Understanding Public Key Infrastructure and Digital Certificates

Farhad Hussain
Technical Specialist at the
Leveraging ICT for Growth Employment and Governance Project under Bangladesh Computer Council

Information security is the major issue for enterprises and governments today. The Internet creates business opportunities, but it also leaves organizations open to security breaches and attacks from viruses, hackers and cyber criminals. The danger comes as often from inside an organization as it does from external sources, for example, from unauthorized access to confidential personnel or customer data, employee misuse or a genuine mistake. Digital Certificates and public key cryptography are emerging as the preferred enablers of strong information security. Many large organizations will deploy public key cryptography and certificates throughout the company in the next few years. Public key cryptography requires a Public Key Infrastructure (PKI), which is a combination of technologies, services and policies for managing digital certificates and encryption keys for people, programs and systems. The principal business issues that a security system needs are the following:

Authentication and authorization; Systems need to identify who and what can gain access, what information they can read or modify, and when and from where that access can be gained.

Privacy/confidentiality; Systems must guarantee that only the intended recipient should be able to see the content of a message.

Examples of PKI Schemes

- * *Italian companies are required to use online reporting and approved digital certificates for change of registration and annual reports; 2.4million certificates are on issue in Italy and used regularly.*
- * *In Taiwan, online gaming subscriptions are controlled using the "Play Safe" PKI card, issued so far to 100,000 users and expected to grow to 5 million.*
- * *Taiwan's National Health Insurance smartcard issued to 22 million citizens is PKI capable; separately, some 340,000 cards and digital certificates have been issued to Taiwanese healthcare professionals.*
- * *The Pan Asia e-commerce Alliance (PAA) oversees nine commercial CAs with 260,000 digital certificates on issue for online trade documentation between Hong Kong, China, Chinese Taipei, Korea, and others.*
- * *Electronic passport chips in the new International Civil Aviation Organization (ICAO) scheme are digitally signed; the system is said to be upgradeable to include personal certificates for passport holders.*
- * *Johnson & Johnson has issued certificates on USB keys to over 100,000 employees for secure e-mail, remote access and e-commerce.*
- * *The credit card companies' new "3D secure" payment protocol is based on digital certificates.*
- * *In Japan, PKI based residential cards are issued by prefectures for government to citizen (G2C) transactions; numbers are estimated as at least 300,000.*
- * *The authority of Taiwan offers a personal digital certificate card for G2C transactions, taken up by nearly 1,000,000 citizens so far; smartcard readers are available at convenience stores for US$10 each.*
- * *In Korea, the six largest banks have issued 10 million certificates between them for Internet banking.*
- * *Hong Kong Post has issued 4 million certificates to date, some on USB keys, and some on the SMARTICS id card.*

Integrity; Systems should provide assurance that messages have not been altered in transit.

Non-repudiation; Messages should be traceable from source and have secure audit trails to prevent parties to a transaction later denying their participation.

Ease of use; Security systems need to be consistently implemented across an organization without unduly restricting the ability of individuals to go about their daily business.

Digital certificates and Public Key Infrastructure are designed to replicate and improve upon the mechanisms used to ensure security in the physical world. For example, digital certificates act as the online equivalent of passports, ID cards, and driving licenses. They are credentials that prove the identities of organizations and individuals and provide the framework of trust that is needed for secure online commerce and communications.

Digital Certificate is the electronic counterpart to a passport, driving license, or membership card. It is a credential, issued by a trusted authority that individuals or organizations can present electronically to prove their identity or their right to access information. Digital certificates enable the holder to digitally sign and also encrypt documents online. When a trusted entity issues a digital certificate, it verifies that the owner is not claiming a false identity, just as a government issuing a passport officially vouches for the identity of the holder.

Public Key Infrastructure (PKI) is a group of technologies, services and policies required to issue and manage digital certificates. The main components of a PKI are:

Certificate Authority (CA) is an entity that signs and issues a unique digital certificate to a requester, upon receiving authorization from the Registration Authority.

Registration Authority (RA) validates identities and their rights to receive certificates.

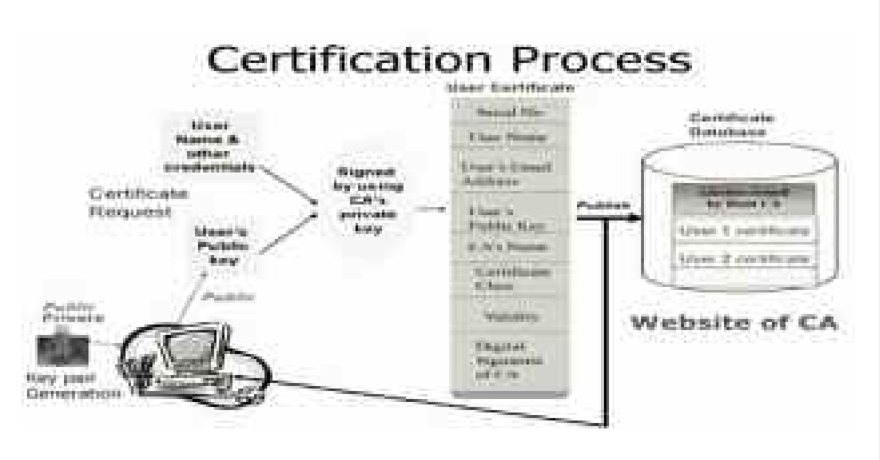
Certification Practice Statement

(CPS) is a published code of practice that governs the issuance and use of certificates to which anyone that relies on that certificate can refer.

Certificate Validation is a process by which an individual or web application confirms that a certificate is valid and has not been revoked (cancelled).

The Repository for keys, certificates and Certificate Revocation Lists (CRLs).

Digital certificates are in essence messages indicating that a public key belongs to a particular person or entity. Digital certificates are themselves digital signatures as a CA uses its private key to validate the message. A CA in turn can be validated by a higher CA, thus creating a certificate chain. Hence, the trustworthiness of a CA may depend on its reputation in traditional business transactions, or, it may be a subscriber of a higher CA, and use the certificate of the higher CA to reassure subscribers and relying parties that it is not a bogus CA. The CA at the pinnacle of the CA hierarchy is known as root-CA and it issues root certificates. The root-CA self-authenticates for purposes of determining the validity of the certificates. The figure below illustrates the certification process:



PKI is emerging literally as the key to safe access to online services. It is remarkable that almost all national identity cards that have been recently announced around the world are PKI capable smartcards. Governments of many countries including the Government of Bangladesh are planning for increased use of digital certificates to secure their transactions with their citizens. Here are some noteworthy examples of contemporary PKI schemes:

The best way to consolidate our understanding of PKI is to examine typical case studies of companies that have deployed a PKI solution. Here we examine how XYZ Inc. has decided to implement a PKI solution to meet its business requirements. XYZ Inc. is a US based retail chain that has over 200 retailer outlets across the United States. The retailer has revenues of over $200 million. However, the revenues have not grown substantially in the last two quarters. The retailer attributes this lack of growth to market saturation and competition from another retail chain that has taken over major market share from the areas that the retailer had plans to explore. To boost its revenues, XYZ Inc. plans to increase its customer base in Asia-Pacific and Europe and has estimated a growth rate of 1.5 percent in the next three consecutive quarters if it ventures into these areas. To accomplish this XYZ Inc. has decided to implement a PKI based solution.

The company plans to establish a corporate office in the United States that will be a central location for managing all the other offices of the company. A number of regional offices will fall under the direct purview of the corporate office. The regional offices will be catering to the business requirements of broad geographical locations. Each regional office will have a number of distribution offices in its purview. The scope of distribution offices will be limited to a more specific region than the regional office. Keeping in mind the hierarchy of XYZ, Inc., the project manager responsible for implementing PKI at XYZ, Inc., has decided to implement a hierarchical PKI architecture. The corporate office in the United States will be the root-CA, which will be responsible for:

Issuing certificates to the regional head offices that fall under its direct purview.

Creating policies for the regional offices.

Acting as the Policy Approval Authority (PAA). As the PAA, corporate office would have the last say in the policies related to issue of certificates.

Considering the vast geographical spread of the company and huge number of distributors and customers, the root-CA will not be able to handle all the certification requests. Therefore, each regional office would act as a second-level CA. The region-level CA cannot accept direct certification requests. Therefore, any certificate request must be routed through a RA, which is responsible for:

Issuing certificates on receiving certificate requests from RAs.

Zonal offices will act as the RAs that forward the certificate requests to the corresponding regional office.

Distribution centers also would act as an RA and route certificate requests to the zonal office, which in turn will route these requests to the regional office.

The hierarchical PKI architecture at XYZ, Inc. will address issues of not only scalability and ease of deployment but also that of a short certification path. Hierarchical PKIs are quite scalable, and to meet the needs of a growing organization such as XYZ, Inc., the root-CA simply needs to establish a trust relationship with the CAs of the entities. In addition, being uni-directional, the hierarchical PKI architecture is quite easy to deploy. The path for the entity to the root or the issuer CA can be determined quickly and easily, and the biggest path in the PKI is equivalent to the CA certificate for each subordinate CA plus the end entity's certificate.

The company plans to make its distribution offices the hub of all transactions with its customers. Each distribution office will register distributors that will be responsible for promoting the company products in the market. The distributors will not be regular employees on the company payroll. When a distributor approaches a distribution center, he or she must fill in a registration form. The distribution center then forwards the form to the Distribution Manager (DM). In this manner, the distribution centers act as the first level of check where the identity of the distributors is verified. The DM verifies the information supplied and forwards the form further to the controlling RA. Each RA then verifies the authenticity of the information supplied in the form.

When the RAs at the distribution and zonal levels are sure about the

▶

information, the information is forwarded to the country-level CA. The country-level CA then issues a certificate to the distributor and signs the certificate with its private key. The corresponding public key of the certificate is stored on the certificate server. The CA dispatches the certificate to the RA, which in turn forwards the certificate to the next level. The certificate is forwarded to the next level, until it reaches the distributor who applied for it. In order to keep a firm control on the inter-region transactions, the top management have also decided that any inter-region transaction must be routed through the root CA (i.e., the corporate headquarter). For example, a distributor in UK urgently needs to acquire a product. At the given point of time, the product is available only in the Malaysian inventory. Instead of buying the product and investing money unnecessarily into the acquisition of the given product, it makes sense if the company transfers the required amount of product into the inventory of the UK.

As per this scenario, the region-level CAs cannot issue certificates to each other and neither can they validate each other. As a result, for every inter-region transaction the certificate would be issued by the root-level CA, the corporate head office. When the root-level CA issues a certificate to the two concerned regional offices, it must also validate the entire chain from the requesting distributor to the supplier distribution center. The interaction with the distributor will be such that each distributor can place its order at the corporate office directly by its Website. This will ensure that the distributor need not wait for the order to be routed through the three levels of company hierarchy, thereby saving time for the procurement of the inventory. The Website will be an important entity in the procurement chain and the failure of the site can cause extensive loss to the company.

To impart maximum security, the company has decided to enable its Website with Secure Socket Layer (SSL) technology, which establishes an encrypted link between a web server and a browser and ensures that all data passed between the web server and browsers remain private and integral. To ensure that only authorized transactions happen on the Website, the company will issue digital certificates to all its distributors. It will also issue digital certificates to all its employees at the regional offices and the distribution offices because these offices will be connected through the Internet and the authentication will be based on digital certificates. The company plans to make this Website available only to its employees and distributors. If a retailer wants to find information about the company and register as a distributor, the retailer can access the promotional Website of the company that has the details of schemes and benefits available to a distributor. The Website also enables a distributor to find a distribution center that is nearest to the distributor's geographical location. Let us now examine a workflow from the registration of a prospective distributor to the transactions made by the distributor. A prospective distributor comes to know about XYZ Inc. by their promotional Website. By using the promotional Website, the distributor examines the policies of the company and locates a distribution point that is closest to its location. The distributor approaches the distribution point and fills the registration form. The distributor then generates a public key/private key pair for itself. The distribution point implements the first level of checks to assure itself of the identity of the distributor. The form is forwarded to the DM, who submits it to the RA. The RA examines the form and verifies the authenticity of the applicant. When the RA is sure that the request for membership is genuine, it forwards the request to the CA.

The CA issues a certificate to the distributor and signs the certificate with its private key. The public key of the certificate is stored on the certificate server. The CA dispatches the certificate to the RA. The RA, in turn, sends the certificate to the concerned DM, who hands over the certificate to the distributor. The distributor is now registered with the company. The company employees also need certificates for secure communication. The company employees need secure communication because, apart from other transactions, they need to update the company databases at the corporate office with the sales revenue that has been generated by each distributor. Certificates are generated for new employees that join the company in the same way as they are generated for distributors. The only difference is that the employees do not need to go through the elaborate verification round. They can directly send their requests to the RAs who, in turn, forward the requests to the CA.

After the certificate is issued to the distributor, the distributor is able to place orders on the corporate Website. Let us examine the processes involved when a distributor places an order on the Website. After the distributor obtains the certificate, it is then installed in the Web browser. When a user begins a session on the corporate server, the following interactions take place:

The client sends information to the server, such as its SSL version number, cipher configuration information, and other information, which the server requires to communicate with the client using SSL.

The server in turn also sends the server's SSL version number, cipher settings, and other information, which the client needs to communicate with the server. In addition the server sends also its own certificate. If a situation arises that the client is accessing the resource, which needs to be authenticated, the server asks the client for its client's certificate.

The client uses the information provided by the server to authenticate the server. For any reason, if the server is not authenticated, the client is warned about the ambiguous server and prompted that a secured connection cannot be established. If the server is authenticated successfully, the client can move ahead to establish a SSL session.

Based on the encryption algorithm, the client creates a pre-master secret for the SSL session. This pre-master secret is encrypted by using the public key of the server and then sent to the server.

If the server requires client authentication, it requests a client certificate. The client signs a fresh piece of data that is unique to this handshake and sends it to the server. Both the client and the server know this data. In addition to the signed data, the client also sends its own certificate to the server along with the pre-master secret.

If the server is not able to authenticate the client, the server terminates the session. If the client is authenticated successfully the server uses its private key to decrypt the pre-master secret and generates a master secret.

Both the client and the server use the master secret to generate session keys. The session key is a symmetric key, which is used to encrypt and decrypt the data that is transferred over the SSL session.

The client informs the server that all the future communications initiating from the client will be encrypted using the session key, then the clients sends the confirmation separately that the client's portion of the handshake is over.

The server also responds to the

client, informing the client that all the future messages from the server would be encrypted with a session key. Like the client the server also sends a separate message confirming that the handshake is over.

At this stage the SSL handshake is complete and the SSL session has begun. Both the client and the server use the session keys to encrypt and decrypt the data they transmit to each other, to validate its integrity.

After the session key is available at the server, the distributor can send data to the server in the form of messages. The message that the distributor needs to send to the server is hashed and encrypted with the private key of the distributor to generate the digital signature.

The digital signature and the message are further encrypted by the session key and sent to the server.

On the server, the session key is used to decrypt the data that is transmitted from the client. The data is decrypted to retrieve a message and a digital signature.

The message is hashed to obtain a message digest. The digital signature is also decrypted with the public key of the client to obtain a message digest.

If the two message digests are identical, the server is sure of the authentication of the data and the transaction is carried out.

XYZ, Inc. has been able to obtain many advantages by deploying a PKI solution. The solution has enabled the company to meet its business requirements effectively. Let us examine how the company has benefited from the PKI solution.

When a distributor enrolls as a member of the company, the two levels of security validations at the DM and the RA levels enable the company to assure itself that the request is genuine. This has ensured that the company is able to provide quality service to its indirect customers.

The company is able to ensure the identity of the distributor each time the distributor transacts on the Website. Even the distributor cannot deny having made the transaction. Thus, transactions are non-repudiated.

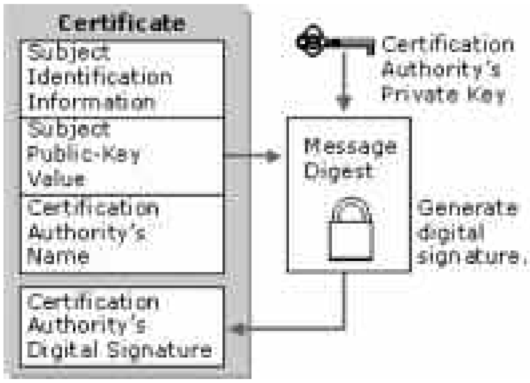
When the distributor shops on the Website, the geographical location of the distributor is determined on the basis of the information obtained when the distributor was issued the certificate. The catalog of products available for the user is filtered accordingly. Therefore, the problem of filtering inventory for different destinations is automatically taken care of.

Employees, at the end of everyday's transactions, update the revenue generated from distributors in the databases at corporate office. The employees are also issued digital certificates for this. Therefore, the transactions across the company network are absolutely secure.

If a distributor does not abide by the company norms or abdicates his or her membership, the certificate issued to the distributor is revoked. Each time the certificate is revoked, the CRL is updated. Therefore, the next time a former distributor attempts to make a transaction, the server checks the CRL, and the transaction is canceled.

The above mentioned point is also applicable for the company employees. Therefore, company employees are also not able to misuse their privileges.

Certificates of distributors are renewed every year. Each time a certificate is renewed, the company has a chance to audit the distributors for compliance to company regulations. Thus, the company is able to maintain a high standard of service to its customers.


Certificate
Subject Identification Information
Subject Public-Key Value
Certification Authority's Name
Certification Authority's Digital Signature
Certification Authority's Private Key
Message Digest
Generate digital signature

Let us now examine the security requirement of XYZ, Inc. during communication, especially when the communication happens at the upper echelon of the company. XYZ will deploy a Pretty Good Privacy (PGP) solution to ensure the confidentiality and integrity of e-mails being exchanged by the top managers of the company. The regional heads of all the regions need to be in constant touch with each other. This is highly important, because:

They always must have an up to date knowledge of the inventory levels in each other's region. This is important because if a region requires a product or some products urgently, time must not be wasted in search and subsequent relocation of the product.

They also must have an up to date knowledge of inter-region resource allocation. This helps the regional heads to accommodate movement of resources, infrastructure, and employees.

Apart from the day to day transactions, extremely confidential company data must also be exchanged between regions. Also, the senior management at the corporate headquarters must be kept informed about the latest happenings including the confidential data. Because of the vast expanse of the company globally, e-mail has emerged as the primary method of communication. However, the company wants the method to offer a high degree of security. There would be no compromise on this score. After a lot of research, the technical support team at the corporate headquarters has arrived at the conclusion that Pretty Good Privacy (PGP) is the best solution in the given situation. PGP is one of the well known public key crypto systems that provides services like authentication and confidentiality and is typically used in securing e-mail messages over the Internet. PGP is one of the most powerful encryption techniques being used today as it makes use of some of the best known cryptographic algorithms used in PKI. Therefore, PGP has gained huge popularity in little time and is now being used by masses worldwide.

The company directors have decided to implement PGP for encrypting their e-mail messages. By deploying this solution, the directors are able to communicate securely. For example, if the director of the UK region needs to send a secure message to the director of the Malaysian region, he can install the PGP client and encrypt it with his private key. For encrypting the message, he can use the PGP menu while composing the mail message. When the encrypted message reaches the director of Malaysia, the director is able to decrypt the message by using the passphrase of the private key. While implementing PKI, the project manager, warrants that every employee of XYZ, Inc. familiarizes himself with the Digital Signatures Act, which lays down the directives for digital signatures.

Through this case study we have examined how a company might implement a PKI solution to meet its business requirements. We have illustrated the role of PKI in enabling secure transactions and attempted to offer some insights into how you might deploy a PKI solution in your organization ◙