist das Herzstück der eSa. Auf diesem Server werden alle Zutrittsrechte abgelegt. Möchte eine Person Zutritt über ein OnlineSchloss haben, so wird dieser Wunsch direkt beim Server abgefragt. Nach Validierung der entsprechenden Rechte wird der Zutritt frei gegeben oder aber blockiert.
Der Server nutzt ein im Serverbereich weit verbreitetes Betriebssystem – Microsoft Windows 2003 Server. Zur Speicherung der Zutrittsrechte und –protokolle wird eine Datenbank genutzt. Diese ebenfalls aus dem Hause Microsoft stammende Datenbank – SQL Server 2005 – wird bspw. innerhalb der Freien Universität für das SAP-System genutzt.
Die Überprüfung der Rechte, das Speichern der Zutritte an OnlineLesern, die Kommunikation mit den ZKZs und alle weiteren zum Betrieb der elektronischen Schließanlage notwendigen Aufgaben werden durch die Software des Herstellers ermöglicht. Diese Software – Visual Web – wurde entsprechend den Vorgaben der Freien Universität installiert und konfiguriert. So ist es beispielsweise nicht möglich, außer dem Namen und der Personalnummer weitere Informationen zu einer Karte einzugeben.
Der Server ist in der ZEDAT im dortigen DataCenter [Serverraum] untergebracht.

3.3.1.7 ClientSoftware

Die ClientSoftware ist die Oberfläche zur Administration der eSa. Hier ist es den berechtigten Nutzern möglich, Rechte zu vergeben, Nutzer anzulegen oder zu löschen.
Jedem Fachbereich steht hier nur der jeweilig genutzte Bereich zur Administration offen. Lediglich berechtigte Mitarbeiter der technischen Abteilung können fachbereichsübergreifend administrative Tätigkeiten durchführen.
Zur Nutzung der Software ist keine Softwareinstallation auf den PCs notwendig. Die Software wird über einen aktuellen Browser [Internet Explorer 6, Firefox 2, ...] aufgerufen und genutzt. Voraussetzung hierfür ist jedoch, dass die PCs zur Administration im Netz der sicheren Bürokommunikation [SBK] sein müssen - anderenfalls ist kein Zugang möglich.
Die Kommunikation zwischen Client und Server erfolgt mit einer Verschlüsselungstiefe von 128 Bit.

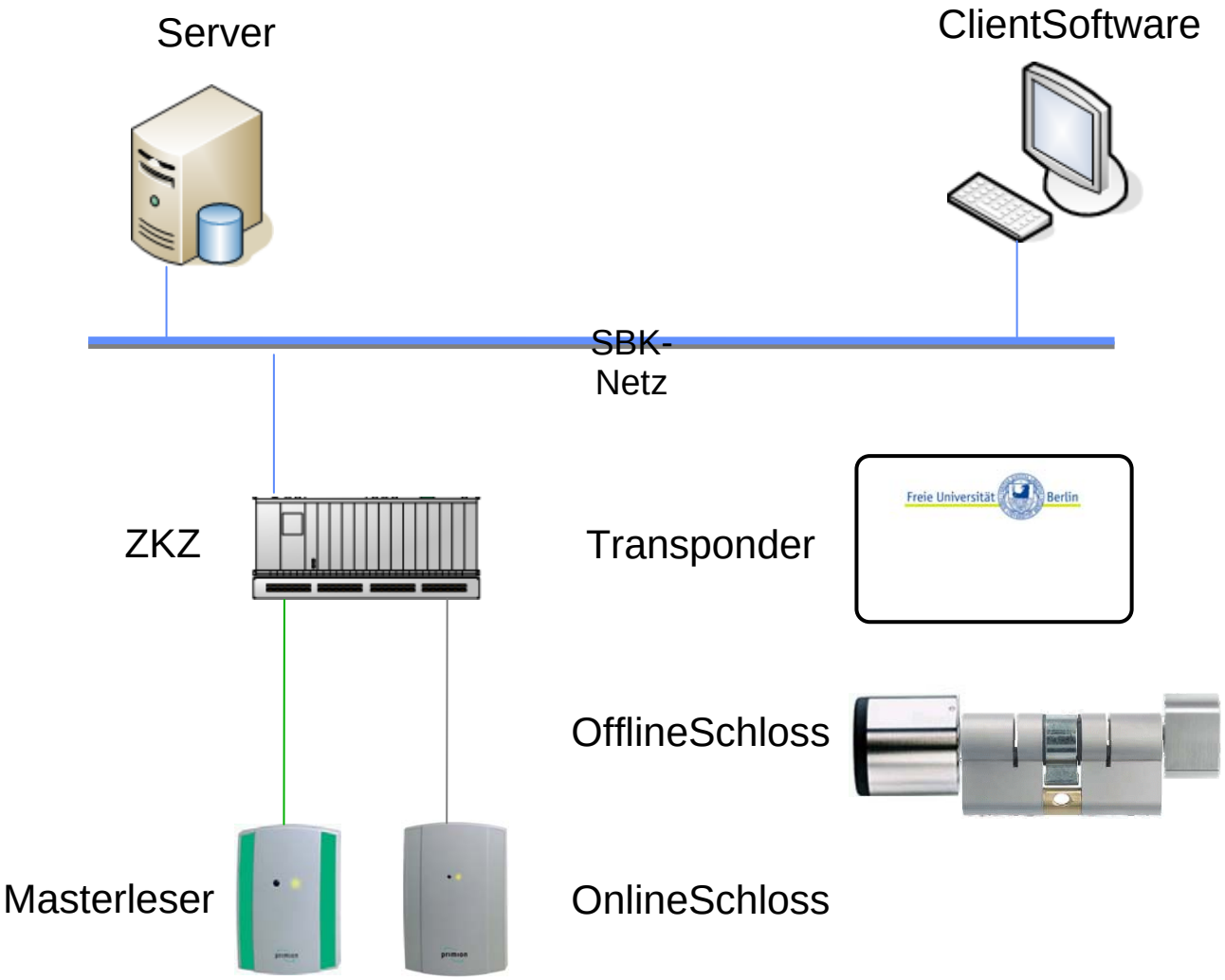

Abbildung 9 | Darstellung Gesamtsystem eSa

3.3.2 Daten

Im Folgenden soll dargelegt werden, wo welche Daten erhoben und abgelegt werden. Hierbei ist zwischen 3 Arten von Daten zu unterscheiden.

1. Daten die durch die Administratoren der eSa angelegt wurden – personenbezogene Daten
2. Daten die durch die eSa selbst erzeugt wurden – Betriebsdaten
3. Daten die auf dem Transponder hinterlegt werden

3.3.2.1 Personenbezogene Daten

Die personenbezogenen Daten der Mitarbeiter werden automatisiert aus FUDIS importiert [vgl. 3.4.1 FUDIS]. Die Eingabe der Daten kann zudem über die Software zur Administration der eSa erfolgen.

Es werden pro Transponder folgende Daten erhoben:

- Nachname, Vorname [Zuordnung der Karte zum Nutzer]
- Personalnummer [sofern es mehrere Nutzer gleichen Namens gibt, ist dies das letztendliche Unterscheidungsmerkmal]
- Gültigkeitsdauer des Transponders [Ende des Arbeitsvertrages]

Weitere Daten werden durch die Administratoren nicht erhoben. Die Software ist so konfiguriert, das weitere Eingaben nicht möglich sind.

3.3.2.2 Betriebsdaten

Daten im OfflineSchloss:

- Nummer/ID des Zylinders
- Uhrzeit durch eigene Uhr
- 500 letzten Buchungen
  - erfolgreiches Lesen eines Transponders -> Transponder gültig
  - fehlgeschlagenes Lesen eines Transponders -> Transponder ungültig
  - Uhrzeit der Zutritte
- Blacklist [gesperrte Transponder]

Daten im OnlineSchloss/Kartenleser:

- Der Kartenleser selbst speichert keinerlei Daten. Die Datenspeicherung und Validierung erfolgt auf der angeschlossenen ZKZ bzw. dem Server.

Daten in der ZKZ:

- Nummer der ZKZ
- Zonenprofil
- ggf. letzte Buchungen [bis zu. 20.000] sofern Server nicht verfügbar
- die von der ZKZ verwalteten Ausweise [bis zu 20.000]

3.3.2.3 Transponderdaten

Fest:
Die Projekt- und Ausweisnummer sowie die Signatur werden bei der Erstellung einmalig auf den Transponder geschrieben und sind vom Nutzer/Administrator nicht veränderbar. Die Projektnummer ist für alle Transponder identisch. Die Ausweisnummer ist nur einmalig in der gesamten eSa vorhanden.

Dynamisch:
Die Berechtigungen können und müssen durch den Nutzer auf den Transponder geschrieben werden. Diese Offline-Daten werden inkrementell über die Masterleser auf den Transponder geschrieben.

3.3.2.4 Visualisierter Datenfluss

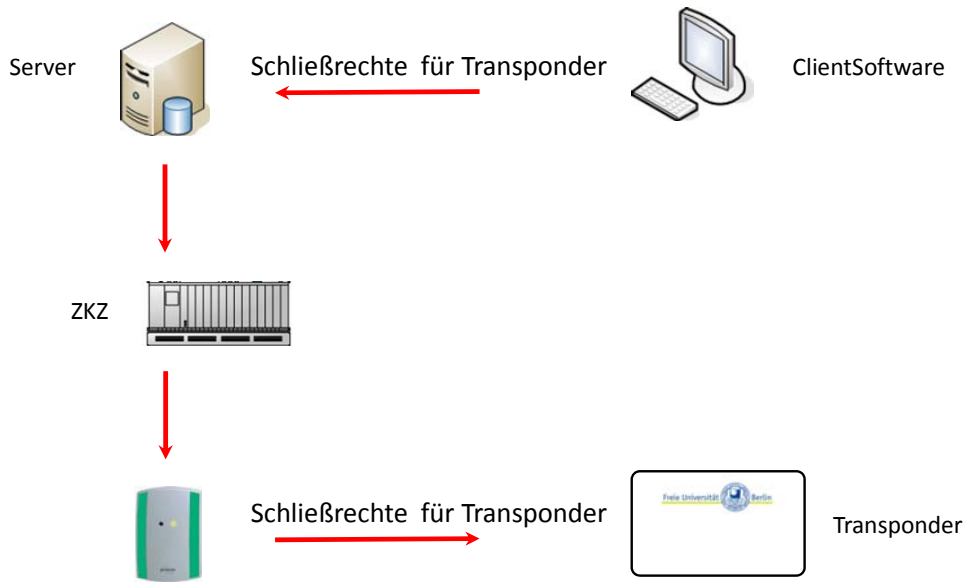

Abbildung 10 | Datenfluss bei Programmierung Transponder

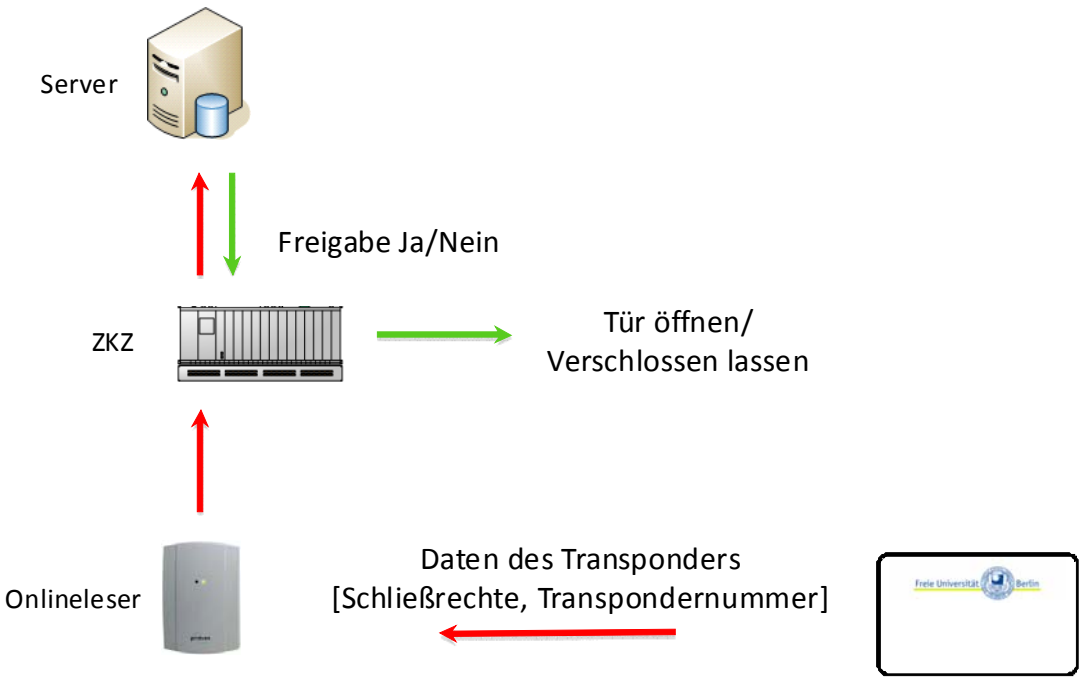

Abbildung 11 | Datenfluss bei Nutzung OnlineSchloss

3.3.3 Rollen

Benutzer
Personen der Gruppe der Benutzer verfügen über einen Transponder mit mind. den Rechten einer Tür und eines Fachbereichs. Der Benutzer kann daher nur die Ihm mittels Transponder zugewiesenen Rechte zum öffnen und schließen mindestens einer Tür ausüben.

Betreiber Teilbereiche eSa
Der Betrieb der elektronischen Schließanlage erfolgt dezentral und zentral. Die Verantwortlichen der Fachbereiche betreiben Ihre eSa – also einen Teilbereich der gesamten eSa - autark. Die Fachbereiche haben folgende Rechte inne:

- Hinzufügen/Ändern/Löschen von Nutzern
- Hinzufügen/Ändern/Löschen von Transpondern
- Hinzufügen/Ändern/Löschen von Schließrechten je Transponder/Nutzer/Gruppe/Gebäude
- Hinzufügen/Ändern/Löschen von Schließzeiten einzelner Türen
- Auslesen von Systemmeldungen der OnlineSchlösser [Öffnung, Schließung der Tür,...] – jedoch keine Anzeige personenbezogener Daten, da diese für diese Rolle gesperrt sind

Betreiber gesamte eSa
Zentrale Aufgaben wie Kartenverlust, Einrichtung neuer Gebäude und Wartungsaufgaben werden durch die technische Abteilung übernommen und ausgeführt. Sofern ein Fachbereich Unterstützung bei der Administration des Teilbereichs der eSa benötigt, kann der Betreiber auch hier aushelfen. Der Betreiber der gesamten eSa verfügt über die Rechte des Betreibers der Teilbereiche und die zur zentralen Administration notwendigen Rechte. Der zentrale Betreiber der eSa verfügt über folgende Rechte:

- Hinzufügen/Ändern/Löschen von Nutzern
- Hinzufügen/Ändern/Löschen von Transpondern
- Hinzufügen/Ändern/Löschen von Schließrechten je Transponder/Nutzer/Gruppe/Gebäude
- Hinzufügen/Ändern/Löschen von Schließzeiten einzelner Türen
- Hinzufügen/Ändern/Löschen von Schlössern/Türen/Objekten/Gebäuden
- Sperren von Transpondern
- Auslesen von Systemmeldungen der OnlineSchlösser [Öffnung, Schließung der Tür,...] – jedoch keine Anzeige personenbezogenen Daten, da diese für diese Rolle gesperrt sind
- Auslesen von Systemmeldungen der OfflineSchlösser [Öffnung, Schließung der Tür, Batteriestatus, ...] – jedoch keine Anzeige personenbezogener Daten, da diese für diese Funktion gesperrt ist

Zutrittskontrolleur
Der Zutrittskontrolleur kann - nur gemeinsam mit dem Betreiber der gesamten eSa - die im System eingepflegten Systemmeldungen um die Anzeige personenbezogener Daten erweitern. Es ist hier ein 4 Augen Prinzip gesetzt. Das heißt, es bedarf zweier festgelegter unterschiedlicher Rollen – in diesem Fall der des Zutrittskontrolleurs und des Betreibers der gesamten eSa – um die Anzeige entsprechend „freizuschalten“. Eine Anwendung findet diese Rolle bspw. bei Diebstahl und/oder anderen Straftaten. Weitere administrative Rechte hat diese Rolle nicht.
Die Rolle des zentralen Betreibers wird durch die für die elektronische Schließanlage verantwortlichen Mitarbeiter der technischen Abteilung übernommen. Die Rolle des Zutrittskontrolleurs obliegt dem Personalrat. [Beschreibung der Vorgehensweise: vgl. 3.3.4.6 Workflow Anzeige personenbezogener Zutritte]

Errichter
Der Errichter – gleichzeitig auch Wartungspartner der eSa – verfügt über die für den Betrieb der eSa notwendigen Rechte. Hierzu wurde dem Errichter ein Zugang zum Server eingerichtet [vgl. 3.4.2 Fernwartung / Teamviewer]. Im Rahmen dieses Zugangs können Konfigurationen an der Software der elektronischen Schließanlage vorgenommen werden.

Hosting
Die Rolle Hosting hat keinen Zugriff auf die eSa. Ihre Aufgabe besteht in der Sicherstellung des Betriebs des Servers. Hierzu gehören folgende Aufgaben:

- Sicherstellung des Betriebs des Servers
- Server ggf. neu starten/beenden/auf andere Hardware umziehen
- BackUp erstellen/einspielen
- Konfiguration des Servers

3.3.3.1 Datenzugriffe der einzelnen Rollen

	Personenbez. Daten	Betriebsdaten	Personenbez. Betriebsdaten	Transponder-daten
Benutzer	Nein	Nein	Nein	Nein
Betreiber Teilb.	Ja	Ja	Nein	Ja
Betreiber Ges.	Ja	Ja	Nein	Ja
Zutrittskontr.	Ja	Ja	Ja	Ja
Errichter	Nein	Ja	Nein	Ja
Hosting	Nein	Nein	Nein	Nein

3.3.4 Workflows

3.3.4.1 Workflow Nutzung OfflineSchloss

1. Nutzer weckt Transponder auf [LED grün]
2. Nutzer hält Transponder vor OfflineSchloss
3. Identifikation des Transponders
4. Übergabe der Rechtegruppe an OfflineSchloss
5. Prüfung im OfflineSchloss [Rechte, Zeitfenster]
6. Übergabe von Systeminfos (Batteriealarm) an Transponder
7. Freigabe [LED grün] oder Sperrung [LED rot] des OfflineSchloss
8. Nutzer öffnet Tür mechanisch durch drehen des Zylinders und drücken der Türklinke

3.3.4.2 Workflow Nutzung OnlineSchloss

1. Leser des OnlineSchloss zeigt Lesebereitschaft an [LED grün]
2. Nutzer hält Transponder vor Leser des OnlineSchloss
3. Identifikation des Transponders
4. Übergabe der Rechtegruppe an Leser
5. Übermittlung der Rechtegruppe an ZKZ
6. Weiterleitung der Daten an Server
7. Prüfung der Berechtigung zum Öffnen der Tür auf dem Server
8. Rückmeldung der Öffnung / Sperrung der Tür an ZKZ
9. Ansteuerung des an der ZKZ angeschlossenen Motorschlosses
10. Riegel der Tür wird durch Motorschloss geöffnet
11. Je nach Tür öffnet sich diese nun vollautomatisch oder aber muss durch den Nutzer durch drücken der Klinke geöffnet werden

3.3.4.3 Workflow Nutzer Software

1. Berechtigter Nutzer meldet sich an der Software an
2. Nutzer sieht alle durch ihn zu verwaltenden Objekte [OfflineLeser, OfflineBereiche, OnlineLeser, ...]
3. Nutzer kann neue Rechte vergeben bzw. bestehende Rechte ändern
4. Änderungen stehen sofort an allen OnlineSchlössern zur Verfügung
5. Änderungen für OfflineObjekte stehen erst nach manueller Übermittlung an einem der MasterLeser dem Nutzer zur Verfügung.

3.3.4.4 Workflow Zutritt sperren [Blacklist] – manuell

1. Nutzer meldet Verlust/Diebstahl des Transponders
2. Transponder wird im System gesperrt, der Blacklist des Systems hinzugefügt
3. OnlineSchlösser übernehmen diese Sperrung sofort, OfflineZylinder müssen die Information manuell übertragen bekommen
4. Administrator speichert Blacklist auf neuem Transponder
5. Jede mit dem gesperrten Transponder zu öffnende Tür muss aufgesucht werden und die Transportkarte vor den OfflineZylinder vorgehalten werden. Hierbei wird dann die Blacklist übertragen und der Zutritt mit dem gesperrten Transponder verhindert

3.3.4.5 Workflow Zutritt sperren [Blacklist] – automatisch

1. Nutzer meldet Verlust/Diebstahl des Transponders
2. Transponder wird im System gesperrt, der Blacklist des Systems hinzugefügt
3. OnlineSchlösser übernehmen diese Sperrung sofort, OfflineZylinder müssen die Information manuell übertragen bekommen
4. Administrator gibt Blacklist für alle Nutzer frei.
5. Nutzer müssen am Masterleser die Blacklist „abholen“
6. Blacklist wird durch alle Nutzer bei Nutzung der OfflineZylinder an die entsprechenden Türen übermittelt

3.3.4.6 Workflow Anzeige personenbezogener Zutritte

1. Betreiber entscheidet, ob Anzeige berechtigt und notwendig
2. Bei OfflineZylinder: Buchungstransferkarte wird genutzt um Buchungen ins System zu transferieren
3. Anmeldung des Betreibers an der Software zur eSa
4. Anmeldung des Personalrates
5. Auswertung der Buchungen der entsprechenden Tür

3.4 Beschreibung der Schnittstellen zu externen Systemen

Im Folgenden werden die Schnittstellen zu Systemen Dritter beschrieben.

3.4.1 FUDIS [FU Directory and Identity Service]

Zur vereinfachten Übernahme der Personaldaten der Mitarbeiter der Freien Universität in die elektronische Schließanlage erfolgt eine Anbindung an FUDIS. Hierdurch wird eine ineffiziente, fehlerbehaftete und zeitraubende doppelte Verwaltung der Mitarbeiter vermieden und der ohnehin zur Verfügung stehende Personalbestand der elektronischen Schließanlage zur Verfügung gestellt.

3.4.1.1 Technische Details

Es wird hierzu täglich ein automatisierter Import der Nutzerdaten aus FUDIS erfolgen. Der Import erfolgt über eine Textdatei [CSV[13]] mit semikolonseparierten Werten. Jede Zeile enthält einen Mitarbeiter. Diese Daten legt FUDIS automatisiert auf dem Server der elektronischen Schließanlage ab. Hierzu wurde ein entsprechender Transferpfad festgelegt.

[13] *http://de.wikipedia.org/wiki/CSV_(Dateiformat)*

Diese Datei wird von Visual Web – der Software auf dem Server der eSa - ebenfalls 1x täglich importiert.

Sollte es zu Fehlern kommen – Nutzer können bspw. keinem Fachbereich zugeordnet werden, oder Daten fehlen - so werden die zentralen Verantwortlichen der Schließanlage [Rolle: Betreiber gesamte eSa] informiert.

Der Import enthält folgende Daten je Mitarbeiter:

1. Name
2. Vorname
3. Personalnummer
4. Gültig von [frühestens Datum des Imports]
5. Gültig bis [Ende des Arbeitsvertrages]
6. Fachbereich
7. Beschreibung des Fachbereichs

Die Daten werden nur aus FUDIS importiert. Ein Export nach FUDIS findet nicht statt. Neue Mitarbeiter werden automatisiert dem jeweiligen Fachbereich zugeordnet und mit einer fiktiven Karten- bzw. Transpondernummer angelegt. Der Verantwortliche der Schließanlage des Fachbereiches muss bei Aushändigung des Transponders die bisherige fiktive Transpondernummer gegen die reale auf der Karte oder dem Schlüsselanhänger aufgedruckte Transpondernummer ändern.

Beispiel eines Imports:

Kowalke; Andy; 00747110815; 01.01.2009;31.12.2009;1;ZEDAT

Innerhalb der Schließanlage würde Herr Andy Kowalke beim Import automatisiert der ZEDAT zugeordnet werden. Der Transponder würde automatisch am 01.01.2010 seine Gültigkeit verlieren, da hier der Arbeitsvertrag beendet ist.

Ausnahmen des automatisierten Imports:

1. *Arbeitsvertrag bzw. Verlängerung des Arbeitsvertrags noch nicht in FUDIS hinterlegt*
   Sofern ein Mitarbeiter darlegen kann, dass sein Arbeitsvertrag verlängert/erstellt wurde, dies jedoch in FUDIS noch nicht hinterlegt ist, kann der Verantwortliche des Fachbereiches hier manuell eingreifen und ein neues Gültigkeitsdatum festlegen. In den letzten 14 Tagen vor Ablauf der Frist eines Nutzers übermittelt FUDIS hierzu diesen Nutzer nicht. Der Nutzer wird erst wieder durch FUDIS zur Verfügung gestellt, wenn das Ende des Arbeitsvertrages mind. 14 Tage in der Zukunft liegt.

2. *Wechsel des Fachbereichs eines Mitarbeiters*
   Wechselt ein Mitarbeiter im Rahmen seiner Tätigkeit von einem Fachbereich in einen anderen, so wird diese Information auch in FUDIS verfügbar sein. Da diese Daten evtl. nicht mit dem Wechsel zur Verfügung stehen, ist eine Interimslösung notwendig. Hierzu wird den Mitarbeitern im neuen Fachbereich ein zeitlich eng begrenzter Transponder ausgehändigt. Bei Verfügbarkeit der Daten in FUDIS bekommt der Mitarbeiter dann seinen entsprechend der Vertragslaufzeit befristeten Transponder.

3.4.2 Fernwartung / Teamviewer

Die Fernwartung kann nur durch den Errichter im Wartungsfall erfolgen und ist daher auch im Wartungsvertrag geregelt. Zur Nutzung ist die vorherige Freigabe durch die ZEDAT notwendig. Die Freigabe wird hierbei telefonisch bei der ZEDAT angefordert.

Als Basis dient die Software Teamviewer[14]. Da diese Software außerhalb des Wartungsfalles auf dem für die elektronische Schließanlage verantwortlichen Server nicht läuft, muss sie Initial von der ZEDAT gestartet werden. Der Fernzugriff erfolgt nur für den Zeitraum der Wartung.

3.4.2.1 Technische Details

Teamviewer ist eine klassische Remote Desktop Software. Der Nutzer kann den Desktop einsehen, den er auch vor Ort hätte. Zudem können Maus und Tastatur aus der Ferne gesteuert werden. Die Übertragung der Daten erfolgt hier per AES mit 256 Bit.

3.4.2.2 Rechte

Der Errichter verfügt im Rahmen der Fernwartung über die gleichen Rechte wie vor Ort in der Freien Universität. Die Fernwartung ist auf den Zugriff auf die Software des Errichters beschränkt. Weitergehende Rechte im Netzwerk und/oder dem Server sind hier nicht vergeben worden.
Die Rolle des Errichters ist insofern unverändert – gleich ob vor Ort oder aus der Ferne.

3.5 Datensicherheit/Verschlüsselung

Die gesamte eSa ist durchgängig verschlüsselt und vor unberechtigten Zugriff geschützt. Es folgt hier eine Aufstellung der verwendeten Schutzmechanismen sowie Verschlüsselungs-algorithmen und deren Verschlüsselungstiefe.

3.5.1 Transponder:

Übertragung beim Lesen/Schreiben:	Crypto1 - 48 Bit Verschlüsselung
Datenhaltung auf dem Transponder:	AES - 128 Bit Verschlüsselung

3.5.2 OfflineSchloss

Übertragung beim Lesen/Schreiben:	Crypto1 48 Bit Verschlüsselung
Datenhaltung im OfflineSchloss:	unverschlüsselt

3.5.3 OnlineSchloss

Kommunikation OnlineSchloss <-> ZKZ:	verschlüsselt
Datenhaltung:	keine

[14] *http://www.teamviewer.com*

3.5.4 ZKZ

Kommunikation ZKZ <-> Server:	3 DES 168/112 Bit
Datenhaltung in der ZKZ:	unverschlüsselt

3.5.5 Server

Datenhaltung Datenbank:	- Zugriff auf Datenbank Passwort geschützt - Daten in Datenbank unverschlüsselt - eSa Passwörter in Datenbank verschlüsselt

3.5.6 ClientSoftware

Zugriff Software:	Zugriff auf Software Passwort geschützt
Kommunikation ClientSoftware <-> Server:	128 Bit SSL
Datenhaltung auf dem PC:	keine

3.5.7 Fernwartung / Teamviewer

Kommunikation Errichter <-> Server:	256 Bit AES

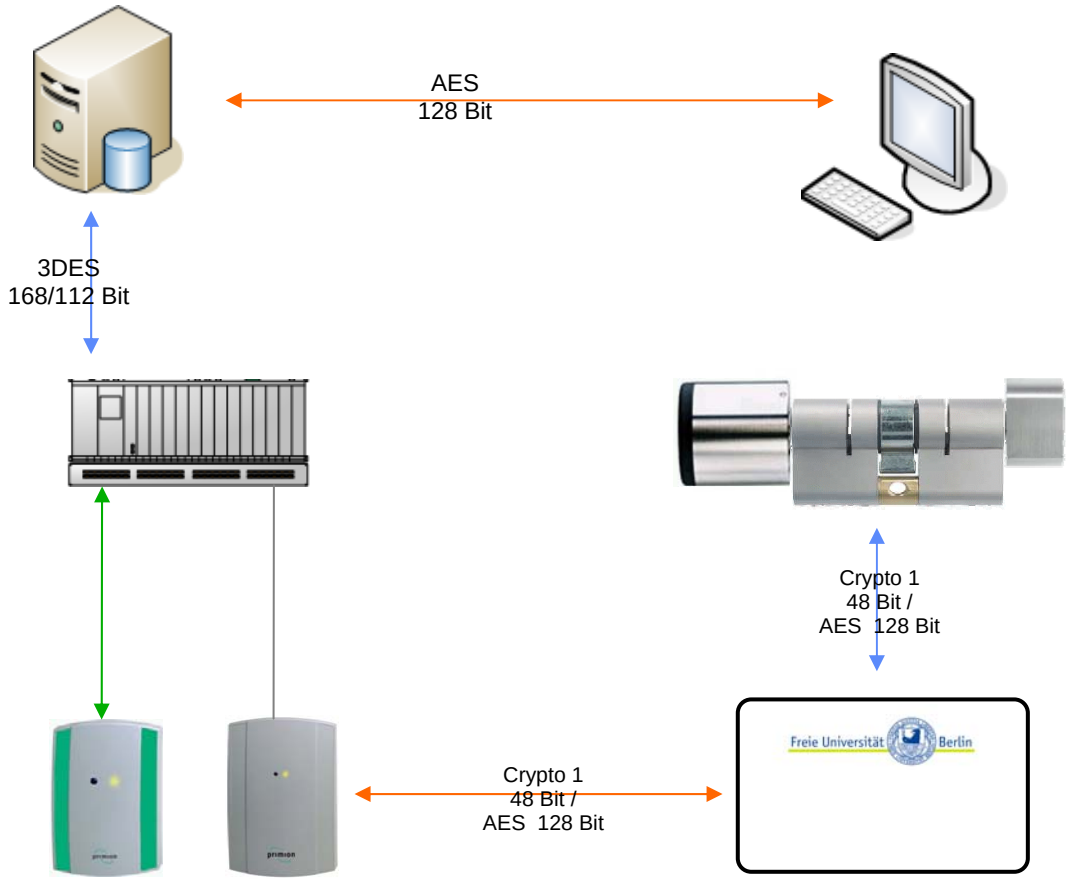

Abbildung 12 Darstellung der verwendeten Verschlüsselungen

4 Schutzbedarfsanalyse

Verlust von		Beeinträchtigung	Personenbezogene Daten	Betriebsdaten	Transponderdaten
			Abschätzung des Schadens		
Vertraulichkeit	Bekannt werden der Daten für Unbefugte…	des informationellen Selbstbestimmungsrechts	Normal	normal	normal
		Verstoß geg. and. Gesetze, Vorschriften und Verträge	Normal	normal	normal
		der persönlichen Unversehrtheit	Normal	normal	normal
		der Aufgabenerfüllung	Normal	normal	normal
		Negative Außenwirkungen	Normal	normal	normal
		Finanzielle Auswirkungen	Normal	normal	Normal
Integrität	Unberechtigte Manipulation der Daten…	des informationellen Selbstbestimmungsrechts	Normal	normal	---*
		Verstoß geg. and. Gesetze, Vorschriften und Verträge	Normal	normal	---*
		der persönlichen Unversehrtheit	normal	normal	---*
		der Aufgabenerfüllung	normal	hoch	---*
		Negative Außenwirkungen	normal	normal	---*
		Finanzielle Auswirkungen	normal	normal	---*
Verfügbarkeit	Verlust der Daten…	des informationellen Selbstbestimmungsrechts	normal	normal	normal
		Verstoß geg. and. Gesetze, Vorschriften und Verträge	normal	normal	normal
		der persönlichen Unversehrtheit	normal	normal	normal
		der Aufgabenerfüllung	normal	hoch	normal
		Negative Außenwirkungen	normal	normal	normal
		Finanzielle Auswirkungen	normal	normal	normal

* siehe 4.1.2 Integrität

4.1 Bewertung der Schutzbedürftigkeit des Verfahrens

4.1.1 Vertraulichkeit

Die zu speichernden bzw. gespeicherten Daten [vgl. Punkt 3.3.2] sind Daten die für fremde Nutzer wenig Relevanz und Nutzbarkeit haben. Eine kriminelle Nutzung der Daten ist daher relativ uninteressant - eine wirtschaftliche Nutzung der gewonnenen Daten ausgeschlossen, da die Daten nur innerhalb der Freien Universität eine Nutzbarkeit haben.
Im Falle eines Diebstahl oder Verlustes des Transponders hat die keine Auswirkungen auf die Vertraulichkeit. Es werden zum einen auf dem Transponder keine personenbezogenen Daten gespeichert und zum anderen sind die abgelegten Betriebsdaten 128 Bit AES verschlüsselt.

Insofern ist der Bereich Vertraulichkeit für alle 3 Bereiche im normalen Bereich.

4.1.2 Integrität

Sofern die Integrität der Betriebsdaten gefährdet ist, ist ggf. die Aufgabenerfüllung gefährdet. Es sind hier Szenarien möglich, die den Nutzern den Zutritt zu den Gebäuden bzw. Büros unmöglich machen. Die Nutzer wären insofern in der Erfüllung Ihrer Aufgaben beeinträchtigt. Das Verlassen der Gebäude ist jederzeit möglich + auch ohne Transponder. Zusätzlich können alle mit einer elektronischen Schließung versehenen Außentüren – in der Regel ein Motorschloss - im Notfall mit einem mechanischen Schlüssel geöffnet werden.
Die Integrität der Tansponderdaten wurde nicht betrachtet. Da die Daten auf dem Transponder zusätzlich zur 48 Bit Verschlüsselung des Transponders [Crypto 1] selbst zusätzlich mit 128 Bit AES-Verschlüsselung verschlüsselt werden – welche gemeinhin als sicher gilt – kann die Integrität der Daten auf dem Transponder sicher gestellt werden.
Ein Angriff auf AES würde aktuell ca. 2^{100} Rechenoperationen benötigen[15]. Insofern ist hier von einem theoretischen Angriff auszugehen.

4.1.3 Verfügbarkeit

Sollten die Daten verloren gehen, so würde dies die gleiche Folge haben wie der Verlust der Integrität der Daten – dem Nutzer würde ggf. der Zutritt verwehrt werden. Das Verlassen der Gebäude ist hiervon wieder völlig unberührt.

4.2 Risikoanalyse

Es werden hier die in der Schutzbedarfsanalyse aufgeführten Risiken betrachtet und Lösungswege aufgezeigt. Die Lösungswege können entweder durch den jeweiligen Fachbereich, die technische Abteilung oder aber den Wartungspartner gegangen werden. Der Wartungspartner hat eine Reaktionszeit zur Behebung von Fehlern und Störungen von 4 Stunden für 365 Tage im Jahr.

4.2.1 Integrität der Betriebsdaten

Der Schaden der durch die Manipulation der Betriebsdaten entstehen würde ist als hoch zu betrachten. Da der Schaden aber „vorhersehbar“ ist, sind auch entsprechende Lösungen zur Minimierung des Schadens auf einen „normalen“ Level zu planen.

[15] *http://eprint.iacr.org/2002/044*

Sofern eine Manipulation der Daten festgestellt wird, der Mitarbeiter ggf. damit vor verschlossener Tür bzw. verschlossenen Türen steht, kann jederzeit durch berechtigte Mitarbeiter der technischen Abteilung eingegriffen werden. Sollten bspw. Transpondernummern geändert worden sein, so kann jederzeit ein neuer Transponder erstellt werden und diesem die bisherig bestehenden Rechte übertragen werden.
Sollten die Betriebsdaten der Gesamtanlage geändert worden sein, so ist auch hier eine schnelle Hilfe möglich. Es wird zentral auf dem Server ein BackUP eingespielt. Damit ist das System wieder verfügbar und die Integrität der Daten wieder hergestellt. BackUps werden täglich automatisiert erstellt.

4.2.2 Verfügbarkeit der Betriebsdaten

Die Verfügbarkeit dieser Daten wird durch mehrere technische Lösungen erhöht.

4.2.2.1 Verfügbarkeit Hardware

Der Server ist ein virtueller Server. Das heißt, dass auf performanter Hardware mehrere virtuelle Server laufen die sich die Hardware teilen. Insofern hat der Server für die elektronische Schließanlage keine eigene Hardware. Sollte dieser Server ausfallen, so kann er jederzeit auf einer anderen Hardware gestartet und genutzt werden. Da die Freie Universität sog. Blades einsetzt – mehrere „echte“ Hardwareserver in einem Gehäuse, ist mindestens immer ein weiterer Server verfügbar.
Zudem verfügt das gesamte DataCenter über eine unterbrechungsfreie Stromversorgung, so dass auch ein kurzer Stromausfall überbrückt werden kann.

4.2.2.2 Verfügbarkeit zentraler Daten

Die für den Betrieb der Anlage wichtigen Daten werden passwortgeschützt in einer Datenbank auf dem Server abgelegt. Insofern ist zusätzlich zu Firewall und Passwortschutz der direkte unbefugte Zugriff auf die Daten verhindert.
Die Datenbank wird jeden Tag komplett gesichert, so dass ggf. Änderungen jederzeit schnell wieder rückgängig gemacht werden können. Das erstellte BackUP wird im Rahmen des BackUPs der ZEDAT mit aufgenommen und entsprechend gesichert bzw. archiviert.

4.2.2.3 Verfügbarkeit der Daten je Gebäude/Fachbereich

Weiterhin gibt es je Gebäude eine ZKZ – eine sogen. Zutrittskontrollzentrale. Diese speichert jeweils die für das Gebäude wichtigen Zutrittsdaten zwischen und stellt so im Falle eines Ausfalls des Servers oder aber der Verbindung zum Server sicher, dass die Anlage weiter funktionstüchtig bleibt. Die Validierung der Daten erfolgt dann automatisiert über die ZKZ. Sowie der Server wieder verfügbar ist, werden die Daten zwischen ZKZ und Server ausgetauscht.
Alle ZKZs werden zudem über eine unterbrechungsfreie Stromversorgung im Falle eines Stromausfalls mit Strom versorgt, so dass selbst im Fall eines Stromausfalls die Anlage weiter genutzt werden kann.

5 Abbildungsverzeichnis

6 Quellenangaben

1 http://www.parlament-berlin.de/pari/web/wdefault.nsf/vFiles/D14/$FILE/Verfassung von Berlin_Times14.pdf
2 http://bundesrecht.juris.de/bdsg_1990/
3 http://www.datenschutz-berlin.de/attachments/346/BlnDSG2008.pdf?1200651252
4 http://www.fu-berlin.de/service/zuvdocs/fu-rundschreiben/2008/it-sicherheitsrichtlinie.pdf
5 http://web.fu-berlin.de/prd/dienst/DV_IT_Grundsatz.pdf
6 http://de.wikipedia.org/wiki/Radio_Frequency_Identification
7 http://de.wikipedia.org/wiki/ISO_7816
8 http://www.nxp.com/products/identification/mifare/index.html
9 http://events.ccc.de/congress/2007/Fahrplan/events/2378.en.html
10 http://de.wikipedia.org/wiki/Advanced_Encryption_Standard
11 http://csrc.nist.gov/publications/PubsSPs.html
12 http://eprint.iacr.org/2002/044
13 http://de.wikipedia.org/wiki/CSV_(Dateiformat)
14 http://www.teamviewer.com/de/