Sicher und bequem

Fingerprint-Zahlenschloss FP100

Elektronische Zugangssysteme sind längst auch in den privaten Bereich eingezogen. Vom einfachen Ziffernschloss über RFID-Zugang bis hin zu biometrischen und verschlüsselt per Funk ferngesteuerten Zugangssystemen findet man heute alle gängigen Techniken an privaten Haustüren. Muss derartige Technik besonders teuer sein? Wir diskutieren dieses Thema anhand des in einem günstigen Preisbereich angesiedelten Fingerprint-Zahlenschlosses ELV FP100, betrachten dabei insbesondere Aspekte der Anlagensicherheit gegen Manipulation, Sabotage und Vandalismus und hier besonders den sicheren Zugang per Wiegand-Interface-Technik.

Sicherer Zugang

Elektronische Zugangssysteme bieten die bequemste Möglichkeit, einen gesicherten Bereich schnell, schlüssellos und ohne Bedienpersonal betreten und vor unbefugtem Zugang sichern zu können. Bereits in [1] und [2] haben wir dazu alle gängigen Techniken vorgestellt. Besonders beliebt sind Systeme, die keine weiteren Hilfsmittel wie z. B. eine RFID-Karte oder das Smartphone erfordern, beliebt sind also biometrische Techniken und nach wie vor die Zifferncodezugänge. Das Fingerprint-Zahlenschloss FP100 ist ein typischer Vertreter dieser Systeme. Es verbindet ein biometrisches System, d. h. einen Fingerabdruckscanner, mit einem traditionellen Zifferncodeschloss. Der Preis dafür liegt bei knapp unter 100 Euro – wird dafür genug Sicherheit an der Haustür geboten?

Die Liste der Features ist dank moderner Mikroprozessortechnik lang: Bis zu 1000 Fingerabdruck-Zugänge und bis zu 2000 Zahlenschloss-Zugänge sind speicherbar, beide Arten sind kombinierbar. Das Gerät verfügt über ein Wiegand-Interface, das einen besonders sicheren Betrieb ermöglicht, und über zahlreiche Sonderfunktionen wie eine Stand-alone-Tür-Ansteuerung oder einen Schleusenbetrieb mit zwei Türen, eine Türkontaktüberwachung, eine Funktion zum Offenhalten der Tür für freie Durchgangszeiten, eine Innentasterschaltung und schließlich, insbesondere für das einfache Konfigurieren mehrerer Anlagen mit gleichem Zugangskreis, eine USB-Schnittstelle, über die per Smartphone-App konfiguriert und verwaltet werden kann.

Über den Relaisausgang kann man u. a. Geräte von Homemmatic oder Homematic IP ansteuern, die einen Schalteingang besitzen und so z. B. auch per Funk eine Keymatic oder einen Garagentoröffner und vielleicht parallel dazu die Beleuchtung ansteuern.

Universeller Zugang

Wie schon angesprochen, kann der Zugang sowohl über eingespeicherte Fingerabdrücke der berechtigten Benutzer als auch über Zifferncodes erfolgen. Zur erhöhten Sicherheit sind beide Methoden kombinierbar. Damit ist bereits eine hohe Zugangssicherheit gewährleistet.

Der Fingerabdruckscanner ist ein Flächensensor, der sich in den ELV Tests als sehr zuverlässig erwies. Seine Bilderkennung toleriert auch leicht andere Fingerkuppenstellungen als bei der ursprünglichen Speicherung der Fingerabdrücke, man muss lediglich mit den systemtypischen Einschränkungen eines Flächenscanners leben, wie eingeschränkte Erkennung bei feuchter Oberfläche oder verschmutzten Fingern. Als positiv ist die Beleuchtung des Scanners anzusehen, die sich erst aktiviert, wenn der Finger aufgelegt wird. Somit lockt das helle Scannerlicht keine Unbefugten an. Man kann die gesamte Familie in einem einzigen Arbeitsgang registrieren, denn der Lernalgorithmus lässt die unmittelbare Eingabe mehrerer Fingerabdrücke in einem Programmiergang zu.

Wichtig – mechanische Sicherheit

Das wetterfeste IP66-Gerät befindet sich in einem sehr robusten Zink-Druckguss-Gehäuse, auch die Bedientasten sind vandalismussicher in Metall ausgeführt. Die Elektronik im Inneren ist gut geschützt, zum einen durch einen Sabotagekontakt, der beim Öffnen des Gehäuses einen externen Alarm und einen solchen über den internen Tonsignalgeber auslösen kann, und zum anderen durch eine komplett vergossene Elektronik, die nicht zerstörungsfrei erreichbar ist. Die verdeckte USB-Schnittstelle ist nur unter definierten Bedingungen zugänglich. Bild 1 zeigt die typische Konfiguration des FP100 in Verbindung mit einem Innentaster, einem überwachenden Türkontakt und einem externen Signalgeber.

Die Montage erfolgt über Schrauben und die Rückwand des Geräts. Dabei sollte man auf sehr robusten, vandalismussicheren Halt in der Montagefläche achten, um ein Abreißen oder Abstemmen des Geräts zu verhindern. Das ist aufgrund des dichten Anliegens auf der Montagefläche und wegen der abgerundeten Gehäuseecken zwar stark erschwert, aber etwa nachlässiges Anbringen mit zu schwachen Dübeln etc. kann einen Angriffspunkt bieten. Hier liegt dann auch eine Schwachstelle aller Geräte, die selbst das Elektroschloss in der Tür ansteuern: gelangt jemand an den nach hinten geschützt herausgeführten Kabelbaum, hat er direkten Zugang zum Schloss. Deshalb eignet sich die direkte Ansteuerung des Elektroschlosses nur für Bereiche, in denen kein brachialer Vandalismus zu erwarten ist, wie z. B. für kamera- bzw. fernüberüberwachte (Privat-)Grundstücke oder Anwendungen im Inneren von Gebäuden. Oder man sorgt dafür, dass tatsächlich kein mechanisches Lösen aus der Verankerung stattfinden kann.

Sicherer durch Wiegand

Wer A zum bequemen Zugang sagt, sollte eigentlich auch B zu erhöhter Sicherheit sagen. Kein technisches System, das Menschen errichten, ist sicher vor anderen Menschen, d. h. Einbrechern. Für dieses Szenario hat man in das FP100 ein Wiegand-Interface integriert, das auch bei einem gewaltsam entfernten Zugangsgerät und Zugang zum Kabel eine hohe Sicherheit bietet. Beim Wiegand-Interface [3] handelt es sich um ein genormtes Interface für den Datenaustausch zwischen Zugangskontrollgeräten, Kartenlesern und Kontroll-Panels. Es wird für den verschlüsselten Datentransfer vom Lesegerät zu einem Kontrollgerät benutzt. So entsteht ein besonders sicheres System, da keine Zugangsdaten im Lesegerät gespeichert werden müssen.

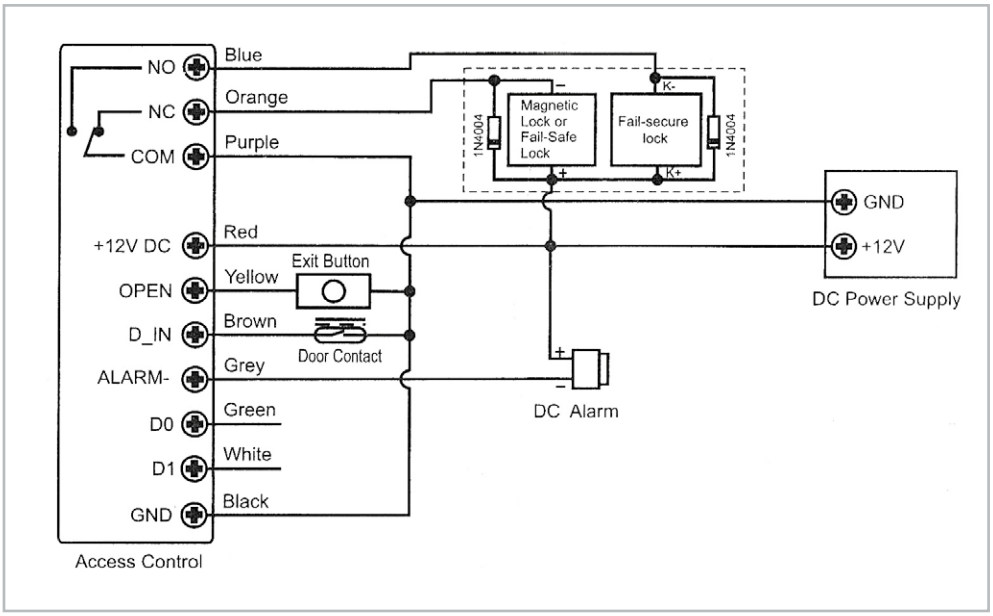

Bild 1: Typische Konfiguration des FP100 im Stand-alone-Betrieb

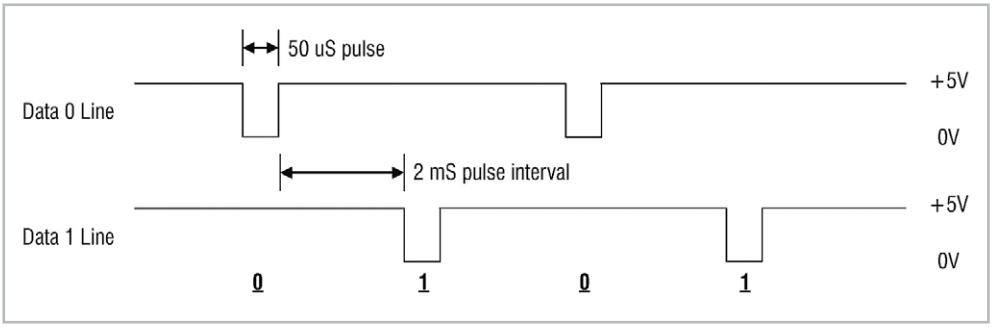

Bild 2: Timing und Pegelverlauf im Wiegand-Übertragungsschema

Das Interface

Das Interface benötigt drei Leitungen:
1. Common Ground (GND, schwarze Leitung)
2. Datenleitung DATA 0 (grüne Leitung)
3. Datenleitung DATA 1 (weiße Leitung)

- Werden keine Daten gesendet, befinden sich beide Datenleitungen (Länge 160 m max.) auf High-Pegel (5 V)
- Wird eine 0 gesendet, geht DATA 0 auf „low“, DATA 1 bleibt auf „high“
- Wird eine 1 gesendet, geht DATA 1 auf „low“, DATA 0 bleibt auf „high“

Timing und Pegelverhältnisse sind in Bild 2 in der Übersicht zu sehen. Dieses Pegelschema sorgt auch dafür, dass besonders lange Leitungswege realisierbar sind. Zusätzlich sind vielfach Signalleitungen für die akustische und optische Signalisierung sowohl zum als auch vom korrespondierenden Wiegand-Controller vorhanden.

Bild 3 zeigt die grundlegende Verbindung zwischen FP100 und einem Wiegand-Controller. Natürlich lassen sich parallel dazu auch die Signalisierungsausgänge nutzen. Die Anschlüsse für Innentaster und Fensterkontakt bleiben hier jedoch ungenutzt, diese werden direkt über den Wiegand-Controller verwaltet.

Das Wiegand-Protokoll

Das Wiegand-Protokoll besteht, je nach Herstellervorgabe, aus 26 bis 44 Bit:

- 1 First-Parity-Bit, Parität gerade, ermittelt aus Bit 2 bis 13 bzw. den ersten 16 Datenbits
- 24 Datenbits (ID bei RFID-Karten/Fingerprints bzw. Pin bei Zifferncodes)
- 1 Stopp-Bit, Parität ungerade, ermittelt aus Bit 14 bis 25 oder den zweiten 16 Datenbits

Die konkrete Zusammensetzung des Protokolls schwankt jedoch von Hersteller zu Hersteller. Teilweise werden auch nur 8 Datebits für Anfang und Ende des binären Signals eingesetzt.

Ein Beispiel soll die Umwandlung eines Pin-Codes in ein verschlüsseltes 34-Bit-Signal illustrieren:

Pin-Code 12345678 → als Hex-Code: BC614E
(jede Hex-Stelle wird binär duch 4 Bit dargestellt)
ergänzt durch First-Parity-Bit und Stopp-Bit:
E 00BC614E 0

E – gerades Parity-Bit aus 00BC = 1
0 – ungerades Parity-Bit aus 614E = 0
Binäres 34-Bit-Signal:
1 0000 0000 1011 1100 0110 0001 0100 1110 0

In Bild 4 ist der im Gebäude anzubringende Wiegand-Controller, hier das weitverbreitete Sboard-II, in der Wi-Fi-Version zu sehen. Er wird mit dem FP100 über lediglich vier Leitungen verbunden: D0, D1, +12 V und GND. Der Controller kann die Fingerprint-Nutzer als „(RFID-)Card-Nutzer” mit ID und die Zifferncode-Nutzer direkt über die Zifferncode-Umwandlung auswerten.

Das Sboard-II WiFi ermöglicht die Verwaltung von zwei Türen und zwei Eingabegeräten und dazu die Fernsteuerung vom Smartphone aus via Mobilfunk und WLAN. So kann man z. B. Gästen oder Besuchern die Tür auch bequem aus der Ferne öffnen.

Eine weitere Option ist die einfache Nutzerdatenverwaltung in größeren Konfigurationen, denn das Sboard-II kann in Master-Slave-Anordnungen mit bis zu zehn dieser Controller ausgebaut werden. Hier können dann Nutzerdaten sehr einfach von Controller zu Controller übertragen werden, etwa, wenn es notwendig ist, mehrere durch Zugangsgeräte geschützte Bereiche zu durchqueren bzw. zu betreten.

Bild 5 zeigt die grundsätzliche Anschlussbeschaltung des Herstellers Secukey. Ein zweites Zugangsgerät kann man hier einfach parallel schalten. Die hier auftauchenden Begriffe „Fail-Safe-Lock” und „Fail-Secure-Lock” kennzeichnen unterschiedliche Schlossarten. Beim „Fail-Safe-Schloss” ist das Schließelement („Bolzen/Riegel”) im Stand-by-Modus eingefahren, das „Fail-Secure-Schloss” hingegen fährt das Schließelement im Stand-by-Modus aus und öffnet bei einem Ansteuerimpuls.

In der Kombination mit einem Wiegand-Controller erhält man am Ende so ein sehr sicheres, gegen Manipulation und unberechtigten Zugriff zuverlässig geschütztes Zugangskontrollsystem. ELV

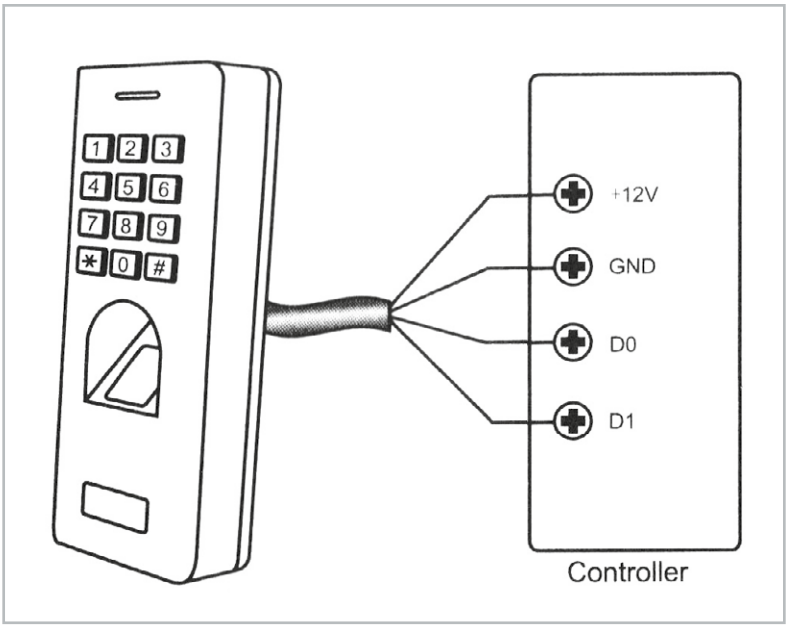

Bild 3: Die Verbindung zwischen dem Zahlenschloss FP100 und dem Wiegand-Controller erfolgt über nur vier Leitungen.

Bild 4: Der Wiegand-Controller Sboard-II WiFi ist eine komfortable und sichere Möglichkeit, das FP100 zu einem sehr sicheren Zugangssystem zu erweitern. Bild: Secukey

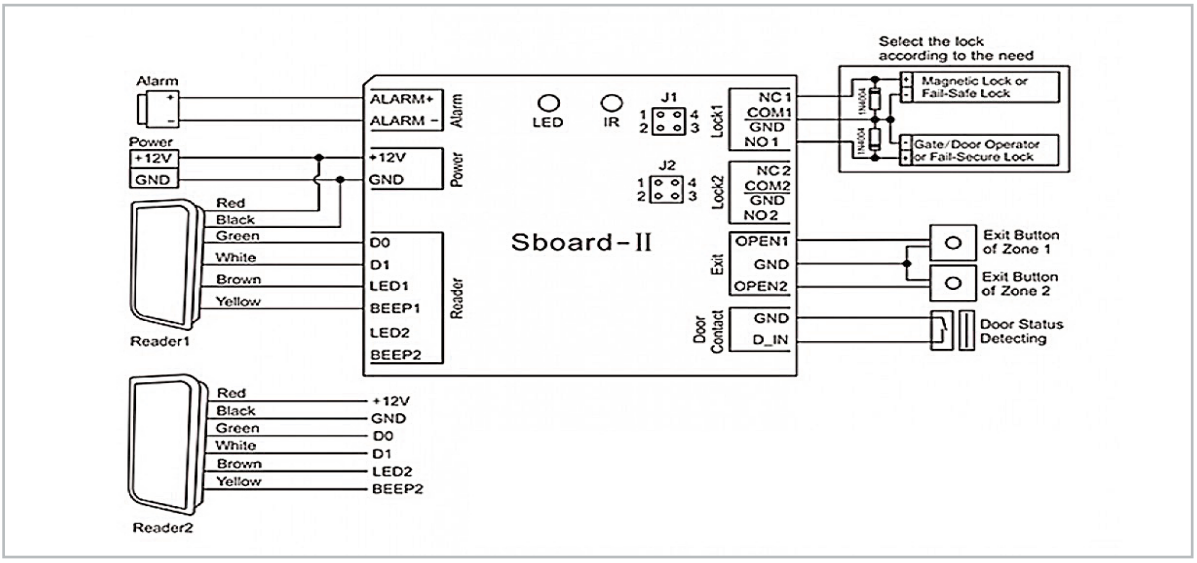

Bild 5: Die grundsätzliche Beschaltung des Sboard-II. Der Anschluss der Lesegeräte ist hier auf RFID-Leser von Secukey bezogen. Grafik: Secukey

Weitere Infos:

[1] Elektronische Zugangssysteme, Teil 1: ELVjournal 6/2018, S. 80 ff.
Fachbeitrag als PDF im ELVshop: Bestell-Nr. 250582

[2] Elektronische Zugangssysteme, Teil 2: ELVjournal 1/2019, S. 62 ff.
Fachbeitrag als PDF im ELVshop: Bestell-Nr. 250627

[3] Secure Wiegand Communications
US-Patent Application Number US 20100034375

Produktbeschreibung zum FB100 auf Seite 110 und im ELVshop unter der Bestell-Nr. 251211

Sboard-II (ohne WiFi) im ELVshop: Bestell-Nr. 251464

Alle Links finden Sie auch online unter: de.elv.com/elvjournal-links