Basics of Cryptography & Digital Certificates

Trusted Internet Services from VeriSign and SafeScrypt.

Introduction :

The solution to problems of identification, authentication, and privacy in computer-based systems lies in the field of cryptography. Because of the non-physical nature of the medium, traditional methods of physically marking the media with a seal or signature (for various business and legal purposes) are useless. Rather, some mark must be coded into the information itself in order to identify the source, authenticate the contents, and provide privacy against eavesdroppers. This white paper discusses the various security challenges for electronic communication and how PKI provides a solution to them all.

Challenges for Security :

The various challenges for security in e-commerce have been listed below. They are popularly know as the five pillars of e-commerce.

i. Confidentiality
ii. Authentication
iii. Integrity
iv. Non-repudiation
v. Interoperability / Universality

i. Confidentiality

You want to be sure the information you are sending, such as credit card information when purchasing goods online, or sensitive business information in e-mail can't be read by anyone other than the intended recipient.

ii. Integrity

You want to make sure no one has intercepted information and changed it in any way. So tampering of the information by anybody should be difficult and evident.

iii. Authentication

You want to be able to check on the identity of users. For example, you wouldn't want a competitor to download your company information from an Extranet, or in the case of a very large financial transaction, you want to feel certain of who placed

the order. As a user, you also want to be certain if you are buying goods from an online store, that the store is legitimate, that you'll actually get the goods you are paying for - -you're not just providing a credit card number with which someone can go on a shopping spree.

iv. Non-repudiation

In the real world, a contract with a written signature is generally binding. There is no real equivalent on the Internet. Someone might buy some stock over the Internet, the price falls, and then they say they never placed the order. There isn't a way to sign a contract electronically except with a certificate.

v. **Interoperability**

Finally, whatever solution you have needs to be interoperable and universal, because the benefits of this model is that everyone can work together and share information across the network transparently. The adoption of standards by Internet vendors has provided this interoperability.

Only digital certificates can provide all of the above.

	PKI	**Passwords**
Authentication	Yes	Yes
Confidentiality	Yes	No
Integrity	Yes	No
Non-repudiation	Yes	No
Enabled in standard apps	Yes	Yes
Proven technology	Yes	Yes
Standards-based	Yes	Yes
Shared identity across apps	Yes	No

Comparison with Password based system

Authentication: While passwords provide authentication, there are security problems. About 20% of people use "bad" passwords, that is passwords that would easily be guessed, your maiden name, your child's name, birthdate etc.. How many of you are guilty? And if you use different passwords, how many of you write it down somewhere on a yellow sticky and place it under your keyboard or mousepad? How many of you use the same password across multiple applications? Once one application is compromised, now all the other applications using the same password are compromised.

Integrity, confidentiality and non-repudiation: Passwords do nothing to prevent the tampering of information, nor do they provide confidentiality; they can't encrypt data. And as we talked about before, passwords are not sufficient to replace written signatures and don't provide non-repudiation.

Shared identity: Passwords don't provide any unique identity information across applications.

History of Cryptography and PKI :

Single Key Cryptography

- Bob has one secret key
- If Alice wants to send Bob a secret message
- Bob Sends Alice a copy of his secret key
- Alice encrypts message with Bob's secret key
- Bob decrypts message with his secret key

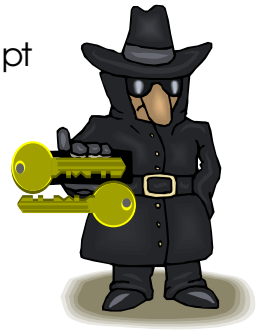
Single key cryptography is where you use the SAME "key" (think of this as a mathematical formula) to both encrypt and decrypt data. This is the kind of cryptography used in WW-II, where code was "cracked" by the enemy so confidential information about troop movements could be gathered.

Problems:
How does Bob get secret key to Alice?
What if Alice is a double agent?
What if Alice, Bob, Charley, & Dan. need to exchange messages? Need n! keys

With single-key cryptography you have the problems of how to share the secret key -- how does Bob get the secret key to Alice safely, and of managing a large number of secret keys.
If too many people share the same secret key, then if even one of them is bad, a mole, all messages are compromised. Or, if Alice, Bob and Charlie all share the same secret key, Bob could claim that Charlie really sent the message. So to avoid this, say all of us want to communicate confidentially and there are about 20 of us in this room, we would have to manage 20 factorial keys -- this is a very very large number.

A Better method : Public Key Cryptography

- Bob has two complimentary keys
- What one key encrypts, only the other key can decrypt
- Bob keeps one key private (Private Key)
- Bob shares the other key (Public Key)
- If Alice needs to send Bob a message
- Bob sends Alice a copy of his Public Key
- Alice encrypts message with Bob's public key
- Bob decrypts message with his private key



Public key cryptography solves these problems. Everyone gets just one unique "key pair", consisting of a PRIVATE key that is kept safe and a PUBLIC key that can be shared freely. What one key does, the other can undo. The analogy might be that you use one key to unlock the safe and put things in the safe, but you need the other key to unlock it to remove its contents. Because anyone can get a copy of the public key, the distribution problem becomes a non-issue.

Some examples of how this works. Bob creates a digital signature attached to his e-mail message using his private key. The recipients know it really came from Bob because only he could have signed it with his private key (since it is never shared or distributed to anyone else).
Or, for sending encrypted e-mail, Bob can give Alice his public key which she uses to encrypt a personal e-mail message she sends to Bob. Bob uses his private key to decrypt and read it. Anyone can use Bob's public key to encrypt a message to Bob, and feel confident that only Bob can read it because only he has the private key.

Advantages:
- Bob can distribute public key freely
- If Alice is a double agent, she can't do any harm with Bob's public key
- Bob only needs one key pair, no matter how many people he speaks to
- Bob can digitally "sign" messages, by encrypting with his private key

Bob can share his public key with as many people as he likes. It doesn't matter what Alice does with it even if she is a mole. It's only good for encrypting e-mail sent to Bob and only Bob can read it.
So in a room of 20 people, you only need 20 key pairs (not 20 factorial keys) one for each person, and everyone can communicate with everyone else. This solves the key management problem.

Problem:
- How does Alice really know that she is using Bob's public key

But this leaves us with one remaining problem. How does Alice know she really is using Bob's public key and it isn't someone pretending to be Bob?

This is where a Certificate Authority or CA comes into the picture. VeriSign and SafeScrypt as its Principal affiliate for India are CAs. Just as we trust a passport office to issue your passport, or VISA to issue credit cards after doing the appropriate level of identity checking, a certificate authority is a trusted third party that issues digital certificates and guarantees that the public key really belongs to a specific person or entity. That's what VeriSign / SafeScrypt does.

Certificate Authority is a trusted third party similar to Passport Office, CPA
Certificate Authorities issue digital certificates.

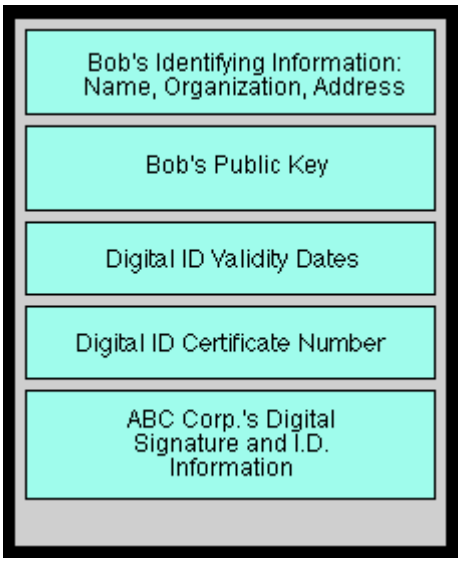
A certificate contains the following:
- Bob's public key
- Bob's name, address, other info
- Expiration date & serial number
- The certificate authority's name, etc.

A digital certificate is "signed" with the Certificate Authority's private key, to ensure authenticity and everyone has CA's public key

Digital Certificates :

Digital Certificates or Digital ID is a kind of digital "passport" or "credential." The Digital ID is the user's Public Key that has itself been "digitally signed" by someone trusted to do so, such as a CA or VeriSign, Inc. The following figure presents a pictorial description of a Digital ID.

Every time someone sends a message, they attach their Digital ID. The recipient of the message first uses the Digital ID to verify that the author's Public Key is authentic, then uses that Public Key to verify the message itself. This way, only one Public Key, that of the certifying authority, has to be centrally stored or widely publicized, since then everyone else can simply transmit their Public Key and valid Digital ID with their messages.



Using Digital IDs, an authentication chain can be established that corresponds to an organizational hierarchy, allowing for convenient Public Key registration and certification in a distributed environment.

Procedure for Secure Electronic Transaction :

- Before sending a secret message--ask to see the other party's certificate--extract their public key
- When signing a document-encrypt using your private key, and send encrypted document plus your certificate
- Before trusting a document, verify signature using the sender's certificate
- Before doing anything with a certificate, be sure you trust the Certificate Authority who issued it

In summary, for electronic transactions or communications, you can check the recipient's public key so you know who you are really sending a message to. Then you can digitally sign your document or message with your private key and send your certificate with it. The recipient can then check your certificate to be sure the message really came from you.

And it is important of course that you trust the CA who issued the certificate, just as we trust VISA or the passport office. The advantage of having a certificate that chains up to VeriSign is that all the latest browsers will automatically recognize and trust VeriSign or VeriSign Trust Network certificates.

In this way using Digital Certificates all the challenges of Security for e-commerce can be met with.

For Further Information...

SafeScrypt Ltd.
667-668 Keshava Towers,
11th Main,
Jayanagar 4th Block,

Bangalore – 560011, India

Phone No: +91-80-6555104
Fax: +91-80-6555300
E-mail: safeexim@safescrypt.com