Sicherheit

Unter diesem Menüpunkt können Sicherheitseinstellungen für die Zutrittskontrolle und zwischen kabelgebundenen Kentix-Geräten konfiguriert werden.

Allgemein

Um die Sicherheit der Kommunikation zwischen drahtgebundenen Kentix-Geräten zu erhöhen, kann ein Kommunikationsschlüssel eingegeben werden. Damit wird die Kommunikation zwischen den Geräten zusätzlich durch eine Kentix-spezifische Verschlüsselung geschützt. Der Schlüssel muss dazu auf allen miteinander kommunizierenden Kentix-Geräten (Main Device und Satellite Devices) gleich sein.

Jedem Benutzer kann unter dem Menüpunkt BENUTZERVERWALTUNG eine eigene PIN zugewiesen werden. Damit können an SmartAccess Komponenten mit integrierter Tastatur Buchungen mit den entsprechenden Berechtigungen des Benutzers durchgeführt werden. Eine höhere Sicherheit kann durch eine längere PIN erreicht werden. Diese kann unter diesem Menüpunkt von PIN-Länge 4 bis PIN-Länge 10 eingestellt werden.

Das Rackschloss DoorLock-RA4 unterstützt nur die Ziffern 1 bis 4.

RFID-Einstellungen

Die Kentix SmartAccess Komponenten nutzen RFID-Token (Radio-Frequency Identification) zur berührungslosen Zutrittskontrolle. Jeder Token zeichnet sich durch eine weltweit eindeutige UID (Unique Identifier) und Verschlüsselungstechnologie aus. Als Technologie wird standardmäßig MIFARE®DESFire® verwendet.

Unter KentixONE kann nun für jeden Benutzer festgelegt werden, ob und welche RFID-Verschlüsselung verwendet werden soll. Wird keine Verschlüsselung verwendet, kann die UID mit jedem MIFARE®DESFire®-Leser ausgelesen und kopiert werden. Die UID dient dann ohne weiteres als Grundlage für das Klonen von Identmedien, wodurch Personen Zutritt zu Bereichen erhalten, in die sie normalerweise nicht gelangen dürften. Um keine Verschlüsselung zu verwenden, muss diese im Menü entsprechend ausgewählt werden.

Standardmäßig werden alle SmartAccess-Komponenten mit einer Kentix-spezifischen Verschlüsselung ausgeliefert.

Nur Token, die nach 06/2018 ausgeliefert wurden, enthalten die Kentix-spezifische Verschlüsselung.

Zusätzlich kann eine eigene Verschlüsselung verwendet werden. Dazu muss eine JSON-Konfigurationsdatei (JavaScript Object Notation) in KentixONE hochgeladen werden. Eine Vorlage für die Konfigurationsdatei kann nach Auswahl von „Eigene Verschlüsselung“ heruntergeladen werden.

```
{
    "mifare_desfire": {
        "app_id": "0xb2c3d4",
        "file_number": 0,
        "file_offset": 0,
        "file_length": 32,
        "file_type": 1,
        "auth_method": 2,
        "des_key": "0xa1b2c3d4e5f6a1b2c3d4e5f6a1b2c3d4",
        "key_number": 1,
        "card": {
            "data": [
                                {
                    "name": "OEM Code",
                    "position_start": 1,
                    "position_end": 64,
                    "encoding": "hexadecimal"
                },
                {
                    "name": "Card Number",
                    "position_start": 65,
                    "position_end": 128,
                    "encoding": "hexadecimal"
                }
            ]
        }
    }
}
```

MIFARE DESFire App ID

`"app_id"`

Die MIFARE DESFire App ID ist eine eindeutige 3-Byte-Kennung, die zur Identifizierung und Trennung verschiedener Anwendungen auf einer MIFARE DESFire-Karte verwendet wird. Sie ermöglicht die Existenz und den unabhängigen Betrieb mehrerer Anwendungen auf derselben Karte, wobei jede Anwendung ihre eigenen Sicherheitseinstellungen und Dateien hat.

Dateinummer

`"file_number"`

Die Dateinummer dient zur eindeutigen Zuordnung der unterschiedlichen Dateien auf der MIFARE DESFire-Karte. Damit eine eigene Verschlüsselung realisiert werden kann, muss in der Konfigurationsdatei für KentixONE die entsprechende Dateinummer hinterlegt werden. Die Dateinummer ist eine 1-Byte-Zahl im Bereich von 0 bis 31.

Offset

`"file_offset"`

Der Offset gibt an, ab welchem Byte die Datei gelesen wird.

Dateigröße

`"file_length"`

Die Dateigröße gibt die Länge der zu lesenden Datei in Bytes an.

Verschlüsselung

`"file_type"`

Die Daten können verschlüsselt oder unverschlüsselt in der Datei abgelegt werden. Daher kann die Variable folgende Werte annehmen:

0 = Daten sind unverschlüsselt abgelegt

1 = Daten sind verschlüsselt abgelegt

Authentifizierungsmethode

`"auth_method"`

Um die Datei vor unberechtigtem Lesen oder Schreiben zu schützen, ist eine Authentifizierung erforderlich. Dabei unterstützt KentixONE zwei verschiedene Verschlüsselungsmethoden, die in der Konfigurationsdatei eingestellt werden können.

0 = Authentifizierung ist ausgeschaltet

1 = Dies ist eine stärkere, aber komplexere Form der DES (Data Encryption Standard) Authentifizierung. Es werden zwei 56-Bit-Schlüssel verwendet, die zu einem 112-Bit-Schlüssel kombiniert werden. Dies bietet ein höheres Sicherheitsniveau als das einfache DES.

2 = AES (Advanced Encryption Standard) ist ein noch stärkeres Verschlüsselungsverfahren, das einen 128-Bit-Schlüssel verwendet. AES ist bekannt für seine Stärke und Effizienz, was es zu einer idealen Wahl für Hochsicherheitsanwendungen macht. Diese Option wird entsprechend dem aktuellen Stand der Technik verwendet.

DESFire Schlüssel

`"des_key"`

Der Schlüssel wird zur Authentifizierung benötigt. Der Schlüssel ist sowohl für die Authentifizierungsmethode 1 als auch für die Authentifizierungsmethode 2 gültig.

Schlüsselnummer

```
"key_number"
```

In der Regel werden mehrere Schlüssel mit unterschiedlichen Berechtigungen angelegt. Damit KentixONE die Datei mit den entsprechenden Benutzerdaten lesen kann, muss in der Konfigurationsdatei der Schlüssel und die Schlüsselnummer mit den entsprechenden Berechtigungen angegeben werden.

Daten

```
"card": {
            "data": [
                                {},
                                ...,
                                {}
                    ]
        }
```

Im Datenblock der Konfigurationsdatei wird die Interpretation der ausgelesenen Daten beschrieben. Der Datenblock kann aus mehreren Teilen (Sektoren) bestehen. Jeder Sektor enthält einen Bezeichner, den Beginn und das Ende des Sektors und wie die Daten konvertiert werden sollen. Zusätzlich kann ein statischer Wert angegeben werden, gegen den immer geprüft wird, z.B. ein Firmenname.

Bezeichner

```
"name"
```

Jeder Sektor benötigt einen Bezeichner, welcher als Zeichenkette gespeichert wird.

Start des Sektors

```
"position_start"
```

Durch Angabe des Start- und Stop-Bits wird der zu lesende Sektor festgelegt.

Ende des Sektors

```
"position_end"
```

Konvertierung der Daten

```
"encoding"
```

KentixONE bietet vier verschiedene Konvertierungen an, welche nachfolgend aufgelistet sind.

	Beschreibung
binary	Jedes Byte kann nur den Wert 0 oder 1 annehmen.
ascii	Im Datensektor befindet sich eine Ascii Zeichenfolge.
bcd	BCD steht für „Binary-Coded Decimal“. Es handelt sich dabei um ein System, in dem jede Ziffer einer Dezimalzahl (0-9) durch einen vierstelligen binären Code dargestellt wird.
hexadecimal	Daten werden als Unsigned Integer interpretiert und können bis zu einer Größe von 64 Bit verwendet werden.

Statischer Testwert

```
"test_value"
```

Der statische Testwert ist eine Zeichenkette und wird immer beim Auslesen der Karte geprüft. Erst nach erfolgreichem Vergleich des Testwertes auf der Karte mit dem Testwert in der Konfigurationsdatei werden die Daten in KentixONE weiterverarbeitet.

Token mit einer Kentix-spezifischen Verschlüsselung können nicht in Verbindung mit einer eigenen Verschlüsselung verwendet werden.