Bezahlen mit dem Smartphone

Mobile Payment via Near-Field-Communication (NFC) & Co.

Elektronisches Bezahlen mit dem Handy ist cool: immer griffbereit, ohne Hantieren mit Kleingeld oder Karten. Doch auch diese neue Technik birgt Herausforderungen und Risiken – der vorliegende Beitrag liefert einen Einblick in aktuelle technische Verfahren und ihre Verfügbarkeit.

Von Georg Lukas, Köln

Auch wenn „Mobile Payment" vieles heißen kann – die Nutzung eines Smartphones als Zahlungsmittel beim Einkaufen in einem Geschäft hat den Begriff geprägt und steht auch in diesem Artikel im Fokus. Während Kunden damit ohne Griff ins Portemonnaie bezahlen können, ist für Händler die schnellere Abwicklung an der Kasse der größte Vorteil, dicht gefolgt von der Möglichkeit, bessere Kundenbindung durch Couponing-Maßnahmen zu erreichen.

Um vor Ort mit dem Smartphone zu bezahlen, gibt es verschiedene technische Lösungen: Ob Near-Field-Communication (NFC), QR-Codes oder alternative Ansätze, die prinzipielle Vorgehensweise ist bei allen Verfahren ähnlich: Ein Kunde kommt mit seiner Smartphone-Geldbörse (Mobile Wallet) an die Kasse und muss zum Bezahlen nur kurz einen App-Bildschirm vorzeigen oder das NFC-Lesegerät „tappen" (mit dem Smartphone berühren), um die Zahlung zu veranlassen. Im Hintergrund sind dazu mehrere Aufgaben zu erledigen: Zuerst muss der Kunde (bzw. seine Geldbörse) *identifiziert,* dann *authentifiziert* werden. Schließlich gilt es, die Zahlung zu *autorisieren,* indem geprüft wird, ob das Mobile Wallet gültig ist und Guthaben oder Bonität ausreichen.

Die Kreditkartenanbieter sind diese Herausforderungen bereits vor einigen Jahren durch die Einführung von RFID-/NFC-Kreditkarten (PayPass bei MasterCard und payWave bei VISA) angegangen – diese Lösungen lassen sich auch für das Bezahlen mit dem Smartphone übertragen: etwa per Google Wallet, mpass/O2 Wallet, dem Targobank „Bezahlchip" oder das „MyWallet" der Telekom.

Daneben existieren auch alternative Ansätze, die nicht die klassische Kreditkarteninfrastruktur nutzen: Netto und Edeka sind 2013 mit einer App gestartet, bei der ein kurzer Zahlencode vom Smartphone-Bildschirm in die Kasse übertragen wird, um die Zahlung zu veranlassen. Zahlreiche weitere Anbieter ohne signifikante Verbreitung bieten QR-Codes oder eigene NFC-Verfahren zum Bezahlen an. Solche proprietären Lösungen haben meist gemeinsam, dass das Smartphone selbst für die Transaktion eine mobile Datenverbindung aufbauen muss, was nicht in jedem Gebäude zuverlässig funktioniert. Im Folgenden geht es daher nur um Lösungen, die auf die eine oder andere Art per NFC eine Kredit-/Debitkarte ins Smartphone integrieren.

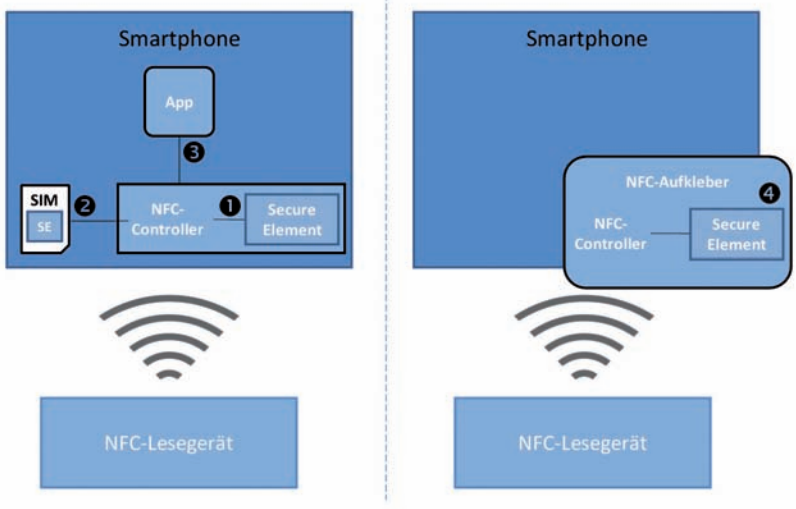

Abbildung 1: Varianten der NFC-Payment-Umsetzung im NFC-Controller (1), in der SIM-Karte (2), als „Host-based Card Emulation" (3) und externes Secure Element (4)

Secure Elements

Kreditkarten mit integriertem NFC sind in den USA bereits sehr weit verbreitet und haben schon mehrere Entwicklungsgenerationen durchlebt. Dabei fungiert die Kreditkarte grundsätzlich als passives Element (NFC-Tag) und wird vom Terminal (NFC-Reader) angesprochen und ausgelesen. Die aktuelle Kreditkarten-Generation nutzt dazu

jedoch keine RFID-Tags, sondern Smartcard-Controller, die für jede NFC-Transaktion eine neue Prüfzahl erzeugen, um ein Klonen der Karten unmöglich zu machen und Missbrauch leichter aufzudecken. Tappt der Kunde seine Karte an das Kassen-Terminal, fordert es über NFC die Kreditkartendaten (Nummer und Prüfzahl) an und fragt über eine VPN-Verbindung beim Zahlungsdienstleister nach, ob die Karte gültig ist. Für größere Beträge muss der Kunde sich durch eine PIN authentifizieren und die Transaktion wird abgeschlossen.

Beim Smartphone fallen zwar der Magnetstreifen und kontaktbehaftete Chip einer modernen Kreditkarte weg, es kommen aber ganz ähnliche Controller als „Secure Elements" (SE) zum Einsatz: Sie sind eigenständige Mikroprozessoren und verfügen über geschützten Speicher sowie gegebenenfalls Embedded-Java-Applets und können kryptografische Signaturen prüfen und erzeugen. Das Hochladen von Anwendungen (Provisionierung mit der Bezahlfunktion) ist nur mit Kenntnis der richtigen Schlüssel möglich, sodass in der Regel ein einzelner Anbieter die exklusive Kontrolle über das Secure Element (und ein darauf aufbauendes Wallet) genießt. Daher haben verschiedene Parteien versucht, eigene Lösungen zu etablieren, die verschiedene Wege der Secure-Element-Integration nutzen: als Teil des NFC-Controllers, in der SIM-Karte des Mobilfunkanbieters oder als externes Modul – eine weniger sichere Variante besteht darin, die Funktionen eines Secure Element in einer Smartphone-App zu emulieren (Abb.1).

Secure Element im NFC-Controller

Die meisten NFC-Controller in Smartphones bringen ein Secure Element mit. Bei Android-Geräten dürfen allerdings nur ausgewählte Apps direkt darauf zugreifen – aktuell lediglich die in Deutschland nicht verfügbare Google-Wallet-App: Bezahlvorgänge über NFC werden dabei transparent via Secure Element durchgeführt, die App schaltet lediglich die Funktion frei (so lässt sich auch sicherstellen, dass die Kreditkartendaten nur bei eingeschaltetem Bildschirm auslesbar sind) – die Kreditkartennummer lässt sich zwar unverschlüsselt auslesen, ist jedoch für Online-Einkäufe und Zahlungen per Magnetstreifen (eine häufige Vorgehensweise beim Klonen von Karten) gesperrt. NFC-Bezahlvorgänge werden wiederum kryptografisch abgesichert – und die Wallet-App kommuniziert mit den Google-Servern über HTTPS.

Um Zugriff auf das Secure Element in einem Android-Gerät zu bekommen, muss man mit Google, dem Gerätehersteller oder dem Mobilfunk-Netzbetreiber, über den das Telefon vermarktet wird, kooperieren, was die Nutzung für eigene Projekte erschwert. Bei Blackberry reglementiert RIM den Zugriff auf ähnliche Weise; bei Windows-Phones ist überhaupt kein Zugriff auf das interne Secure Element möglich.

Secure Element in der SIM-Karte

Die SIM-Karte (Subscriber Identity Module) ist ebenfalls ein eigenständiger, manipulationsgeschützter Mikroprozessor. Daher hat die Mobilfunkanbieter-Vereinigung GSMA spezifiziert, dass NFC-fähige Handys auch eine (NFC-)Verbindung zur SIM-Karte ermöglichen müssen, die ein Secure Element beherbergt. Entsprechende Lösungen sind das „O2 Wallet" und das „MyWallet" der Telekom – weitere Netzbetreiber stehen bereits in den Startlöchern.

Technik und Sicherheit sind mit einem ins Smartphone integrierten Secure Element vergleichbar, allerdings kontrolliert hier nun der jeweilige Netzbetreiber das gesamte Wallet-Ökosystem – dementsprechend kann man das Wallet auf dem SIM beim Telefontausch mitnehmen. Die Provisionierung (Einrichtung der Kreditkartenfunktion) erfolgt hier zudem über das Mobilfunknetz und nicht über eine – leichter angreifbare – Internetverbindung.

App-Emulation des Secure Elements

Die meisten in Smartphones verbauten NFC-Controller unterstützen als weitere Betriebsart die so genannte Host-based Card-Emulation (HCE). Dabei werden die von einem externen NFC-Reader empfangenen Kommandos an eine Smartphone-App weitergegeben und deren Antworten per NFC zurückgesendet – so lassen sich beliebige NFC-Anwendungen bis hin zur Kreditkarte komplett in Software realisieren.

Diese Funktion war allerdings bis vor Kurzem lediglich auf Blackberry-Geräten freigeschaltet. Unter Android war dazu lange Zeit eine Betriebssystem-Anpassung notwendig, was lediglich von SimplyTapp (www.simplytapp.com) genutzt wurde – mit Android 4.4 (KitKat) hat Google jedoch Ende Oktober 2013 die HCE-Funktion freigegeben, sodass hier mit neuen Entwicklungen zu rechnen ist.

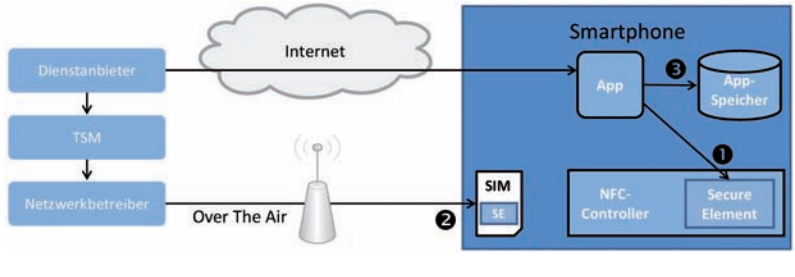

Abbildung 2: Provisionierung einer Bezahlfunktion in NFC-Controller (1), SIM (2) oder App (3)

Das bereits angesprochene SimplyTapp hat hierüber eine Kreditkarte „in der Cloud“ realisiert: Die App speichert selbst keine sensitiven Daten sondern leitet lediglich die NFC-Kommunikation an den SimplyTapp-Server weiter – hat der Nutzer am „Point-of-Sales“ (PoS) keine Internetverbindung, scheitert der Bezahlvorgang. Speichert man (bei anderen HCE-Verfahren) die Bezahldaten jedoch in der App, können sie gegebenenfalls durch Malware missbraucht werden.

Externes Secure Element

Da NFC-fähige Smartphones weiterhin nicht universell verfügbar sind, bieten einige Dienstleister (mpass, Targobank) stattdessen einen NFC-Chip („Tag“) als Aufkleber für die Rückseite des Smartphones an. Diese Aufkleber ähneln einer Kreditkarte im Miniformat, sind aber lediglich über NFC ansprechbar – eine direkte Schnittstelle zum Smartphone oder einer App ist nicht vorgesehen, vom Aufkleben auf ein NFC-Smartphone wird sogar abgeraten.

Für die Kärtchen existieren zwar Apps, diese nutzen aber lediglich eine Internetverbindung zu den Servern des Kreditkartenherausgebers, um auf dem Smartphone ein gegebenenfalls vorhandenes Prepaid-Guthaben, letzte Zahlungsvorgänge und Promotion-Aktionen anzuzeigen. Da keine Schnittstelle zum NFC-Aufkleber besteht, ist es auch nicht möglich, dessen Funktion beim Sperren des Handys zu deaktivieren – der Chip ist immer erreichbar und kann auch bei gesperrtem Smartphone angesprochen werden.

Dieser Unterschied macht zwei zusätzliche Angriffe auf solche Bezahlsysteme möglich: Zum einen kann man ein gestohlenes NFC-Tag für Bezahlvorgänge einsetzen. Zum anderen können zwei Angreifer einen so genannten Relay-Angriff durchführen, bei dem ein direkt am NFC-Tag platziertes Smartphone die Kreditkartendaten zum Bezahlen an ein anderes Smartphone weitergibt. Beide Angriffsszenarien sind jedoch bei den existierenden Verfahren auf 25 € pro Zahlungsvorgang begrenzt, sofern die Angreifer nicht auch die PIN des Nutzers ermitteln können.

Eine hybride Lösung befindet sich zurzeit bei der Volkswagen-Bank in der Erprobungsphase: Hier wird eine iPhone-Hülle mit integriertem NFC-Chip und Secure Element angeboten, die über den Docking-Anschluss des iPhones auch mit der mitgelieferten App kommunizieren soll – diese Lösung setzt dabei auf VISAs payWave-Technik.

Obligatorischer Cloud-Kontakt

Während externe NFC-Aufkleber bereits vor dem Versand an den Kunden provisioniert wurden, müssen Kreditkarten-Anwendungen in SIM-Karte oder Smartphone online auf das jeweilige Secure Element übertragen werden (Abb. 2).

Bei der SIM-Karte wird dazu die Mobilfunkverbindung („Over The Air“ – OTA) verwendet, die komplett in der Hand des Netzbetreibers liegt, der auch die SIM-Karte herausgegeben hat. Da die zu übertragenen Daten von einer Bank stammen, wird ein zusätzlicher Diensteanbieter, der Trusted Service-Manager (TSM), dazwischengeschaltet: Der TSM erhält die Provisionierungsanfragen von der Bank und leitet sie OTA an die betroffene SIM-Karte weiter. Auf diese Weise sind sowohl das Einspielen einer neuen Kreditkarte als auch deren Sperrung oder Konfigurationsänderung möglich. Ein Abfangen der Daten ist nur über einen aktiven Angriff auf das Mobilfunknetz möglich.

Anders sieht die Situation beim ins Smartphone-NFC integrierten Secure Element (SE) aus: Hier erfolgt die Provisionierung durch eine App, die auf dem Smartphone läuft und über das Internet mit einem Backend-Server kommuniziert. Diese Datenübertragung lässt sich zwar mittels Transport-Layer-Security (TLS) absichern, doch könnte ein Smartphone-Trojaner theoretisch System-Rechte erlangen und dann die Provisionierungsdaten abfangen, um die Karte zu klonen.

Dieses Problem besteht bei HCE-Apps sogar dauerhaft, wenn

NFC: Reichweite und Angreifbarkeit

Near-Field-Communication (NFC) ist ein kontaktloser Standard, der auf Radio-Frequency-Identification (RFID) aufbaut. NFC ist mit dem Ziel entwickelt worden, nur auf kurze Entfernung (bis 10 cm) zu funktionieren. Als Übertragungsverfahren nutzt es Rückkopplungen im magnetischen Feld bei 13,56 MHz, sodass die Wellen sich anders ausbreiten als bei normaler Funkkommunikation.

Ein passives Mithören von aktuellen Übertragungen ist selbst unter idealen Bedingungen auf wenige Meter Entfernung begrenzt [1], ein aktives Auslesen einer NFC-Karte oder eines Smartphones, wie es zum Klonen oder für Relay-Angriffe nötig ist, gelang bisher nur über maximal 25 cm [2].

Während das Klonen durch geeignete kryptografische Protokolle unterbunden werden kann, sind Relay-Angriffe nur durch Abschirmung des NFC-Elements beziehungsweise Abschalten der NFC-Funktion bei gesperrtem Smartphone-Bildschirm zu verhindern. Eine optische Prüfung wie beim elektronischen Reisepass und Personalausweis (wo das Lesegerät vor dem Auslesen via RFID die gedruckte Ausweisnummer einscannen muss) ist zwar prinzipiell denkbar, aber für den Anwendungszweck Mobile Payment nicht praktikabel.

Die Produktfamilie TRAVIC ist die plattformunabhängige und skalierbare IT-Lösung für alle Standards des Online- und Electronic Banking

TRAVIC ist eine der vielseitigsten Produktfamilien für Electronic Banking auf dem Markt und bietet für jede Aufgabe im Zahlungsverkehr, im Filetransfer oder in der Sicherheit die passende Lösung.

TRAVIC ist bewährt im Einsatz bei fast allen deutschen Banken, sowie deren Rechenzentren, bei Direktbanken sowie Versicherungen, Krankenkassen. Ist geeignet für Kommunen und Versorgungsunternehmen und alle Dienstleister mit Zahlungsabwicklung im Internet.

TRAVIC-Link ist die universelle Kommunikationsplattform für den automatisierten und sicheren Datenaustausch

Electronic Banking und Zahlungsverkehr mit EBICS
TRAVIC-Link ist ein automatisierbarer und standardkonformer EBICS-Client für die sichere Übertragung von Zahlungsdateien (v. a. SEPA SCT/SDD) zu allen Banken und Sparkassen in Deutschland.

Gesicherter Filetransfer mit ONGUM-IP Datenaustausch
Das in TRAVIC-Link integrierte Filetransferprotokoll ONGUM-IP ermöglicht gesicherte Übertragungen von Dateien beliebigen Inhalts über IP-basierte Netze zwischen mehreren TRAVIC-Link-Systemen auf allen Plattformen (Windows, UNIX, Linux, z/OS).

Integrationsplattform für Filetransfer-Verfahren
Nahezu alle Standardverfahren im datei- und nachrichtenorientierten Datenaustauch sind entweder in TRAVIC-Link integriert oder können über entsprechende Schnittstellen integriert werden:

- Integrierte Electronic-Banking- und Filetransferverfahren: EBICS, ONGUM-IP, Secure FTP
- Über Schnittstellen integrierbare Standard-Software, u.a.: Connect:Direct, rvs, MQSeries, CFT
- KKS-Kommunikation: FTAM TCP/IP, FTAM ISDN, Mail, HTTP

TRAVIC-Link bietet:

- Automatische Erkennung von zu versendenden Dateien über eine Dateischnittstelle
- Auftragsschnittstelle (API)
- Automatische und gesicherte Dateiübertragungen inklusive Restart-Verfahren und zeitgesteuerte Abholung
- Automatische Vor- und Nachverarbeitung von zu versendenden Dateien
- Automatische und manuelle Erstellung von Elektronischen Unterschriften
- Verschlüsselungsverfahren und Komprimierung
- Gesicherter Ad-Hoc-Filetransfer (Up- und Download) über Browser
- Protokollierung aller Aktivitäten und Signalisierung bei Ereignissen
- Grafische Benutzeroberfläche mit Dialogen für Installation und Konfiguration, Bedienung und Überwachung

TRAVIC-Link ist verfügbar für die Plattformen Windows und Unix (AIX, Solaris, Linux) und z/OS.

http://www.siz.de/ebanking/produkte-uebersicht.html

Malware Zugriff auf sensitive Daten im App-Speicher erhält – selbst wo die App mit einer PIN geschützt ist, könnte diese durch Ausspähen auf dem Smartphone oder einen Offline-Angriff ermittelt werden.

Weniger kritisch sind hingegen die Anzeige von Zahlungsvorgängen sowie Transaktionen durch eine Wallet-App (unabhängig davon, wie die Zahlungsfunktion implementiert ist): Die App wird über das Internet synchronisiert, erhält auf diesem Wege aber keine Kreditkartendaten. Lediglich eventuell vorhandene „Geld Senden"-Funktionen könnten hier zum Angriffsziel werden.

Verfügbarkeit

Für Endkunden

Die Kreditkarten zum Aufkleben von mpass und Targobank sind seit 2012 verfügbar (für letztere fällt eine jährliche Gebühr an) und nutzen die PayPass-Technik von MasterCard. O2 bietet seinen Vertragskunden mit einem Samsung Galaxy SIII oder ACE 2 ein kostenloses NFC-Pack, das eine neue SIM-Karte mit Secure Element enthält, auf die eine (dann interne) mpass-Kreditkarte aufgespielt werden kann. Die Telekom und Vodafone bereiten derzeit Lösungen vor, die auf PayPass respektive VISA payWave aufbauen, aber noch nicht verfügbar sind.

Unter den Händlern, die PayPass akzeptieren, finden sich bereits mehrere große Ketten: Neben Tankstellen von Aral und Star sind vor allem Unternehmen der Douglas-Gruppe (Douglas-Parfümerie, Christ, Hussel, Thalia, Appelrath-Cüpper) und Vapiano-Restaurants mit geeigneten Kassensystemen ausgestattet. Mit payWave kann man dagegen außer bei Douglas-Unternehmen und Star auch bei Karstadt und HIT bezahlen. Da die technische Grundlage für beide Systeme gleich ist, steht jedoch zu erwarten, dass sich die Händlerliste nach und nach angleichen wird, sobald die Händler entsprechende Zertifizierungen und Lizenzen erhalten.

NFC-lose Verfahren mit Zahlencodes sind bereits bei Netto (deutschlandweit) und bei Edeka (im Raum Berlin) verfügbar – hier erfolgt die Abwicklung jedoch nicht über eine Kreditkarte, sondern als Banklastschrift mithilfe der Deutsche Post Zahlungsdienste GmbH.

Für Händler

Um per NFC Zahlungen entgegenzunehmen, muss der Point-of-Sales natürlich mit einem passenden Lesegerät ausgestattet sein, das entweder in das Zahlungsterminal integriert oder über eine externe Schnittstelle an ein bestehendes Terminal angeschlossen werden kann. Ferner muss die Terminal-Software das gewünschte Zahlungssystem unterstützen, womit dann aber auch automatisch die recht weit verbreiteten Kreditkarten mit NFC-Chip akzeptiert werden.

Es ist alternativ möglich, die eigenen Kassen mit einem proprietären System auszustatten, das Zahlen- oder QR-Codes nutzt – die Zahlungsabläufe sind damit jedoch nicht so schnell wie bei NFC und die Marktdurchdringung ist noch sehr gering.

Fazit

Das Bezahlen mit dem Smartphone kommt jetzt – wenngleich deutlich später als erwartet – auf den deutschen Markt. Erste Lösungen (Netto/Edeka, mpass/O2, Targobank) sind verfügbar, weitere Anbieter stehen in den Startlöchern.

Die auf Kreditkartenverfahren aufbauenden NFC-Lösungen haben einen technologischen Vorsprung durch die Erfahrung der Kartenherausgeber und durch das Secure Element. Integrierte Lösungen koppeln sinnvollerweise die Zahlung per NFC an die Bildschirmsperre des Smartphones, was gegen Diebstahl und Auslesen „im Vorbeigehen" schützt, sind allerdings nur für sehr wenige Smartphone-Modelle verfügbar.

Lösungen zum Aufkleben sowie proprietäre Online-Lösungen sind hingegen für eine breite Palette an Geräten verfügbar. Dieser Unterschied ist nicht zuletzt auf die bisher starke Reglementierung des Zugriffs auf das im Smartphone verbaute NFC-Modul zurückzuführen, die einerseits die Sicherheit gegen Missbrauch deutlich steigert, andererseits aber lange Zeit kleine Anbieter mit neuen Ideen zugunsten der etablierten Marktteilnehmer ausgeschlossen hat.

Durch Googles Freigabe der Host-based Card-Emulation (HCE) sind in den nächsten Monaten auf NFC-fähigen Android-Systemen spannende neue Lösungen für Mobile Payment zu erwarten – aufgrund der Umsetzung in Software/Apps sind diese jedoch auch anfälliger für Missbrauch. ■

Dr. Georg Lukas ist Sicherheitsberater bei der rt-solutions.de GmbH.

Literatur

[1] Florian Pfeiffer, Klaus Finkenzeller, Erwin Biebl, Theoretical Limits of ISO/IEC 14443 type A RFID Eavesdropping Attacks, in: Proceedings of the 2012 European Conference on Smart Objects, Systems and Technologies (SmartSysTech), VDE-Verlag, Berlin, 2012, ISBN 978-3-8007-3441-2

[2] Ilan Kirschenbaum, Avishai Wool, How to Build a Low-Cost, Extended-Range RFID Skimmer, in: Proceedings of the 15th USENIX Security Symposium, 2006, online auf www.usenix.org/legacy/events/sec06/tech/kirschenbaum.html

Sind Sie verantwortlich für die IT-Sicherheit?

<kes> liefert alle relevanten Informationen zum Thema IT-Sicherheit – sorgfältig recherchiert von Fachredakteuren und Autoren aus der Praxis.

In jeder Ausgabe finden Sie wichtiges Know-how, Hinweise zu Risiken und Strategien, Lösungsvorschläge und Anwenderberichte zu den Themen:

Internet/Intranet-Sicherheit
Zutrittskontrolle
Virenabwehr
Verschlüsselung
Risikomanagement
Abhör- und Manipulationsschutz
Sicherheitsplanung
Elektronische Signatur und PKI

<kes> ist seit 20 Jahren *die* Fachzeitschrift zum Thema Informations-Sicherheit - eine Garantie für Zuverlässigkeit.

Jetzt Probeheft anfordern!

<kes>-online

<kes>-Leser können neben der Print-Ausgabe auch <kes>-online unter www.kes.info nutzen. Hier finden Sie ohne Zugangsbeschränkung, das Thema der Woche, viele interessante Links, Stichwort-Lexikon IT-Security-Begriffe, Verzeichnis relevanter Veranstaltungen und außerdem aktuelle Artikel zum Probelesen.

Abonnenten erhalten zusätzlich ein Passwort mit dem sie Zugriff auf alle aktuellen Artikel und auch auf das Online-Archiv erhalten.

PROBEHEFT-ANFORDERUNG

☐ **ja,** bitte schicken Sie mir gratis und unverbindlich ein Exemplar der <kes> - Die Zeitschrift für Informations-Sicherheit zum Probelesen zu.

Es kommt nur dann ein Abonnement zustande, wenn ich es ausdrücklich wünsche.

Das Abonnement beinhaltet ein Passwort zur Nutzung des Abo-Bereichs auf www.kes.info

Datum | Zeichen | Unterschrift

Lieferung bitte an

Telefon Durchwahl

FAX an +49 6725 5994

SecuMedia Verlags-GmbH
Abonnenten-Service
Postfach 12 34
55205 Ingelheim