WHITE PAPER
SECURE IDENTITIES IN THE DIGITAL WORLD

T · · Systems ·

CONTENTS

WHITE PAPER ON **SECURE IDENTITIES IN THE DIGITAL WORLD**

INTRODUCTION

Navigating the Internet has become second nature for virtually all of us. And we're accustomed to using different identities for different purposes. In chat rooms, we might prefer to stay anonymous, but in our online shopping, we of course use our real name. In some social media channels, we prefer a pseudonym. When we log on at the office, we have to use the user name our employer has assigned us.

Users of cyberspace often have many identities. Since you don't need to provide ID in order to register for an online shop or a chat room, shop operators and chatters usually have no way of knowing what real identities the digital identities they see are hiding. This situation allows fraud to thrive just about anywhere one might care to look. Thieves use false identities to make purchases, plunder online banking accounts and exploit chats.

So a key question one often has to ask is, "who's behind that identity?"

In the real world, it's usually easy to verify identity. People carry ID, i.e. physical proof of their real identity.

In the digital world, it's much more difficult to verify identity. People who interact with each other – such as business and chat partners – often don't know each other and often have no way of meeting. Online shops, banks and social media channels usually verify their users' identities by means of a combination of user name + password, both of which users choose for themselves when they register. This simple procedure has been presenting growing risks, however, since user names and passwords are often stored in vulnerable databases or can be intercepted via phishing sites. As a result, thieves have been stealing large numbers of digital identities and then selling them or using them for their own criminal purposes.

Although new cases of identity theft keep emerging almost by the month, and although case after case hits a new high-water mark for damages, many users still seem oblivious to the risks. Or they simply consciously ignore them, thinking that this is the only sane way to stay connected. It's now almost impossible to find an Internet service that does not require users to register and to define personal access data.

And since no one can remember different passwords for all the different services and sites he or she uses, users tend to use the same passwords – including passwords that are often too short or too trivial – for online shopping, e-mail, Facebook, etc. For cybercriminals with special software, passwords that are easy to remember are easy to crack, in seconds, and "one-size-fits-all" passwords, once cracked, open many different doors.

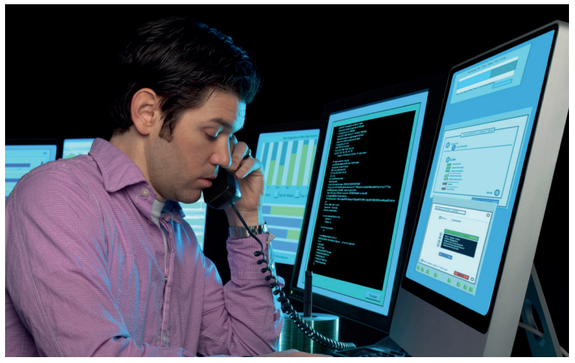
Companies and infrastructure operators face completely new types ofthreats, in the "Internet of Things" and "Industry 4.0." Until recently, industrial control systems (ICS) tended not to be connected to other IT systems and networks. This meant, for example, that cybercriminals had no way of accessing the software that controlled a production line. But now more and more machines, cars and individual devices are being connected to the Internet. Like computers, printers and smartphones, such things are being assigned their own IP addresses – i.e. addresses at which they can be remotely accessed via the Internet. Gartner, the technology research and advisory company, is now predicting that a total of 25 billion devices will be connected to the Internet by 2020. When such devices are "protected" by their owners'/operators' user names and passwords, thieves who steal such names and passwords can access the devices remotely.

The present white paper has been written in order to present alternative ways of authenticating digital identities – techniques that are much more secure than "one-factor authentication" via user name and password. The central strategies they use are "two-factor authentication" and secure-source key generation and storage. Two-factor authentication, which verifies identification via a combination of a user-held secret and a "token," makes it possible to securely correlate users and things.

RISKS ON THE INTERNET

More and more cybercriminals have been discovering a lucrative new business area: identity theft. Thieves have been using stolen identities to hijack Facebook accounts, steal online shops' login and payment data and go on wild shopping sprees. They've been turning stolen identities into social-media aliases that allow them to insult, harass and even threaten innocent network users. They've been e-mailing huge amounts of spam, often with attached malware that can vandalize third-party IT systems or skim off even more data, and they've been fraudulently entering into cell phone agreements, ordering credit cards and opening bank accounts.

In early 2014, hackers stole 16 million e-mail addresses including access data from third-party systems. A short time later, they stole details for an additional 18 million e-mail accounts. Those two attacks were among the largest cases of identity theft, involving complete digital identities, ever to emerge in Germany. For the Federal Office for Information Security (BSI), those two cases are just the tip of the iceberg. This is because most cases of theft of e-mail addresses, passwords and PIN numbers are never detected. The BSI counts identity theft among the very largest risks of Internet use, since even user systems that receive continual password changes and have up-to-date virus scanners and firewalls are not really protected against skilled hackers – and hackers have been getting more and more skilled. A representative online survey of the Schufa credit-information company has confirmed the BSI's concerns, noting that 15 percent of all German Internet users have already fallen victim to identity theft.



Criminals use a range of different methods for stealing digital identities. The simplest of all is not digital in itself; it's good old-fashioned hands-on theft. It consists of stealing physical smartphones – with their data "coming along for the ride," so to speak. People who store PIN numbers and passwords in unencrypted form on their smartphones are simply asking for trouble and can quickly be victimized.

The most common method of thievery is to use malware to skim data from computer systems. Hackers keep coming up with ever-more ingenious methods for getting malware onto victims' computers. For example, "phishing" fraudsters create forged websites – designed to look like reputable sites that users trust – where they hide viruses and links to malicious pages (for example, in banner ads). According to Sophos, an IT-security company, some 30,000 so-infected websites are added every day. Another trick used by phishing fraudsters is to send forged e-mails that are designed to look like messages from real banks, well-known companies or victims' acquaintances. Such mails ask users to click on links that, needless to say, are poisoned – that install malware or lead directly to specially prepared websites at which victims are requested to "update" their data, such as credit card numbers and passwords, by entering them into special forms. Needless to say, the identity data so entered are handed to the thieves on a silver platter! Yet another tactic is to send virus-infected mails that exploit computer vulnerabilities completely discreetly – for example, by implanting data loggers that capture and transmit data invisibly.

So how can we guard our digital identities? How can I protect myself and keep fraudsters from stealing my identity and using it for their own purposes?

IMPROVED SECURITY AS A RESULT OF TWO-FACTOR AUTHENTICATION

As described in the preceding sections, a user's digital identity normally consists of a combination of user name and password. The security – i.e. the meager security – provided by such "one-factor authentication" lies in the secret password that goes together with the user name.

Two-factor authentication, for which a number of different procedures are available, is a more-secure alternative to one-factor authentication. The security it provides is not limited to a secret password, the "first factor," because it provides a second factor as well – for example a special hardware module.

One established procedure for two-factor authentication involves the issuing of one-time passwords via user-held "one-time password tokens" (OTP tokens), which can be either separate, stand-alone devices or modules residing on smartphones. In this procedure, the secure online session begins with the OTP token generating a one-time password. To register with the relevant service, the user then logs on with the OTP and an additional password. The background system then compares the user's OTP with a one-time password generated by an authentication server. This works because the authentication server and the token use the same keys and algorithms and thus can generate the same passwords. The first factor is thus the OTP token (which the user has to own), while the second is the additional password (which the user has to know). Additional security is realized if the server component of the two-factor authentication process is operated in a highly secure, certified environment.

Along with OTP, other hardware-based procedures using two-factor authentication are also available that can significantly enhance the security of digital identities. Such other procedures carry out the authentication process based on "certificates", with the help of a chipcard or a USB token. In this context, a certificate is an electronic collection of identity characteristics of the user, such as name, address or date of birth, that are certified, via digital signature, by a universally recognized agency – a "certification authority" (CA) – in a "trust center".

THE FUNCTION OF A TRUST CENTER

In Germany, the process of issuing a card-based digital identity is as follows: a trust center certified by the Federal Office for Information Security (BSI) first generates a certificate. To receive such a certificate, the applicant must prove his or her identity, either to the trust center itself or to a recognized registration agency, by presenting a physical ID document in person. If the applicant uses the new national identity card now available in Germany, he may also prove his identity online.

For the digital identity, the trust center then generates a key pair consisting of a private key and a public key. It securely saves the private key to a token and then generates a certificate that contains a) the public key, b) the user's verified identity characteristics and c) the trust center's digital signature, which certifies that the certificate is authentic. The certificate then guarantees that the key pair was generated in a trustworthy environment, that the private key has been securely saved and that the identity characteristics on the certificate can be trusted. This then provides the basis for an "electronic relationship of trust." Such certificates can be issued to all subscribers within a public-key infrastructure (PKI), and they can be published in suitable directories.

BACKGROUND

THE COMPONENTS OF A PUBLIC-KEY INFRASTRUCTURE (PKI)

Digital certificates	Digitally signed electronic data that can be used to verify the authenticity of objects.
Trust center	Issues CA certificates and assumes responsibility for signing certificate applications.
Registration authority	An agency to which one can apply to obtain certificates for persons and machines. It checks the correctness of data and approves certificate applications as appropriate.
Certificate revocation list (CRL)	A list of certificates that have been revoked because their key material has been compromised or their certificate data have become invalid.
Directory service	A searchable database of certificates that have been issued.
Validation service	A service that checks the validity of certificates in real time.

BACKGROUND: CRYPTOGRAPHY

Originally, "cryptography" was a collective term for the science of information encryption. Today, it refers to a broad spectrum of information security aspects and issues, from design and specification of information security concepts to the implementation of information systems that are highly resistant to unauthorized data read-out and modification.

The most important concepts used in cryptography include information authenticity, integrity, confidentiality, availability and non-repudiation. Initially, the term "cryptography" was applied only to the encryption process itself, i.e. to a process used to protect the confidentiality of information. This entailed converting information from a plain-text format (plaintext) into secret, undecipherable formats (ciphertext). Decryption refers to the reverse process, i.e. the conversion of ciphertext into plaintext. As time went on, the meaning of the term was continually broadened. Cryptography is now used as a collective term for all functions that are needed for protecting information.

In cryptography, a distinction is made between symmetric and asymmetric cryptography, as illustrated in the following example of encryption:

SYMMETRIC ENCRYPTION

Current situation:
- Sender Bob wishes to send recipient Alice an encrypted message.

Procedure:
- For their secure communications, Alice and Bob hold a common, symmetric key.
- Bob uses the symmetric key to encrypt his message for Alice.
- Alice then uses the same symmetric key to decrypt the message.
- This encryption system can be thought of as a padlock for which both parties have a key.

Fig. 1: Symmetric encryption

SASYMMETRIC ENCRYPTION

Current situation:
- Sender Bob wishes to send recipient Alice an encrypted message, without having previously defined a common encryption key with her.

Procedure:
- For their secure communications, Alice holds a key pair that consists of a public key and a private key. She then sends Bob the public key.
- Bob uses the public key to encrypt his message for Alice.
- Alice then decrypts the message with her private key, which is known only to her. The message can only be decrypted with that key.
- This system may be thought of as a mailbox. Bob can see and use the mail slot, but only Alice possesses the key to the mailbox.

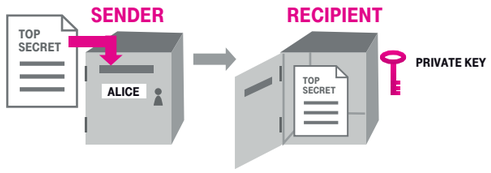


Fig. 2: Asymmetric encryption

A trust center operates a "directory service" for the certificates within a relevant PKI. Such a service may be likened to a telephone directory, in that certificates can be looked up in it by name. And just as a telephone subscriber can opt not to be listed in the local telephone directory, a certificate owner can choose not to be included in the relevant directory service.

Via their trust center's revocation service, certificate owners can have their certificates blocked. Blocked certificates immediately lose their validity and are placed on the center's list of revoked certificates. A trust center's revocation list can be downloaded from the center's website.

Consumers have been using two-factor security solutions for quite some time already, without really being aware of this fact. One example of such a solution in wide use is the smartcard version of the EC card. Users of such cards authenticate themselves on ATMs via a combination of their card and their secret PIN (number). Although this procedure is not completely immune to fraud, it is far more secure than any use of user name + password could be. If any unauthorized person wishes to withdraw money with an EC card, he or she has to steal an actual card and learn the PIN for it. Anyone who suffers the loss or theft of such a card can easily have it blocked immediately, i.e. can easily make it immediately unusable.

BACKGROUND: THE T-SYSTEMS TRUST CENTER

T-Systems operates an accredited trust center within a high-security data center. In December 1998, that center became the first trust center nationwide to be officially authorized to operate a certification authority for electronic signatures pursuant to the German Digital Signature Act (Signaturgesetz; SigG). The authorization was issued by the Regulatory Authority for Telecommunications and Posts (today: Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railway (Bundesnetzagentur). Qualified certificates (provided via the TeleSec Public Key Service) have been a part of the portfolio of the Telekom Trust Center since 1999. Since October 2013, that service portfolio has been certified in accordance with ISO 27001, on the basis of the BSI's "IT-Grundschutz" standard.

T-Systems offers trust center services for key accounts, small and medium-sized enterprises (SMEs) and end customers. Its portfolio comprises qualified certificates and advanced certificates. T-Systems plans, implements and operates a range of special public key infrastructures for a wide spectrum of major customers, including industry customers, government agencies, Länder administrations and other organizations.

Its trust center also offers SMEs various standardized solutions for authentication, encryption and electronic signature functionalities. Certificates for web servers are also an important area of the trust center services. Yet another important area consists of provision of standardized interfaces and protocols that can easily, and cost-effectively, be integrated in our customers' applications.

To date, EC cards and credit cards are really the only area in which two-factor authentication has become adopted on a large scale. A number of other mature two-factor security solutions have been available for years now but have failed to be accepted by the market. This is due to their inadequate user-friendliness and complex login procedures.

Fig. 3: High-security area – Security made in Germany

But now, slowly but surely, hardware-based authentication solutions are emerging from their niche-market role. As cyberspace threats have continued to mount, large corporations in particular have been recognizing an urgent need to act, since virtually no business processes are now viable without Internet connectivity. The dilemma is compounded in that companies' employees often work with highly sensitive data or control business-critical procedures. When cybercriminals manage to pilfer access passwords, therefore, they can find it all too easy to tamper and vandalize as they wish. In worst-case scenarios, an identity theft can force a company to completely shut down applications. That, in turn, can bring their business operations to a complete halt – temporary, or even permanent – within days.

Additional impetus for two-factor authentication may well come from Google, which has also been questioning the validity of the user-name + password approach and has been promoting digital identities that are doubly secured, via hardware and a password. Google now plans to equip the next versions of its Android and Chrome systems with interfaces for authentication solutions using tokens. Yet another push for stronger authentication could come via hardware-based Fast IDentity Online (FIDO) tokens, which consumers can purchase in any electronics store and which support secure registration for a range of different services.

HARDWARE-BASED SECURITY TOKENS

Once its private key is compromised, a digital identity is vulnerable to fraudulent use, as a stolen identity (see above). The security of a digital identity is largely dependent on the security of its private key. That security, in turn, depends not only on how securely the private key is stored, but also – and more strongly – on the entire life cycle of such a key, i.e. on how securely it is generated, stored and used and then destroyed, at the end of the cycle.

As noted above, secure keys are generated in the secure environment provided by a trust center. Hardware-based security solutions – known as "security tokens" or "hardware tokens" – have been developed for secure key storage and use. Such solutions, which are usually based on smartcard technology, provide secure, hacker-resistant storage of a private key together with the certificate for its correlating public key. In addition, they support the execution of cryptographic operations with the private key. This enables the key to remain in the token's secure memory, even during execution of operations – it does not have to be read out.

A number of different versions of hardware-based security tokens are now available. For example, they are now produced as keychains that users can carry with them. When a user loses his key-bearing token, he is likely to notice the loss right away and move quickly to block the pertinent certificate. Even if he is slow to discover the loss, he is still protected in that the token is useless without the proper password.

Hardware-based security tokens are proving especially useful for companies. A company can now issue each of its employees a key with which he can authenticate himself with respect to defined applications, in keeping with his area of responsibility. This allows the definition of access authorizations for specific sections of buildings, for example. Employees can also use the tokens to log onto computers, digitally sign documents and encrypt e-mails. They can even use the tokens for cashless payment of their meals in the company's cafeteria.

Fig. 4: A Deutsche Telekom key generator – German crypto-codes protect digital technologies

BACKGROUND:
THE SECURITY-TOKEN-BASED AUTHENTICATION PROCESS

The token-based authentication process normally proceeds as follows:

- The user initiates data exchange between the token and the verification system – for example, by inserting the token into a reading device or holding it in front of such a device.
- The reading device identifies the token via its unique identification number.
- Using a defined cryptographic verification procedure, the verification system compares the data record read out from the token with local reference data.
- For added security, the local reference data set is compared with additional reference data taken from the database of a remote server.
- If the token is invalid, the verification system denies access.
- To enable the authentication (attempt) to be traced, the event data for the verification process are transmitted to the remote server.
- If the token is valid, the verification system authorizes the functions and/or data for which the owner of the token is basically authorized.

THE ADVANTAGES OF HARDWARE-BASED SECURITY

Hardware-based security tokens use smartcard technology. This gives them a number of key advantages over software-based solutions.

The key is hard-wired into the smartcard and can't be read out.

To be able to prove he is the rightful owner of a private key – and, thus, to prove his identity in connection with the key – a user has to use the smartcard pertaining to the key. And such use involves inserting the smartcard into a reading device; without the reading device, the smartcard cannot be used for authentication purposes. What is more, the smartcard is also PIN-protected. In other words, the possibility to use the smartcard depends on more than simple possession of the card; one also has to know its PIN. The security of the authentication process thus depends on two factors – possession of the smartcard and knowledge of the PIN.

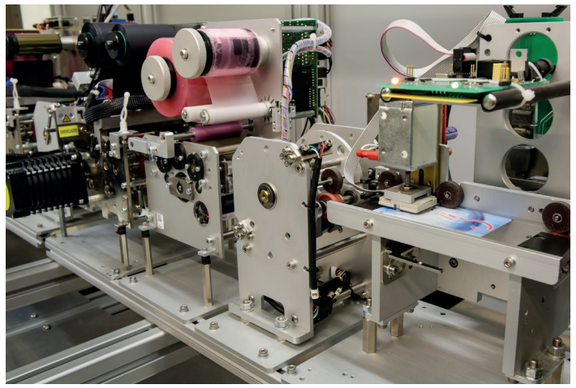


Fig. 5: TCOS smartcard personalization – secure digital identities from Germany

The Smartcard's data is accessed via a microprocessor on the card.

The card's data memory cannot be read out directly – it has to be read out via the card's input-output (I/O) unit and processor (CPU). The card's processor guards the stored data against unauthorized access by running specially developed cryptographic routines. The programs that run on the smartcard are hard-wired into the card's chip, meaning that they cannot be modified.

Smartcards, for secure storage of passwords and keys.

Smartcards have a secure operating system that supports a broad range of cryptographic functions. Those functions, in turn, support secure data storage and use. Often the security of a smartcard has been certified by an independent certification agency. Smartcards are also normally equipped with a range of different sensors and hardware-based mechanisms that, in combination with the card's operating system, are able to effectively ward off so-called "side-channel attacks". In comparison to hardware-based solutions, software-based solutions are much less effective in protecting against side-channel attacks. For technical reasons, they cannot mimic the protective mechanisms available in smartcard technology.

Unlike purely software-based solutions, smartcard tokens cannot be copied and their functions cannot be tampered with or reverse engineered. In addition, tokens' secure, multi-stage identification process, involving a combination of knowledge (such as knowledge of a password) and possession of a token, is more secure than software-based authentication processes. Finally, the security of a smartcard token can be evaluated according to the "Common Criteria", and certified, by a recognized certification agency.

Smartcards support secure, high-performance execution of cryptographic operations.

Smartcards carry out cryptographic operations with the help of special cryptographic coprocessors.

Smartcards simplify processes.

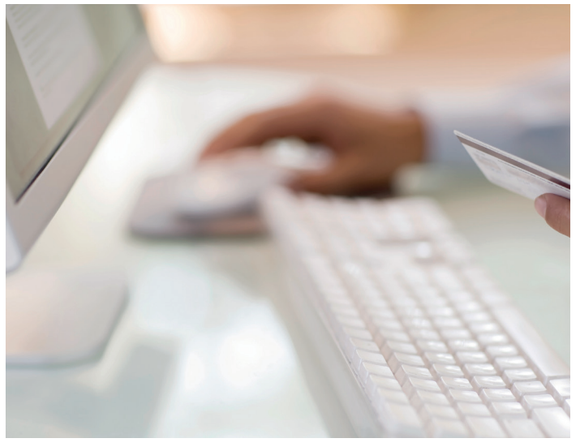
Thanks to smartcard tokens' secure storage of key material, and to the patented secure-shipping solutions that have been developed, the rollout process for smartcard tokens is especially simple. What is more, smartcard tokens can support clear identification of IT components and protect them against copying and plagiarism. Smartcard tokens can also significantly enhance user acceptance of products and entire IT systems. This is because they build users' confidence by guarding against all (unauthorized) modifications of software or data, i.e. even modifications that produce little or no damage – and yet still quickly undermine trust.

Fig. 6: Example of a smartcard from T-Systems

BACKGROUND: SIDE-CHANNEL ATTACKS

Side-channel attacks are attacks that use crypto-analytic methods to exploit the ways cryptosystems are physically implemented within devices (such as smartcards, security tokens and hardware-based security modules) or in software. Instead of targeting devices' cryptographic processes, such attacks focus on specific implementations, meaning that an attack against one implementation can leave a neighboring implementation completely unscathed.

Such attacks function by observing cryptographic devices as they execute their cryptological algorithms, and thereby deducing correlations between the so-observable data and the hidden key being used. The observable, characteristic data can include data such as algorithm runtimes, processor energy consumption during calculations and electromagnetic emissions. The spectrum of such attacks also includes invasive attacks, i.e. active interventions within a device, in order to trigger telltale errors in the execution of a cryptographic algorithm.



TCOS – A HIGHLY SECURE SMARTCARDOPERATING SYSTEM MADE IN GERMANY

As we have seen, smartcard-based security tokens have a secure operating system, a "chip brain" that supports secure key storage and that provides and runs the necessary cryptographic algorithms. The TeleSec Chipcard Operating System (TCOS) is one such operating system.

More than 100 million passports, ID cards (including company ID cards), digital tachographs and electronic tickets in Europe are now equipped with this highly secure operating system from Deutsche Telekom. The Federal Office for Information Security (BSI) has certified many TCOS-based applications in keeping with the internationally accepted "Common Criteria" scheme.

Consider TCOS-based passports, for example. Thanks to its certification, the TCOS smartcard operating system is one of the most secure systems available for international travel documents. The digital data stored on the passport's chip is protected by multiple security mechanisms. A special mechanism, the so-called PACE protocol, protects the data from unauthorized reading via contactless interfaces. The information stored on the passport chip includes the passport photo and the bearer's fingerprints. The operating system carries out the necessary encryption, signature calculation, authentication with respect to reading devices and secure readout of personal data for authorized persons – and protection of the data against unauthorized access.

TCOS is used in many other applications as well. For example, the TCOS Signature Card supports both advanced and qualified digital signatures pursuant to the German Digital Signature Act (Signaturgesetz). The security modules in the terminals of German public transportation systems use TCOS, as do tachograph cards in trucks; secure terrestrial trunked radio (TETRA) communications of government agencies and emergency services, etc.; and the new electronic health card now in service in Germany. Another major area of application consists of multifunctional company IDs that cover such functions as access, flexitime logging, cafeteria payments and control of multifunctional printers.

In principle, hardware-based security tokens with the TCOS operating system can be provided in many different physical designs and with many different form factors. The best-known form factor is probably the basic smartcard with TCOS chip. Depending on requirements, it can be designed for either contact-based or contactless addressing. In addition, tokens with the TCOS operating system are available as MicroSD smartcards – for example, for mobile devices; as keychains with Bluetooth functionality; as USB flash memories; or as embedded security modules that can be integrated within devices, machines and vehicles.

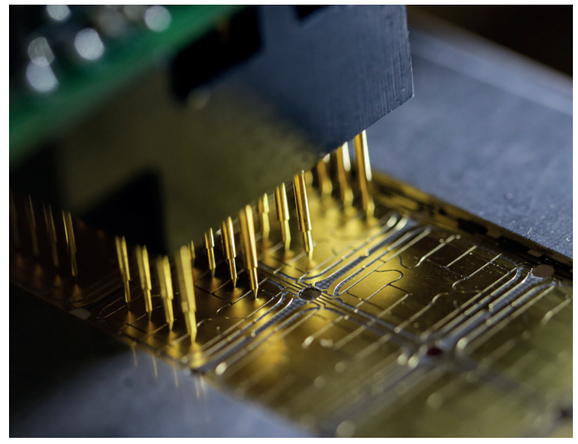


Fig. 7: Production of a security smartcard chip module with T-Systems' TCOS operating system

For years, T-Systems has collaborated with leading chip manufacturers on he production of secure electronic IDs. The TCOS/security chip combination has been designed to meet both German and international requirements for electronic identification documents. Working in cooperation with a number of chip manufacturers, T-Systems continually tests new smartcard technologies and new areas of application. Relevant new areas of application include mobile security, enhanced multifunctional ID cards in companies, digital driver's licenses (such as the European Driving License), data security in connection with "smart metering" (using "smart" electricity meters) and security solutions for the automotive, health-care and "Industry 4.0" sectors.

TCOS-IDKEY TOKENS – SECURE IDENTIFICATION MADE IN GERMANY

The TCOS-IDKey token has been developed especially for identification applications using ranges of different identifiers and for authentication using symmetric and asymmetric keys or one-time passwords.

It is available as a regular smartcard, MicroSD smartcard or embedded module, and it can be used via both contactless and contact-based addressing and via I2C.

The TCOS-IDKey is provided as a non-personalized cryptochip with T-Systems' TCOS 3.0 (TeleSec Chipcard Operating System) operating system. Its applications have been optimized for use in Windows environments.

During production, each token receives private keys from the Deutsche Telekom Trust Center – for support of secure-identity functionalities. Each key is produced by a highly secure key generator, and each is unique. Each is securely stored on its token, in a form unreadable for unauthorized parties, in keeping with the latest technical standards. The quality of the asymmetric keys is certified by the Trust Center's seal of quality.

The cryptographic keys, of which no copies exist, are unique, in conjunction with their pertinent physical-card numbers, and can be used as a basis for various types of digital identities.

The keys within the chip of a TCOS-IDKey token can be used only when they are "shown the valid password" – i.e. when a valid PIN is entered. The private keys, when used cryptographically in combination with the pertinent certificates – via the relevant public keys – make it possible to unambiguously correlate specific actions with a person or system.

As delivered, IDKey contains various asymmetric key pairs, along with pertinent certificates of origin in T-Systems' Trust Center production.

IDKey supports Windows Life Cycle Management (ILM) and, under Windows, can be used for the following areas of application:

- PC access authorizations
- authentication with respect to servers, networks and cloud-based services
- data integrity assurance
- secure e-mail communication (encryption, decryption and digital signature)
- encryption and decryption of any files

IDKey tokens also support additional applications, such as a special access application (TCOS myAccess), an OTP application and an application for implementation of flexitime accounts.

IDKey is supplied in the null-PIN status. The null PIN ensures the integrity of the product and eliminates the necessity of sending PIN letters. Before using IDKey, the user has to replace the null PIN with his own user-defined PIN. Cards are assigned to specific persons or systems (personalization) after they have been delivered; such assignment is carried out by the customer's own agencies.

TCOS MYACCESS+ – SECURE OVER-THE-AIR (OTA) IDENTITY PROVISIONING

TCOS MyAccess+ is an enhanced version of the MyAccess application on the IDKey token. Via a web application, TCOS myAccess+ can be provisioned to various JAVA-based tokens.

A range of options are available for setting up a MyAccess solution on a smartphone or another token.

To begin with, a user can order a MyAccess solution from a portal or online shop. To do this, he must provide a telephone number and his SIM-card ID or token ID. In another option, companies can place collective orders for groups of end users. The SIM-card IDs / token IDs are needed for the process of providing data individually for each token. This approach to data provision ensures that each token is unique, and it prevents cloning of data – and, thus, cloning of identities.

When an order is placed, the data it contains are checked for plausibility and proper format. In addition, T-Systems checks the legality of each order and of the requested access rights. If all data pass these checks, the Smartcard Service generates the relevant access data and obtains the required key material, via a secure pathway that is robustly protected against unauthorized access, from the Deutsche Telekom Trust Center. It then compiles the data records – each of which has been individually encrypted for a specific token or SIM card – needed for provisioning the MyAccess solution.

In cases involving SIM-card provisioning, the Service Provider Trusted Service Manager (SP-TSM) wirelessly transmits (in keeping with the "Over-the-Air" (OTA) standard) the complete data set, along with the latest valid pertinent applet, to the SIM card of the relevant Mobile Network Operator (MNO) i.e. its relevant end user. Such applets can be administrated via a smartphone's mobile wallet app. For transmission of the applet, IPSec tunnel mode and processes pursuant to the GlobalPlatform standard are used.

In cases involving provisioning to other tokens, a user can download the data – individually compiled for his token – via a web interface and add it to his token himself. Alternatively, a user can provide an IP address at which the relevant token can be reached.

Fig. 8: Devices with TCOS chips

CURRENT APPLICATIONS WITH TWO-FACTOR AUTHENTICATION

E-PASS

E-Pass, an electronic passport, is equipped with a radio-frequency (RF) chip. The RF chip is a certified security chip, with a cryptographic coprocessor, that can store both standard passport data and biometric data. Equipped with the TCOS operating system, the chip presents a major obstacle for would-be forgers. The biometric data stored on the chip can be machine-checked. This makes it possible to determine with certainty whether a passport and the person presenting it truly go together. Access-protection mechanisms block unauthorized reading of the data on the RF chip and eavesdropping of communications with the chip.

THE NEW ID CARD

Many persons now carry security tokens with them; more than 100 million passports (e-Pass), and a great many personal ID and company ID cards, with such tokens have been issued to date. The users of these documents entrust their personal data to the TCOS operating system which, according to the Federal Office for Information Security (BSI), is one of the most-secure operating systems available.

The new German ID card (Personalausweis) can also be used for two-factor authentication procedures. Providers can register with the Federal Office of Administration (Bundesverwaltungsamt) and, if approved, use the ID card as a "second factor." It can then be used as such in connection with a cardreader and suitable software.

E-TICKET/ASSOCIATION OF GERMAN TRANSPORT COMPANIES

One of the most important projects of the Association of German Transport Companies (VDV) involves the nationwide introduction of electronic tickets (eTickets) for public transport services. To this end, VDV eTicket Service GmbH & Co. KG (VDV eTS), in cooperation with industry partners, has developed a special "VDV core application" that supports convenient, cashless ticket purchases (by passengers) and reliable billing (by transport associations). The success of this system has depended centrally on the comprehensive security management provided by T-Systems. It includes issuing of certificates, for tickets, in the secure Trust Center, and development and delivery of TCOS-based security modules (Secure Application Modules (SAMs)) for the customer terminals T-Systems also provides. The terminals have been continually improved and upgraded since 2006.

The SAMs enable the VDV core application to run cryptographically secure, and to produce forgery-proof customer invoices. Use of certificates makes it possible to issue forgery-proof tickets and check them as necessary. Thanks to consistent interface specifications, all system components are interoperable. In sum, T-Systems has provided VDV eTS with a secure, high-performance security management system, consisting of a Public Key Infrastructure (PKI), a Key Management system (KM) and the Secure Application Modules (SAM).

DE-MAIL

In contrast to regular e-mail services, De-Mail allows to clearly verify the identities of communication partners, and to clearly confirm the sending and receipt of transmissions (De-Mails) at all times. The content of a De-Mail cannot be read or modified while the De-Mail moves through the Internet. The confidentiality of De-Mails is assured by secure registration procedures, secure connections to De-Mail providers and encrypted transmissions between De-Mail providers. De-Mail thus significantly enhances the security of electronic communications in comparison to conventional e-mail.

To be able to use De-Mail, a user requires a De-Mail account and a pertinent De-Mail address. A user obtains a De-Mail address by registering with a De-Mail provider. When a user registers, he verifies his identity by presenting an ID card or passport. De-Mail providers can also offer identity verification via the online-ID function (eID) in the new German national ID card.

To send a De-Mail, or to read a De-Mail he has received, a user logs onto his De-Mail account. If he wishes to have a "high" level of security (i.e. especially high), he uses a token. Different providers handle such two-factor authentication in different ways:

- smartcard with eID function, such as the new German ID card or a signature card
- USB flash-memory device that provides a PIN-protected or password-protected authentication function
- one-time-password (OTP) generator with which a user requests a password that is valid solely for a single session

Deutsche Telekom is the provider for De-Mail. In cooperation with T-Systems, it has designed and established security management systems for various De-Mail providers.

DEUTSCHE TELEKOM: MYCARD

Deutsche Telekom uses TCOS tokens as digital identities for all of its employees. Deutsche Telekom employees use MyCard to log onto systems at their work site, to sign and encrypt e-mails and files, to print at multifunction printers, to make cashless payments – for example, in company cafeterias – and to enter facilities. MyCard is provided in a range of forms – as a regular smartcard with contact-based and contactless functionality, as a MicroSD smartcard and as a keychain with Bluetooth functionality.

LIST OF FIGURES

CONTACT

Marketing
T-Systems International GmbH
Uli Kunesch
Market Intelligence
Fasanenweg 5
70771 Leinfelden-Echterdingen
Germany
Uli.Kunesch@t-systems.com

UNIT CONCERNED
T-Systems International GmbH
Dr. Friedrich Tönsing
Security Engineering & Solutions
Deutsche-Telekom-Allee 7
64295 Darmstadt
Germany
Friedrich.Toensing@t-systems.com

PUBLISHER

T-Systems International GmbH
Hahnstraße 43d
60528 Frankfurt am Main
Germany

http://www.t-systems.com

Last updated: February 2015

T · · Systems ·