Biometric
Solutions

ZUTRITTSKONTROLLE

Technische Informationen und Anforderungen

Inhaltsverzeichnis

Copyright

Vorwort

Dieses Dokument dient in erster Linie als Beschreibung der erweiterten Zutrittskontrolle für einen Raum oder ein Gebäude, in dem eine Dokumentenausgabebox® steht.

Das Dokument beschreibt die technischen Elemente und den Ablauf.

Zur besseren Lesbarkeit wird in der vorliegenden Anleitung auf die gleichzeitige Verwendung männlicher und weiblicher Sprachformen verzichtet. Es wird das generische Maskulinum verwendet, wobei beide Geschlechter gleichzeitig gemeint sind.

Weitere Informationen sowie aktuelle Neuigkeiten finden Sie auch unter Biometric Group (biometric-group.de).

Zutrittskontrolle

Vorstellung der UniLock-Zutrittskontrolle

Dokumentenausgabeboxen von Biometric Solutions werden unter anderem zur Abholung von Reisepässen benutzt, sodass Bürger ihre Pässe als Selbstbedienungslösung abholen können. Dokumentenausgabeboxen werden jedoch auch zunehmend intern von Verwaltungen genutzt, sodass Mitarbeiter Dokumente, IT-Ausrüstung, Telefone, Zugangskarten usw. abholen können.

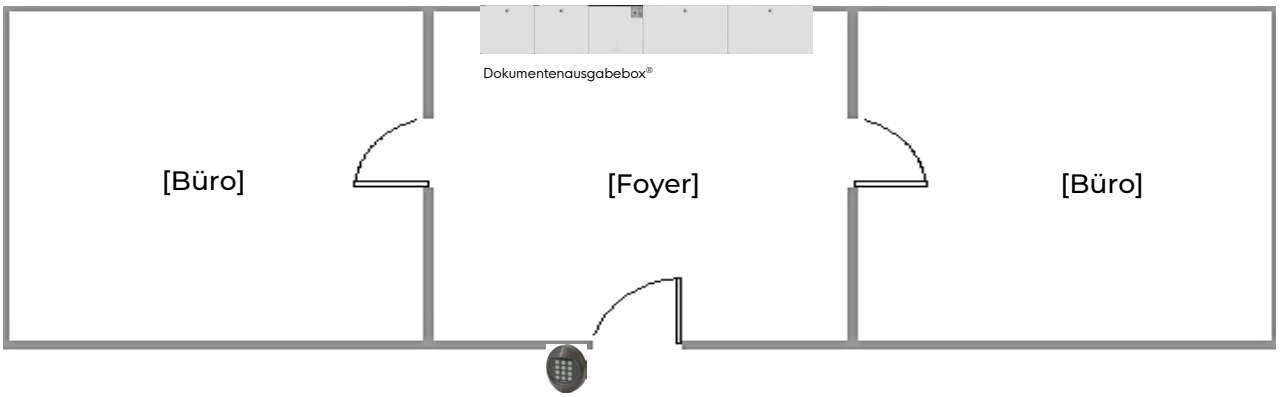
Dokumentenausgabeboxen stehen typischerweise in Bürgerämtern, Bibliotheken oder anderen öffentlichen Gebäuden mit Öffnungszeiten, die Bürgern Zugang zur Ausgabebox ermöglichen.
Um Bürgern mehr Flexibilität zu bieten, ist es möglich, eine Option mit Lobby-Zutrittskontrolle hinzuwählen, sodass man eine hundertprozentige Selbstbedienungslösung erhält. Somit können Bürger rund um die Uhr erscheinen und Dokumente abholen.

Natürlich ist es auch möglich, die Zeiten weiter einzuschränken, innerhalb derer Bürger Zugang zur Dokumentenausgabebox haben. Bürger erhalten Zutritt durch die Tür, indem der Abholcode verwendet wird, der bereits für die Dokumentenausgabebox benutzt wird. Der Code ist in dem Zeitraum gültig, in dem auch Zugang zur Abholung von Dokumenten besteht.

Die Integration von Biometric Solutions und Unitek bietet den Vorteil, dass man sich keine Gedanken über die Verwaltung des Benutzerzugangs zu dem Gebäude machen muss, in dem die Dokumentenausgabebox steht. Sobald Dokumente in die Ausgabebox gelegt werden, werden SMS mit einem Abholcode an den Bürger versendet, der Zugang zum Gebäude und zur Dokumentenausgabebox gibt.

Der Ablauf

Wenn die Dokumentenausgabebox in einer Bibliothek, einem Rathaus oder Ähnlichem aufgestellt wird, gelten häufig Öffnungszeiten, innerhalb derer Bürger Zugang zu den Räumlichkeiten haben, und diese Öffnungszeiten können mit UniLock verwaltet werden. Außerhalb der Öffnungszeiten wird der Zutritt dann durch den Abholcode ermöglicht, der den Bürgern per SMS zugeschickt worden ist.



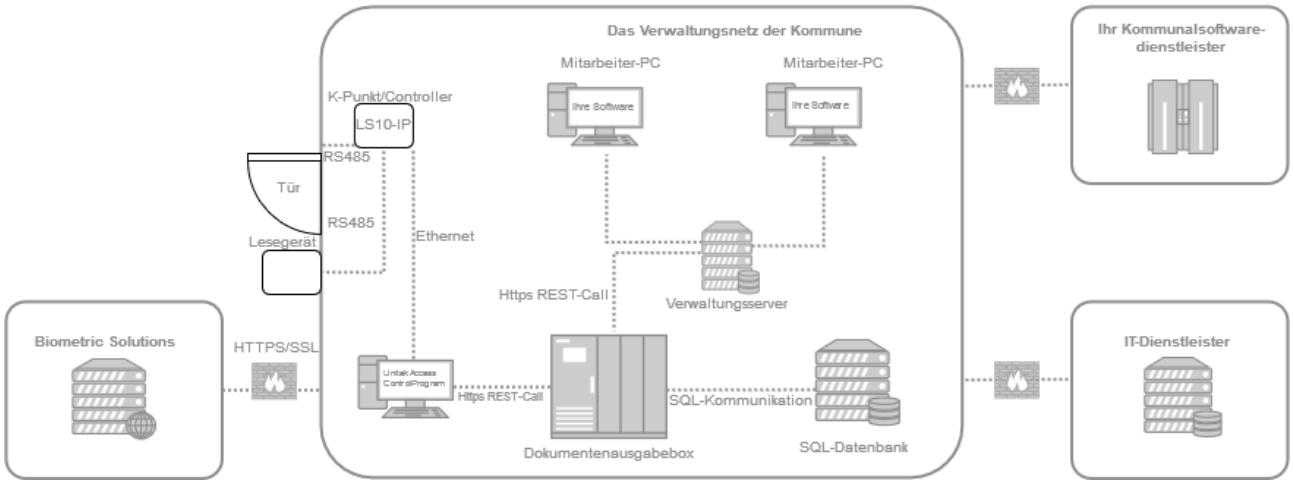
Vorteile

- Erweiterte Öffnungszeiten
- Keine Terminvereinbarung
- Verringerung des Infektionsrisikos
- Erhöhte Sicherheit
- Bürgerfreundlichkeit beim Abholprozess wird erhöht

Netzwerkarchitektur

Technisches Schaubild

Die Abbildung unten gibt einen Einblick in die Netzwerkarchitektur und die einzelnen Komponenten. Die Verbindungen mit dem Sicherheitssystem UniLock sind grün markiert.



Technische Details

Die gesamte Netzwerkkommunikation kann mit Ethernet-Kabelverbindung realisiert werden. Das Sicherheitssystem kann zusätzlich aber auch über WiFi oder das Mobilfunknetz verbunden werden, wenn entfernte Gebäude (mit eventuell schlechter Internetanbindung) dies erfordern. Im gezeigten Beispiel sind keine weit entfernt stehenden zusätzlichen Gebäude eingezeichnet, diese können je nach Bedarf, auf verschiedenste Weise in UniLock eingebunden und angesteuert werden.

Folgende Kommunikation zwischen den einzelnen Elementen ist zu berücksichtigen:

HTTP ist bei der Kommunikation im Verwaltungsnetz der Kommune erforderlich. Es ist nicht notwendig, intern HTTPS zu benutzen, da die Kommunikation nur im gesicherten Verwaltungsnetz der Kommune stattfindet, aber wir empfehlen es. Kommunikation mit Systemen außerhalb der Verwaltung (weit entfernte Gebäude, Überwachung des Alarmsystems im Homeoffice) sollte immer abgesichert sein.

Wenn die Kommune im Verwaltungsnetz HTTPS benutzt, muss ein Zertifikat erstellt und laufend aktualisiert werden. Dies wird mit der Verwaltung, dem gewählten Dienstleister für Kommunalsoftware und Biometric Solutions abgesprochen.

Die HTTPS-Verbindung zu Biometric Solutions wird für fünf Funktionen benötigt:

- Software-Updates
- Berichterstattung
- Protokollinformationen
- Fernwartung
- Administration der Dokumentenausgabebox

Biometric Solutions setzt nur technisches Personal ein, um den Support der Verwaltung zu unterstützen. Genutzt wird ein Zugang via HTTPS-Verbindung. Auf Wunsch der Verwaltung wird eine Verschwiegenheitserklärung für die betroffenen Mitarbeiter erstellt.

Das Schaubild zeigt auch den IT-Lieferanten und den gewählten Dienstleister für Kommunalsoftware, in diesem Beispiel werden jedoch keine Daten mit ihnen ausgetauscht. Sehen Sie hierzu auch die Softwarearchitektur weiter unten im Dokument.

Software-Updates (Biometric Solutions)

Die Dokumentenausgabebox sucht jede Nacht zwischen 21:00 und 06:00 Uhr nach Software-Updates. Wenn ein Update verfügbar ist, wird es automatisch heruntergeladen und auf dem Computer der Dokumentenausgabebox installiert.

Die Updates werden von

https://ws.biometric.dk/wsbio.asmx

heruntergeladen. Alle Dateien sind SHA-hashed und werden beim Download validiert.

Software-Updates

UniLock erhält laufend Updates mit den neuesten Programmfunktionen und Anpassungen an neue Versionen von Windows. Neue Programmversionen sind 100 % abwärtskompatibel mit älteren Versionen.

Monitoring

Jede Minute sendet die Dokumentenausgabebox eine Berichterstattung an unseren Server, der uns Echtzeitinformationen zum Status jedes Produkts gibt. Es werden keine bürgerbezogenen Daten oder Aufnahmen übertragen.

Die Daten über die Systemlebensdauer werden an folgende Adresse gesendet:

https://ws.biometric.dk/wsbio.asmx

Protokollinformationen

Die Protokollierung aller Ereignisse findet direkt an den Kontrollpunkten (Zugangscomputern) statt. Die Informationen werden je nach Voreinstellungen in regelmäßigen Abständen oder kontinuierlich weitergeleitet und in der SQL-Datenbank gespeichert. Es kann vom Arbeitscomputer aus eingesehen werden, wer wann zu welchem Zeitpunkt das Gebäude betreten oder verlassen hat. Es wird sowohl der Zeitstempel abgespeichert, wann die Interaktion mit dem Kontrollpunkt stattgefunden hat als auch der Zeitstempel, wann die Logdatei weitergeleitet wurde.

Fernwartung

Zu Fernwartungszwecken führt Biometric Solutions einen Fernzugriff auf den Computer der Dokumentenausgabebox aus, um unseren Kunden einen effizienten Support zu bieten.

Wir verwenden die Fernwartung der einzelnen Verwaltungen oder IT-Dienstleister und senden die Namen und E-Mail-Adressen der bei uns verantwortlichen Kollegen.

Wir erwarten, dass alle Fernwartungssitzungen beim IT-Dienstleister als Video aufgezeichnet, protokolliert und archiviert werden und dass Details durch einen Fernwartungsvertrag geregelt werden.

Biometric Solutions benötigt keinen Fernzugriff auf andere Computer im Netzwerk der Verwaltung.

Anforderungen

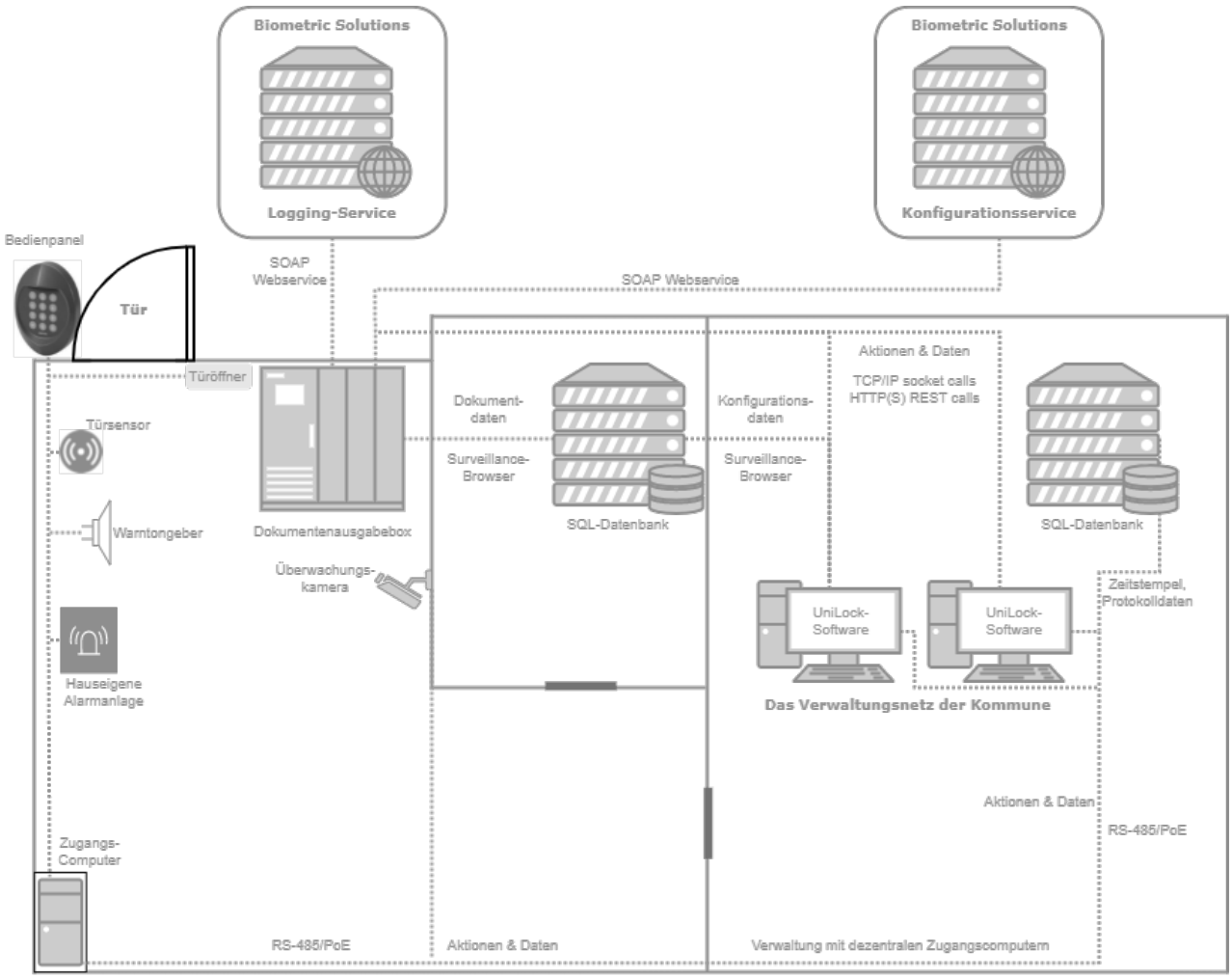
UniLock wurde entwickelt für Windows 7 und neuere Betriebssysteme. In diesem Sinne können Minimalanforderungen definiert werden als:

- Ein Prozessor mit 1.6 GHz. Bei großen Anlagen muss ein entsprechend größerer Prozessor verwendet werden
- Minimum 8 GB Ram oder mehr. Es ist schwierig, generell etwas über die Anforderungen an das RAM zu sagen, da es hier darauf ankommt, wie viele Programme gleichzeitig laufen
- Minimum 20 GB Festplattenspeicher
- Es wird ein Bildschirm mit 17'', 1600 x 1200 Pixeln und mindestens 60 Hz Wiederholungsrate empfohlen
- Soll das Programm in einem Netzwerk installiert werden, so soll die Verbindung zu den Arbeitsstationen mindestens 10 Mbit/s betragen
- Es wird empfohlen, zumindest während der Installation von UniLock auf dem Installationscomputer eine Internetanbindung bereitzustellen, damit die Microsoft-Komponenten und der SQL-Server vollständig installiert werden können

Softwarearchitektur

Technisches Schaubild

Die untenstehende Abbildung gibt einen Einblick in die Softwarearchitektur und die einzelnen Komponenten. Die Verbindungen mit dem Sicherheitssystem UniLock sind grün markiert.



Technische Details

Die gesamte Softwarekommunikation kann mit Ethernet-Kabelverbindung realisiert werden. Das Alarmsystem kann zusätzlich aber auch über WiFi oder das Mobilfunknetz verbunden werden, wenn entfernte Gebäude mit eventuell schlechter Internetverbindung dies erfordern.

Folgende Kommunikation zwischen den einzelnen Elementen ist zu berücksichtigen:

Kommunikation mit der SQL-Datenbank

Die Dokumentenausgabebox wird Nahaufnahmen bei Abgabe und Abholung aufzeichnen, die als unterstützende Dokumentation dienen. Die Nahaufnahmen werden unverarbeitet und direkt in der SQL-Datenbank gespeichert.

Die Datenbank muss mindestens Microsoft SQL 2012 oder eine aktuellere Version verwenden. UniLock verwendet die SQL-Datenbank, um Protokolldateien und Logdateien zu speichern. UniLock unterstützt alle SQL-Server-Versionen. Als Standard wird häufig die Version 2014 Express verwendet. Für UniLock und für die Aufzeichnungen der Dokumentenausgabebox kann dieselbe SQL-Datenbank verwendet werden, die Anwendungen können aber auch verschiedene Datenbanken benutzen.

Kommunikation mit dem Zugangscomputer

Die Aufgabe des Zugangscomputers ist es, die Zugangsberechtigungen am jeweiligen Zugangspunkt zu verwalten. Der Zugangscomputer wird mit 230 Volt versorgt. Im gezeigten Beispiel wird nur der Zugang am Haupteingang kontrolliert, die innenliegenden Durchgänge sind manuell verschlossen. Es ist möglich, mehrere Türen mit mehreren Zugangscomputern zu verwalten, auch in verschiedenen Gebäuden. Alle Zugangskennungen (Abholcode, etc.), Zeitpläne, Sicherheitsniveau usw., die darüber entscheiden, ob ein Benutzer Zutritt hat, werden in den Zugangscomputern dezentral gespeichert. Der Zugangscomputer sendet die Autorisierung zur Türöffnung an das Schloss und wird geschützt in der Nähe der Tür aufgestellt. Verbindung mit dem Arbeitscomputer im Büro der Verwaltung ist nur notwendig, wenn Daten geändert oder gelesen werden sollen. Jeder Zugangscomputer speichert auch Logdateien mit Zeitstempel für seinen zugehörigen Zugriffspunkt.

Kommunikation mit der weiteren Ausstattung

Sämtliche Einheiten wie Bedienpanel, Türöffner usw. werden mit dem Zugangscomputer über RS-485 mit dem Türcontroller verbunden. Das bedeutet, dass auch bei Ausfall der Arbeitscomputer im Büro, bei Ausfall der Netzwerkverbindung oder bei Ausfall anderer Zugangscomputer der Zutritt am überwachten Haupteingang kontrolliert werden kann. Im Falle eines Stromausfalls kann der Zugangscomputer auch mit einer zusätzlichen Batterie ausgestattet sein. In den Endmodulen wie dem Bedienpanel/Lesegerät sind keinerlei Kontrollsysteme für die Türen enthalten, sondern es wird ausschließlich die Zugangsberechtigung gelesen und weitergeleitet, was die Sicherheit erhöht.

UniLock

Mit dem Programm UniLock können die mit den Zugangscomputern eingerichteten Kontrollpunkte sowie das Alarmsystem und die Videoüberwachung verwaltet werden. Es kann eingerichtet werden, wer wann wie Zugang hat und es wird mit Zeitstempel protokolliert, wer kommt und wer geht.

Das Programm beinhaltet einen Zugangseditor, die Übersicht zur Speicherung der Daten in der Datenbank und die Kommunikation mit den anderen Elementen des Überwachungssystems.
Der Zugangseditor ist das Programm, das im Alltag am meisten verwendet wird. Hier können Kontrollpunkte (Türen), Personen und Zeitpläne eingerichtet werden und es können Überwachung, Nachforschungen und die generelle Verwaltung durchgeführt werden. Ändert ein Mitarbeiter die Daten in der Datenbank, so sendet das Kommunikationsmodul die Änderungen automatisch an die Kontrollpunkte (die Zugangscomputer für die Türen). Das Programm kann mit einer Vielzahl von anderen Programmen Informationen austauschen und ist so konzipiert, dass alle Funktionen mit ein bis zwei Mausklicks ausgewählt werden können.

Installation

UniLock erhöht die Sicherheit in Ihren Räumlichkeiten, ersetzt aber nicht ein ausgearbeitetes Sicherheitskonzept. Überlegen Sie sich bereits vor der Installation, wer wann wie Zugang zu Ihren Räumlichkeiten erhalten soll. Gibt es Administratoren, die einen ständigen Zugang benötigen? Gibt es Arbeitszeiten, außerhalb derer das Gebäude von bestimmten Mitarbeitern nicht mehr betreten werden soll? Welches Sicherheitsniveau soll wann gelten?

UniLock ist so konzipiert, dass bei der Installation (wie auch bei Updates) alles möglichst automatisch ablaufen soll. Es muss nur ausgewählt werden, in welcher Ordnerstruktur die Programme und die Datenbank installiert werden sollen. Das Programm erkennt selbstständig, ob es sich um ein Update handelt. Dateien und die Lizenz werden automatisch angelegt. Bei der Installation wird eine Beispieldatenbank mit einer Reihe von Namen, Kontrollpunkten und Zeitplänen erstellt. Diese kann als Ausgangspunkt für eigene Eingaben verwendet werden oder gelöscht werden. Es ist auch möglich, bereits bestehende Datenbanken zu importieren. Halten Sie am besten alle Daten bereit, um Ihr persönliches Sicherheitskonzept umzusetzen.