

Hui Zhao (101159615@georgebrown.ca)

Professor Jackey Min (jmin@georgebrown.ca)

CRYPTOGRAPHY & NETWORK SECURITY

18 Feb 2020

Technical Analysis of PKI Development in Enterprise Network

I. Why Public Key Infrastructure?

There are many advantages to PKI, the major ones are: (Editor *PKI - The Pros and Cons* - Cogito Group *PKI: Public Key Infrastructure*)

1) Reality of non-repudiation:

KPI will provide the recipient with proof of the origin of the message. It will protect against any attempt by the originator to falsely deny sending the message. (Wu et al. *How to achieve non-repudiation of origin with privacy protection in cloud computing* Chapter 3)

2) Cost effectiveness:

Some argue about the cost of buying certificates for SSL and security signature by code signing will cost venture for small business. For example, SSL certification used to cost 35,000 to 100,000 (*Total Cost of Ownership for Public Key Infrastructure* Inputs: The Costs of VeriSign Managed PKI). However, a free SSL service is now available on the market, such as *Let's Encrypt*

MANAGED PKI FULL PUBLIC	SMALL 250 - 1,000*	MEDIUM 1,001 - 5,000	LARGE 5,001 - 10,000
<i>Per User</i>	\$38	\$29	\$18
<i>Annual Managed Service Fee</i>	\$35,000	\$45,000	\$100,000
<i>Total Annual Service Fee</i>	\$44,500 - \$74,000	\$74,029 - \$190,000	\$190,018 - \$280,000
<i>Total on a Per-User Basis *Minimum of \$50,000</i>	\$74	\$74 \$38	\$38 \$28
<i>One-Time Set-Up Fee (Standard Implementation)</i>	\$10,000	\$10,000	\$10,000

Fig.1. VeriSign White Paper

3) Government approved:

PKI is widely used by federal organizations, such as gov email service and website; the health and bank system also depend on PKI for authentication and authorization, such as online banking and mobile banking.

4) Cross platform supported:

The KPI can be seamlessly implemented with TCP/IP protocol suits. It means that if the TCP/IP protocol is supported by the platform, KPI will be supported as well. All the modern operation systems such as Android, IOS, macOS, IOs, windows, Linux, and Unix support PKI.

II. Introduction to PKI

PKI is a solution to facilitate the secure electronic transfer of information for a range of network activities, such as e-commerce, internet banking and confidential email. Before PKI, the private key was universally used by cryptography. But private key cryptography has its limitations, such as, no support for security key exchange keys remotely. For

example, a Toronto customer wants to buy a product from China. It is not ideal and practical that the customer flies to China and exchanges his private key for the seller's private key. The PKI address this issue by the two parties in the deal can exchange their key pairs without meeting in person. The PKI fulfills the demand of modern global business.

The first development of PKI was secretly happened in the early 1970s at the British intelligence agency (GCHQ). The first public disclosure of both security key exchange and asymmetric key algorithms was in 1976 by Diffie, Hellman, Rivest, Shamir, and Adleman. It includes hardware, software, people, policies, and procedures required to create, manage, distribute, use, store, and revoke digital certificates. In cryptography, the PKI helps to bind public keys with corresponding user identities by means of a certificate authority (CA).

(Wikipedia *Public key infrastructure Design*)

III. PKI Mechanism

PKI uses asymmetric key pairs to guarantee confidentiality and integrity. The foundation of PKI is the mathematical fact of the difficulty of factorization of large prime numbers. In another words, it is easy to calculator the product of two prime numbers, but it is hard to find the factors of a number only has large prime factors.

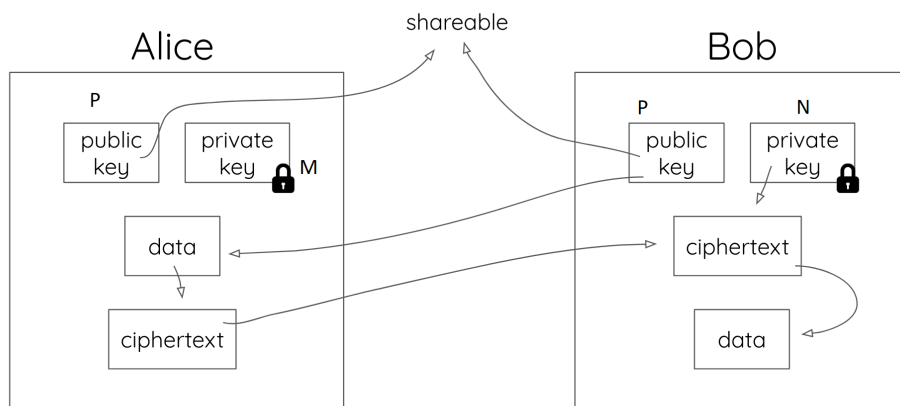


Fig.2. Ideal use case of PKI

The basic idea is:

- a) Alice wants to send a coded message to Bob.
- b) Except Alice, only Bob knows how to decode the cyphered message.
- c) Alice and Bob both know how to code the message.

Ideally, the sender Alice chooses two large prime numbers m and n , then use their product p ($p = m * n$) to code the message. The key pair (m and n) will become the private key of Alice(m) and Bob(n), respectively. When the message is received by Bob, it is decoded by Bob's private key(n). Due to the difficulty of big prime factorization, only Alice and Bob can decode the cyphered message. Thus, it guaranteed authentication of the data.
(Public Key Cryptography)

IV. PKI Modes

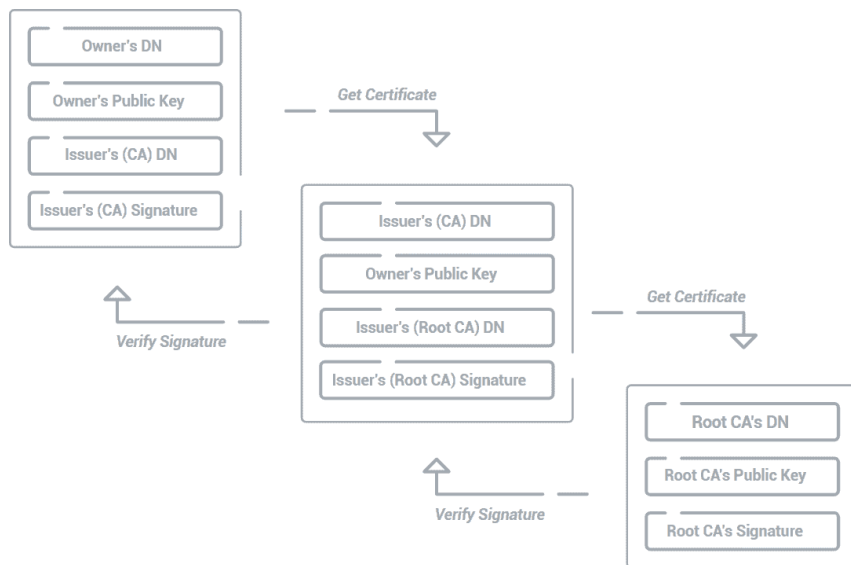


Fig.3. Root vs Intermediate Certificates and CAs

There are three key components in PKI: digital certificates, certificate authority and registration authority. There are several types of certificate authority: root CA, intermediate CA and Trust anchor. They are connected by the Certificate Trust Chain. It is a typical tree structure:

- 1) The root is the beginning of the trust chain.
- 2) The chain goes through intermediate certificate(s).
- 3) The chain ends with the last certificate, called Trust anchor.
- 4) Each client trusts his parents.
- 5) Using tracking backward to their parents to confirm the validation.
- 6) The backward tracking could be recursive until the root.
- 7) One CA trust, all CA should trust, same to the revoke.

(Root vs Intermediate Certificates and CAs)

The trust chain is like the bitcoin chain block, which is not managed by compute power but human.

V. Enterprise PKI Deployment Use Cases and Certificate Profiles

Basically, the profile is a definition of how a certificate is expected to be generated for a certain use-case. Most use-cases are already defined in the existing profile. But you can still define your own certificate profile, but you may end up re-inventing the wheel.

For example, RFC 5280 defines a profile for X.509 certificate and CRLs for internet usage.

The profile, its section 4.1, describes what is expected of the service compare to other network such as X.25. Meanwhile, it defined the typical extensions. You can define your own extension by heritage that profile. Like in OOP, heritage from a class to make your own

class. (Finlay WeberFinlay Weber 78833 silver badges1212 bronze badges and
garethTheRedgarethTheRed 98666 silver badges1717 bronze badges)

4. Certificate and Certificate Extensions Profile

This section presents a profile for public key certificates that will foster interoperability and a reusable PKI. This section is based upon the X.509 v3 certificate format and the standard certificate extensions defined in [X.509]. The ISO/IEC and ITU-T documents use the 1997 version of ASN.1; while this document uses the 1988 ASN.1 syntax, the encoded certificate and standard extensions are equivalent. This section also defines private extensions required to support a PKI for the Internet community.

Certificates may be used in a wide range of applications and environments covering a broad spectrum of interoperability goals and a broader spectrum of operational and assurance requirements. The goal of this document is to establish a common baseline for generic applications requiring broad interoperability and limited special purpose requirements. In particular, the emphasis will be on supporting the use of X.509 v3 certificates for informal Internet electronic mail, IPsec, and WWW applications.

4.1. Basic Certificate Fields

The X.509 v3 certificate basic syntax is as follows. For signature calculation, the data that is to be signed is encoded using the ASN.1 distinguished encoding rules (DER) [X.690]. ASN.1 DER encoding is a tag, length, value encoding system for each element.

```
Certificate ::= SEQUENCE {
    tbsCertificate      TBSCertificate,
    signatureAlgorithm  AlgorithmIdentifier,
    signatureValue      BIT STRING }

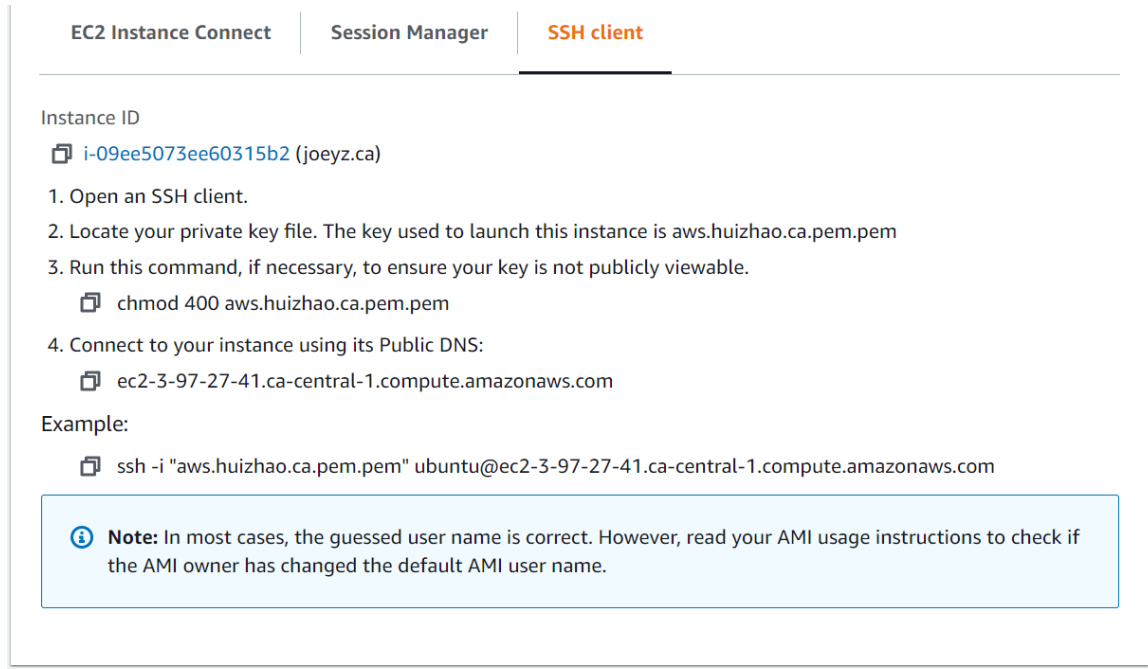
TBSCertificate ::= SEQUENCE {
    version             [0] EXPLICIT Version DEFAULT v1,
    serialNumber        CertificateSerialNumber,
    signature           AlgorithmIdentifier,
    issuer              Name,
    validity            Validity,
    subject             Name,
    subjectPublicKeyInfo SubjectPublicKeyInfo,
    issuerUniqueID     [1] IMPLICIT UniqueIdentifier OPTIONAL,
                      -- If present, version MUST be v2 or v3
```

Fig.4. RFC 5280 (*Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile* Section 4.1)

VI. PKI Case Study: SSL on the Internet

By using digital certificates, SSL, for authentication, enterprises could significantly improve their security and productivity. The typical use-case is:

1) Authentication for Wi-Fi / VPN / OS



EC2 Instance Connect | Session Manager | **SSH client**

Instance ID
 i-09ee5073ee60315b2 (joeyz.ca)

1. Open an SSH client.
2. Locate your private key file. The key used to launch this instance is aws.huizhao.ca.pem.pem
3. Run this command, if necessary, to ensure your key is not publicly viewable.
`chmod 400 aws.huizhao.ca.pem.pem`
4. Connect to your instance using its Public DNS:
`ec2-3-97-27-41.ca-central-1.compute.amazonaws.com`

Example:
`ssh -i "aws.huizhao.ca.pem.pem" ubuntu@ec2-3-97-27-41.ca-central-1.compute.amazonaws.com`

Note: In most cases, the guessed user name is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI user name.

Fig.5. AWS EC2 SSH needs .pem file (digital certification)

Digital certificates are universally used for the authentication of Wi-Fi network login. Due to digital certification are mandatory during the login progress, it can effectively stop the unauthorized login attempt. Even the password is leaked, the digital certification file still can protect the Wi-Fi network from brutal force cracking. This applied to VPN and SSH login as well. Cloud services, such as AWS and Azure, recommend using digital certification for the SSH or RPD connection.

2) Integrity for Web Application

Using SSL to help keep the data integrity including Web service such as https service, email, CMS, CRM etc... The mainstream http server support SSL features. Accommodate the client-side software, usually are browsers such as Chrome, Firefox, will inform user which data is authentic and which one is not guaranteed. It is widely used in online banking and commercials.

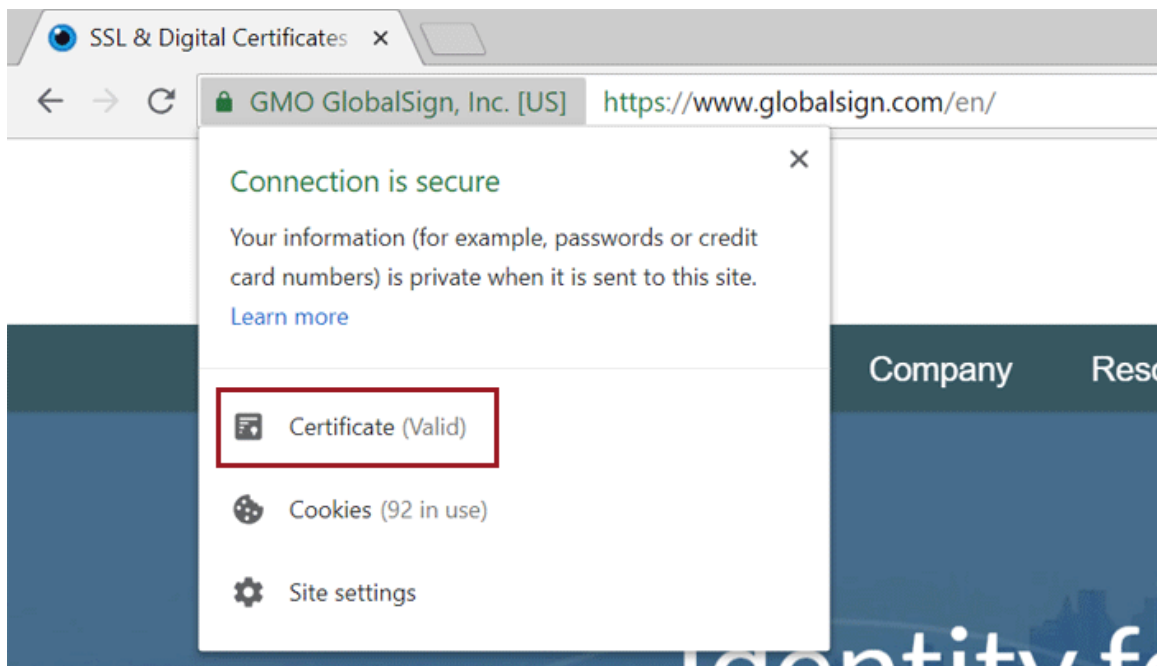


Fig.6. Browser built-in SSL feature.

As discussion in the earlier paraphs, SSL is broadly be used today in our daily life. Such as online shopping, online banking, online chatting, email, SSH, VPN, and so on, you named it. Without SSL(PKI) or the equivalent solution, there will be no Amazon, eBay, and PayPal, and so on, those e-commercial giants.

VII. Conclusion

Above all, PKI resolves all the roadblocks of modern lifestyles. From online banking to shopping, from meeting to messaging. It has become the infrastructure of cyber life. Without the guarantee of authentication and integrity of data provided by PKI, we still need to wait for a month after sending the order to the seller from the newspaper ads.

Now You Can Be TALLER Instantly!



By at least **2 FULL INCHES** with amazing new invisible "LIFTEE" HEIGHT INCREASE PADS

Are you handicapped in your social contacts because of a short appearance . . . tired of being called shorty? Now, at last you need not suffer this embarrassment any longer with the aid of "LIFTEE", the new amazing HEIGHT INCREASE PADS. Simply slip these invisible pads in any pair of shoes. Now step into them and add 2 inches in height. THE SAME HEIGHT INCREASE AS EXPENSIVE HEIGHT INCREASING SHOES, for a fraction of the cost, to give you new poise and self-confidence—a key to success and romance. No one will suspect that you are wearing them — but what an impressive difference they make! These LIGHTWEIGHT FOAM RUBBER AND CUSHION CORK PADS fit securely without gluing and interchangeable in any shoes. "LIFTEE" is scientifically designed for real walking comfort and an aid to better posture. "LIFTEE" is worn by thousands of smart men and women in all walks of life. Durable and shock absorbing. State man's or woman's shoe size.

ONLY \$1.98 per pair AMAZING LOW PRICE!

FREE 10 DAY TRIAL COUPON!

THE LIFTEE COMPANY, DEPT. 823
Box 608, Church Street, New York, N.Y. 10008

Rush my "Liftee" Height Increase Pads in the size checked. I will pay postman on delivery only \$1.98 plus postage. I must be satisfied or I can return the pads within 10 day trial for a full refund.

Check Box — State Shoe Size

Mens Shoe Size _____ Ladies Shoe Size _____

Check here if you wish to save postage by sending only \$1.98 with coupon. Same money back guarantee. 2 Pairs \$3.50

3 Pairs \$5.00

NAME _____

ADDRESS _____

CITY _____ STATE _____ ZIP _____

SEND NO MONEY!

Free 10 Day Trial! Mail coupon today ➔

Pay postman on delivery, only \$1.98 plus postage per pair of "LIFTEE" HEIGHT INCREASE PADS. Or send only \$1.98 with order and we pay postage. (2 Pairs \$3.50, 3 Pairs \$5.00). 10 DAY TRIAL MUST SATISFY OR MONEY WILL BE REFUNDED.

Fig.7. mail advertisement on newspaper (https://dangerousminds.net/comments/vintage_comic_book_ads_that_were_too_good_to_be_true)

Works Cited

- Editor, Cog. “PKI - The Pros and Cons - Cogito Group PKI: Public Key Infrastructure.” *Cogito Group*, 27 May 2020, cogitogroup.net/pki-the-pros-and-cons/.
- Finlay Weber Finlay Weber 78833 silver badges 1212 bronze badges, and
 GarethTheRed GarethTheRed 98666 silver badges 1717 bronze badges. “What Is an X509 Certificate Profile?” *Stack Overflow*, 1 Feb. 1969, stackoverflow.com/questions/60675308/what-is-an-x509-certificate-profile#:~:text=Basically%2C%20the%20profile%20is%20a,good%20reason%20to%20do%20so.
- “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.” *IETF Tools*, tools.ietf.org/html/rfc5280.
- “Public Key Cryptography.” *NRICH*, nrich.maths.org/2200.
- “Public Key Infrastructure.” *Wikipedia*, Wikimedia Foundation, 10 Feb. 2021, en.wikipedia.org/wiki/Public_key_infrastructure.
- “Root vs Intermediate Certificates and CAs.” *SecureW2*, 7 Jan. 2021, www.securew2.com/blog/root-vs-intermediate-certificates-cas.
- VeriSign. “Total Cost of Ownership for Public Key Infrastructure.” *WHITE PAPER*, VeriSign, 2005, www.imaginar.org/sites/ecommerce/index_archivos/guias/G_tco.pdf.
- Wu, Wei, et al. “How to Achieve Non-Repudiation of Origin with Privacy Protection in Cloud Computing.” *Journal of Computer and System Sciences*, Academic Press, 26 Mar. 2013, www.sciencedirect.com/science/article/pii/S0022000013000640.