



Smartcards and thin clients:

Secure environment to work comfortably.



While just a few years ago, corporate discussions and presentations revolved around the performance specifications of the hardware of information and communication systems, security is equally important and a top priority today. As businesses increasingly depend on IT systems, data security, both internally and externally, has become a question of survival, not only for corporations, but for any kind of organization.

Viruses, Trojans, worms, phishing, adware, hacker attacks – anybody who works with computers has long been aware of the dangers lurking on the outside. Data theft, even inside an organization, is a recognized problem which is taken into consideration in the development of security strategies. A host of protective measures and security products are available to protect data and keep unauthorized users out of modern networks.

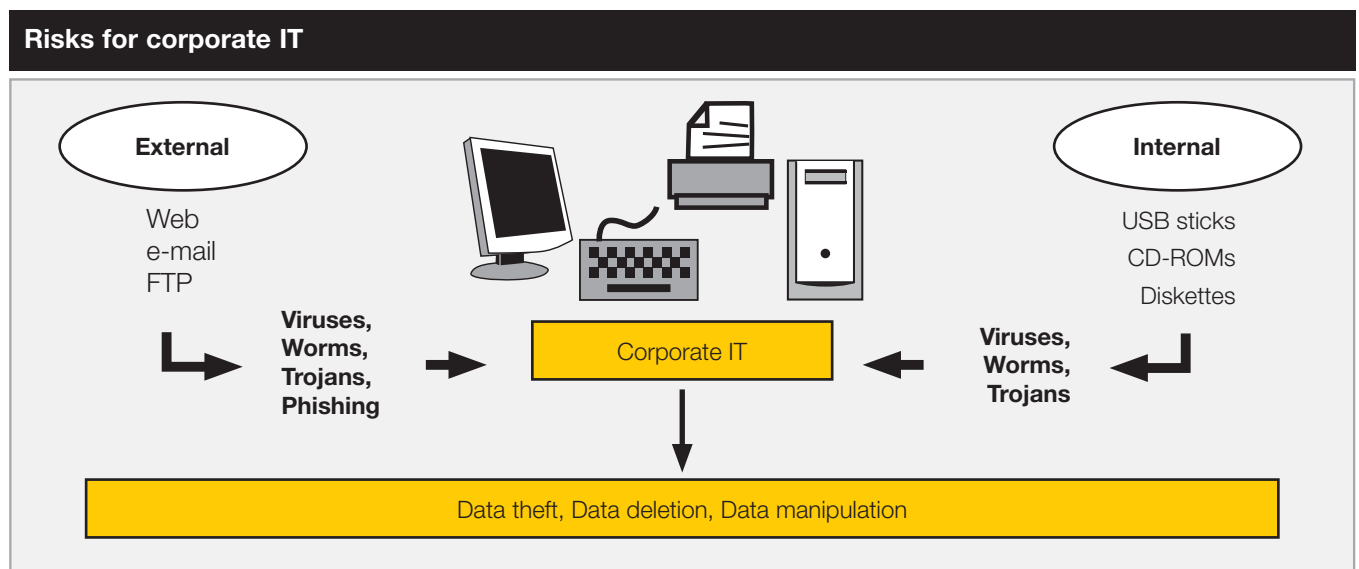
The methods of accessing internal network infrastructures have radically changed over time. While initially a user name was simply assigned to each user to log on to the network, both the higher risk potential and the infinitely higher complexity associated with utilizing IT networks resulted in ever more complicated identification procedures. The introduction of strict password guidelines was a signal to every last employee that computer systems are targets for both internal and external “enemies”.

Password chaos

Soon it was found, however, that a single password was not enough. Mobile work calls for identification and authentication to allow remote access to an internal network. In addition, more and more applications require unique access authorization: e-mail, databases, business applications, such as SAP or CRM, secure “virtual rooms” for project teams, Intranet, etc. Today, it is not unusual for an employee to access ten or more different secured areas on any given workday, where access control requires identification. This leads to a confusing array of passwords, PIN numbers, access IDs, in addition to physical objects, such as conventional keys and chip cards. The variety in itself poses a potential risk: Unable to remember all the passwords, we write them down on a piece of paper where someone might find them.

Many industries are affected

Particularly burdened by this situation are industries and business segments involved in sensitive, critical company or personal data. Therefore, they have a keen interest in effectively protecting such information against internal as well as external spies and thieves. Examples include controlling, accounting, research and development, and human resources in companies and other organizations, and even entire industries, such as banking, insurance, health insurance funds, accounting service providers, and last but not least, medical institutions of any kind with their enormous pool of patient information.



The IGEL solution: Smartcards

Today, the most widely used technical solution to these security problems are the so-called 'Smartcards'. The term refers to a type of plastic card the size of a credit card, which generally contains a chip with hardware logic, a memory or a microprocessor and whose capabilities exceed the application spectrum of magnetic cards by far. A Smartcard could in fact be viewed as a kind of minicomputer sealed into a plastic cover with limited computing and memory capacities.

Here is how it works

A Smartcard is inserted into the so-called 'Smartcard reader' which is also responsible for power supply. Data communications between the card and the applications of a computer are handled through a serial interface which is controlled through the reader and pertaining drivers. The lifetime of Smartcards is several times longer than that of magnetic cards: They can be used up to 100,000 times, plus, they offer the advantage of being immune to magnetic fields and include integrated protection against high-voltage discharge.

Intelligent and programmable

However, the most important feature of the Smartcard is its intelligence, which ultimately means its programming capacity. For example, a processor card may contain codes, which cannot be read-out, but which can be utilized for programs running on the card. Modern authentication processes apply the so-called 'challenge-response' mechanism where each new question has to be followed by the proper response. The response can be generated only by means of the correct code, which in this case, is computed by a program on the Smartcard.

Memory Cards

Smartcards basically have sufficient intelligence and memory to control even complex security processes, such as identification and authentication procedures, up to the latest encryption technologies. Depending on the requirements, however, cards of varying capabilities are used. The 'basic Smartcard' is a so-called 'memory card' or 'synchronous chip card', which substantially consists of an intelligent storage medium, which means, it is rewritable multiple times. Individual memory cells can be accessed sequentially via a respective interface. Memory cards are used when data storage is the only priority, while protection against reading-out or unauthorized manipulation is not at issue.

Processor chip cards

The most intelligent version of Smartcards are the so-called 'processor chip cards' or 'asynchronous chip cards', which are equipped with a microprocessor to permit access to the stored data. The data stored on the card can be protected against unauthorized access through cryptographic processes in the processor. Examples of such Smartcards are money cards, for example, which are money purses in chip form or cards containing personal information, such as the health card which will be introduced in the future, all kinds of identification, or decoder cards, for example for pay-for-view TV, where the card is equipped with certificates to decode the TV signal.

There is an entire spectrum of other versions of intelligent cards between memory cards and processor chip cards covering the most diverse needs. The appropriate version depends on the task for which it is intended.

Table Application Examples:

Application	Processor Card	Memory Card
1. —	—	Smartcard
2. Banks	Money card	—
3. Health insurance company	Health card	health insurance card
4. Public authorities	IDs	—
5. Pay-TV	Decoder card	—

Ingenious plus smart

As demonstrated by the variety of cards described above, there is an adequate Smartcard version for any requirement. Memory cards are more than sufficient to satisfy a broad range of applications. Especially in cases where different people need to access data in the network quickly, securely and easily, they are the ideal medium. Potential scenarios are hospitals, for example, where physicians or nurses can use local workstations in different places or wards to access patient information, inventory databases, etc. The memory card ensures that each user is able to retrieve the data he/she is authorized to access through user and session data stored on the card without requiring complex authentication procedures.

This applies similarly to libraries where visitors, through generally available terminals, are able to access various research resources that are not equally open to all users, such as fee-based databases.

Especially in the areas of application mentioned above thin clients provide an ideal solution. Therefore, most thin client manufacturers integrate Smartcard readers into their clients. IGEL Technology, for example, offers most thin client product lines (such as the Compact, Elegance and Premium series) complete with Smartcard readers which are suitable for all types of Smartcards. IGEL Smartcards are 'synchronous' or memory cards and contain a variety of information, such as user authentication data. Before the card is delivered, the network administrator sets the card up specifically for each user through appropriate menus to allow multiple application-specific sessions, for example, without the need to reenter a password. As a result, a number of important and comfortable solutions can be developed for many frequently occurring user scenarios. For example, with the memory card it is possible to 'lock' the terminal, in this case the thin client, before leaving for a meeting to make it inaccessible to others, while it is not necessary to terminate a session started earlier.

Even more important is another common scenario:

Similar to the example of physicians in a hospital or visitors to a library, it is often desirable to interrupt a session and continue at another terminal (in-office mobility based on Citrix smooth roaming). Thin clients with server-based computing architecture are perfectly suited for this, because all processes run on the server, the clients do not require much space and therefore, they can be installed in many convenient, even tight places in clinics or libraries, whereas a PC workstation would be too bulky. At such terminals, authorized users can then access the information they need. Without Smartcards, on the other hand, each user would have to log on again separately to each client and would then be forced to call up the previously closed applications and data again.

Mobile work sessions made possible by the Smartcard

By using a Smartcard, however, you can literally 'carry' the started session to another location and simply continue at any other available client. Unlike PC architectures, under the thin client concept of server-based computing all applications run on the central server, and therefore, the session is not tied to the location of the client. Only server-based thin client technology makes such 'mobile work sessions' possible, and the Smartcard provides the necessary user comfort.

Numerous advantages

The advantages of this method quickly become obvious: A user logs on to any thin client at the beginning of a session with the Smartcard and starts the session. If he wants to leave the terminal, for example at a production line or in a lab and interrupt, but not terminate the session, he simply removes the Smartcard from the reader. He is now automatically logged off, while the work session remains open on the central server and can be continued any time and any place, such as another lab, by plugging the Smartcard into the reader. (Administrators can define a timeframe after which the applications close automatically so that the user does not necessarily have to return to terminate the session.) Meanwhile, the originally used client is available to any other user to start his own mobile session.

When optimal security has to be guaranteed through state-of-the-art authentication systems, more powerful Smartcards have to be used. In such cases, thin clients use standardized Smartcard readers supporting the Personal Computer/Smartcard Standard (PC/SC), which means they have a PC/SC interface. The standard ensures that the functions stored on the Smartcards are able to run independent of platform, manufacturer and application so that these smart cards can be used in most every IT infrastructure.

In service at Humboldt University Berlin

An example for using these advanced Smartcard solutions is the Department of Natural Sciences at Humboldt University in Berlin, which converted to thin clients in the process of combining the computer center and the complete IT system of the university library. A comprehensive authentication system was introduced for the clients in the secured areas on the basis of PC/SC Smartcard readers and certificates. The various user groups of the new central server-based IT architecture (i.e. students, visitors from outside the University, scientists, etc.) were assigned different user environments, which include authorization for using the Intranet, different databases, or a range of applications, such as the programs of the Star Office family, Acrobat Reader or various print functions. With a student account, for example, all Microsoft Windows 2000 functions can be used with separate memory space for personal files, the entire scope of Microsoft Office programs as well as Intranet and Internet. Each terminal user group is authenticated via Smartcards, and the pertaining Smartcard readers are integrated in the keyboard.

Public key encoding and digital signature

Modern Smartcard technology also allows secure authentication through PKI (Public Key Infrastructure). Unlike conventional encoding, where both partners of the authorization process require the same key, the public key method uses different keys for coding and decoding. A decoding process requires a private key and a public key. Since the public key is available to anybody, encoded information can be sent to anyone who then decodes the message with the private key.

This method supports the development of digital signatures to create tamperproof 'signatures' which guarantee document authenticity, authenticate users and include the so-called 'Single Sign On' process allowing users to access applications and resources for which they are authorized with a single proof of identity. It is understood that the private key has to be kept strictly confidential. Instead of securing the key via password, it is considerably safer to store it on a Smartcard.

Smartcards – simple, yet effective

Naturally, even Smartcards are unable to provide 100 percent security. For example, memory cards can be copied, and quite generally, Smartcards can be made available to others. However, the intelligent cards are a vital factor of IT security. Smartcards are a simple, yet highly effective method of securing data and information and represent a key element of state-of-the-art authentication processes.

Germany (HQ)

IGEL Technology GmbH
Schlachte 39/40
28195 Bremen
Germany
Tel +49 (0) 421 1769 240
Fax +49 (0) 421 1769 302

United Kingdom

IGEL Technology Ltd
1210 Parkview
Arlington Business Park
Theale · Reading · Berkshire
RG7 4TY · UK
Tel +44 (0) 870 351 4522
Fax +44 (0) 870 351 4523

United States

IGEL Technology Inc.
5353 NW 35th Avenue
Fort Lauderdale
FL 33309 · USA
Tel +1 954 739 9990
Fax +1 954 739 9991
Toll Free (US only): +1 877 GET
IGEL

Singapore

IGEL Technology
Care of: C. Melchers GmbH & Co.
Singapore Branch
101 · Thomson Road
24-01/05 United Square
Singapore 307591
Tel (65) 6259 9288
Fax (65) 6259 9111

Hong Kong

IGEL Technology
Care of: Melchers (H.K.) Ltd.
1210 Shun Tak Centre
West Tower
168-200 Connaught Road C.
Hong Kong
Tel +852 25469069
Fax +852 25596552

