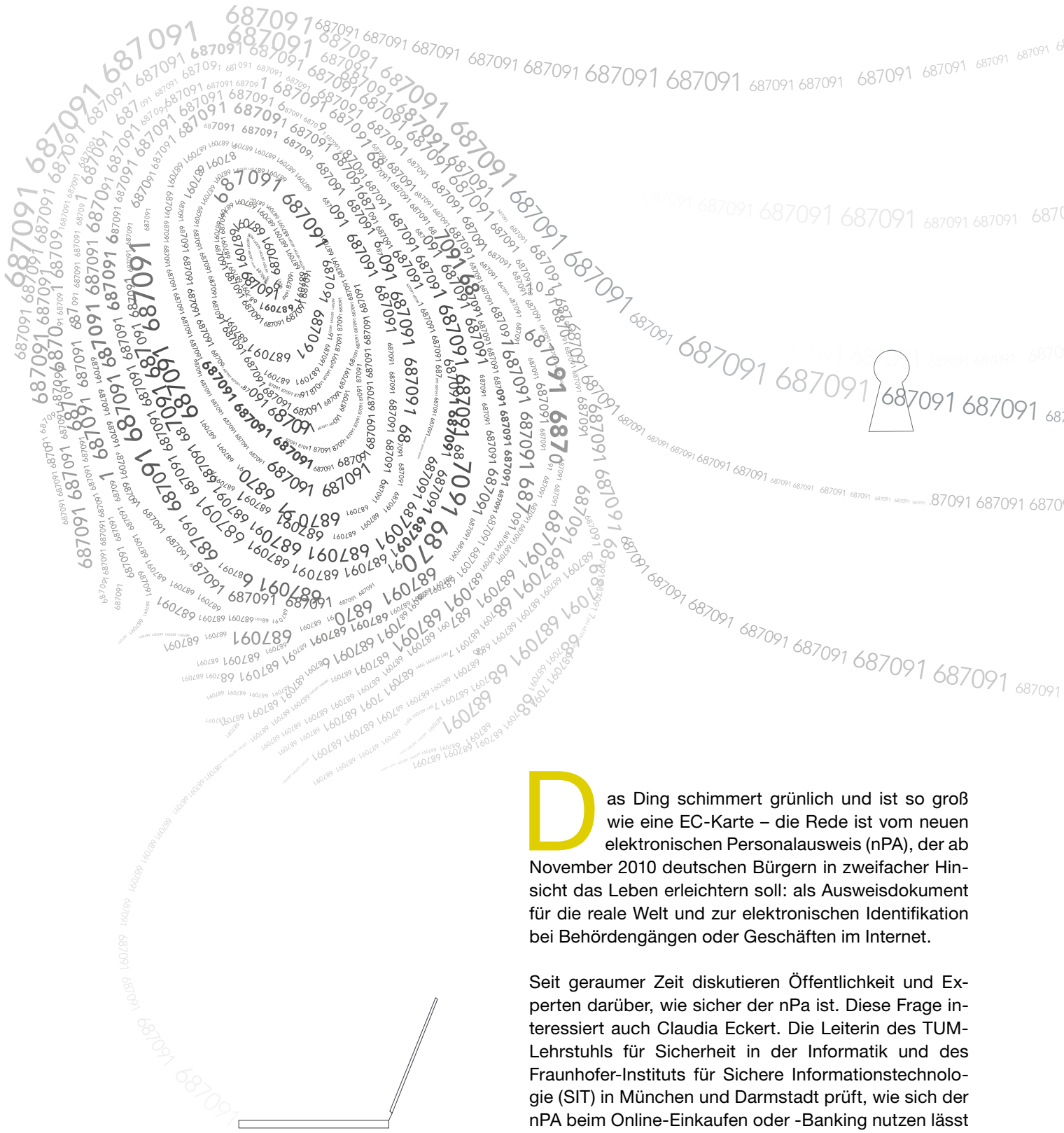
Claudia Eckert entwickelt unter anderem Technologien, die gegen Produktpiraterie schützen sollen. Die Professorin leitet den TUM-Lehrstuhl für Sicherheit in der Informatik und ist gleichzeitig Direktorin des Fraunhofer-Instituts SIT in Darmstadt und München. Sie berät die öffentliche Hand in allen Fragen der IT-Sicherheit

Foto: Eckert / Heddergott, TUM; Illustration: ediundsepp

Sicher durch elektronische Welten

Forscher am Lehrstuhl für Sicherheit in der Informatik testen den neuen elektronischen Personalausweis und entwickeln neue Verfahren, um eingebettete Systeme noch sicherer zu machen

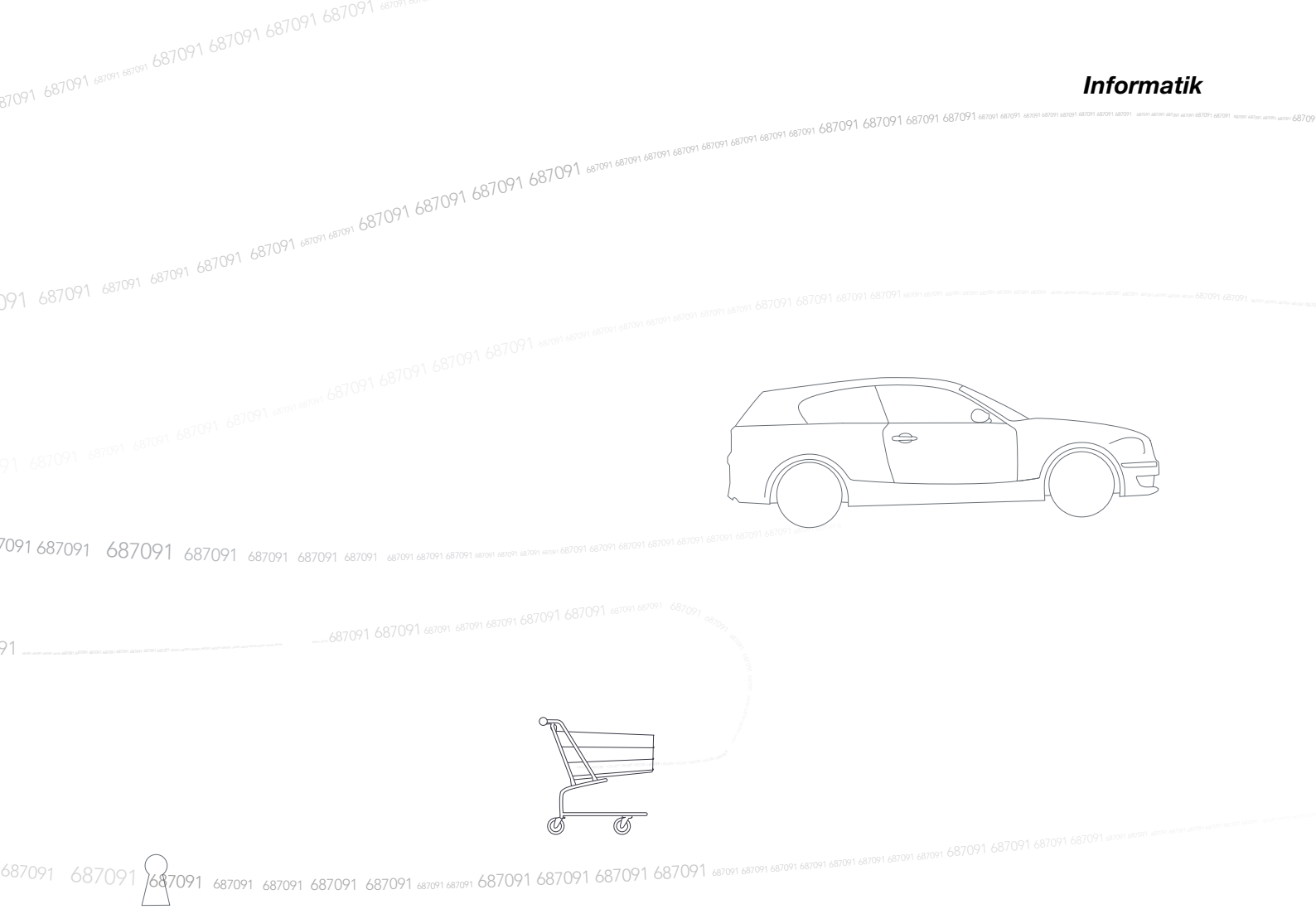


Das Ding schimmert grünlich und ist so groß wie eine EC-Karte – die Rede ist vom neuen elektronischen Personalausweis (nPA), der ab November 2010 deutschen Bürgern in zweifacher Hinsicht das Leben erleichtern soll: als Ausweisdokument für die reale Welt und zur elektronischen Identifikation bei Behördengängen oder Geschäften im Internet.

Seit geraumer Zeit diskutieren Öffentlichkeit und Experten darüber, wie sicher der nPa ist. Diese Frage interessiert auch Claudia Eckert. Die Leiterin des TUM-Lehrstuhls für Sicherheit in der Informatik und des Fraunhofer-Instituts für Sichere Informationstechnologie (SIT) in München und Darmstadt prüft, wie sich der nPA beim Online-Einkaufen oder -Banking nutzen lässt und ob es Sicherheitslücken gibt. Eckerts Team betreibt ein Test- und Sicherheitszentrum und entwickelt eigene Anwendungen, um die Firmen, die den nPA derzeit testen, bei der korrekten und sicheren Umsetzung der neuen Technologien zu unterstützen.
Jeder nPA enthält die Personendaten, zusätzlich gibt es einen zweiten Bereich für E-Business-Anwendungen, in dem Name, Adresse und Geburtsdatum hinterlegt sind. Auf Wunsch kann der Bürger die sogenannte elektroni-

Links

www.sec.in.tum.de
www.sit.fraunhofer.de



sche Identitäts-Funktion (eID) für Online-Geschäfte aktivieren. Damit wird eine sichere Online-Identifizierung des Ausweisinhabers möglich, sodass beispielsweise im Online-Banking die heute üblichen PIN- und Transaktionsnummern überflüssig werden.

Sicherheit durch RFID-Chips

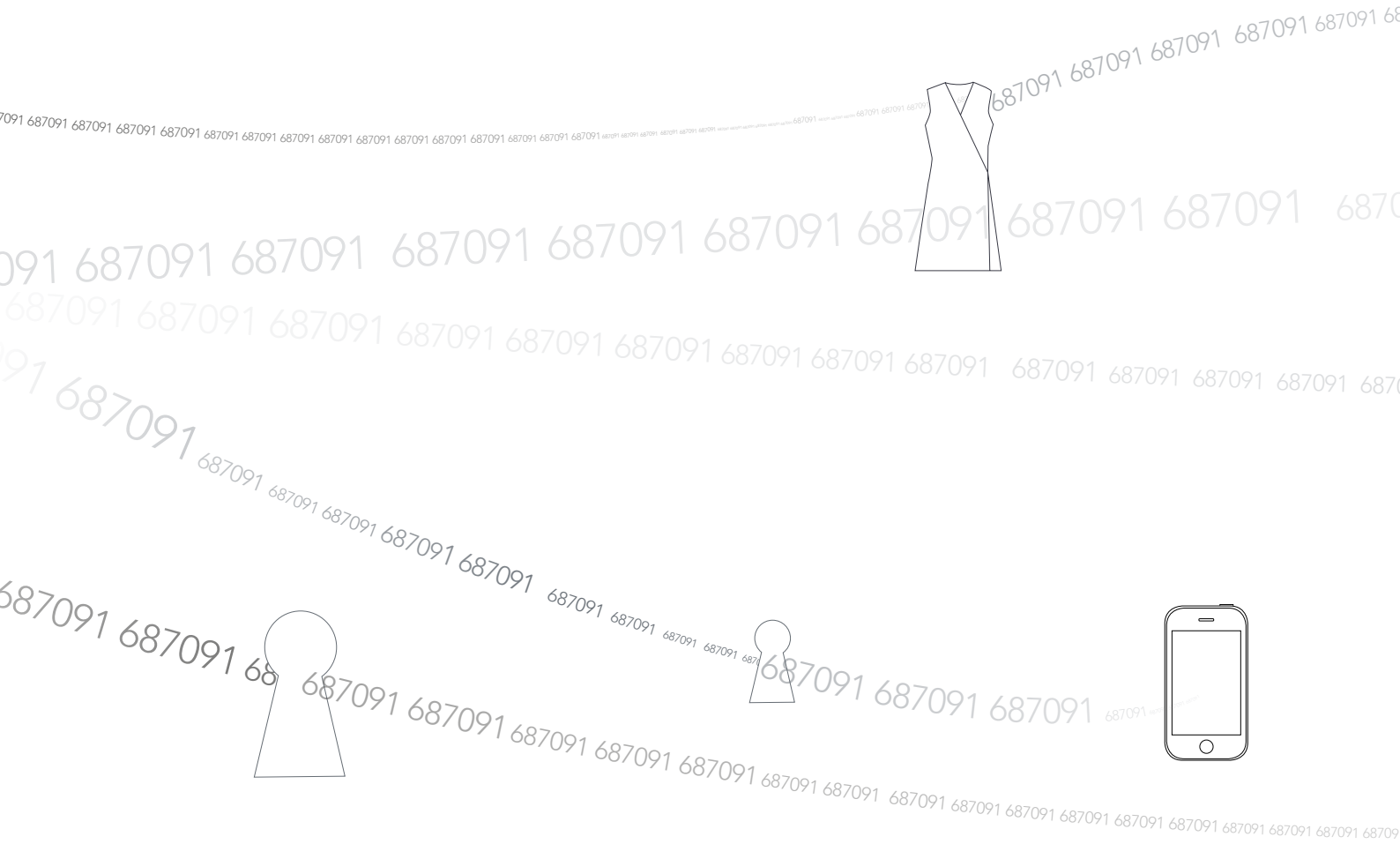
Der Test-nPA, den Claudia Eckert aus ihrem Portemonnaie fischt, hat außer dem Format nicht viel mit einer EC-Karte gemeinsam. Frau Mustermann schaut einen freundlich von ihrem Foto an, statt eines Magnetstreifens ist ein RFID-Chip (Radio Frequency Identification) eingearbeitet. Damit können die gespeicherten Daten, die in verschlüsselter Form vorliegen, per Funk ausgelesen werden. „Es handelt sich um einen Hochsicherheitschip mit geringer Sendeleistung. Das heißt, er sendet im Zentimeterbereich. Die Übertragung findet verschlüsselt statt. Die Daten lassen sich aber nur auslesen, wenn der Bürger auch seine sechsstellige PIN eingibt“, beruhigt die Informatikerin.

Bei den meisten Szenarien für Online-Geschäfte gehen die Entwickler davon aus, dass der Bürger von zu Hause aus seine Internet-Geschäfte abwickelt. Dafür benötigt er ein Lesegerät und eine Softwareanwendung (sogenannter Bürgerclient) für seinen Rechner. Was aber, wenn er unterwegs ist? Hierfür gibt es bereits erste Lösungsansätze: Auf der diesjährigen CeBIT hat Eckerts Team eine Konzeptstudie präsentiert, bei der das Mobiltelefon den Zugang zum Internet schafft und gleichzeitig als Lesegerät für den Ausweis dient.

Am Flughafen per Handy einchecken

Die Forscher nutzen dazu die NFC-Technologie (Near Field Communication), einen Standard für die kontaktlose Funkübertragung von Daten für kurze Strecken. Möchte der Nutzer etwa für eine Flugreise per Handy einchecken, surft er zur Online-Präsenz seiner Fluglinie, die über ein offizielles Zertifikat verfügt. Sobald er sich anmeldet, wird ihm dieses übermittelt. Der Fluggast hält im Anschluss seinen nPA an sein Mobilfunkgerät. Dessen integrierter NFC-Leser baut den Kontakt zum nPA auf. Nach dem Überprüfen des Anbieter-Zertifikats kann der Reisende entscheiden, ob er sich bei seiner Fluggesellschaft über die eID-Funktion seines elektronischen Personalausweises ausweist und welche Daten er übermittelt. Erst wenn er seine persönliche PIN eingetippt hat, sind diese auch freigegeben. „Die ▷

Illustration: ediundsepp

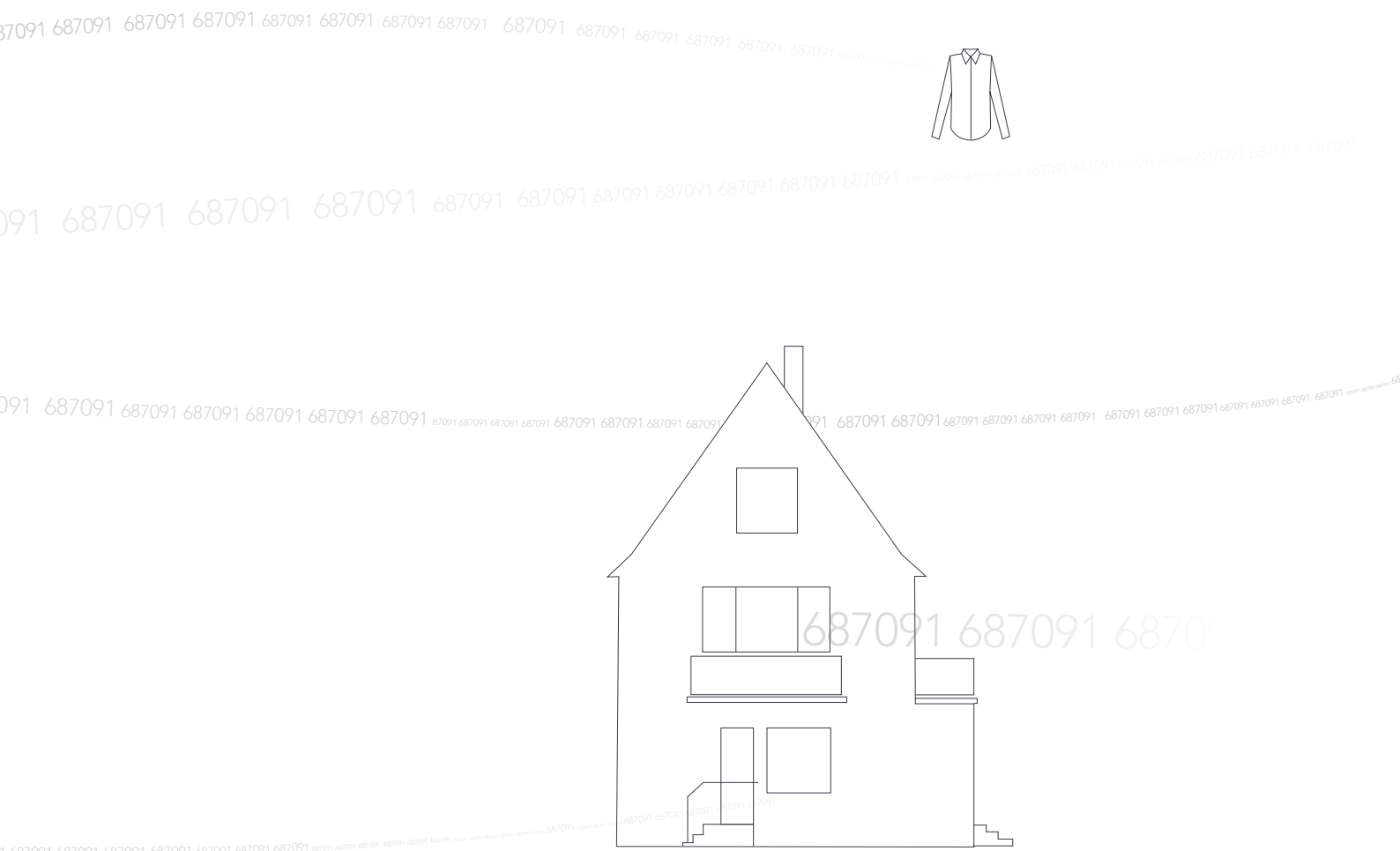


Anwendung lässt sich bereits mit heutigen Mobilfunknetzen realisieren. Es sind zwar noch nicht viele Mobiltelefone mit NFC ausgestattet, aber das wird sich sicher ändern. Es gibt allerdings zu viele unterschiedliche Handy-Plattformen, da fehlen noch Standards. Außerdem wird eine Software benötigt, die wie der Bürgerclient auf dem PC auch die sichere Zusammenarbeit zwischen Handy und elektronischem Personalausweis regelt“, beschreibt Claudia Eckert die Aufgaben, die auf die Entwickler warten.

Funketiketten gegen Produktpiraterie

Funketiketten sind aber nicht nur für den elektronischen Ausweis interessant. Damit könnten sich Unternehmen vor Produktpiraterie schützen. Indem beispielsweise Originalbauteile mit speziellen Identitätsmerkmalen bestückt und untrennbar verbunden werden. Hier sind die Informatikerin und ihre Mitarbeiter dabei, ein noch junges Forschungsgebiet zu erobern. Die Vision der Forscher: Aus Fertigungsabweichungen von Chips im Subnanometerbereich möchten sie Identifikationsmerkmale erzeugen, die nicht kopierbar sind. „Die Idee besteht darin, aus den physikalisch einzigartigen Strukturen, die aufgrund von nicht beeinflussbaren Variationen bei der Herstellung entstehen, eine Art Fingerabdruck des jeweiligen Chips abzuleiten“, erläutert Dominik Merli, einer der Forscher in Eckerts Team. Physical Unclonable Functions (PUF), also physikalisch nicht kopierbare Funktionen, nennen Experten dieses Verfahren. Sie sind vergleichbar mit biometrischen menschlichen Merkmalen wie Iris oder Gesichtsbild. PUF würden also jedes physikalische Objekt einzigartig machen. Damit ließe sich jedes einzelne Produkt kennzeichnen und der Hersteller könnte verhindern, dass ein Bremsbelag oder ein Medikament als billige Kopie nachgebaut wird.

Claudia Eckert erklärt, wo noch Forschungsbedarf besteht: „Will man die Identität eines Menschen mit biometrischen Merkmalen prüfen, so vergleicht man diese unverwechselbaren Merkmale mit Referenzwerten. Zunächst muss jedoch ein Sensor das Merkmal erfassen. Dabei können Abweichungen etwa durch Verschmutzungen, Alterungsprozesse oder geänderten Lichteinfall auftreten. Man benötigt Korrekturmaßnahmen, um zuverlässig entscheiden zu können, ob das leicht abweichende Merkmal mit dem Referenzwert innerhalb eines Toleranzbereichs noch übereinstimmt. Das gleiche Problem ergibt sich bei der Verwendung von physikalisch



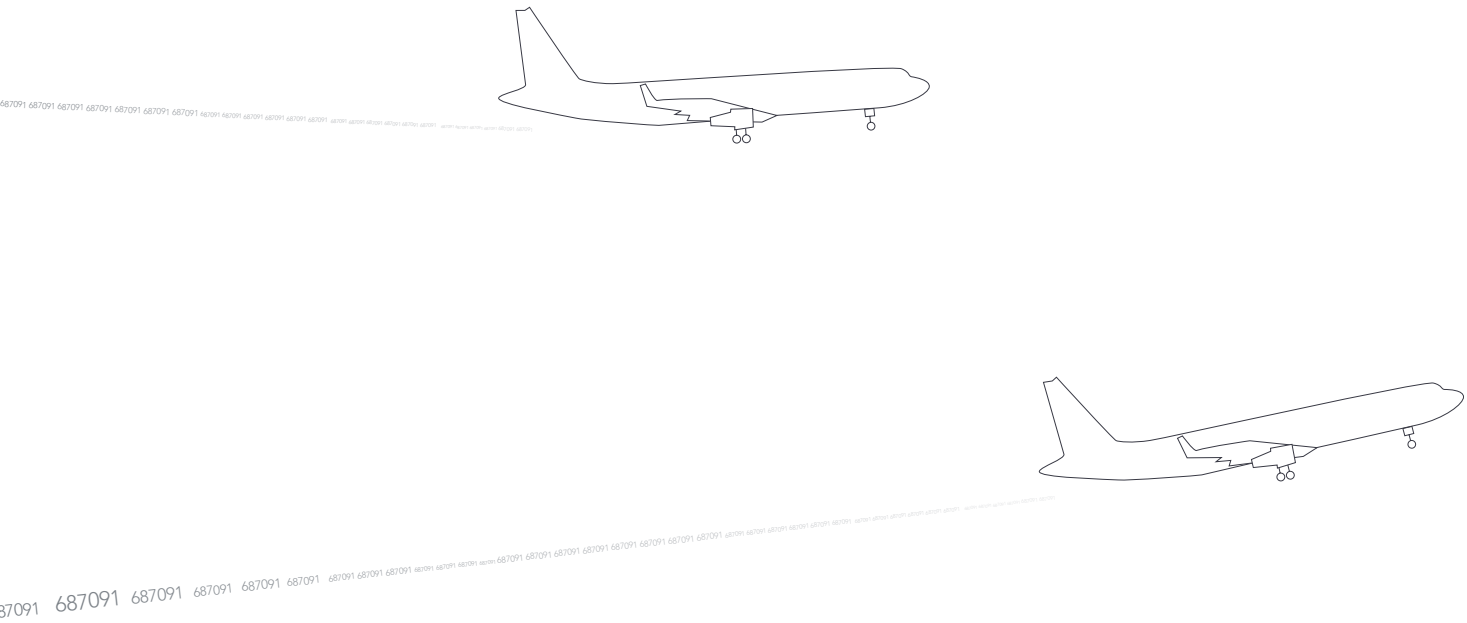
nicht kopierbaren Funktionen zur Objekt-Identifikation. Diese Korrekturen vorzunehmen, ist nicht immer einfach. Denn man will vermeiden, dass womöglich ein gefälschtes Objekt, das leicht abweichende Merkmale aufweist, dennoch als korrekt akzeptiert wird. Die Aufgabe besteht darin, das Rausch- und Entropieverhalten der PUF zu optimieren. Ein weiteres Forschungsfeld sind die Alterungsprozesse von Materialien."

Sicherheit für Cloud Computing

Derzeit ist Eckerts Arbeitsgruppe dabei, mit der Bundesdruckerei Forschungsmittel zu beantragen, um entsprechende Lösungen zu bearbeiten. Sehr viel weiter ist dagegen die Technik beim sogenannten „Cloud Computing": Vor allem kleinere und mittlere Unternehmen erhoffen sich eine Kostenersparnis, wenn sie Daten, Anwendungen und Netze auf externe Server auslagern, beispielsweise Rechnerkapazitäten für Mail-Server oder Kundenverwaltungs-Systeme. Die dazu notwendige Hard- und Software schaffen sie nicht mehr selbst an, sondern mieten je nach Bedarf Kapazitäten bei Dienstleistern wie IBM, Amazon oder Google. Die Unternehmen sind somit flexibel und können sich ganz auf ihre eigenen Kompetenzen konzentrieren.

Es spricht also einiges für Cloud Computing. Deshalb ist es nicht verwunderlich, dass sich immer mehr Wolken in elektronischen Welten bilden. Doch wer auf externe Dienste vertraut, macht sich abhängig von diesen. So kann ein Hackerangriff oder eine Schadsoftware die Geschäfts- oder Produktionsprozesse einer Firma lahmlegen. Ausfälle und Störungen sind bei Cloud-Anwendungen keine Seltenheit. Weitere Gefahrenquellen sind Datenverluste bzw. -lecks, Diebstahl von Konten, Dienstleistungen oder Datentransfers. „Zwar setzen die Cloud-Service-Anbieter Basis-Sicherheitstechnologien zur Absicherung der verwalteten Daten ein, es bleiben aber viele Sicherheitsfragen offen. Die heutigen Isolierungsansätze reichen nicht aus, um eine vollständige Abschottung der Nutzerdaten durchgehend zu garantieren und unberechtigte Datenzugriffe zu verhindern", sagt Claudia Eckert. „Notwendig sind auch zusätzliche Verfahren zum Beispiel zur Markierung und Filterung von Daten. Damit ein Unternehmen sensible Informationen, wozu unter anderem datenschutzrelevante Daten zählen, nicht ungeschützt in der Cloud ablegt." Was Eckert verwundert: „Da vereinbaren die Unternehmen zwar einen Rund-um-die-Uhr-Betrieb, vernachlässigen aber sicherheitsrelevante Garantien." ▷

Illustration: ediundsepp



Sie müssten sich folgende Fragen stellen: Wie sicher sind die Firmengeheimnisse auf den externen Servern? Welche Zugriffsrechte hat ein Sub-Unternehmer des Cloud-Anbieters? Was passiert, wenn die Anwendung abstürzt? Dabei lassen sich mit sogenannten Service-Level-Agreements Rechte und Pflichten zwischen den Nutzern und Anbietern genau festlegen. Die heute üblichen Vereinbarungen enthalten jedoch nur minimale Garantien für die Dienstgüte des Cloud-Service. Sicherheitsgarantien sind kaum vorhanden und die dafür notwendigen Funktionen, die der Cloud-Anbieter bereitstellen müsste, sind nicht dokumentiert. Damit tragen die Nutzer das gesamte Risiko. „Unter kontrollierbaren Rahmenbedingungen lassen sich die Dienste nutzen. Vorher sollte man detaillierte Informationen vom Anbieter anfordern und anhand von Checklisten eine Risikobewertung durchführen“, meint Eckert.

Trotzdem gibt es auch bei Cloud Computing noch eine Reihe offener Fragen. Eine technische Herausforderung ist neben den oben angesprochenen Themen die Frage des korrekten Zusammenspiels verschiedener Softwarepakete in der Cloud: Wie wird beispielsweise ein über die Produktgrenzen hinweg einheitliches und durchgängiges Identitäts- und Zugriffsmanagement durchgeführt, sodass nicht ein schwacher Sicherheitsmechanismus die gesamte Sicherheitskette zerstört? Welche Komponenten sind wofür geeignet und wie kann man deren Qualität durch gezielte zusätzliche Maßnahmen verbessern? Eckerts Arbeitsgruppe möchte herausfinden, wie die Systeme in der Cloud zusammenarbeiten. Aus diesem Grund wird derzeit in Garching ein Cloud-Labor aufgebaut. Das können dann auch Dienstleister nutzen, die ausprobieren möchten, ob ihre Anwendung funktioniert, beziehungsweise können sie die Sicherheit der Anwendung testen lassen.

„An einer Standardisierung kommen die Anbieter nicht vorbei“, meint die Informatikerin. Erste Ansätze dazu gab es vergangenes Jahr mit der Gründung der Cloud Security Alliance (CSA) in den USA, bei der sich eine Reihe namhafter Unternehmen zusammengeschlossen hat. Es fehlen jedoch juristische und regulatorische Vorgaben, die unter anderem die Cloud-Anbieter in die Pflicht nehmen, nachprüfbare Aussagen über deren eingesetzte Sicherheitsstandards zu machen. „Hier können wir nichts mehr tun“, sagt Claudia Eckert. „Das ist jetzt Aufgabe der Politik.“ *Evdoxía Tsakiridou*

Illustration: ediundsepp