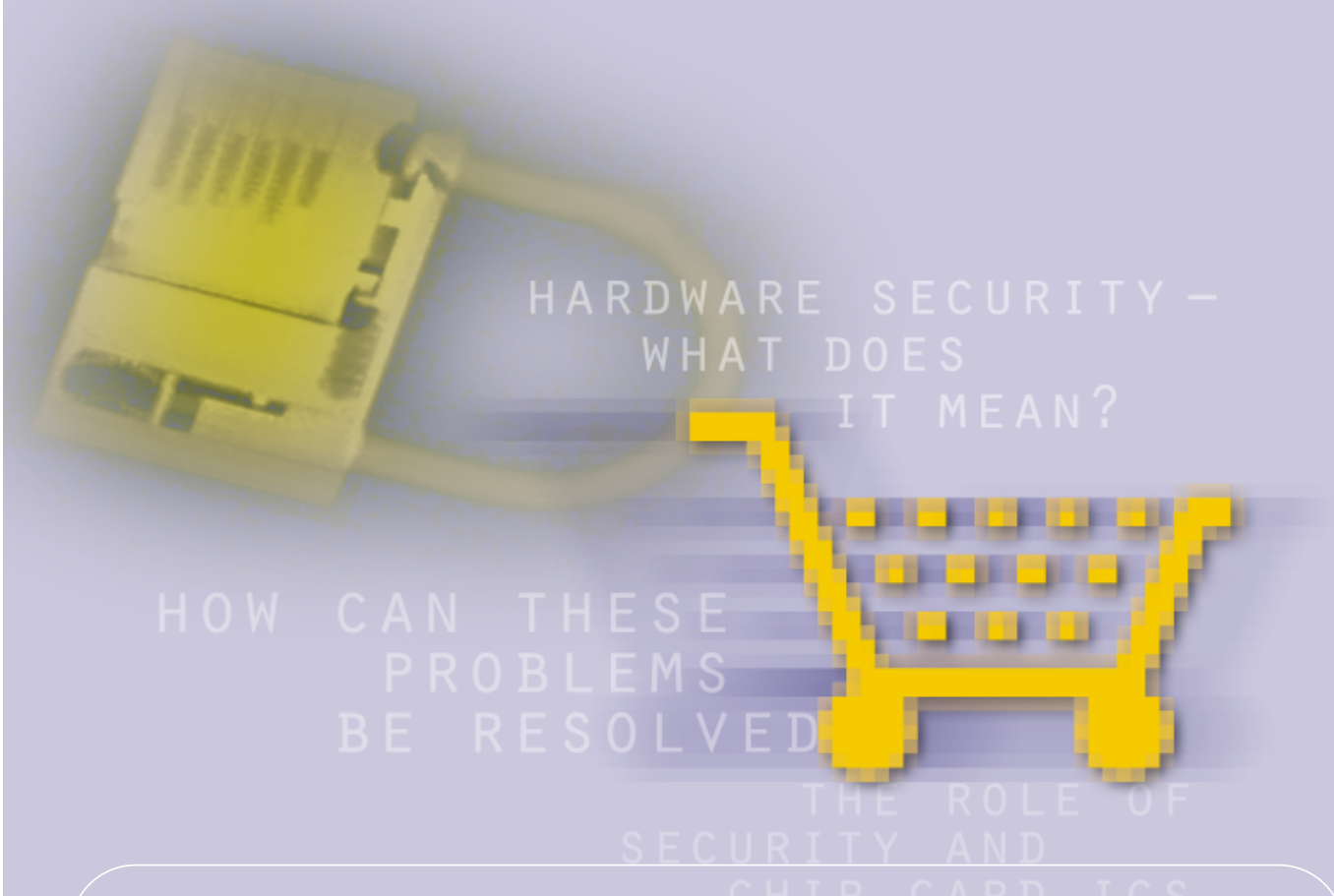
In recent years the term e-commerce has become the accepted buzzword, with huge markets predicted for this particular segment and the added bonus of large opportunities for a lot of companies. This growth ensures a successful future, as well as new, comfortable ways, of exchanging information and doing business over the net for private customers and organizations alike. However, e-business has changed. It is no longer the old view of e-commerce: "doing transactions on a PC". E-business is a way to conduct, manage and execute business transactions via an electronic network. The customer will use devices that they find more convenient. And while the convenience for the user grows, devices will get smaller and their functionalities will expand. At the same time network access becomes cheaper, and online attractions will also grow.



Hardware Security for e-business

By Monica Bremer
Infineon Technologies AG

The first period of Internet business focused on earning revenue through advertising (web banners) and numbers of users for network access. Customers today are used to getting online content and services for free - this will change in the future. The new business models and trends will concentrate on online education, high value content and personal services with the benefit of added value that the customer is willing to pay for.
But up to now, these trends have not yet been realized. Everyone is prepared, a powerful infrastructure exists, but the mass consumers are not moving down the road of e-business.
The missing element is trust. Trust has always been the basis for conducting every type of business. Powerful guidelines for the electronic market place have to be established in order to give all involved parties a trusted key for doing e-commerce. Asymmetric cryptography, like public key cryptography, together with tamperproof devices for storing private keys, are the two basic components that will help to justify the hype of e-commerce.

Dangers and Risks

Making use of the Internet for e-business has the advantage of utilizing a widespread infrastructure as a physical basis for the electronic market place, at no cost. On the other hand, users have to struggle with security issues, as the Internet wasn't designed for commercial usage. From its origin there was no need for a security infrastructure, which means that people using the Internet for e-business have to face several risks. The first risk is one of confidentiality. By default, information traveling through the web is in plain text - an open book to nearly everybody. The idea that company confidential data involved in business transactions can be read by anyone, is a limiting factor for the use of the Internet. The second risk is that data integrity has to be assured. In the same way everybody can read transmitted information, it is also possible to change it. Imagine your salary is re-directed to Mr. X, just because he changed the number of your bank account to his. From this example it is clear that the question of authenticity is a crucial one. How can a person be sure that the web-page they're looking at, is from the organization that it is claiming to be? Last, but not least, the risk of 'denial of service' attacks could close down the doors of a cyber-shop and drastically limit its business.

How can these problems be resolved?

One of the main questions is "who is liable for ensuring that the e-business process is secure for the end customer"?
E-business applications using the Internet as a platform, have to solve the requirements for confidentiality, integrity, authentication and the question of non-repudiation. Since the Internet itself does not cover these problems, protocols and applications of the upper layers have to be designed in order to realize secure solutions. What does a secure solution really mean? The user needs to have the means for hiding the content of their transactions from the eyes of a third party. They need to have the possibility to check whether their partner is the one they claim to be (and by the way, the reverse also holds true). Both need the legally binding commitment to a deal, including a legally accepted signature and a certification of time stamp.

Since these are crucial requirements, legislation all over the world has dealt with this topic in the last few years, to offer a framework for common accepted solutions.

In the USA, Utah came up with a law for digital signatures back in 1996. California followed last year and several other federal states are preparing comparable laws. In Europe, Germany stated its digital signature law (SigG) in 1997. This was later specified more clearly by "Signaturverordnung" and "Maßnahmenkatalog" of BSI (Bundesamt für Sicherheit in der Informationstechnik). Its goal was to establish a framework, which allows the qualification of electronically signed documents to have the same legal authority as manually signed paper documents.

The technology basis for signatures should be the use of asymmetric key pairs for public key methods. The certification authority has the task to ensure that the digital ID, together with the private key, is securely stored in a security token. This practically implies the use of crypto Smart Cards. Other countries have followed with laws concerning digital signatory, such as Italy, Austria and Finland (who have started to issue personal ID cards with a digital identity). Work has already started on a European level in order to achieve a common approach to these issues.

Hardware Security – What does it mean?

Up to now there are some very specific basic requirements that have to be fulfilled in order to provide a strong basis for secure business over the Internet. Generally speaking, a chain of trust has to be built up between both customers and dealers. Modern cryptography, based on the public key infrastructure, together with a secure device to execute cryptographic functions and to store private keys, are the solution to these requirements. On an application level both the ease of use and the high level of security are crucial for the success of these solutions.

From the software point of view, a lot of improvements have been achieved in recent years. In the end, Internet applications became additional features, providing basic security mechanisms. IPsec (Internet Protocol Security) for network layer, SSL (Secure Socket Layer) or TLS (Transport Layer Security) for transport layer and SHTTP (Secure Hypertext Transfer ProtocolHyp) for the applications layer, are all techniques that deal with the different topics of confidentiality, integrity and authentication. These techniques are powerful tools to upgrade the functionality and level of security of the communication path from the home PC, over the Internet and into the server of the service provider. But in this process, both the transmitter of information and the receiver of the information, and their clear identification, play an important role. To build up the trust relationship, the combination of the personal identity and the digital one has to be guaranteed. In order to prevent misuse of digital identities, a security device is needed that operates separately from untrustworthy platforms (like a PC) and have the capability of storing keys in a tamperproof way, as well as performing cryptographic functions. Using such a security hardware token, the private key never leaves this sealed environment. Crypto controllers known from such products as Smart Cards, are ideal candidates to fulfill these tasks. In the non-volatile memory, private data and keys can be stored securely. The powerful crypto part of the controller can perform signature of hash values. The internal logic of the device allows access only by receiving the right PIN (personal identification number) from its user. With these two powerful capabilities, crypto controller based security tokens will be the first important part in the chain of trust from customer to dealer, and therefore one big enabler for e-commerce applications. Above all else, the user doesn't have to bother about all the internal details, because the Smart Card manages all this work for the user. Thus the Smart Card is really a personal computer that is as simple as possible to operate.

The Role of Security and Chip Card ICs

As you have seen, the use of hardware security tokens follows the demand for a trusted end-to-end security process, by both the customer and dealer and by many upcoming laws for digital signature. The requirements for secure storage of keys and the performing of crypto functions like signature of hash values, are fulfilled by Smart Cards today. But it is the crypto controller that is the really important part in this process and there is no need for this to be embedded in a plastic card form factor defined by the ISO7816 norm.

Since the PC is the most important platform for e-commerce today and nearly every PC is equipped with a universal serial bus (USB), new so-called USB-tokens have arisen. They can achieve the highest level of security if they are supplied with a crypto controller. One further advantage of this solution, is that there is no need for an additional reader like a Smart Card reader. This would significantly save costs for implementation of solutions based on a USB crypto token.

In the future, the dominant platform for Internet access will be mobile devices like PDAs or smart phones. As in the PC world, it would be best for a supplier to provide his customers with a personal hardware security device. As the mobile phones are developing very rapidly, there will soon be different possibilities to plug in such security tokens. But there are other solutions almost upon us. Within the year, we will have mobile phones from major players equipped with a MultiMediaCard™ slot. Whereas its original use is for functions like MP3 music players within the phone, secure download and so on, this is in fact a possible slot for a secure hardware token. Again, it is possible to integrate the technique of crypto controllers in the form factor of a MultiMediaCard™.