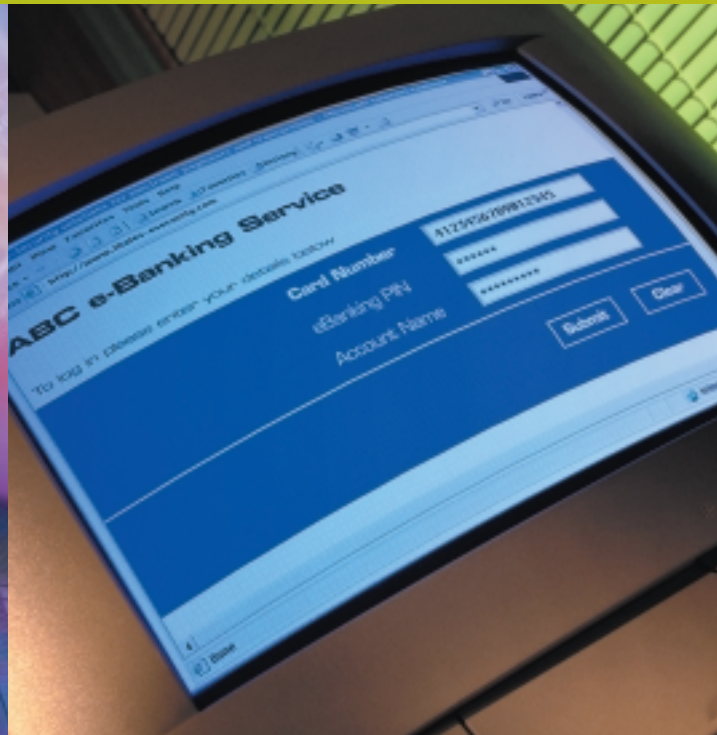




WebPIN™

Security for today's online transactions



- Solves SSL Security Weaknesses
- Bank Grade Security
- End-to-End, Thin Client, Solution
- Transparent to End User
- Cost Effective and Simple to Integrate



WebPIN™

WebPIN™ is a hardware and software solution, providing 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 then use the standard user authentication method (PIN) with which they are already familiar. The two main parts of WebPIN™ are a downloadable Java applet library and a Thales Hardware Security module.

The Problem

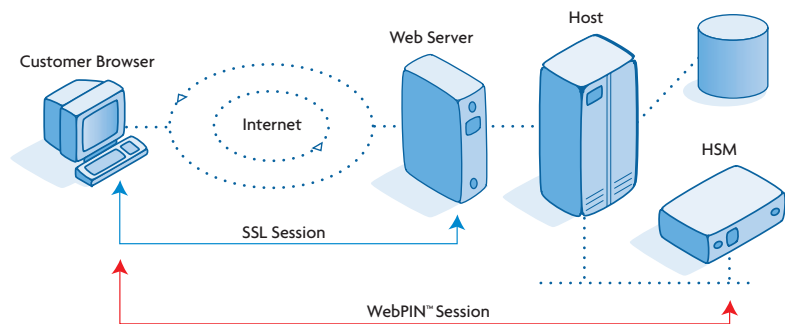
The use of Secure Sockets Layer (SSL) in sensitive banking and retail Web Sites is today commonplace. However, SSL is only designed to protect data in transit between the Browser and the Web Server and is unable to protect sensitive customer details once they have arrived at the Server. PINs and payment card details are therefore left stored in plain text on the server and are a prime target for criminals. WebPIN™ addresses these security weaknesses providing an end-to-end security envelope.

Benefits

- Capitalises on a Bank's existing investment in ATM and EFTPOS systems when implementing Internet Banking systems
- Protects sensitive customer data on the WebServer from disclosure
- Transparent to your Internet customers as there are no changes required in how they use the service
- Makes possible the offering of more and higher risk services which attract premium prices
- Cost effective solution that is easy to implement and manage

Features

- Java Applet technology downloaded from the Web Server with the Web Page
- PIN block encryption to banking standards with standard Message Authentication both using 112bit 3DES Keys
- 1024bit RSA key for key management
- Works within standard browser SSL to produce an End-to-End security session



WebPIN™, Security for today's online transactions

WebPIN™ offers End-to-End, strong, banking grade security for Internet based applications needing to execute secure transactions between a customer browser and the application server or backend processing systems. Security 'hot-spots' in the Web Server can be eliminated so that sensitive customer data is protected and is simply not available in clear text format to web site hackers or internal attackers.

Building on the standard SSL security available from all Web Server packages, WebPIN™ extends the security envelope seamlessly out to the customer. Designed for Home or Online Banking applications and retail online shopping payments WebPIN™ allows the customer to continue to use the same PIN authentication method with which they are familiar in face to face 'real world' transactions.

WebPIN™ Components

The WebPIN™ Security solution comprises several components from Thales e-Security working together seamlessly to produce a true end-to-end security envelope.

WebPIN™ Java Class Application Library Modules

WebPIN™ comprises 3 basic functional modules. The function calls available from these modules are compiled into a Java Applet, which is downloaded from the Web Server when called in the relevant web page.

WPProtect - The WPProtect module provides for PIN protection and basic message authentication using 3DES technology. The PINs are protected using industry standard techniques fully compatible with those used in Banking ATM (or ABM) Cash Machine networks.

WPTransact - The WPTransact module provides full 3DES message authentication facilities using industry standard MAC technology. Additionally this module provides for RSA based Digital Signature verification on messages sent to the customer's browser.

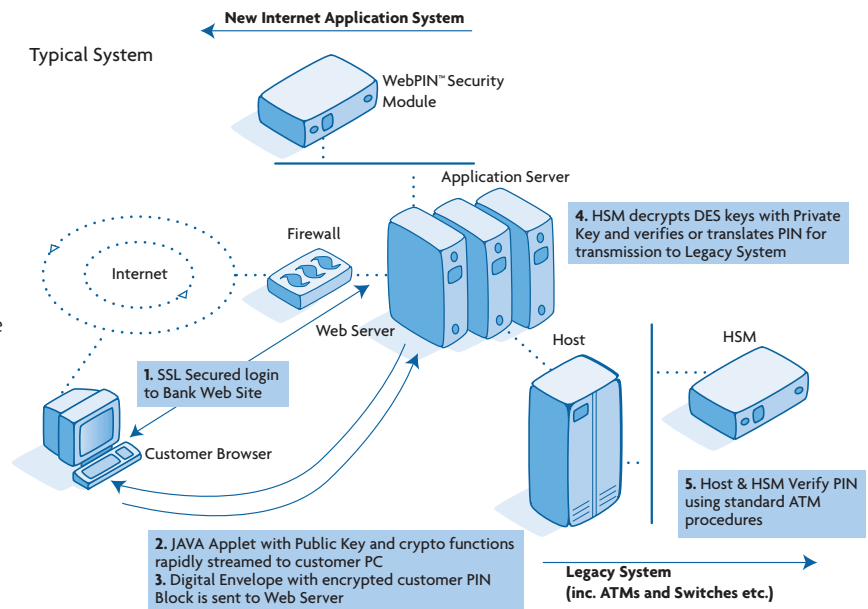
WPCrypto - The WPCrypto module provides full data encryption facilities using strong 3DES both from the customer browser to the host systems and from the host back to the browser.

WebPIN™ Security Module Support

Complementing the security provided in the WebPIN™ Java class and applet is functionality built in to Thales Hardware Security Modules. Typically a special Thales HSM (called a WebPIN™ Security Module) will be used at the Web Server for the protection and cryptographic translation of the cryptograms created by the applet. By translating the protected PIN Blocks from the 'Web Zone' to the 'Host Zone' the WebPIN™ Security Module allows standard banking ATM systems to carry out the PIN Verification for the transaction.

The WebPIN™ Applet functions are supported in the WebPIN™ Security Module by the addition of a special functional set and the installation of the appropriate RSA co-processor in a Thales HSM.

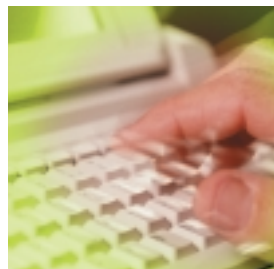
Where needed, in support of the use of a WPCrypto Java class module in the browser, a PCI or Ethernet connected WebSentry device may be deployed at the host application server for the data encryption and decryption tasks.



Case Study: Internet Banking

1. An Internet customer logs onto the bank web site and an SSL session is automatically established.
2. Java applet is automatically downloaded from the bank Web Server to the customer web browser, transforming the PC into a smart cryptographic machine.
3. The Java applet enables the PC to choose sensitive data requiring protection (i.e. PIN, credit card numbers, expiry date) Once the customer enters his/her PIN, it is encrypted and a MAC (message authentication code) complying with existing banking security standards is applied.
4. When the transaction arrives at the application server it is converted to appear like a PIN verification request from an ATM making it easy to handle at the Bank host.
5. At the Application Server, the transaction remains encrypted until the PIN has been verified at the bank's host by the Thales HSM, a secure processor used by the majority of financial institutions around the globe for transaction processing.

This whole process provides what is known as 'End-to-End Security'.





WebPIN™ – Technical Specifications

Java Class Specification

Applet is compliant with version 1.2.2 of the Java Development Kit (JDK).

Browser Compatibility

The WebPIN™ Java Class has been verified to work with Microsoft Internet Explorer versions 4.x and 5.x and with Netscape Communicator versions 4.x. and 6.x.

Web Server Compatibility

The applet is only stored on the Web Server ready for download to the client browser. The applet therefore may be used with any Web Server software capable of serving Java Applets.

WebPIN™ Security Module

These Ethernet connected hardware security modules support the cryptographic functions of the WebPIN™ Applet. DES and RSA processing are provided with support for DES keys to 112bits and RSA keys to 1024bits. Two variants providing different performance levels are available depending on anticipated transaction rates.

Compatibility with Thales WebSentry

The WebPIN™ Crypto Java Class Module is compatible with the RSA key management and 3DES data cipher operations of the WebSentry hardware security module range.

WebPIN™ Java Class Modules

PIN Block Protection (WPProtect)

Provides encoding to ANSI X9.8 format and ISO 9564-1 format 0 with support for PINs from 4 to 12 digits. Message Authentication (MAC) is to ANSI X9.19 and uses the ASCII character set. The 3DES encryption process used employs single use, randomly generated 112bit keys.

Message Authentication (WPTransact)

Provides Message Authentication (MAC) to ANSI X9.19 and uses the ASCII character set. The 3DES encryption process used employs single use, randomly generated 112bit keys.

RSA Signature Verification is also available using a 1024 bit Public Key and either a MD5 or SHA-1 hash.

Message and Data Encryption (WPCrypto)

Provides either ECB or CBC modes of encryption using 3DES with randomly generated 112 bit keys. Data is padded to the nearest 8 bytes using binary zero.

WebPIN™ Java Class Module Availability

WebPIN™ Base Module set

Any two of the above three Java Class modules.

WebPIN™ Optional Module

The third Java Class module from the above three not included in the Base Module set.



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-ecurity.com

Americas

THALES e-SECURITY, INC.
Sawgrass Technology Park
1601 North Harrison Parkway
Building A, Suite 100
Sunrise, FL 33323, USA
Tel: +1 888 744 4976
or: +1 954 846 4700
Fax: +1 954 846 3935
e-mail: americas.sales@
thales-ecurity.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-ecurity.com

www.thales-ecurity.com