ALBERTA efuturecentre

Secure E-Transactions

An initiative of:

10 YEARS of Service Excellence
THE BUSINESSLINK Business Service Centre

Funded by:

Western Economic Diversification Canada | Diversification de l'économie de l'Ouest Canada | Canada

ALBERTA efuturecentre

Enabling Technologies for Secure E-Transactions

Enabling technologies refer to the web-based platforms and programs upon which B2B and B2C web sites are constructed. While many business people may want to focus strictly on online selling and buying and leave the technical aspects to IT specialists, they still need to have a sound understanding of these key "under-the-hood" enabling technologies to better appreciate their full e-business potential and limitations. The technologies are encryption, Secure Sockets Layer (SSL), SET, and Smart Cards.

Encryption

Encryption is the process of making data unreadable to everyone except the receiver.

Encryption is the process of making data unreadable to everyone except the receiver.

The process has four key elements:

Authentication. This allows customers to be sure that the merchant they are sending their credit card details to is who they say they are. It can also allow merchants to verify that the customer is the real owner of the credit card.

Integrity. This ensures that a third party has not tampered with the messages during the transmission.

Non-repudiation. This prevents customers or merchants from denying they received or sent a particular message.

Privacy. This prevents third parties from reading intercepted messages. The main elements of an encryption system are the plaintext, the cryptographic algorithm, the key, and the ciphertext. The plaintext is the raw message or data that are to be encrypted. A cryptographic algorithm, or cipher, is a mathematical set of rules that defines how the plain text is to be combined with a key. The key is a string of digits. The ciphertext is the encrypted message.

Two main types of encryption are in common use today: secret-key and public-key encryption.

Secret-key. Secret-key encryption involves the use of a single key that is shared by both the sender and the receiver of the message. After creating the message, the sender encrypts it with their key and passes it to the recipient who then decrypts it by using a copy of the same key used to encrypt it. Secret-key encryption does have some limitations, particularly with regard to key distribution. For privacy to be maintained, every transmitter of messages would need to provide a different key to everyone
they intend to communicate with; otherwise, every potential recipient would be able to read all messages whether it was intended for them or not.
While this is manageable where a small number of parties are involved (for example, sending a private e-mail to a friend), it is not practical for web commerce which can involve communicating with thousands of customers. Another limitation with secret-key encryption is its inability to support non-repudiation. As both parties share the same key it is possible for one party to create a message with the shared secret key and falsely claim the other party had sent it. Secret-key encryption on its own, therefore, is not suitable for web commerce. Instead, a system known as public-key encryption is used.

Digital certificates provide the basis for secure electronic transactions.

Public-key. Public-key encryption involves the use of two keys: one that can be used to encrypt messages (the public key); and one that can be used to either encrypt them or decrypt them (the private key). These key pairs can be used in two different ways - to provide privacy or authentication. Privacy is ensured by encoding a message with the public key, because it can only be decoded by the holder of the private key. Authentication is achieved by encoding a message with the private key. Once the recipient has successfully decrypted it with the public key, she can be assured it was sent by the holder of the private key. Since the public key can be made widely available - for example, from a server or third party - public-key cryptography does not suffer from the same key distribution and management problems as the secret-key system.

One disadvantage of the public-key system is that it is relatively slow. Therefore, when it is being used only for authentication, it is not desirable to encrypt the whole message, particularly if it is a long one. To get around this, a digital signature is used. Digital signatures are implemented through public-key encryption and are used to verify the origin and contents of a message. The recipient of the digital signature can be sure that the message really
came from the sender. And because changing even one character in the message changes the message digest in an unpredictable way, the recipient can be sure that the message was not changed after the message digest was generated.

Authentication can be further strengthened by the use of digital certificates which involve a trusted third party or certificate authority (CA). Owners of public keys submit them to a CA along with proof of identity and the CA then digitally signs and issues a certificate which verifies that the public key attached to the certificate belongs to the party stated. Digital certificates provide the basis for secure electronic transactions as they enable all participants in a transaction to quickly and easily verify the identity of the other participants.

Secure Sockets Layer (SSL)

Netscape's Secure Sockets Layer (SSL) protocol is currently the most widely used method for performing secure transactions on the web and is supported by most web servers and clients, including Netscape Navigator and Microsoft Internet Explorer. The Secure Sockets Layer (SSL) protocol provides several features that make it particularly suitable for use in e-commerce transactions.

Privacy is guaranteed through encryption. Although information en route can still be intercepted by a third party, they will be unable to read them because they wouldn't have access to the encryption key. Integrity is also ensured through encryption. If information is received that will not decrypt properly, then the recipient knows that the information has been tampered with during transmission. Authentication is provided through digital certificates. Digital certificates provide the basis for secure electronic transactions as they enable all participants in a transaction to quickly and easily verify the identity of other participants.

A further advantage of SET is that the merchant has no access to credit card numbers.

Essentially, SSL is secret-key encryption, nested within public-key encryption, that is authenticated through the use of certificates. The reason that both secret key and public-key encryption methods are used is because of the relatively slow speed of public-key encryption compared to secret-key encryption. Initially, the client and server exchange public keys, and then the client generates a private encryption key that is used only for this transaction. This is referred to as a session key. The client then encrypts the session key with the server's public key and sends it to the server. Then for the rest of the transaction, the client and the server can use the session key for private-key encryption.

An SSL connection is initiated by the client (normally a web browser) by requesting that a document be sent through the HTTPS protocol, as opposed to the standard HTTP protocol.

This is done by simply prefixing the URL by "https" instead of "http". For example: http://server.domain.com/index.html. This requests the document index.html be sent through the standard HTTP protocol, while Secure Electronic Transactions (SET) requests that the same document be sent using the https protocol that incorporates SSL.

SET is the Secure Electronic Transactions protocol developed by Visa and MasterCard, specifically for enabling secure credit card transactions on the Internet. It uses digital certificates to ensure the identities of all parties involved in a purchase and encrypts credit card information before sending it across the Internet.

Like SSL, SET allows for the merchant's identity to be authenticated via digital certificates; however, SET also allows for the merchant to request user authentication through digital certificates. This makes it much more difficult for someone to use a stolen credit card. A further advantage of SET is that the merchant has no access to credit card numbers, and thus another source of fraud is eliminated.

There are many pilot schemes that use the SET protocol, but mainstream adoption has been slower than predicted. The main reasons behind this are the growing

acceptance of SSL for secure credit card transactions and the complexity and cost of the SET system.

In a typical SET transaction, there is private information between the customer and the merchant (such as the items being ordered) and other private information between the customer and the bank (such as the customer's credit card number). SET allows both kinds of private information to be included in a single, digitally signed transaction. Information intended for the bank is encrypted using the bank's public key while information for the merchant is encrypted with the merchant's public key. This means that the merchant has no access to the credit card details, which eliminates a source of fraud. In addition to this encryption, both sets of information are digitally signed. Finally these two signatures are combined to produce one signature that covers the whole transaction. While SET shows a lot of potential, it is not widely used.

Smart Cards

The potential for smart card use is enormous.

Although similar in appearance to a normal credit or debit card, smart cards differ in at least three key ways - they store much more data, are password protected, and incorporate a microprocessor that can perform processes such as encryption.

Although relatively unknown in North America, smart cards are by no means a new invention. Their use in Europe is widespread for applications such as credit cards, telephone payment cards and the payment of road tolls. France is the leading adopter, having started issuing cards in 1967, and now has some 25 million cards in circulation. However, their use is predicted to grow rapidly worldwide over the next few years on the back of the Internet, e-commerce explosion.

The potential for smart card use is enormous, but there are three key functions of interest to the web store merchant - storage of encryption keys, electronic purses, and user profile portability.

Storage of Encryption Keys

Smart cards can provide a very secure way of generating, storing, and using private keys. In its most basic implementation, smart cards can be used to store private keys

and digital certificates protected by a password. Security can be further enhanced by using a microprocessor within the card to generate the public and private key pairs and to perform the actual encryption. Data to be decrypted or digitally signed are passed to the card where the microprocessor performs the operation and then passes the data back to the computer. That way the key never leaves the card and is therefore not vulnerable to attack by rogue programs scanning the computer's memory for keys.

Electronic Purses

Many applications in place today use a smart card as a replacement for cash because of the higher security they offer over standard credit cards. Although most of these systems (for example, Mondex, VisaCash, CLIP and Proton) were developed for point-of-sale applications, their use is likely to extend to web commerce, because they provide an easy and secure way to handle cash transactions. Many individuals predict that smart card readers will become a standard component of PCs.

User Profile Portability

One factor that could potentially restrain the growth of web commerce is restricted access to the Internet.

One factor that could potentially restrain the growth of web commerce is restricted access to the Internet. Although the number of home and office computers with Internet access is continually growing, it is still not universally available and even the introduction of low-cost access devices (for example, Web TV) will not solve this completely. Also, even those with individuals with Internet enabled computers are unable to access them when away from their office or desk. Smart cards could provide an answer to this by providing secure access over public Internet terminals or screen phones. Personal profile
information could be stored on the card so no matter what device is being used, the appearance would be the same. The on-board microprocessor would be able to encrypt all messages, thus eliminating security risks.