Zutrittssteuerung

Zutrittssteuerung) mit NFC*

Grundlagen, Randbedingungen und Ausblick

Smartphones (nachfolgend auch alternativ als Handys bezeichnet) werden zunehmend als multifunktionale Terminals für unterschiedliche Anwendungen genutzt. Seit Einführung der NFC-Technologie stehen weitere mobile Einsatzmöglichkeiten, wie das elektronische Bezahlen und die Nutzung bei der Zutrittssteuerung zur Verfügung. Für betriebliche Anwendungen sind jedoch viele Einflussfaktoren zu beachten: Nicht alle Mitarbeiter verfügen über NFC-fähige Firmenhandys, der Austausch personenbezogener Daten ist mitbestimmungspflichtig und zusätzlich sind mögliche Kompatibilitätsprobleme zwischen den Systemkomponenten (Zutrittsperipherie, Leser, Betriebssysteme, Software, etc.) zu berücksichtigen. Neben den NFC-Grundlagen, Randbedingungen und Einflussfaktoren für die betriebliche Nutzung werden nachfolgend einige Lösungsansätze zur Zutrittssteuerung aufgezeigt.

Was ist NFC?

NFC steht für „Near Field Communication“ (Nahfeldkommunikation), die in einer Distanz von wenigen Zentimetern (in der Praxis bis ca. 4 cm) eine gesicherte Datenübertragung auf einer Frequenz von 13,56 MHz ermöglichen. Es handelt sich hier um eine RFID-basierende Technologie gemäß ISO 14443A (wie z.B. Legic advant, Mifare classic, Mifare DESFire EV1, iCLASS). Diese etablierte und bewährte Technik wird für viele betriebliche kartengesteuerte Anwendungen, wie die Personenidentifikation, Zutrittssteuerung und Zeiterfassung genutzt. RFID- und NFC-Chips in Ausweisen (Transponder) sind immer passiv, wogegen ein RFID-Leser immer aktiv betrieben wird. Wichtigster Unterschied ist, dass NFC-Chips in NFC-fähigen Smartphones in nachfolgend beschriebenen Modi betrieben werden können.

- Im passiven Modus emuliert das Mobilgerät einen RFID-Datenträger. Die Daten können auch dann gesandt werden, wenn das Gerät ausgeschaltet ist. Hierbei wird die Energie aus dem RF-Feld der aktiven Komponente, z. B. des Zutrittslesers gezogen.
- Im aktiven Modus fungiert das Gerät als Schreib-/Lesestation, oder arbeitet im sogenannten Peer-to-Peer-Modus (gleichberechtigte Kommunikation) zum Datenaustausch zwischen zwei Geräten. Hierfür muss das Mobilgerät eingeschaltet und per PIN-Eingabe freigeschaltet sein. Außerdem benötigt das Gerät eine eigene Energiequelle, wie einen integrierten Akku. Bei nicht aufgeladener Stromquelle steht dieser Modus nicht zur Verfügung.

Die Nahfeldkommunikation kann im Gegensatz zur Bluetooth-Funkübertragung ohne gegenseitige Anmeldung bzw. zeitraubende Authentifizierungseingaben der Teilnehmer sofort genutzt werden. Dazu muss lediglich das Mobilgerät in den Nahbereich eines (meist fest installierten) Terminals oder einer RFID-Karte (gemäß ISO 14443A) gehalten werden, um eine Transaktion abzuwickeln. Die derzeit maximale Datenübertragungsrate bei NFC wird mit 424 kbps (kbit pro Sekunde) angegeben, was etwa 185 MB/h entspricht und für den schnellen Austausch von Berechtigungsdaten ausreicht.

Erläuterung der Abkürzungen: s. letzte Seite

Neben der Verschlüsselung der Funkverbindung ist mit der geringen Reichweite ein gewisses Maß an Sicherheit bereits in den Standard eingebaut, denn es ist nicht möglich, aus der Ferne eine ungebetene Verbindung (zum Ausspähen der Daten) mit NFC herzustellen. Zugleich hat diese Beschränkung den Vorteil, dass ein relativ schwaches Funksignal genügt, wodurch auch verhältnismäßig wenig Energie benötigt wird. Die mobilen Nutzungsmöglichkeiten sind sehr vielfältig und reichen von bargeldlosen Zahlungen, über Kundenbindungssysteme, Fahrscheinersatz, Personenidentifikation, Zeiterfassung und Zutrittssteuerung bis hin zur sicheren Zugangs- und Zugriffskontrolle an Automaten und PCs.

NFC zur Zutrittssteuerung - Risiken und Chancen

Beim Einsatz von NFC auf einem Smartphone sind viele Randbedingungen zu berücksichtigen. Speziell bei sicherheitsrelevanten Lösungen wie der Zutrittssteuerung steht der Datenschutz an oberster Stelle. Es muss sichergestellt sein, dass keine kritischen Daten unverschlüsselt auf dem Smartphone gespeichert werden, die beim Hacken ausgelesen werden können. Außerdem hat nicht jeder Mitarbeiter ein NFC-fähiges Smartphone und bei APP-basierten Lösungen sind noch die unterschiedlichen Betriebssysteme (Android, iOS, Windows Phone, BlackBerry OS, u.a.) und die Sicherstellung der Softwareaktualisierung zu beachten.

Außerdem ist zu beachten, dass in vielen Firmen oder Bereichen (z. B. medizinische Einrichtungen, Spionage gefährdete Abteilungen) die Mitführung eines Smartphones (z. B. wegen Fotografierverbot; EX-gefährdete Areale, etc.) untersagt ist. Nicht jeder Mitarbeiter möchte sein privates Gerät für den betrieblichen Einsatz nutzen. Bei Bereitstellung von Firmenhandys zur Zutrittssteuerung ist dies durch den Betriebsrat mitbestimmungspflichtig. Hierbei sollten auch die Sorgen der Mitarbeiter vor ständiger Überwachung („gläserner Mensch“) beachtet werden, z. B. dass ein Smartphone unbemerkt Sprachaufzeichnungen ermöglicht oder geortet werden kann, um den Aufenthaltsort festzustellen.

Andererseits gestatten oder wünschen Unternehmen es zunehmend, dass Mitarbeiter ihre privaten Smartphones für betriebliche, mobile Anwendungen nutzen. Dieses Vorgehen wird als „Bring Your Own Device (BYOD)“ bezeichnet. Der Einsatz von BYOD in einem solchen Umfeld erfordert allerdings gewisse Sicherheitsvorkehrungen, genaue Planung sowie die richtige Technik und Infrastruktur. Denn private Smartphones können ein Sicherheitsrisiko darstellen, da diese unter Umständen hinsichtlich Updates, Datensicherung, etc. nicht so administriert werden können wie firmeneigene IT-Geräte. Meist können diese mobilen Geräte nur mit strengen Vorgaben und hohem Aufwand in die IT-Infrastruktur integriert werden. Der Datenschutz von zu verarbeitenden, gespeicherten oder übertragenen personenbezogen Daten muss gewahrt bleiben. Auch rechtliche Fragen müssen geklärt sein, z. B. für den Fall, dass solche Mobilgeräte bei der Nutzung zu Schaden kommen oder sogar im Betrieb Störungen/Schäden an anderen Geräten oder Produktionseinrichtungen verursachen.

Das Smartphone als Identifikationsmittel bietet dann Vorteile gegenüber Schlüsseln und Chipkarten, wenn Zutrittsberechtigungen mobil und ortsunabhängig ausgestellt und versandt werden müssen. Beispielsweise kann für Außendienstmitarbeiter, die generell ein Firmenhandy nutzen, der Einsatz zur Zeiterfassung und Zutrittssteuerung einige Vorzüge bieten. Besonders wenn eine flexible Zutrittsberechtigung benötigt wird, z. B. der Servicetechniker mit spontanem Zutritt zur Außenstelle oder die Hotelberechtigung für Geschäftsreisende, liegen die Vorteile im doppelten Sinne in der Hand.

Für die Zutrittssteuerung in Hochsicherheitsbereichen dürfte eine NFC-Kommunikation nicht geeignet sein. Nach ISO 15408 wird eine NFC-Kommunikation gemäß den allgemeinen Kriterien für die Bewertung der Sicherheit von Informationstechnologie (Common Criteria for Information Tech-

nology Security Evaluation; kurz auch Common Criteria oder CC) als nicht sicher eingestuft. Diese Aussage zielt zur Zeit zwar auf Bezahlvorgänge mit NFC-Smartphones, doch die Forderung nach zusätzlichen Sicherheitsvorkehrungen lässt sich auch auf die Zutrittssteuerung übertragen. Nach den CC-Definitionen ist die verbindungslose Nutzung nicht sicher gegen Attacken von Dritten. Erteilte Geräte-Qualifizierungen nach ISO 15408 wurden bisher nicht bekannt bzw. veröffentlicht.

Mittlerweile gibt es eine Vielzahl an Veröffentlichungen zur NFC-Thematik. Da Smartphones immer öfter für Bankgeschäfte genutzt werden, sind sie zunehmend ein interessantes Ziel für Hacker. Für eine sichere Authentifizierung wurde von IBM-Forschern eine Zwei-Faktoren-Authentifizierung für das Mobile Computing vorgestellt (Quelle: www-03.ibm.com/press/de/de/pressrelease/42218.wss). Hierfür wird eine PIN und eine kontaktlose RFID-Chipkarte (z. B. eine Bankkarte oder ein von einem Unternehmen herausgegebener personalisierter RFID-Ausweis) verwendet. Für die NFC-Zutrittssteuerung dürfte diese Art der Authentifizierung aufgrund der umständlichen Handhabung der Identifikationsträger nicht akzeptabel sein. Zur Erhöhung der Sicherheit wäre hier eher eine Zwei-Faktoren-Authentifizierung mittels RFID-Ausweis und biometrischem Merkmal sinnvoll.

Technische Lösungsansätze zur Zutrittssteuerung

Am Markt gibt es derzeit unterschiedliche technische Lösungsansätze die aber meist an bestimmte Smartphone-Technologien (Betriebssystem, Sicherheitsphilosophie, Betriebsarten, etc.), ZK-Produkthersteller und/oder Provider gebunden sind.

Emulation von RFID-Ausweisen („Card Emulation“ gemäß ISO 14443A)

Momentan ist davon auszugehen, dass im betrieblichen Umfeld (Industrie, Banken, Versicherungen, etc.) für Zeiterfassung und Zutrittssteuerung weiterhin ein RFID-Ausweis oder Transponder genutzt wird.

Nur wenn die rechtlichen Randbedingungen (Betriebsvereinbarung) geklärt sind, können Mitarbeiter (z. B. Vertriebs- und Service-Mitarbeiter) ihr NFC-fähiges Dienst-Handy für die Zutrittssteuerung nutzen. Dies setzt voraus, dass in den ZK- und ZE-Terminals und an den zutrittsgesicherten Eingängen weiter die klassischen RFID-Leser zum Einsatz kommen. Diese Infrastruktur könnte mit NFC-fähigen Smartphones genutzt werden, wenn dort die „Card-Emulation“ erlaubt wäre. Eine Funktion, die zur Zeit noch nicht für die gängigen Smart-Phone- Betriebssysteme verfügbar ist.

Soweit das Smartphone nur als Ausweisersatz genutzt wird, ist eine einmalige Gebühr, z. B. für die SIM-Karte (Subscriber Identity Module) zu berücksichtigen. Solche SIM-kartenbasierte Applikationen haben den Nachteil, dass mobile Zahlungs- und Zutrittsfunktionen nur mit Unterstützung des Providers, der auch die Hoheit darüber hat, kostenpflichtig angeboten werden können. Deshalb verlangen NFC-Zutrittslösungen ein System, das den Datenaustausch mit dem Server minimiert. Ähnlich wie bei RFID-Karten und -Lesern, die auch erst erkennen müssen, ob und wie sie miteinander kommunizieren dürfen, muss eine Struktur definiert und Schnittstellenabstimmungen getroffen werden.

Sicherungskonzepte für die verschlüsselten ID- und ZK-Daten

Soweit ein NFC-Smartphone, z. B. mittels Universal-SIM-Karte oder einer Secure Micro-SD-Karte, einen ISO 14443A-Identträger emuliert, ist hierbei eine sichere Verschlüsselung der abgespeicherten Daten wie Ausweisnummer und, wenn auf dem „Ausweis“ gespeichert, Zutrittsberechtigungen zu beachten. Die Schreib-Leseschlüssel müssen also in einem extra gesicherten Bereich liegen. Dieses so genannte „Secure Element“ kann wie folgt vorhanden sein:

- **Secure Element auf SIM Karte**
  Seit Anfang des Jahres 2013 liefern die MNOs (MNO = Mobile Network Operator) neue universelle SIM-Karten (USIM) aus, die einen gesicherten Speicherbereich für die Schlüssel unterstützen. Der Nachteil hierbei ist, dass die USIM und die Daten darauf dem jeweiligen MNO gehören, also nicht mehr dem ZK-Anbieter bzw. den jeweiligen Kunden.
- **Secure Element auf zusätzlicher spezieller Speicherkarte bzw. Erweiterungsmodul**
  Nicht alle Smartphones haben einen Steckplatz für eine zusätzliche Speicherkarte, in die eine Prozessorchipkarte gesteckt werden kann, die eine „Card Emulation“ erlaubt. Ein Lösungsansatz ist z. B. der Einsatz von Secure Micro-SD-Karten, meist eingebaut in Erweiterungsmodulen (wie in Form einer Hülle) mit Antenne. Falls Smartphones nicht NFC-fähig sind (beispielsweise die aktuellen IPhone-Modelle), können diese damit nachträglich ausgestattet werden. Auf diesen Prozessorchipkarten mit einem JCOP Betriebssystem (Java Card Open Plattform) kann eine Legic advant 4k-Karte (card in card) und Mifare classic 1k-Karte emuliert werden. Dabei ist zu beachten, dass für die Freischaltung der advant-Emulation pro Karte Lizenzen an Legic fällig werden.
- **Secure Element auf Speicher im Smartphone**
  Die unsicherste Lösung dürfte sein, die Schlüssel in den Speicher des Smartphone zu legen, denn dieser Speicher kann nur sehr schwer vor Ausspähen geschützt werden.

Anwendungs- und Einsatzbeispiele

Bereits heute gibt es viele Möglichkeiten, ZK-Anwendungen mit NFC-Technologie zu erweitern, nachfolgend eine kleine Auswahl an Beispielen:

NFC als Alternative für Barcode-gesteuerte Zutrittssteuerung

An Flughäfen hat sich die Zutrittssteuerung mittels Smartphone und Barcodeerkennung mittlerweile als Alternative zum Ticket bewährt. Ähnlich könnte eine Zutrittssteuerung zu bestimmten Räumen (z. B. Besprechungsräume) funktionieren. Mit Mitarbeiterausweisen und NFC-fähigen Handys könnten die mit entsprechenden Lesern bzw. Terminals ausgestatteten Eingänge von Berechtigten genutzt werden. Der Zutritt von Mitarbeitern oder Besuchern ist abhängig vom entsprechenden Equipment (NFC-Terminal, RFID- oder Barcode-Ausweis, Firmenhandy).

Für das Hotelgewerbe (vgl.: http://qrtool.de/nfc-in-sicherheitsanwendungen-die-zutrittskontrolle/)

Hier könnte die NFC-Technik die Hotelzimmerschlüssel und Zutrittskarten verdrängen. In Zukunft erhalten Gäste nach der Buchung eine Reservierungsbestätigung und Check-in-Meldung auf ihrem Smartphone. Dies hätte den Vorteil, dass Gäste ohne Umschweife direkt auf ihr Zimmer gehen können – denn Zutrittsberechtigung bzw. Zutrittsdaten sind bereits auf dem Smartphone vorhanden. Zum Öffnen der Zimmertür muss das Handy lediglich an den mechatronischen Türbeschlag gehalten werden. Über das PMS-System wird der Rezeption mitgeteilt, dass der Gast angekommen ist. Bei Abreise können Gäste automatisch auschecken, unabhängig von Uhrzeiten und ohne Kontakt zu den Hotelangestellten.

Für Filialbetriebe

Eine sehr kostengünstige und insbesondere für Filialbetriebe geeignete ZK-Lösung besteht darin, das NFC-fähige Smartphone nur als mobiles Administrations-/Parametrier-Gerät und nicht als Ausweis zu nutzen. Auf einem gesicherten Server werden alle Mitarbeiter mit ihren Stammdaten angelegt und die jeweiligen Zutrittsrechte (wer darf wann und wo Zutritt erhalten?) vergeben. Diese grundlegende Arbeit kann von jedem PC mit Netzzugang aus erfolgen. Der Datenzugriff z.B. durch die einzelnen Filialleiter erfolgt mittels NFC-Smartphone über eine Webanwendung „Zutritt

per Web“. Sie bietet alle ZK-Funktionen, die für den Betrieb mit nicht kabelgebundenen Türterminals notwendig sind: Terminals parametrieren, Buchungs- und Userkarten erstellen bzw. kodieren u.s.w. Die Applikation kann als Webservice gemietet oder bei Eigenbetrieb auf eigenen Systemen unter Windows oder Linux installiert werden.

Über eine APP des NFC-Smartphone kann die Administration des ZK-Systems erfolgen. Durch Tippen auf das entsprechende Symbol können über einen Internet-Browser die Konfiguration der Türterminals und die Zutrittsberechtigungen der Mitarbeiter online abgerufen werden. Diese Informationen werden dabei nicht lokal auf dem Smartphone gespeichert und es bleibt somit frei von sicherheitsrelevanten Daten. Mit dem NFC-Handy können dann die Konfigurations- oder Berechtigungsdaten auf die zugehörigen Service- oder Mitarbeiterkarten geschrieben werden. Durch Vorhalten der Servicekarte an dem zugehörigen Türterminal erfolgt dann die Programmierung und Rechtevergabe.

Für die Zutrittssteuerung, ggf. auch Zeiterfassung können die vom Anbieter freigegebenen Mitarbeiterausweise, die ebenfalls mittels NFC-Smartphone mit den Berechtigungen beschrieben werden, genutzt werden. So muss nicht jeder Mitarbeiter mit teuren und mitbestimmungspflichtigen NFC-Smartphones ausgestattet werden. Mit dieser Lösung ist sichergestellt, dass selbst bei einem Hakker-Angriff auf das Smartphone des Filialleiters keine kritischen Daten gestohlen werden können. Da die Zutritte mittels klassischer RFID-Ausweise erfolgen, sind nur die Providergebühren für das Beschreiben der RFID-Karten zu berücksichtigen. Diese ZK-Lösung minimiert die Kosten beim Provider. Bei dieser Lösung wird nicht das Smartphone selbst als Identmedium eingesetzt, sondern weiterhin die bewährte Zutrittskarte.

Zusammenfassung, Status und Ausblick

NFC ist multifunktional: es kann für Zeiterfassung genau so gut eingesetzt werden wie bei Zutrittssteuerung oder der Erfassung von anderen betrieblichen Daten. Und beruflich genauso wie privat. Jedoch stellt sich die Frage, ob Mitarbeiter dafür ihr privates Smartphone nutzen wollen. Unabhängig davon ist die Erfassung, Verarbeitung und Übertragung personenbezogener Daten mitbestimmungspflichtig, egal mit welchem Identmedium und insbesondere bei Nutzung eines Smartphones.

Wie bereits beschrieben, kann ein NFC-Smartphone nur begrenzt einen RFID-Ausweis oder Transponder ablösen. Neben den rechtlichen und technischen Randbedingungen, muss nochmals erwähnt werden, dass in manchen Betrieben oder in deren Sicherheitsbereichen Smartphones mit Mikrofon, Kamera, USB-Anschluss und Funkmodulen nicht erlaubt sind. In großen Unternehmen ist oft das sichtbare Tragen von Ausweisen mit Passbild vorgeschrieben.

Die Möglichkeiten und Anwendungsbereiche für NFC sind vielfältig. Momentan scheinen sich aber die Vorteile noch mit den Bedenken und Problemen die Waage zu halten. Für einige Spezialanwendungen sind aber NFC-fähige Handys die organisatorisch und sicherheitstechnisch beste Lösung. Viele Fragen sind noch unbeantwortet, z. B. bei der Sicherheit, dem Datenschutz, der Akzeptanz von betrieblichen NFC-ZK-Lösungen und ob dazu private oder Firmenhandys genutzt werden können. Genaue Prognosen, ob und wann sich die Technologie zur betrieblichen Zutrittssteuerung durchsetzen kann, sind zur Zeit schwierig. Sehr großen Einfluss wird dabei auch haben, ob die Ticketing- und Bezahlfunktionen von privaten NFC-Smartphones Akzeptanz und Verbreitung finden werden.

Links zu ergänzenden NFC-Informationen

NFC-Forum

Das NFC-Forum bildet die öffentliche Plattform für die NFC-Förderung. Das Forum hat ca. 100 Mitgliedsfirmen und erarbeitet die Architektur und die technischen Spezifikationen für die NFC-Technik.
www.nfc-forum.org/home/

Anbieter von NFC-Smartphones

www.handy-deutschland.de/nfc-handy.html

NFC-Chiptypen und Kompatibilitätsliste

In nachfolgendem Link werden die NFC-Chiptypen aufgelistet: www.nfc-tag.de/nfc-chiptypen

Nicht alle NFC-Tags sind mit allen NFC Smartphones kompatibel. In nachfolgender Kompatibilitätsliste wird aufgeführt welcher NFC-Tag zu welchem Smartphone kompatibel ist.
www.nfc-tag.de/kompatibilitaetsliste

Abkürzungen und Begriffe

Nachfolgende Tabelle gibt einen Überblick über die im Dokument verwendeten Abkürzungen.

APP	engl. Kurzform für Application
BSI	Bundesamt für Sicherheit in der Informationstechnik
BYOD	Bring Your Own Device; Nutzung des privaten Smartphones für betriebliche, mobile Anwendungen
CA	Chip Authentication: Authentifizierung der Karte und Aufbau eines sicheren Kanals (Analog authentifizierter Server bei SSL / Homebanking)
CC	Common Criteria; anerkannte Sammlung von Sicherheitsnormen
ID	Identifikation
JCOP	Java Card Open Plattform
MNO	Mobile Network Operator
NFC	Near Field Communication; Nahfeldkommunikation
OTA	Over the air
PIN	Persönliche Identifikations-Nummer
PMS	Property Management System - Hotelreservierungssysteme, die das computergestützte Verwalten und Steuern eines Hotels ermöglichen
RFID	Radio Frequency Identification
RI	Restricted Identification; Sektorspezifisches, eindeutiges Merkmal zur Wiedererkennung
SAM	Secure Access Module
SD	Secure Digital
SE	Secure Element
SIM	Subscriber Identity Module
SP	Service Provider
TSM	Trusted Service Management
USIM	Universal SIM
ZE	Zeiterfassung

*) Zutrittsregelung, Zutrittssteuerung oder Zutrittskontrolle?

Obwohl die deutsche Übersetzung der europäischen Zutrittsnorm EN 50133-1 den Begriff „Zutrittskontrolle“ festgelegt hat, nutzen Anwender und Anbieter meist „Zutrittsregelung“, „Zutrittssteuerung“ oder auch „Zutrittsmanagement“.
Auch wenn der BHE großen Wert auf Verwendung der normgerechten Bezeichnungen und Definitionen legt, verwenden auch wir die Bezeichnung „Zutrittssteuerung“ statt „Zutrittskontrolle“, da sie den Zweck und Sinn besser trifft, und das englische „access control“ besser übersetzt. In den Abkürzungen bleibt der bislang gebräuchliche Begriff „ZK“ für Zutrittskontrolle (=Zutrittsteuerung) bestehen.
Die normgerechte Definition bleibt jedoch unverändert: Zutritt ist der Vorgang des Betretens oder Verlassens eines Sicherungsbereiches.

BHE - Feldstraße 28 **Telefon: 06386 9214-0** **Internet: www.bhe.de**
66904 Brücken **Telefax: 06386 9214-99** **E-Mail: info@bhe.de**