> The year of e-commerce
Interview with Dr. Hansjörg Leichsenring
on trends in mobile payments

> The Swiss knife of the future

> Scaring away malware
The year of e-commerce

Technology and telecom companies, cellular phone operators, and credit card corporations are currently all participating in the race for the electronic consumer wallet. And what roles do financial institutions play in this scenario? Dr. Hansjörg Leichsenring, a respected expert and bank consultant within the German-speaking markets, takes a closer look at trends in mobile payments.

The Swiss knife of the future

The cell phone is the future Swiss knife. Mobile Internet is indispensable for many users, whether they only want to check the weather service and watch the stock market, or whether they are already using their cell phone for banking transactions. The trend is clear: Before too long, more people will be accessing the Internet via their mobile devices than at their stationary computer.

Doing money transactions with applications

The mobile phone is changing our lives, our economy, and our business models. The music and movie industries are already in the middle of this revolution. Newspaper publishers fear for their customer relations, because third-party companies like Google and Apple can control access to editorial articles via iPad and cell phone. Payment traffic is no exception: It’s also being affected by this trend.

A prepaid card for the Internet

Last November, the "Internet Cash" card was launched by Swiss Bankers Prepaid Services – in cooperation with MasterCard. The Swiss Bankers company was founded 36 years ago by the banks as the center for travelers’ checks, and today is a bank itself.

Online payments without credit card

Recently, a new, global, safe and secure method to make and receive payments on the Internet without the use of credit cards has become available. For the first time in payment traffic history, SuisseID, the secure electronic proof of identity, is being used by the SwiKey company.

Scaring away malware

In recent years attacks on Internet banking services have evolved from rather simple credential stealing attacks to advanced content-manipulation attacks by means of malicious software seeded on the client end-devices. A praxis implementation at UBS shows how to counter those risks with regard to convenience and mobility of the customers while maintaining the highest level of security.
Dear readers,

After considerable euphoria around the turn of the millennium, an abrupt implosion of high-flying plans and dreams, and a subsequent long-lasting dry spell, the e-business topic is rapidly increasing in significance again. In Switzerland, eight of ten people have their own Internet access, more than 95% of these have already purchased something online, there is a cell phone in more than 90% of all households and approximately 2.4 million people in Switzerland are registered on Facebook. It comes as no surprise that payments, too, are increasingly being “virtualized.”

This development is currently mostly driven by non-financial institutions, with PayPal acting as the trailblazer, having firmly established itself as an Internet payment option. But the telecommunications companies have proven successful as payments providers, offering banking services via mobile phones in third-world countries. There are other organizations currently developing virtual payment traffic solutions at full speed. Facebook, for instance, has launched a virtual online currency to pay for Internet services. And Google and Apple are expected to launch their own payment services for this market within the coming months. These two companies especially are believed to be capable of successfully developing and commercializing such a business solution.

And that could indeed prove to harbor a whole new set of challenges for the financial institutions. In a better scenario, they might potentially miss leading-edge developments which they’d have to catch up to with tremendous investments and efforts; in a worse case, the new providers completely block access or participation in their (closed) payment systems. This would hurt the financial institutions in a direct ratio to the success rate with which such a payment option would establish itself. And the worst case would be if third-party providers were to succeed in advancing into other banking business areas via payment options, such as account transactions or microfinance.

This issue of CLEARIT demonstrates that the Swiss financial center is actively watching these developments and taking them seriously. It covers in detail the virtualization of payment transactions and, among other topics, reports about newly developed applications for mobile phones, new payment cards, developments in the security area or about a payment application based on SuisseID – a new, standardized electronic identity for electronic business transactions. Over the past years, the Swiss financial center has shown that, when it comes to customer- and future-oriented solutions in payments, it remains cutting edge. And it will have to continue to do so in the future. <

Marcel Schuler
Chairman of the Board, SIX Interbank Clearing Ltd
Head of Client Support Center, Credit Suisse Group Ltd
The year of e-commerce

Technology and telecom companies, cellular phone operators, and credit card corporations are currently all participating in the race for the electronic consumer wallet. And what roles do financial institutions play in this scenario? Dr. Hansjörg Leichsenring, a respected expert and bank consultant within the German-speaking markets, takes a closer look at trends in mobile payments.

CLEARIT: When I google “investing money,” I get hits from an exotic woods investor, a photovoltaic systems builder, two fiscal agents and issuers, a newspaper, an international investment management group, an online trading bank, and a Liechtenstein and US controlled Swiss bank. How come well-established Swiss financial institutions aren’t in there fighting for ad space?

Hansjörg Leichsenring: If I were an established provider, I wouldn’t be spending my money on Google ads either. And furthermore I would only very selectively spend money for preferential search results. Instead, I would invest in search engine optimization and design my website so that it’s easily findable by Google (and other search engines). Certainly, content is an important consideration, but so is the way services are being “sold” on the net.

Generally speaking, I would highly recommend that established banks think about how they will invest their marketing and advertising budgets over the next years. Looking at the significance of social networks, my recommendation is to invest a minimum of 20% – or better yet, 30% to 40% – in social media instead of in classic marketing instruments. And by that I don’t mean to just create a fancy Facebook profile. It’s crucial to first have a social media strategy in place.

Last November, Google introduced a new smart phone with NFC technology, which is supposed to enable payments. These mobile phones can not only function as your wallet, but can also take over credit card functions, or even replace the credit card. Where do you think this journey is leading?

In my opinion, there is a serious distinction between the markets of the United States and other countries, like Switzerland or Germany. In the United States, credit cards play a major role in reference to revolving credit – something that does not exist in that form here in Switzerland. Debit cards are positioned differently, there, as well. By the end of this year, more than 70 million cell phones are scheduled to be equipped with NFC in the United States, with the potential of mobile NFC payments estimated at USD 75 billion by 2013. Keep in mind that these estimates are adjusted upward on an almost-monthly basis.

Here, too, I see a lot of potential for the use of NFCs in mobile phones. Not only as a means of payment, but also to purchase public transportation, movie or theatre tickets, driver’s licenses, and similar uses.

However, the deciding factor is the option of submitting offers in relation to the user’s geographic location per NFC – geolocation services. Imagine that you’re strolling down Bahnhofstrasse in Zurich and receive a text offering you coffee and a croissant at half price at the pastry shop Sprungli. All you have to do is to go in and redeem the offer using your cell phone.

Mobile phones with NFC

Near Field Communication is a contactless, easy-to-use communication standard that operates near distance (3–5 cm), is supported by the mobile communications industry, and enables secure applications. Contactless payment by credit card is already firmly established. 75 million contactless credit cards are accepted by 230,000 retailers worldwide. Another application is cashless payment by cell phone. There have been successful pilots that took place in Switzerland, as well. Broad use will only become a reality when the makers of mobile phones routinely equip their devices with NFC chips. Major cell phone manufacturers will be releasing these models this year.

You are talking about markets in different countries. What’s missing are functioning, uniform, international standards. When will it be possible to use the same cell phone to buy a public transportation ticket in New Jersey, London and Zurich?

The new providers actually do have uniform standards. When PayPal, Google, and others offer mobile payment, customers with an account or mobile phone will be able to use them all over the world. Basically, you can already do this today using your credit card, so it will be interesting to see what it will take for us to start using something different in the future.
Short biography

Dr. Hansjörg Leichsenring has been professionally focusing on banks and financial services providers for more than thirty years. After having completed a banking apprenticeship, he studied economics and business administration in Mainz, Germany, and St. Gallen, Switzerland, followed by various positions, including as Director at Deutsche Bank, executive of a savings bank, and business manager of an online broker.

He provides services for banks and financial institutions in the areas of (temporary) management and consulting. One of his main focal points is the use of social media. He is also a representative for Meniga, an innovative provider of white-label solutions in the area of Personal Financial Management (PFM) for Germany, Austria and Switzerland.

In his bank blog, which he publishes, he regularly reports about current and general developments and trends around banks and financial service providers. Beyond that, he has published numerous articles in various trade publications.

Furthermore, he is a speaker and facilitator for in-house and industry events and conferences nationally and abroad, and has a lectureship assignment at the Hamburg University of Applied Sciences, Germany, for business administration.
“While payment traffic is only a part of the business with private customers, it is a very important one.”

Until very recently, the bank account was the hub for any payment traffic. Today, it seems to be expendable – at least in the online consumer area, where PayPal, Twitpay and Facebook process payment and credit transactions via non-banking, independent value-added chains. It’s possible to pay directly via mobile telephone billing at Google Checkout. How do you assess the danger that the bulk payment transaction business might be slipping out of the financial institutions’ control?

While payment traffic is only a part of the business with private customers, it is a very important one. You’re right to call it a hub; it’s a very central function of the service array offered to their customers by the banks.

It will be important for the banks to at least remain involved with payment flows in that area; otherwise, they will lose valuable information about their customers in a first step, and in a second one, they will lose the customers themselves. It will be a gradual process, not a revolution, but the margins will continue to decrease, and the banks will end up with a smaller piece of the pie, if they’re not careful.

And it wouldn’t be the first time that the banks have lost the connection with the customer...

Could the banks counteract this gradual process by providing new services? By introducing new payment methods, such as e-payments? What do you believe would happen if the customers were able to pay for their daily online purchases directly from their accounts, in real time?

Hard to say whether the banks will still be able to hop on this train. At the Swiss Banking Operations Forum, Rabobank’s Mrs. Ineke Bussemaker did speak about the banks’ efforts to develop a uniform standard within the SEPA area. I’m not entirely convinced this will work within the foreseeable future. Perhaps individual banks should just offer their customers their own solution, in order not to lose any more time.

As to the second part of your question: What’s bad about customers being offered new services that seem to be covering their needs? Case in point: PayPal is used widely. I find the question interesting, whether the providers will succeed in getting their offers – which were limited to the Internet until now – to the customers (and the retailers) at the shops’ POS.

“The banks have to be on the lookout.”
It’s difficult to keep tabs on the new mobile payment initiatives. There is the bilateral option PayPal and Starbucks are pursuing, allowing the customers to pay for their coffee using a smart phone app, and that seems to be functioning reasonably successfully. Then there are multilateral projects, like the one between three US telecommunication organizations. ISIS promises the mobile wallet without credit or debit cards, tickets, gift certificates, etc. How promising are such types of cooperation? It only makes sense that mobile telephone providers don’t just want to leave their infrastructure for others to use, but instead want to benefit themselves from the predictable, and rapid, development of the mobile payment market. Surely there will be others that follow. Apple alone has stored the data of more than 200 million credit cards in their iTunes. With iTunes, the shop is ready, with the iPhone or iPad as a mobile tool – the only thing missing is a payments infrastructure. Certainly, there are enough funds available, and what would keep Apple from founding its own bank in order to take advantage of the entire value-added chain? One thing is for certain: The banks have to be on the lookout!

Isn’t Facebook right in the middle of covering exactly this value-added chain, including the payments infrastructure? The world’s largest social network founded a subsidiary for payment processing in March; it even has its own currency, Facebook credits, that are used as a means of payment. How exactly should the financial institutions behave, vis-à-vis such developments?

Indeed, Facebook has named the year 2011 the “year of the e-commerce”; the credits are mandatory within Facebook Apps starting 1 July 2011.

For the banks, that results in two challenges simultaneously: On the one hand, they must counter these new providers with something, and that’s exactly what we’re talking about here. On the other hand, they urgently and quickly have to educate themselves about those no-longer-new social media. The banks seem to have great difficulties with them, yet some of the greatest opportunities lie right here. My recommendation to a bank’s top management is to retreat to a strategy workshop specifically focusing on the ins and outs of handling social media and to consider developing an appropriate strategy. It might be best to bring in an outside expert as a facilitator – someone who is familiar not only with social media, but also with banking and strategies.

“I find it hard to believe that a major bank doesn’t consider payment traffic a strategic business area.”

Perhaps it makes sense to differentiate between large, international banks, and smaller, more regional financial institutions. Let’s assume that bulk payments are not a core business for a major bank, allowing it to react with less urgency to the challenges of the Internet giants. But how do you see the scope of an institution focused on payment traffic?

I find it hard to believe that a major bank doesn’t consider payments a strategic business area. It’s an important hub in both private and corporate banking. I believe that no bank can consider itself unaffected. An institution like the Swiss PostFinance, which is still without banking status and for which payment traffic is of higher significance, must remain particularly alert and think of something in order to keep their customers’ loyalties. But, according to my observations, that is part of their corporate thinking.

One option I see is to offer additional services in connection with payments and account management, such as Personal Financial Management (PFM), a new link between financial planning and Web 2.0. In the United States, this is already considered a good standard at the retail banking level; in Europe, we’re just being exposed to the first offers. This is also one of the rare chances for the banks to position themselves on the market and differentiate themselves from the competition, in my view.

What is Web 2.0?

“Web 2.0” is a term that describes a complex of usage patterns and modern online technologies. It is best characterized by “customer created content”. Social software comprises the main component of this complex. It supports the building of relationships and communications in a social context and is based on principles such as self-organization, social feedback, linking of contents and transparency among people, relationships, contents and evaluations.

“There is one thing in particular that banks must focus on: To design their own new proprietary mobile content, offering services customers want to use while they’re on the go.”

Research institutes assume that mobile terminals will be more important for Internet access than PCs. In addition, mobile channels will accelerate turnover growth in e-commerce. What are the resulting consequences for the financial industry?

I recently read a report that iPad users spend more time on
The cell phone is the future Swiss knife. Mobile Internet is indispensable for many users, whether they only want to check the weather service and watch the stock market, or whether they are already using their cell phone for banking transactions. The trend is clear: Before too long, more people will be accessing the Internet via their mobile devices than at their stationary computer.

That's why it's apparent that in future, the cell phone will also be used as a wallet. Instead of carrying many different plastic cards, our constant companion will also become our customer card, payment card, transportation ticket, and access key, and will perform many other functions.

The next dimension
The resulting advantages are many: The cards will never again be lost or forgotten and their use becomes much more manageable, since account balances and customer loyalty rewards, like the Cumulus or Supercard points can be called up. Until now, the last link was still missing: the distance from the mobile phone to the POS terminal or to the access reader at the entrance. Now, the new technology Near Field Communication (NFC) makes the connection between the virtual and the real world. The end user experiences a whole new dimension for shopping, traveling, and working on the go:

- Customers carry their payment and loyalty cards in their cell phone while shopping
- A small payment is significantly faster and easier than any cash transaction
- Account and point balances can be displayed
- Collection programs can be linked with online services, opening up the potential for new marketing channels
- Gift certificates and coupons can be distributed and redeemed easily by cell phone, as well as being transferred from one individual to another (viral marketing)
- Targeted offers can be sent to the (potential) customers’ cell phones
- Receipts and warranty slips can easily be collected and organized
- Social networks can be enlarged by two phones touching one another
- Tickets can be ordered directly by mobile phone and stored there until needed
- Keys can be issued with a specific life span (home care or repair persons receive access for a very specific place/time)
- Transactions are executed by a single touch. This is intuitive and easy for all target groups, whether they are old or young, and all of this is secure and reliable.

Should e-banking be mobilized, as well?
That is already happening. Although I doubt that the customers will muster much excitement when they receive the fifth app from their third important bank. According to experience, very few functions are actually used on the go, such as the available account balance.

The greatest benefit for customers would be a modern PFM actually provided by their bank, one that would help with daily and non-daily expense planning and assist budgeting in such a way that there would be funds left at the end of the month for special purchases. And if indeed the customers were able to obtain real mobile support, all the better.

Interview: Gabriel Juri, SIX Interbank Clearing
gabriel.juri@six-group.com
As secure as any bank card
This is not new technology. We have known contactless payment cards like PayPass and payWave or LEGIC for access for several years. What’s new is that Near Field Communication makes it possible to “virtualize” these cards and allows for their use by mobile phone.

Near Field Communication is based on RFID, the reliable, tried and true wireless communication technology. Use includes the ability to touch an advertising poster and automatically retrieve information about it directly from the Internet. Instead of painstakingly typing the URL, a single touch at the TouchPoint is all it takes. For collecting coupons, etc., using “open NFC,” the cell phone is a mobile NFC reader (reader mode).

But in order for the Near Field Communication device to be able to pay at a terminal, it has to emulate cards and process these transactions as securely as any bank card. To make secure NFC possible, NFC mobiles have a secure area, the “secure element,” which can be read both from a terminal and from a cell phone application via the “card emulation” feature.

In practice, there are various secure element form factors: A special SIM card, the USIM, which is also capable of storing secure NFC applications and exchanging them with the NFC mobile via the single-wire protocol. Many manufacturers integrate this secure element chip directly into the device. It’s also possible to retrofit certain mobile models with NFC-equipped micro SD cards or NFC adaptors later on.

Competition and cooperation
But it’s not how the secure element is physically executed that will be a deciding factor for the commercial launch, but rather who issues and manages it logistically. A USIM is issued by the Mobile Network Operator (MNO).

To this end, a commercial agreement and technical link must be established with the MNO for the distribution of NFC applets, such as the ones from PayPass or payWave. In order to prevent each mobile services provider from having to enter into commercial agreements with each MNO or distributor of secure elements, the new role of Trusted Service Manager (TSM) has emerged in the NFC ecosystem.

Whenever banks, retailers, or transportation companies – centralized as service providers within the ecosystem – want to distribute contactless products on the customers’ NFC cell phones, the “production” of the secure applets from the TSM occurs over the air. Customers can have their mobile credit cards loaded onto their cell phones within minutes. Additionally, the TSM guarantees that this process is secure and user-friendly.

The features offered to an end-user by the TSM aren’t just limited to the original issuance. When a customer gets a new cell phone, the Trusted Service Manager manages the move of the applications, blocks services in case someone loses their mobile device, and can update data, such as renewing public transportation passes.
In this emerging NFC market, the Trusted Service Manager is reimbursed for distributing the virtual cards by the service providers. The TSM pays the issuer of the secure elements for providing the multifunctional storage, such as the USIM, in the case of Mobile Network Operators. Due to the different NFC form factors, other organizations, such as banks, can issue micro SD cards and thus offer NFC services independent of Mobile Network Operators. In practice, both competitive and cooperative models will be emerging among the participants.

Obviously, what’s important for the customer is the actual acceptance ratio – where can they pay, collect points, etc. More and more providers are offering their terminals with a standard contactless interface that accepts NFC payments in addition to the 600,000 contactless credit cards in circulation in Switzerland.

Why will NFC succeed? Added value for the customer, improved and faster services, specific offers and a new user shopping experience overall will be an integral part of our future. In order to make these added values available with a cell phone, a mobile wallet will manage our cards and keys. The NFC wallet turns the mobile phone into the Swiss knife of the future.

Kurt Schmid, CEO NEXPERTS GmbH
kurt.schmid@nexperts.com

The different roles in the NFC ecosystem
The mobile phone is changing our lives, our economy, and our business models. The music and movie industries are already in the middle of this revolution. Newspaper publishers fear for their customer relations, because third-party companies like Google and Apple can control access to editorial articles via iPad and cell phone. Payment traffic is no exception: It's also being affected by this trend.

With the launch of the iPhone in 2008, Apple completely changed the market. The combination of an easy-to-use tool and new concepts – like the app store for reaching the customer, service conception and operation – can all be applied profitably to payments.

A personal financial assistant in your pocket
Many financial institutions had already taken the first step in the direction of mobile banking back at the end of the 1990s, when they made account balances available by text on the account holder’s cell phone. Because of the increasing use of apps, mobile banking has drawn attention again. In the fall of 2010, PostFinance integrated its text-based services – like account balance inquiries, funds transfers and loading up prepaid cell phone credit – into a single app. In that same app, users can find the locations of PostFinance ATMs, post offices, and branches, and the current stock market and exchange rates can be tracked.

Simplicity and data security
The customer initially has to register with strong authentication to gain access to financial transactions or account information. This is done by way of the established login procedure using the PostFinance Card, a reader/terminal and a challenge-response process. After the initial registration, the user can access all information, transfer smaller amounts and load his prepaid account.

Multi-layered encryption and identification processes make data unavailable and unreadable to any unauthorized persons.

Opportunity and risk
The cell phone will bring banking and payment services that were formerly provided separately closer together. Account access services and payment functions in third-party applications, such as the Swiss Federal Railways SBB, the retail group Coop or the online supermarket LeShop, can merge over the mid-term. But will bank customers want to move funds from one account to another using various processes, templates and security processes? The answer to this question holds both opportunity and risk and is the key for the financial industry to hold, maintain and grow customer relations in the money business.

Roland Greber, Head of Competence Center PostFinance Mobile
roland.greber@postfinance.ch

Box: Sabrina Jantschik, SIX Card Solutions
sabrina.jantschik@six-group.com

App is a mobile terminal
Starting in the summer of 2011, SIX Card Solutions offers a new mobile card terminal. The Saferpay mobile app is an expansion of Germany’s first mobile credit card terminal, iPayMobile, which was introduced a year ago. In addition to regular credit cards, it also processes German direct debits. This new app is even easier to handle and offers many new features. One of those new features is the ability to process credits for credit card payments.

The app is particularly well suited for messenger services, taxi drivers and any kind of delivery service (e.g., pizza delivery).
A prepaid card for the Internet

Last November, the "Internet Cash" card was launched by Swiss Bankers Prepaid Services – in cooperation with MasterCard. The Swiss Bankers company was founded 36 years ago by the banks as the center for travelers’ checks, and today is a bank itself.

Approximately 70% of the Swiss population shops on the Internet. More than half of those worry that their credit-card data could be abused. Another 25% would like to shop online, but don’t have a credit card. Internet Cash by Swiss Bankers and MasterCard can meet the needs of those consumers, as well. What’s more, for bank customers this card is a sensible complement to their existing credit cards. There is no annual fee for Internet Cash. Users generally pay a fee of 2% of the loading amount, plus CHF 3, EUR 2 or USD 3 per transaction, depending on the currency.

Experience and investment

The distribution of payment instruments through banks is part of the Swiss Bankers’ core business and is rooted in history. In 1975, the Swiss Bankers Travelers Cheque Center was founded by various banks as a corporation to issue the checks in Swiss francs. In 2008, the company changed its legal status. In addition to Easy Cash and Internet Cash, Travel Cash is the Swiss Bankers’ core product. It’s the evolution of Travelers Cheques and is issued by 160 banks in Switzerland. Travel Cash has laid the foundation for the future-oriented business, with prepaid payment instruments to be used electronically. The company can draw on well-developed platforms and established processes without needing to invest anew for each launch of additional prepaid cards.

Prepaid cards in Switzerland

In addition to Swiss Bankers, the following organizations are issuing prepaid cards: Cornèr Bank ("Cornèrcard Reload": MasterCard and Visa), Post-Finance ("Value": MasterCard only), Viseca ("PrePaid": MasterCard and Visa), Valartis ("Advanced Card": Visa only) and SIX Multipay ("CASH"). By the end of 2009, there were 67,600 prepaid cards in circulation, accounting for approximately 16 million transactions and a turnover of CHF 70 million. (Sources: Cornèrcard, PostFinance, Viseca, Valartis, BIS)

Partners

The Internet Cash card issued by Swiss Bankers is linked to the worldwide MasterCard acceptance network. Thus, owners of this card can use it to pay at millions of vendors online. The transactions are processed by MasterCard. The card can be loaded at more than 140 currency exchange counters of the Swiss Federal Railways SBB, and purchased and (re)loaded at the St. Gallen Cantonal Bank. MasterCard® SecureCode™ provides additional protection on the Internet against fraudulent use of the card data.

The St. Gallen Cantonal Bank, a shareholder of Swiss Bankers, was the first distribution partner. The new product could be introduced without much investment in time or money, since all processes, as well as the ordering and accounting systems, are identical with the one used for the Travel Cash Card. There is no obligation for shareholders to be distributors. And, of course, non-shareholding financial institutions can become distributors, too. <

Thomas Beck, CEO Swiss Bankers Prepaid Services Ltd
thomas.beck@swissbankers.ch
Online payments without credit card

Recently, a new, global, safe and secure method to make and receive payments on the Internet without the use of credit cards has become available. For the first time in payment traffic history, SuisseID, the secure electronic proof of identity, is being used by the SwiKey company.

The intention is to enable Internet customers to pay for their purchases using money in Swiss francs, euro or dollar that they have loaded onto reloadable coupons at various points of sale.

Every registered SwiKey member (individuals and/or companies and organizations) owns an electronic wallet (e-wallet) that can be loaded in a number of ways: by bank credit transfer, via PostFinance’s E-Finance or with the PostFinance (debit) card, by using reloadable coupons that will shortly be available at various points of sale and (coming soon) by using credit cards.

Members can transfer funds to another member or pay at another partner’s web shop. The fees (1% for direct payments or 3% for brokered ones, such as for Internet auctions) are charged to the seller. An exchange mechanism allows for the currency conversion.

There are two types of e-wallets: Limited and unlimited. In the first case, identification documentation is not required; however, transactions are limited to CHF 5,000, EUR 3,500 and USD 4,700 per year. In the case of unlimited wallets, owner identification is required before use. SuisseID registration is convenient and fast, and a very secure connection can be obtained to one’s own e-wallet. The registration process is accelerated, since it isn’t necessary to mail in identifying documentation. According to the user’s preference, the wallet can be accessed either via a very secure SwissID navigator or by using a one-time password (mobile OTP). Beyond that, the free iPhone App “MPayment” offers the following options: Checking account balances, transferring funds to another member, transferring funds to one’s own bank account and (re)loading the wallet.

On the partners’ side, SwiKey services integration takes place conveniently and securely with an Instant Payment Notification (IPN), for which documentation is available upon demand.

Joe Farage, SwiKey SA
joe@swikey.ch
In recent years attacks on Internet banking services have evolved from rather simple credential stealing attacks to advanced content-manipulation attacks by means of malicious software seeded on the client end-devices. A praxis implementation at UBS shows how to counter those risks with regard to convenience and mobility of the customers while maintaining the highest level of security.

Content-manipulation attacks targeting the transaction data entered via the client PC are considered the most common and most threatening. They typically manifest after malware has infected the client PC. The reason is because in practice the same PC is used for both browsing/e-mailing and for e-banking and attacks tend to focus on this PC who’s security is not controlled by the bank.

Transaction confirmation independent from Internet and PC
The only long-term solution to this exposure is to complement strong authentication at login with sensitive data authentication during transaction placement, and for the additional confirmation step to use a trusted platform not exposed to the Internet and the client PC. In other words, the process of confirming sensitive transaction data must be moved from the PC to a trusted device, which at least includes a display, one or more buttons and the user credentials. In this way, the user can reliably verify critical transaction details on the trusted display, such as the beneficiary account of a payment instruction, and then confirm the respective data via the trusted buttons. The device then typically generates a transaction specific signature to be sent to the banking server. Credentials used to do this are never exposed to the client PC. In other words, the trusted device always signs what the user has seen and approved on the same device.

Disconnected reader solution
One of the solutions that is in use worldwide by all customers with a Swiss UBS e-banking contract is the so-called UBS Access Card Reader solution. It is based on a standalone code generator device that is not connected to the PC or any network. The device is comprised of a smart card reader including a simple display and a keypad. The user also has a smart card personalized with a key and a counter that is used to generate a response for a given challenge. For user authentication the back-end server provides a user-specific random challenge on a web page. After card insertion and PIN code entry, the user manually copies the challenge from the web page to the reader, which sends it to the smart card for response calculation. Finally, the user copies the response displayed on the reader back to the web page to submit it to the server.

Effective beneficiary confirmation
Although practice can differ from one country to another, the success of a payment order often does not depend on the correctness of the specified beneficiary name and/or address, but solely on the correctness of the specified beneficiary account and/or payment reference number. To achieve an effective beneficiary confirmation, it is essential to identify what uniquely determines the beneficiary of a transaction, depending on the beneficiary’s bank and the type of payment, and have the user check and confirm only this.
This authentication solution has been extended to support beneficiary confirmation. To achieve this, the server requests a response for a transaction related challenge, the beneficiary account, before a transaction request is processed. This means the user enters the beneficiary account into the reader and copies the response back to the web page, just as with user authentication. At this point in time the account number is not displayed on the web page since the PC display is not considered trusted. Instead, the user is forced to become accustomed to retrieving the number from another supposedly more trusted source, such as a paper invoice. If the account number is too long to be used as a challenge, the web page indicates which part of the account number shall be used. For example, if the account number is 123456789 and 34567 shall be used as the challenge, the web page displays 12xxxxx89 to guide the user. Requiring the user to carry out this rather time-consuming confirmation process for every transaction would be impractical. The solution becomes practical for most users only in combination with the white list management approach.

Practical results
From a security perspective, this solution reliably thwarts content-manipulation attacks as long as the user is aware of his or her responsibility and due diligence.

With regard to business relevant aspects, such as convenience, mobility, integration and cost, the new approach considerably increases user benefits in comparison to contemporary solutions. The approach is intuitive, works with all standard PCs, operating systems, and web browsers without requiring any software installation. As a result, it is easy to carry around and it can be used almost anywhere, although its built-in keypad makes it somewhat bulky. Last but not least, costs are appropriate for large scale deployment.

From the level of attacks faced at the time of writing, it is to be concluded, that modern Internet banking services will be able to survive only if banks place great emphasis on the reasonableness of their solutions and users strongly care about their responsibility and due diligence to protect credentials and validate transaction data whenever needed.

White list
It is crucial for the effectiveness of beneficiary confirmation to ask for a confirmation only when the beneficiary is neither globally trusted by the bank nor known to be trusted by the user. Keeping track of globally and personally trusted beneficiaries essentially requires the use of global and personal white lists that are managed by the bank and the user respectively. Beneficiary confirmation is then equivalent to the functionality of adding a new beneficiary to the personal white list and needs to be complemented by a corresponding functionality enabling the user to also remove a beneficiary from the personal white list. Before executing a transaction the banking service in such a case simply checks whether the beneficiary is on the bank’s global white list or on that user’s personal white list and requests an extra confirmation only in the exceptional case where a non-globally-trusted beneficiary is used by that user for the first time. With such a multi-level white list approach, convenience will typically be very high for the large majority of occasional users who primarily deal with globally trusted beneficiaries.

Alain Hiltgen, UBS AG
alain.hiltgen@ubs.com

Stefan Brunner, UBS AG
stefan-pascal.brunner@ubs.com
For more ample information on the UBS Access Card Reader as well as the corporate customers solution (UBS Access Key): http://www.ubs.com/authentication

Additional information about the Swiss payment traffic systems can be found on the Internet at www.six-interbank-clearing.com