THALES e-SECURITY

Securing Internet Home Banking

In this paper:

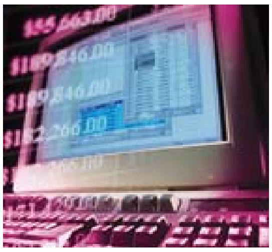
Security for today's online transactions

Banks realise today that the provision of traditional transactional services has become common-place and that they have a need to differentiate themselves from their competitors. The provision of interactive online services which are not simply another "shop window", is now consequently a key area for many corporations today. The offering of these services allows companies to open new competitive areas for their products and address quickly many new customers. Such offerings also allow access to new geographic markets without the costs and problems of opening channels and retail sites in each country. Allowing customers to use your services outside of traditional opening hours also offers many advantages in today's competitive market places.

This new marketing tool is not without its risks however and the new technology, with almost global reach, is as open to criminals as it is to the law-abiding. The fact is in moving to a virtual or Web presence there is a loss of security compared with the normal physical world. You can no-longer see the person with whom you trade nor they you. The virtual world has to replace this with other measures which resolve the problem allowing both parties to be confident that they are trading with bona fide partners.

The tools for doing this vary and there can substantial cost implications which must be offset against the "gains" of dealing in the virtual world. A balance must be found which is matched to the risks posed.

Analysing the problem

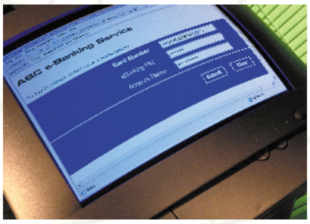


Many Web-oriented systems today are provided with simple security measures such as the Secure Socket Layer (SSL) technology. In addition passwords are globally accepted as a minimum requirement for the identification of system users. Unfortunately both these techniques are open to misuse and many do not understand the limited nature of the protection they provide. While such mechanisms may be acceptable for some, criminals are attracted to the gains that can easily be made from attacks on web based facilities run by Banks. Money movements between accounts open the possibility of losses that may run out of control, undetected, if not suitably protected.

The standard SSL technology can only protect against attacks from the Internet. Once the data arrives at the Web Server it is automatically converted back to its unprotected form rendering it open to attack. We should also note that attacking a message in transit across the Internet is both difficult and not very rewarding compared to the amount of effort needed. In contrast, web servers represent concentrations of several thousand times of this information and are therefore a much more attractive target for the criminal.

Passwords are notoriously easy to guess and do not offer any suitable level of protection. Consequently Banks have traditionally relied on the use of PINs with bankcards when identifying customers at their ATMs and the customers have come to trust this identifier.

So what options exist for us to solve this problem? The normal approach to this involves "Something you have" and "Something you know" or "Something you are". The latter is best epitomised by the "Biometric" identification route and while very good it suffers some problems in the implementation often falsely rejecting valid users or impinging on civil liberty and rights. The banking industry has been using the first two mechanisms of what you have and know for years in its ATM cards and associated PINs. In order to implement this in the Internet environment a card reader and secure PIN entry pad is required at every PC and Internet usage device. While this is possible there are a wide variety of devices in the market and finding, managing and supporting the distribution of suitable devices can be problematic. From the user's perspective the requirement for an additional device associated with identification brings its own problems. Now a card reader as well as the card has to be available when needed and while the card will normally be kept in the wallet the card reader or PIN entry device must be separate. Such an extra both causes inconvenience to the user and costs the system provider on a per user incremental basis.



Typical Internet Home Banking Log-on Screen

Faced with these obstacles most banks and system implementers have adopted what can best be described as multi-password mechanisms in the hope of increasing the complexity and hopefully the "security". Unfortunately the greater the complexity the more likely the user is to record the multiple passwords required as the task of remembering them becomes onerous.

Users may also be asked to agree to terms which are less than attractive essentially signing away all their rights for the privilege of using an insecure medium. In any case it is important to make the solution match the risk and, for example, to avoid the more onerous user authentication practices just so the user can obtain an online statement!

WebPIN^{TM} High security for online banking

Thales introduced WebPIN to address these problems in an end-to-end security solution, where sensitive information, such as a PIN, is protected from its point of entry until it is validated or used by the application. Using Java based technology yet based on Thales' proven hardware security, WebPIN provides an Internet ready end-to-end security envelope. WebPIN uses Banking industry standards combined with "best of breed" Internet security techniques but avoids the need for additional hardware at the users web browser. By providing a end-to-end security envelope it is possible to protect the important data forming a transaction and not to leave plain text customer details lying on the Web Server to be collected by criminals. WebPIN Integrates with existing facilities allowing banks to capitalise on their existing investment in their ATM PIN verification systems.

WebPIN is designed for Banks wanting to offer services to their customer base over the Internet channel. Offering compelling services which allow the bank to compete well against other financials will involve higher risks but brings with it the possibility of being able to charge for these services.

Issues:

Protect PINs and Passwords.

Keep private data secret

Check server generated signatures on data

WebPIN has three primary functions:

- User Authentication based on PIN Verification from a 3DES encrypted ANSI PIN Block sent from the Client to the Web Server.
- Message Authenticity based on the use of standard 3DES ANSI MACs sent from the Client to the Web Server.
- Data Privacy based on the use of 3DES ECB or CBC encryption of messages sent to and received from the Web Server.

In addition to this WebPIN is provided with a facility to verify a Digital Signature on data received from the WSM supported Web Server using the installed Public Key.

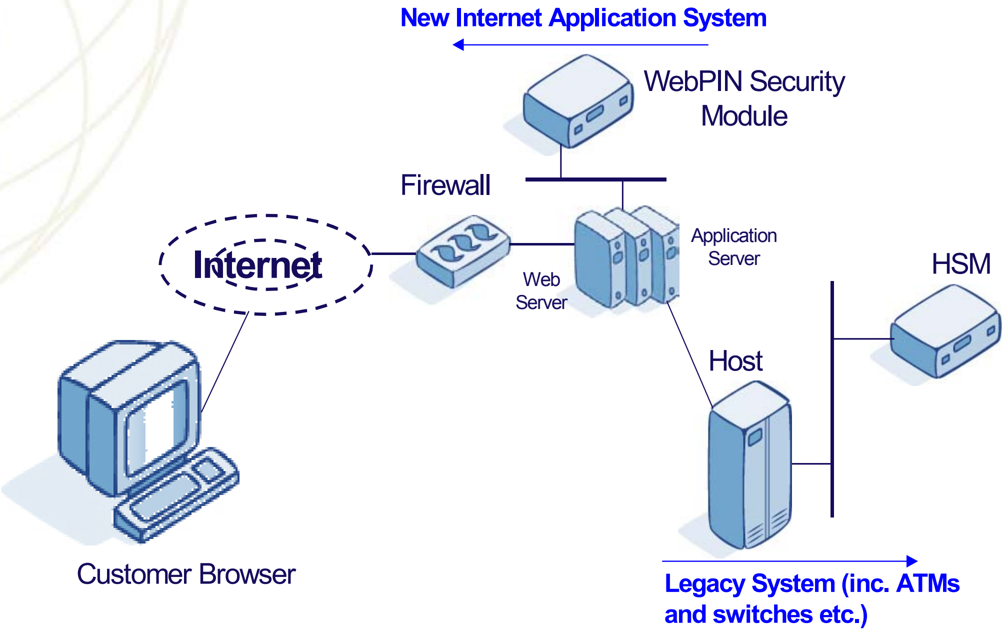
The WebPIN product offering comprises two main elements.

- A set of Java Classes, employed at the client end, which are used to provide the necessary cryptographic functionality and to create a finished applet which will be delivered to the client browser in a suitable Web page,
- A hardware security module (WebPIN Security Module) sited at the Bank's Web Server or Application Server which provides the cryptographic interface between the internet environment and the Banks current PIN management or verification system.

The WebPIN Java Classes are used by the Bank's system integration team to create one or more Java Applets that provide the cryptographic data protection required. These applets are stored at the Web Server until required within each session and are downloaded to the Customer Browser when requested by the relevant Web Page. Once loaded to the browser the applet is called and runs as specified in the Web Page. The applet creates a protective envelope for the data, which can only be opened by the WebPIN Security Module. This tamper resistant hardware security module ensures that the sensitive data protected by the applet is maintained in a secure state as it is delivered onward into the Bank's existing system. **WebPIN therefore provides an end-to-end protection for the data that is not available from the use of the industry norm, Secure Sockets Layer (SSL) encryption**.

Typical WebPIN system implementation diagram

Shows new Internet Banking implementation plus existing "legacy" ATM management system installation



WebPIN^{TM} plugs SSL weaknesses

SSL suffers from the fact that it only protects the data flow from the Browser to the Web Server. While SSL helps prevent hacking when the data travels across the internet, once the data arrives at the Web Server SSL leaves it in plain text and vulnerable to attack at just the point where there is an attractive concentration of data useful to a hacker.

In an Internet banking system the data in question might be a PIN issued to the customer for Log-on purposes but can also include other data such as account number, type and value of transaction, transaction identifier etc. The WebPIN enabled applet uses a banking industry standard format for protecting the PIN (ANSI PIN Block format 0) and the WebPIN Security Module is capable of translating this format to any PIN Block format required by the Host verification system. The PIN is passed to the Host system encrypted under a standard DES or 3DES Master / Session Key typically called a Zone PIN Key. Consequently the PIN will appear to the Host System to have come from an ATM transaction conducted on behalf of the Bank by another Bank or ATM Network (sometimes called an ATM Switch). The ability to process PINs from sources such as these is a standard feature of most ATM Management Systems (AMS) and as a result the PIN can be verified without the need to modify the AMS. **This powerful feature allows Banks to put a new Internet banking system in place while capitalising on their existing investment in their ATM system.**

WebPIN^{TM} allows Banks to offer Internet home banking and verify the internet users through their existing ATM PIN validation system.

In addition to the PIN protection facilities WebPIN also offers the ability to authenticate messages using a MAC, which ensures the contents of a message have not been changed in transit. WebPIN can also be used to cipher data, to and from the host, where that information should remain private. The MAC facility is useful for low risk transactions while the bi-directional data privacy facility is important when sensitive data could become exposed such as during loan applications or share dealing. In every case WebPIN can provide a true end-to-end solution not possible with SSL alone.

When running in a customer's Browser the operation of WebPIN is transparent to the user and in fact they may be totally unaware of the high level of protection being used for their benefit. For the Bank also the use of WebPIN has a low impact being easy to implement and manage.

Implementing WebPIN^{TM}

The following implementation details will need considering:

1. Suitable Java Applets will need to be coded to execute the desired functions. These will be compiled using the Thales WebPIN Java Classes.
2. The applets will need to be called from within the appropriate Web Pages as required.
3. At the Web Server the applet(s) will need to be stored and delivered when demanded.
4. Server side controls or scripting will be required to receive the data from the applet enabled Web Page and to have that data processed by the WebPIN Security Module (WSM).
5. Finally the server will pass the data on in to the existing Host system for appropriate transactional processing using a suitable messaging format.

There are a number of system or key management tasks which are needed to ensure the system runs smoothly. WebPIN supports these standard business and banking security practices.

1. An RSA Public Key will need to be encoded into the applets and this must be generated by the WebPIN Security Module and stored for subsequent use. The RSA private Key will be provided by the WSM encrypted under a Local Master Key (LMK) and can safely be stored in a file for later retrieval or loading into the WSM.
2. The finished applets should be signed using a suitable RSA Public and Private key pair obtained from a respected source. This will help Bank customers ensure the applet has come from the Bank and not some other source. Customers will need to be encouraged to set their browsers to check such code signatures and the corresponding public key certificate issued by the bank and certificate authority.
3. In order to protect PINs in transit to the ATM Host PIN validation system a Zone PIN Key (ZPK) must be established between the WSM and the HSMs attached to the ATM system. This is done using a manually transferred Zone Master Key (ZMK) as per normal Banking practices.

Provision should be made in the design for the routine update or change of keys such as the WSM Local Master Keys (LMKs), the ZMK and ZPK. While the LMK and ZMK need only change relatively infrequently, say annually, the ZPK will typically change frequently depending on the number of transactions it has been used to protect.

WebPIN^{TM} Securing business transactions

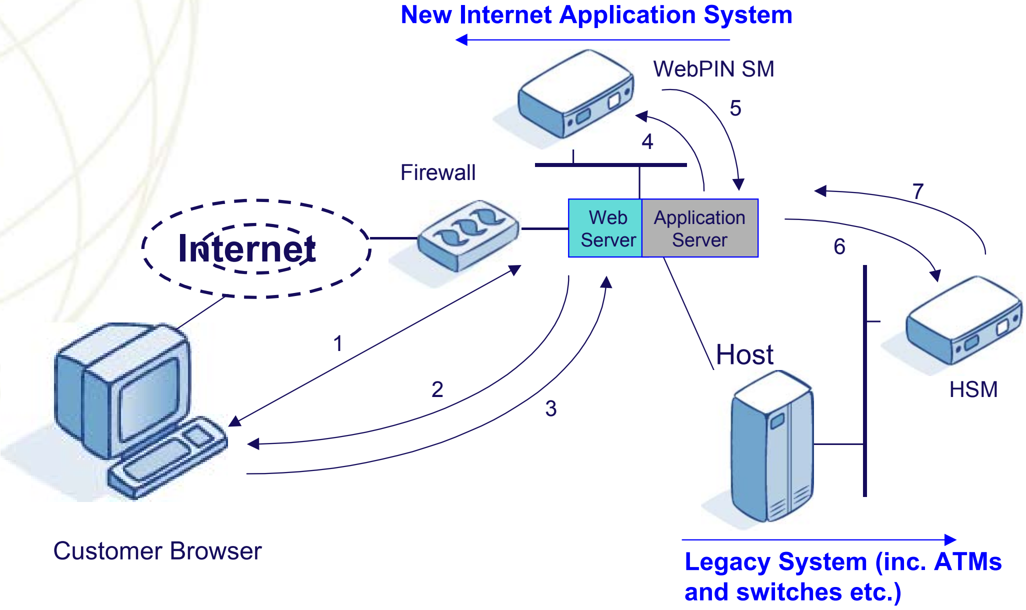
WebPIN comprising a set of specialised security Java classes and Thales hardware security module, provides end-to-end security for online transactions. Capitalising on existing investments in host processing facilities WebPIN helps Banks extend their services to their internet connected customers, who can then identify themselves using the standard user authentication method with which they are already familiar, their PIN. WebPIN offers a cost effective, end-to-end, solution to the problem of securing banking transactions over Internet connections while making the most of existing bank authentication technology.

More-over WebPIN protects sensitive customer data on the Web Server from disclosure but is transparent to your customers while making it possible to offer more and higher risk services which can attract premium pricing. WebPIN offers a measured solution to the conundrum of securing web based transactions.

Example : Log-on Application

WebPIN Log-On Application

Shows message flow for PIN protection and validation with the PIN being verified by the ATM system



The following examples each explore how WebPIN is used to execute the above functions and show the true end-to-end nature of the solution.

Note the numbered message flows on each diagram are described in the steps in the examples.

The first example covers the use of PIN encryption to check a customer's identity at Log-on.

1. The customer opens an Internet session to the Bank's Web Server, which sets up an encrypted SSL session.
2. In the appropriate Web Page the WebPIN enabled applet is downloaded to the Browser typically for the login screen.
3. The user is invited to enter the login data, Account number, PIN etc. and the applet then forms the PIN block, encrypts it and constructs and MACs the packet of data to go back to the Web Server. The packet will also contain the randomly generated 3DES key material for the PIN encryption and MACing keys encrypted under the Public RSA Key embedded in the applet.
4. The server side application passes the packet of data created by the applet to the WSM where the MAC is checked, the PIN decrypted and re-encrypted under the Zone PIN Key (ZPK) for transfer to the Host system.
5. The WSM passes back the re-encrypted PIN Block (under the ZPK) and calculates a new MAC (using a Zone Authentication Key) over the data to be passed to the Host.
6. The Host passes the data string on to its HSM which first checks the MAC. The Host uses the HSM to verify the PIN as being the one for use against that particular account.
7. The HSM returns to the host an indication of whether the MAC and PIN passed verification. The Host will then pass back a suitable confirmation to the Web Server or Application Server which will action this in the session with the customer's browser.

The WebPIN^{TM} Security Module is based on the Thales HSM

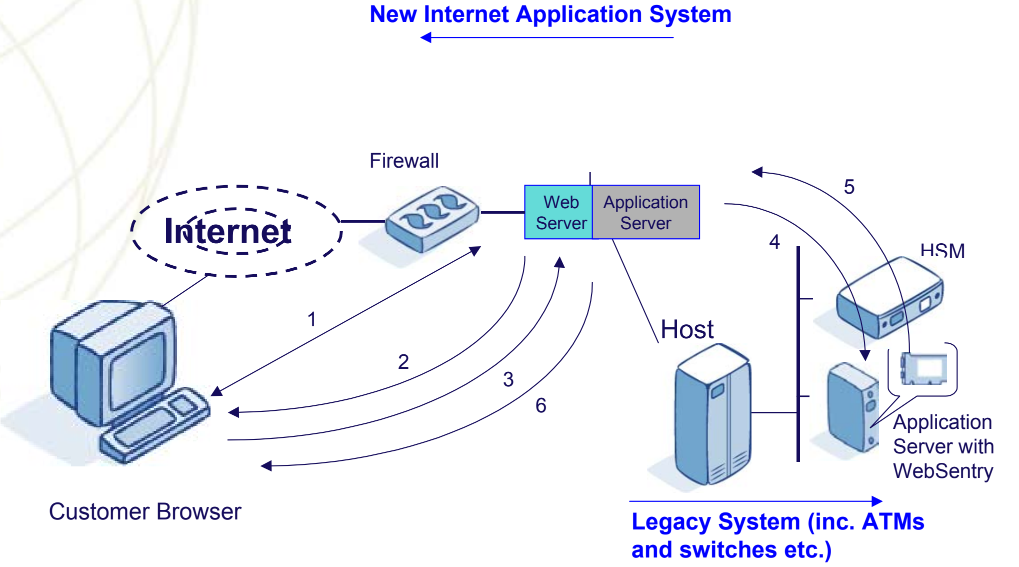
In the same way MACed messages are verified at the WSM, which may also be used to create a MAC over messages transmitted to the Host. In each case the WSM will return an indication to the application as to whether the MAC verified satisfactorily.

Since the WSM has access to the Private RSA Key used in the Applet it has a function that allows it to create Digital Signatures at the request of the application over data to be sent to the customer browser. At the Browser Web Page receiving this data a WebPIN enabled Applet is invoked which checks the signature using its Public RSA Key.

Example : Data Privacy Application

WebPIN Data Privacy Application

Shows message flow for end-to-end data privacy. Customer private data is kept secret through the system to its point of usage.


New Internet Application System
Firewall
Internet
Web Server
Application Server
5
4
HSM
1
2
3
6
Host
Application Server with WebSentry
Customer Browser
Legacy System (inc. ATMs and switches etc.)

In the second example WebPIN at the customer browser is interacting with an application and a WebSentry hardware security module installed at an Application server within the Bank's Host computer site. This configuration does not require the WSM and will probably use a different RSA Key pair from that used for an Applet operating with the WSM. Here the application has to handle details that the customer would like kept private, for example while applying for a Loan.

1. The customer opens an Internet session to the Bank's Web Server, which sets up an encrypted SSL session.
2. In the appropriate Web Page the WebPIN enabled applet is downloaded to the Browser, typically where the customer is being asked to provide private details in an on-line loan application.
3. Once the data has been collected from the customer the WebPIN enabled Applet encrypts the data using a randomly generated 3DES Key. This Key, encrypted under the WebSentry's Public RSA Key, is included in the message which is then submitted to the Web Server. If a ciphered reply is expected from the Host Application Server the 3DES key is also protected and reserved locally pending the arrival of the reply.
4. The Web Server passes the Ciphered data packet, complete with Key material, directly on to the Host Application Server. Here the response from the customer is decrypted by the WebSentry security module and returned to the Application.
5. If an encrypted reply to the customer is required this is submitted to the WebSentry security module which returns the cipher text. The application forwards the reply to the Web Server for onward transmission to the customer's browser.

When the reply arrives at the Customer's Browser the 3DES key is recovered from local storage and the Applet decrypts the data ready for displaying to the Customer.

WebSentry™ offers hardware cryptographic services supporting WebPIN's end-to-end data privacy functionality.

THALES

EUROPE, MIDDLE EAST, AFRICA
THALES e-SECURITY LTD.
Meadow View House
Long Crendon, Aylesbury
Buckinghamshire, HP18 9EQ, UK
Tel: +44 (0)1844 201800
Fax: +44 (0)1844 208550
e-mail: emea.sales@thales-esecurity.com

AMERICAS
THALES e-SECURITY, INC.
2200 N. Commerce Parkway
Suite 200
Weston, Florida 33326, USA
Tel: +1 888 744 4976
or: +1 954 888 6200
Fax: +1 954 888 6211
e-mail: americas.sales@thales-esecurity.com

ASIA PACIFIC
THALES e-SECURITY (ASIA) LTD.
Asia Pacific
Units 2205-06, 22/F Vicwood Plaza,
199 Des Voeux Road
Central, Hong Kong, PRC
Tel: +852 2815 8633
Fax: +852 2815 8141
e-mail: asia.sales@thales-esecurity.com

The Thales policy is one of continuous development and consequently the equipment may vary in detail from the description and specification in this publication.