Market Trends and Hardware security for banking and brokerage applications

By Monika Bremer, Infineon Technologies AG

After the unprecedented hype for e-business transactions, the online world is changing once again. The first online business models focussed on the winning of online users. Access fees for online providing services and secondly web advertising with a correspondent click rate promised financial success. But the use of these business models meant that only in very few cases was money actually made. Fees for the online access decreased drastically while web banners have not lived up to their promise of a high yield (click rate) and the numbers of web sites in the last years grew faster in proportion to corresponding budgets for online advertising.

New solutions for successful online business models have to be created. The future will be dependant upon high valued content that the user is willing to pay for, e.g. personalised services, from which the user gains individual added value or e-learning and e-support. Only those businesses who possess, or who produce, high value content themselves, in combination with value added services, convenience for the user and personalized services, will be successful in the future.

But what does the future of the banks and online business look like? The online world for banking started with home banking and online standard transactions. The banks, in particular the direct banks, are moving away from the mere online trader offerings towards more of a global online investment house. The future of the banks lays in the extension of their offered products - online, and in the personalization of their banking services.

In the past, the online offering of banks and brokers was based on transactions in the financial and stock business: cash transactions, standing orders, buying and selling of securities. Their next advance was to extend the offering of their core business. Nowadays, everything considered a payment transaction is counted among the online banking business. Transferals and standing orders are commonplace, account statements and account abstracts, transacting saving agreements online, e-mail support, credit card applications, credit calculations and news complete their online service offering. Due to the complexity of the security business in comparison to payment transactions, the brokerage business presents a much larger field. The buying and selling of stocks, fixed interest bearing shares (stocks, securities) and standard warrants are self-evident. These services are value added due to real time trading, where the broker sets binding prices online for a certain amount of time (e.g. 10 sec) and it is up to the customer to decide whether they agree to the price offered or not.

Today stock exchange information systems deliver real time prices, without time delay, directly from the trading floor. The bank itself often incurs these additional costs. With so-called watch lists customers are able to deposit the securities that they don't have obligations to in their depots but still watch the price quotations. Alert functions make it possible to inform the customer if a stock has reached a specific price, e.g. via SMS (Short Message Service). Further stock information e.g. of the company itself or news about the stock market and the economy, are taken for granted today. The customer registers online either an individual profile or selects directly from the services offered to get all relevant information with only one click. The ongoing trend is to represent all their products and services online and the winning of customer's loyalty with stock close services or the merchandising of products and services, which support online trading. Not only are customer bulletins counted among these services, but also subsidised offers of books, magazines and PC's with already installed online access related to the subject, are provided to motivate the customer to change from the customary distribution channel such as letter, fax or call center to the possibility of online trading.

But what is the motivation of the banks and direct brokers, to transact as much as possible online? The decisive factor is the idea of **"straight through processing".**

Whereas the distribution channel of the branch, the call center, letter or fax communication still has a manual interface, today, at least, the processing of stock transactions without any manual interfaces is possible. From the input of the transaction data, through the execution at the stock market up to the accounting of the order, everything happens automatically. Until a certain capacity of the engaged systems is reached, the more transactions the better; for the costs of processing per transaction does not increase in proportion with the transaction revenues, which the customer pays through transaction fees.

But still, not all customers are convinced of the advantages of online business. A lot of them don't want to abandon the personal contact they have to the banks' employees. That is usually because

they feel unfamiliar with the new technology and systems they are confronted with. And in particular, for financial issues this can be a big element in not using the new online services.

Security aspects

The online banking and brokerage businesses started connecting customers to the Internet with PC and corresponding special banking software from the likes of BTX (Bildschirmtext) and AOL (American Online). Internet trading followed shortly after. WAP-banking (Wireless Application Protocol) is now also possible and in Germany a broker has just released a PALM-trading application for those customers who use PDA's. Eventually, in a few years, the use of the Internet with the correlating applications will be part of daily life worldwide and its usage will be as self-evident as the telephone is today.

Security and trust will be key factors to make online applications successful.

Asking the banks about security issues, one answer dominates: with our cryptographic software our banking is secure enough. This is correct, in that the banking software presently in use enables a secure transfer of transaction data from A to B. But software alone is not able to protect users, devices and the storage of data.

User authentication in the banking sector presently takes place with a PIN (Personal Identification Number), a TAN (Transaction Number) or sometimes with an Identifier (an added password using password-software). This software administrates the data in general using a database. Successful attacks on PIN and TAN data show that the data protection by software alone is not sufficient.

Two components have to be taken into account when speaking about user authentication. On one side the bank wants to know if the legitimated account holder or a legitimately authorized person is really doing the transaction. The banks and brokers rely on the customer's self-responsibility to safe keep their confidential access data. On the other side, the customer should be sure about the identity of the bank's online web site that they use for trades and services. The customer wants to know that the site they are using is not a manipulated one.

First solutions in the market have already been established. Through the use of PKI (Private Key Infrastructure) banks and brokers can now exchange encrypted data. This can be transaction data as well as customer related data or information. The encryption takes place by using a public key, provided by the bank. This data is only legible, if the recipients using their own private key to decrypt it.

Certificates, as a secondary existing market solution, can also be issued by trusted third parties (Trust centers or neutral third organizations like TÜV). The organization proofs and verifies the legitimacy of the customer and assigns an electrical certificate as legitimacy confirmation. This can be used as a digital signature in the e-business environment.

Biometrical identification aims to identify users by their fingerprint, which is recognized by a FingerTip sensor. This sensor, which receives the picture of the fingerprint, can be implemented either in a terminal or in a card. Thus, biometrics replaces PIN and TAN functions or may even be combined with them.

The fundamental, unsecured set up of PC's and mobile devices makes them very attractive for attackers, since the CPU (Central Processing Unit) does not distinguish between "good and evil"- meaning between user software and attacking programs.
Meanwhile thousands of viruses, Trojan horse viruses and spy programs like "Key Loggern", (which records the keyboard entries of the user), are known about and in use. An initiative consisting of leading manufacturers has been founded to check the security status of a PC by the user and as well by the Internet trader/bank before a transaction may be done. The goal of the "TCPA" (Trusted Computer Platform Alliance) is to implement a security module named TPM (Trusted Platform Module) on the motherboard of the PC. The TPM is, among other things, able to spot changes of the operating system or single program parts (e.g. home banking programs) and is able to alert the owner of the PC before the PC is damaged or altered. The secure execution of the booting can also be controlled by TPM.

Mobile Banking

The requirements for mobile banking and brokerage security concepts are of a similar nature: the customer, the bank or broker and the terminal to be used have to be authenticated securely and a secure data transfer has to be guaranteed. At the same time the platform and the mobile device have to be protected against software attacks.

Today every GSM (Global System for Mobile Communication)-mobile phone

possesses a SIM (Subscriber Identity Module)-card, whose microcontroller is used for authentication, serves for the login of the subscriber into the mobile network and furthermore generates an individual key for voice encryption for every conversation, which it then passes to the mobile phone.

For applications in the m-commerce arena, the SIM as a security microcontroller can take over further jobs such as authentication and data encryption; but as the SIM-card is handed out by the network operator, it cannot always be assumed that all wished-for banking applications will be integrated into the card. Interesting alternatives to the single multi-functional SIM-card are mobile phones that have added slots for further cards: known as Dual-slot-mobiles. They may have a dual SIM-slot for a dual SIM-solution or, as in the case of the Siemens mobile phone SL-45, a dual card slot, where a MultiMediaCard™ can be inserted. These solutions all require a security microcontroller, which can be protected against attacks and manipulations.

Due to more complex cryptographic solutions e.g. PKI, future security microcontrollers cannot abandon specific cryptographic hardware. The Infineon security microcontroller is tuned specifically to the needs of modern PKI-requirements, e.g. 1.024 bit RSA, 32 EEPROM. This coprocessor has been optimized for fast arithmetic operations with extreme high numerical value and is implemented into an integral security concept of the whole controller.

Form Factor

The Infineon controllers can be implemented into many different form factors. Due to the specific feature of the form factor, it is normally only suited for a particular use. To enable an optimal use of the aforementioned services, it is advantageous that the form factor for mobile banking and brokerage is both removable and has memory storage capabilities.

Basically, the hardware security has to be distinguished into the removable and the non-removable elements. The aforementioned TPM is implemented as a fixed feature on the terminal's motherboard and so is named as a non-removable element.

The following removable elements have to be distinguished:

- The SIM-cards are the main product of network operators. As owner of these cards they also define their functions and applications as it is in their own business interest.
- The Smart Card in EC-card-format according to ISO-norm 7816 is the current form factor in the market nowadays. Up to now the magnetic stripe dominated as form factor for data protection, but in the future it will be replaced by a chip due to new regulations for data security. The banks are still the owner of the EC-Cards when handing them out and so they define the functions, the running time and the recipient of the card. It would be preferable if these advantages could also be guaranteed for mobile solutions for banks and brokers.
- The Small Card as a form factor, for example, the Ingentix Secure MultiMediaCard™, fulfils the requirements for mobile banking and brokerage. Today's dual slot solution – the Secure MultiMediaCard - with its size of 32mm x 24mm x 1.4mm - is ideal for mobile device slots. It can be inserted completely into a mobile phone as well as into a PDA such as a PALM pilot. Since it is a removable element, it can also be replaced and recorded over, either on a PDA or on a laptop or a PC with a corresponding adapter.

  In short, the Secure MultiMediaCard may be an alternative implementation of the WAP WIM.

  The similarities to a Smart Card implementation are not by chance, since it is based on Smart Card technology.

Function and application of the Secure MultiMediaCard for mobile banking and brokerage

Ingentix, a joint venture between Infineon Technologies AG and Saifun Semiconductor Ltd., is a semiconductor company that produces flash memory-based mass-storage products, which are based on Saifuns's NROM™ technology. The initial products include high-density standalone flash chips, MultiMediaCards and Secure MultiMediaCards. Mass storage based on solid-state NVM (Non-Volatile Memory) is much more reliable than mechanical storage elements - such as hard disks - and is key for all portable applications.

The MultiMediaCard is not only the smallest storage card world wide, but also extremely robust and light-weight, low-current, fast, well-priced and because of its standardized interface, a easy storage media to implement. It is particularly suited for the insertion into mobile devices like telephones, PDA's and e-books.

The MultiMediaCard, a mass storage product, is being developed with the functions of the Infineon security controller incorporated onboard, resulting in a leap from a simple storage card towards a multifunctional smart storage card. Furthermore the implementation of the controller SLE66CX322P on the MultiMediaCard, creates a Secure MultiMediaCard, meaning that the Secure MultiMediaCard with the controller functions will be adequate for today's PKI and digital signature requirements. Consequently, a whole range of possibilities are open for new services in the mobile banking and brokerage market.

PKI encrypted transaction data supports and accelerates today's software security. It is also possible for the acknowledgement of transaction data transfer, for example as a message, when the recipient has performed the decryption of the transaction data. All transaction data, the transaction (order, order time, order reference number

etc.) itself, as well as the execution report, can be securely stored on the card and, for example, be compared with the bank's online order book. In this way, the bank or broker raises the trust it has with its customers. The customer then is able to compare his activities with those of the bank in a direct and prompt way.

All data, which the bank provides for the customer in the future, can be offered as a download and so be read by the customer offline. It is even possible to change the terminal. If for example, the download at home takes place over fast ISDN/DSL-internet access, it can be stored on the Secure MultiMediaCard and then read offline on such devices as the PALM pilot. The offering can range from stock exchange news to personalized services (Market information, watch-lists, portfolio-analysis, reporting tools, etc.).

Marketing Opportunities for Banking

A large storage capacity in a small media in combination with security functions can bring about many opportunities. For example, it is possible to furnish the MultiMediaCard with a label and to define the date the card expires. In this way the bank or broker can issue the Secure MultiMediaCard, yet still remain the owner of the card and therefore in a position of defining the card's applications. The bank also has the possibility to install its own software as well as both on and offline updates on the card. In this case, the customer is, with this banking software, also mobile in terms of key applications for trading, stock exchange information systems, news and services that require application-specific software.

If the bank or broker offers its own services for download, for which the customer might have to pay a fee, then a copy protection of the data is in the bank's interest as digital rights management for all data stored on the Secure MultiMediaCard is evident.

Conclusion

The changes of the online business models require new security solutions. The protection of high value content is getting more and more important, since the banks and brokers offer their services online and transactions are done via a mobile device – and so are interesting targets for attackers. Different form factors, into which the Infineon microcontroller can be implemented, are possible solutions for the increasing demand for security of data, user and device.

Due to its special features and characteristics, the Secure MultiMediaCard is able to protect not only the data and the device in use, but also guarantees the identification of the user/trader himself. Due to these capacities, one could say that the Secure MultiMediaCard is a real security solution, that fulfils not only all requirements of the mobile banking and brokerage business, but also facilitate value added services, both now and in the future.