Chip and PIN: two-factor authentication
As online banking fraud continues to grow, consumers’ deep-seated security fears remain one of the biggest barriers to online banking in Europe. But now BT is developing a service offering for two factor authentication that can help banks tackle customer fears head on. Steve Martin reports

There are three reasons why internet banking requires increased security: online fraud is on the up; customers need reassuring; and changes in the industry demand it.

There is no doubt that chip and PIN is helping in the battle against many types of fraud. Losses due to fraudulent card activity are down 13% year-on-year since the arrival of chip and PIN.

But it is not all good news. Criminals are switching their attack to online transactions. In 2005 card not present (CNP) fraud was estimated at £183.2m, up 21% on 2004, (APACS). Much of this CNP fraud is committed online – £23.2m in 2005 (APACS). These figures may rise dramatically as criminals increasingly target the perceived weaknesses in online security.

Chip and PIN: two-factor authentication
Protecting your customers

We know that many potential internet customers are put off by worries about security. Any big increase in fraudulent activity would play to these fears and make it even more difficult to develop this channel.

While customers should be responsible for keeping their finances secure, they still look to their banks for action and reassurance. According to the FSA, “An overwhelming majority (95%) also feel their bank has at least some responsibility in providing online protection, and almost half feel their bank is solely responsible… Our survey suggests that over three-quarters of customers would simply stop banking online if liability were shifted.” (Research conducted by NMG Research/IPSOS on behalf of FSA in October/November 2005).

Clearly, banks have to demonstrate their commitment to protecting their customers online.

Providing an authentication system that is much more secure than the normal log-in and password will go a long way towards easing these fears. Changes in the industry are also fuelling worries about online banking fraud. Autumn 2007 sees the introduction of faster payment clearing for electronic transactions. Reducing the time electronic transactions take to clear will give banks even less opportunity to spot fraudulent activity – so there is a strong case for introducing improved authentication for safer customer log-in before these changes come into effect.
Secure and simple

The need to do more to enhance online security is clear. A static password is no longer enough. In spite of all the warnings, people are still duped into revealing their log-in details. And savvy scammers with the right software can steal log-in information direct from customers’ PCs.

The challenge facing the industry is how to increase security while keeping access simple and straightforward for the genuine customer.

Two factor authentication (TFA) can go a long way towards achieving enhanced security. It is based on something the user knows – a password – and something they have – like a token, a mobile phone, a PC or a chip and PIN card. The second factor can even be based on biometric data.

**Two factor authentication from BT** is designed to deliver this requirement. It works by providing customers with a unique access code each time they log in. This is generated by a device or process not connected to the PC and is valid for a single transaction, making it much more difficult to steal or be guessed.

BT’s hosted TFA service, based on a range of authentication devices, from EMV card readers and one time password generating tokens, to SMS and voice authentication will greatly improve security at minimum cost and with little commitment of resources.

The FSA endorses two factor authentication: “Delivering TFA to their retail and business banking customer bases will enable banks to provide stronger authentication mechanisms and reduce the risk of fraudulent access and transfer of money out of accounts.” Financial Risk Outlook 2006.
Chip and PIN

With a view to keeping things simple for the user, the two factor authentication service from BT will initially be delivered through EMV card readers that use the chip and PIN process that consumers are now familiar with. Other authentication mechanisms such as OTP tokens, SMS and voice authentication will follow.

Each private or business customer will have a card reader via which the second form of identification will be issued. Customers simply insert their card into the card reader and enter their PIN. They will then be presented with a code on the display. This one-time code, which changes every time the card is used, is then transmitted to the authentication server which authenticates the user to permit access.

BT will manage the whole process and provide all the IT infrastructure needed, from the delivery of card readers through to customer help desk support and authentication of users on its own secure servers. Authorisation of access will remain with the bank.
Why choose BT?

BT is more than able to deliver the full TFA package, because it has extensive experience in providing two factor authentication for secure remote access to corporate networks and the provision, distribution and support of devices to its millions of broadband customers.

Risk is minimised because the only company banks need to work with is BT, which is the single owner and provider of the IT infrastructure.

As for financial services competency, BT is a trusted supplier of secure financial services solutions. For example, BT’s SettleNET service, handling share settlement in London markets, is built for full disaster recovery and business continuity and provides its own certification authority approved by the FSA and the Bank of England.

Looking to the future, BT is preparing for the next stages of two-factor authentication as it migrates across other channels into new mechanisms such as voice and mobile/SMS. So banks can be sure that any BT solution they choose now will be fully future-proofed, with migration to alternative channels provided as and when required.
Why go it alone?

The FSA recognises that it may not be cost effective for banks to develop TFA themselves. But it does say that pursuing such a policy would demonstrate to customers that fraud is being tackled. Partnering with BT offers a much more viable solution, since BT will supply everything required to run the service, assist with application integration and offer attractive commercial options. Costs can be kept down because the necessary infrastructure is already in place and BT can draw on economies of scale.

There are added benefits in choosing BT’s two-factor authentication service: BT future proofs the two factor authentication service by providing a range of device options suitable to many customer segments.

None-core IT device management can be outsourced to a capable and trusted provider.

Reduced time to market.
For more information

The two factor authentication service from BT will enable financial services organisations to interact with customers in a significantly stronger and more secure environment. It will play a major part in reducing internet banking fraud, and will demonstrate the industry's commitment to doing business securely online. The outcome should be an increase in consumer confidence, enabling banks to develop their online banking business.

For more information about two factor authentication from BT, contact justin.kimber@bt.com

BT’s ability to provide a complete and effective solution, short guaranteed delivery times and high quality data centres were a critical factor in Friesland Bank’s decision to choose it to host a secure internet banking environment for its customers.