



PKI Certificate Authority

CCRA Electronic Commerce Security FAQ



Table of Contents

<i>Table of Contents</i>	<i>ii</i>
1 Security Overview	1
1.1 What are the impacts to my personal privacy with electronic services?	1
1.2 What does “Security for Electronic Services” mean?	1
1.3 What security options will the CCRA use to reduce risks of electronically exchanging information?.....	1
1.4 What is a Shared Secret?.....	2
1.5 What are Personal Identification Numbers (PINs) and Passwords?	2
2 Security Fundamentals	3
2.1 How does encryption work?.....	3
2.1.1 What is Symmetric (or Single Key) Encryption?	3
2.1.2 What is Asymmetric (or Key Pair) Encryption?.....	3
2.2 What is the significance of key length?	3
2.3 What is a Hash?	3
2.4 What is a Digital Signature? How is it created? How is it used?.....	4
3 Security Implementations	5
3.1 How does a Shared Secret work?.....	5
3.2 What is Secure Sockets Layer (SSL)? How does it work?	5
3.3 What is a Public Key Infrastructure (PKI)? How does it work?.....	5
3.3.1 How a PKI protects a Message	6
3.4 What are the primary differences between PKI and SSL?.....	7
4 Implementing Electronic Commerce Security	8
4.1 As an employee why would I need a PKI?	Error! Bookmark not defined.
4.2 Why would Canadian businesses and/or individuals need Digital Certificates?....	8
4.3 What is the Government of Canada PKI - (GOC-PKI)?	8

1 Security Overview

1.1 What are the impacts to my personal privacy with electronic services?

Privacy is a major concern surrounding the electronic delivery of government services. Privacy concerns include the protection of information as it is transmitted electronically, the storage of sensitive information, and the consolidation of personal information in a central repository.

Information obtained via electronic channels will be subject to the same rigor and protection as that information obtained through other delivery channels (The Privacy Act, Access to Information Act, Archives Act). Bill C-6, once passed, will govern how information is shared not only by governments, but also by private enterprises. It also puts in law the term “digital signature” as an alternate equivalent to hand written signatures.

There are a number of mechanisms that are available to protect information as it is electronically transmitted. Typically, business needs dictate the level or degree of protection required. Below, we will discuss some of the different ways of ensuring the privacy of information sent electronically.

1.2 What does “Security for Electronic Services” mean?

When talking about electronic services and security, there are five requirements for electronic security:

- **Authentication**
The ability of an individual, organization, or device to prove its identity.
- **Authorization**
The control of access to particular information or privileges once identity has been established.
- **Confidentiality**
The secrecy of data and/or information, and the protection of such information from unauthorized access (i.e. the data is only viewable by the intended party).
- **Integrity**
The protection of data from modification either while in transit or in storage.
- **Non-Repudiation**
The protection against a party involved in a transaction or communication activity that later falsely denies that the activity occurred, that they were the participant, or that the message occurred when it did (i.e. the sender cannot claim they were not the originator of the message).

1.3 What security options will the CCRA use to reduce risks of electronically exchanging information?

Services offered electronically by the CCRA will use different mechanisms to protect information and systems including:

- **Secure Sockets Layer**
A network protocol that seamlessly encrypts data over unsecured networks.
- **Public Key Infrastructure**
A trusted security facility that employs digital certificates to provide a full set of security services.

Electronic Transactions can be secured through a variety of ways, depending on the degree of security required. The decision has to be made in determining the most appropriate solution for the business problem trying to be solved, and for the degree of security that is required.

1.4 What is a Shared Secret?

A shared secret is information that is ideally known only to two entities; a secret that each can reasonably expect only the other will know. It can be a password or a piece of personal information such as a social insurance number, or a parent's maiden name. Generally, shared secrets rely on several pieces of information that are used together to verify identity. The odds of an unauthorized individual knowing all of the pieces that comprise the shared secret are rare.

For example, if someone were to call the CCRA to inquire about their tax owing, they would be asked a series of questions that must be answered correctly. The questions are personal enough that the enquiries agent can be reasonably sure the caller is who they claim to be. If the caller cannot reasonably answer the questions, they will not be able to access any information surrounding the account.

1.5 What are Personal Identification Numbers (PINs) and Passwords?

Personal Identification Numbers (PINs) are numerical passwords. They are a series of numbers known only to the cardholder. They are frequently used to verify that the client is who they claim. A common usage of PIN security is using a bankcard to access an account at an ATM machine. When used in conjunction with the bankcard, the PIN allows the cardholder to access their account from ATMs, debit machines, and the like. Passwords can also be used in conjunction with user identification: verifying information the user provides against what the system already knows about the user.

Web Access Codes (WAC), the CCRA specific PINs, are used in conjunction with other personal information to allow an individual to access specific information electronically over the Internet.

2 Security Fundamentals

2.1 *How does encryption work?*

Encryption is the process of taking sensitive information and scrambling it so that the file is unreadable. Decryption is the reverse, taking unreadable data and transforming it into the original data.

There are two main forms of encryption, Single Key (or Symmetric) encryption, and Key Pair (Asymmetric) encryption.

2.1.1 What is Symmetric (or Single Key) Encryption?

Symmetric encryption uses a single piece of information (called a key) to perform the encryption-decryption processes. The sender would take the key (which is known by both parties) and encrypt the data by some process (this process is called the algorithm). The receiver, knowing the key and the algorithm, would take the message, reverse the process using the same key, and would get the original message. The strength of this process is that generally symmetric encryption algorithms are quite fast. The drawback is determining a means that both parties can know the key, without any other parties eavesdropping (the algorithm used is generally public information, and is generally not protected).

2.1.2 What is Asymmetric (or Key Pair) Encryption?

Asymmetric encryption works differently in that a user would have a key pair, one public and one private. These keys are carefully chosen so that a message encrypted with a public key could only be decrypted with the private key. So for example, the sender would locate the receiver's public key (they could even have it emailed to them, since it is public information), and use that to encrypt the message. The receiver would then decrypt the message with their private key. The advantage to this is that no sensitive key information was ever transmitted, so the eavesdropping threat is virtually eliminated. The drawbacks to this are the available set of key pairs are limited (there are still enough to make this process practical), plus asymmetric encryption algorithms are significantly slower.

2.2 *What is the significance of key length?*

The length of the key is important to prevent other parties from determining what was the key used to encrypt the data. Assume a computer existed that could check 1 billion possible keys per second. Doing a brute-force check (starting from zero and working up in order) of a 40bit key (key length is expressed in binary form), this computer could on average find the result in around 150 hours, or a bit over 6 days. A 56bit key on the same computer would take a bit longer, approximately 10008000 hours, which means 417 000 days, or 17 375 years. 128bit keys would take $5.04 \cdot 10^{24}$ years.

The trade-off is that while it will take a malicious user a significant amount of time to come up with a key, it will also take some time and resources for the intended parties to encrypt and later decrypt the data.

2.3 *What is a Hash?*

A hash function takes data of any length as input, and produces a digest or hash (hence the term) of a finite, usually 128 or 160 bits, in length. This hash is then used to represent (not replace) the original piece of data. A hash function can successfully represent the larger data if it has the following properties:

- Consistent
The same input file will always product the same output (i.e. hash).
- Unpredictable
Given a particular hash, it will be practically impossible to reverse the hash process and produce the original message.
- Volatile
This may seem like a contradiction with the first property, but it is essential that a slight change in the input message will produce a drastic change in the hash. This reduces the possibility of a change in one bit of the data being ignored by the hash function and producing the same hash.

An example of a hash is shown in the table below. Notice how the original input messages are quite different from the resulting hashes, plus how even a slight change in the input message produces a quite different hash. These hashes were generated using the Secure Hash Algorithm, as defined by NIST, the US National Institute of Standards and Technology (the de facto Hashing algorithm standard in the computing industry):

Message	Hash (using hexadecimal to represent the bits)
Today is November 01, 1999	5ABF9254 90626928 5DE857F9 50A46EFE 595ACC60 ₁₆
Today is November 02, 1999	10656678 351FCA2D 33FAA294 DB41589F 8B03A7FA ₁₆

2.4 What is a Digital Signature? How is it created? How is it used?

A digital signature is an electronic means of validating the integrity and authenticity of a given piece of data. For example, suppose someone received a document electronically. How does the receiver know if some third party corrupted the file? Even if encryption was used, the receiver needs to ensure that the file was not changed by any means. This is especially important when dealing with electronic commerce applications.

To create a digital signature, the sender takes the message and processes it with a hashing algorithm. The sender then encrypts this hash with their own private key, and delivers it along with the message. The receiver then takes the encrypted hash, and decrypts it with the sender's public key. Then the receiver takes the original message and runs it though the same hashing algorithm. If the two hashes are identical, then the receiver knows the message was not altered during transmission. And since the matching hash was derived from the encrypted private key of the sender, the receiver trusts that only the sender could have been the author of this message.

3 Security Implementations

3.1 How does a Shared Secret work?

When contact is initiated between the two parties, questions are asked to determine if each party is who they claim to be. For example, if someone were to call the CCRA to inquire about their tax owing, they would be asked a series of questions that must be answered correctly. The questions are personal enough that the enquiries agent can be reasonably sure the caller is who they claim to be. If the caller cannot reasonably answer the questions, they will not be able to access any information surrounding the account.

3.2 What is Secure Sockets Layer (SSL)? How does it work?

Secure Sockets Layer (SSL) is a security protocol that provides communications privacy over the Internet. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery. It is the security service most commonly used on the Internet to secure Web browser transactions.

When establishing a SSL connection, the client (generally a browser) and the server agree to a cryptographic algorithm, and then determine a unique key. The algorithm chosen will be the strongest algorithm with the largest possible key that both machines can operate. This is important because some machines may not have support for an acceptable algorithm, so the encryption used may not be as strong as required by law. The symmetric key is determined without the key actually being passed between the machines, so an eavesdropper will not see the key in any network traffic.

Once these parameters have been agreed to, a secure channel is created between the two machines. All of the client data is encrypted and sent over to the server machine through this channel. The server also responds through it, so there is no chance of an eavesdropper finding any sensitive information. Once the session is closed, the channel is broken, and the channel parameters are lost. The next time these two machines want to communicate, the algorithms and the key will be renegotiated.

As with most security options, there are several variations of SSL available. The safest version of SSL is generally regarded to be 128bit encryption. (Version 3 of SSL allows for the client to be authenticated via digital certificates). What is important to remember about SSL is that it enables the communication between two parties to be secured but not necessarily any attached files or records. As well, when using SSL, the security level is only as strong as the weakest link. If a client using 128 bit encryption on their browser dials up a site using 40 bit encryption, the lower level is the one that is used to encrypt the session between the two parties.

3.3 What is a Public Key Infrastructure (PKI)? How does it work?

A Public Key Infrastructure (PKI) is an automated key management system for the secure generation, maintenance, and delivery of encryption and digital signature keys. There are four main components of a PKI:

- Certificate Authority / Key Management System
The heart of a PKI is the Key Management System. Essentially, it is a trusted database that allows keys to be created and maintained.
- Public Directory Service
Where users go to locate public certificates. This is the most used piece of equipment in a security infrastructure.
- Client Software

How the users interface with the PKI. It is important that the client software be flexible enough to serve many uses (i.e. securing files, folders, email, real-time sessions, etc...), but be transparent enough so that users do not feel burdened by using secure products.

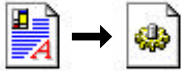




- Policies and Procedures

The most important part of implementing a PKI. In order for a PKI to work, there must be guidelines and rules that govern how the technology will be used. This is the most difficult and time-consuming portion of PKI, and must be constantly maintained so that it reflects the intended use of the resources.






The primary product of a PKI is a pair of digital certificates, one for encryption/decryption and the other for signing/verification. A certificate is important as it tells who authenticated the user and provided the certificate. These certificates contain information such as the name of the user owning the certificate (in PKI terms this is referred to as the Distinguished Name), the Authority who provided the certificate and the validity period of the certificate (all certificates will expire). A full PKI implementation will satisfy all five of the original security requirements.

3.3.1 How a PKI protects a Message

The following shows how a message is protected using a public key infrastructure:

- Hashing the Message
The original message has a hash created for it. 
- Encrypting the Hash
The sender will then use their private signing key, and encrypt the hash. This will be the digital signature of this message. 
- Encrypting the Message
The sender will then generate a unique symmetric key, and encrypt the message with this key. This key is only used for this session, and a new key will be generated for subsequent messages. 
- Protecting the Symmetric Key
The final processing is to protect the symmetric key, which uses the receiver's public encryption key. The sender will either have to retrieve this from the receiver's public directory, or have the recipient send it to them prior to the secure message being prepared. 
- Packaging the Message
The data being sent to the receiver looks nothing like the original message. Included in the final package is the digital signature, the encrypted message, the encrypted session key, and a copy of the digital signing key (the sender's public verification certificate). Also included are the hashing and encryption algorithms used. 

So now the message has been delivered to the intended receiver. They will now reverse the process to determine the original message and verify its authenticity.

- Determining the Encryption Key
The symmetric session key is unencrypted using the receiver's private decryption key. 
- Decrypting the Message
The receiver takes this unique key and decrypts the message. 
- Hashing the Message
The receiver then hashes the original message, just as the receiver did. 
- Unencrypted the Received Hash
The receiver then takes the enclosed public verification certificate, and decrypts the enclosed hash. 
- Comparison of the Hashes
The final step is to verify that the message was not altered in any way. The receiver will take the two hashes and compare them. If the hashes are identical then the receiver is satisfied that the message has not been altered. If not, then the user has no reason to trust the authenticity of this message. 

3.4 What are the primary differences between PKI and SSL?

There are various differences between these levels of security. Both PKI and SSL can be used to protect session information but how they do so differs. A PKI is more difficult to implement, but the result is a more useful and flexible security infrastructure.

SSL only uses a single key pair for its authenticity. So, for example, the sender encrypts a message for the receiver using the receiver's public key, and signs the message using their own private key. The receiver then decrypts the message with their own private key, and retrieves the sender's public key to verify the message. Using only one key pair reduces the complexity of the system, but it greatly enhances the opportunity for the keys to be compromised. Another drawback is the inflexibility of the SSL architecture. It cannot be used to protect files, folders, or email messages. It can be used in conjunction with other types of security options such as shared secrets, PINs, WACs, etc.

Whether or not to use SSL or PKI is fundamentally a business decision based on the needs and risk assessment of the organization. It is entirely conceivable that an organization will choose a combination of security protocols for different aspects of its business. For more information on choosing the right solution, please contact your IT Security Officer.

4 Implementing Electronic Commerce Security

4.1 Why would Canadian businesses and/or individuals need Digital Certificates?

Frequent transactions with the federal government involving confidential or sensitive information could warrant the use of PKI. Those businesses or individuals who interact with the government could regularly save time and money by not having to continually re-authenticate themselves to government. A certificate would assure both parties that each was who they claimed to be, thus avoiding the need to re-authenticate each other by re-keying historical information every time a transaction was initiated. PKI could save the federal government money if each program conducting Electronic Commerce / Electronic Service Delivery could share the cost of authenticating common clients.

Currently, the business case for providing PKI on a large scale is under consideration by the federal government. The CCRA is providing input into this process.

4.2 What is the Government of Canada PKI - (GOC-PKI)?

The Government of Canada PKI is the infrastructure that integrates other technologies (i.e., Electronic Authorization and Authentication, smart cards, etc.) into a seamless solution for secure departmental information management and electronic commerce (whether internal or external to government). The Government of Canada PKI will provide a uniform key management and key certification process for confidentiality and digital signatures across the government. PKI enables an organization to effectively manage large volumes of digital signatures.

The Policy Management Authority (PMA) is an interdepartmental committee chaired by the Treasury Board Secretariat. It will approve the policies and practices that Certificate Authorities use in issuing certificates. Currently some departments and agencies are using PKI technology and establishing certification authorities to support electronic commerce and security applications.