Trustability of certification systems

Alexandre Kervadec

***Abstract*—This paper is a synthesis of a E.Gerck's paper : *"Overview of Certification systems: X.509, CA, PGP and SKIP"*[1], but not only. First, it gives an overview of (the mains) certification systems which are X.509 and CAs, PGP, SKIP, DANE and the Certificate transparency by Google, with thoughts on pros and cons of each system, on a technical point of view and about the government's stranglehold on data exchanges.**

I. Overview of certification systems

First sections talk about existing (sections I-A and I-B) or extinguished (section I-C) certification systems. Then, further sections (I-D and I-E) deals with new, not implemented yet, technologies of digital certification which may solve current issues.

A. X.509 and CAs

X.509 and CAs[7] infrastructure is based on a directory method.
With this kind of certification system, there are three different entities, which are :

1) **CA : Certification Authority**, an entity that controls authentication services and management of digital certificates. It can be public (like banks with their clients), commercial (such as *Verisign* which sells its services) or private (like a compagny department, for an internal purposes).
2) **Subscriber :** the entity which sends informations to the CA to add it to his certificate. This entity is one that need to be trusted by the *user* entity.
3) **User :** ask informations about *subscribers* to CA(s), it's central to the process, since the user party is relying on the informations given by *CAs* and is thus at risk.

The way that certification system is the following:

- A subscriber gives informations to the CA, in order to create a digital certificate for itself in the CA directory.
- The CA receive those informations and put it in a certificate.
- A user (the public in general) receive a certificate from a subscriber. In order to authenticate this subscriber, the client ask to the CA if the transmitted certificate matches with the subscriber's identity.
- The CA answer to the user to give him the precious informations about the subscriber's identity.

There is a not outwardly perceived entity in this system, it is the Naming Authority (DN). It provides to the CA a unique distinguished name (DN) which matches to the subscriber identity in the certificate.
Note that the CA can double in NA, but they provide two different services: the CA certificate refers to a name but does not denote it, the NA does.

The main concerns about authentification services provided by CAs are :

- The content of a certificate needs to be discussed, as well as certificate revocation. For example, a subscriber can generate multiple DN for a same CA or the same DN to multiple CAs, so maybe, a better subscriber identificator need to be added.
- Are the validation procedures for the certified data that is included in a certificate solid enough? Because each CA has its own self-defined rules (Certification Practice Statement[1]), which can by completly different from one CA to another.

Going deeper with user validation : DN scheme based on X.500 Recomendation, but it is not completly defined, and will (in 1998) probably not be. Also, X509 certification depends on many others such as ISO, ANSI, ITU and IETF. Thus lead to a lack of harmonization. Plus, there is a big problem with CPS (Certification Practice Statements), that also can be seen such as flexibility (for pros), because each CA answer specific needs, so no harmonization again.

Also, regarrding to the law, CAs deny all leak of information from themselves.

Some kind of conclusion about harmonization (lack of), in a world wide vision, if space there is.

B. PGP (Pretty Good Privacy)

PGP, created thanks to Phil Zimmermann researches. It has two parts: certification and encryption, following text only deals with certification.
Compared to X.509, PGP is more *internet-like*, this because of its *introducer-model* base.
PGP depends on a chain of authentificators: the users themselves. This chain forms a ring, but not in a closed way but in a mathematical way like a list or a *web-of-trust*. You may not know everyone in this ring, but you can assume that you will know somebody who know this user. You can also assume that different rings can have some contact points to garantee the referrals.

Thus, we can figure out that PGP breaks the traditional hierarchical trust architecture with this *web-of-trust* approach.

Let's get an example[2]: Bob want to exchange datas with Oscar, which he didn't knew before. But Jack, a colleague of Bob's, signs Oscar's public-key certificate whch he knows is

Tutor : A.Guermouche

[1]CPS
[2]Example from "The PGP trust model"[4]

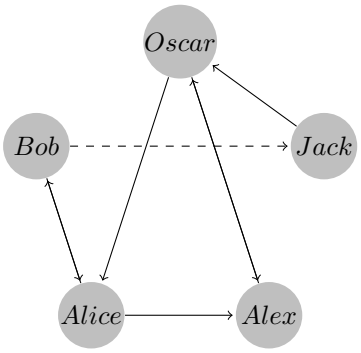

Figure 1. Communities of trust: Jack introduces Oscar to Bob's public-key certificate before Bob receives it.

authentic.
Oscar then forwards his signed certificate to Bob who wishes to communicate with Oscar privately.
Bob, who knows and truts Jack as an *introducer*, find out, after verification, that Jack is among Oscar's certificate signer. Therefor, Bob can be confident that Oscar's public key is authentic.

However, had Bob not known or trusted Oscar's signers, including Jack, he would have been skeptical about the authenticity of Oscar's public-key. Oscar would have to find another introducer whom Bob trusts to sign Oscar's public-key certificate. This is illustrated in Figure 1.
This is illustrated in Figure 1, where the dotted arrow indicates "Bob trusts Jack as introducer" and the solid arrow indicates "Jack trusts Oscar's public key validity".

PGP also includes a public-key certificate and an introducer trustwhorthiness. They have different levels, for a public-key certificate they are:

- *Undefined:* we cannot say wether this public-key is valid or not.
- *Marginal:* this public-key *may* be valid but we cannot be sure.
- *Complete:* we can be fully confident that this public-key is valid.

For an introducer, those levels of trustworthiness are the following:

- *Full:* this public-key is fully trusted to introduce another public-key.
- *Marginal:* this public-key can be trusted to introduce another public-key, but, it is uncertain whether it is fully competent to do that.
- *Untrustworthy:* this public-key should not be trustedto introduce another, therefore any occurence of this key as a signature on another public-key should be ignored.

Only the trustworthiness of public-key's validity is automatically evaluated by PGP. Introducer's worthiness is manually assigned by each user of to the public key, and exists only within each individual user's public-key ring[3].

The big point is the use of such a tool in a world wide range: that is raisonnably not possible. We can assume to use it in a little group, where trustworthiness is effective, but in a more wide area, it is problematic to trust such a amount of people, or find trusted introducers.

[3]PGP allows users to have files representing multipke *key rings* to store public or secret keys[4].

C. SKIP (Simple Key-Management for Internet Protocol)

D. DANE (DNS-Based Authentication of Named Entities)

DANE is not implemented yet, but a IETF team is working on the standard.

E. CATA: Certificate Authority Transparency and Auditability

Because of a case of Google CA's usurpation, Google is working on a new system that can improve certification systems.

REFERENCES

[1] E.Gerck, Overview of Certification Systems: X. 509, CA, PGP and SKIP, 1998.
[2] Ashar Aziz, Tom Markson, Hemma Prafullchandra, Sun Microsystems, Inc., v.06, 1995. https://tools.ietf.org/html/draft-ietf-ipsec-skip-06
[3] Oracle, SunScreen SKIP User's Guide, Release 1.1, 2010.
[4] Caronni, G. (2000). Walking the web of trust. In Enabling Technologies: Infrastructure for Collaborative Enterprises, 2000.(WET ICE 2000). Proeedings. IEEE 9th International Workshops on (pp. 153-158). IEEE.
[5] P Hoffman, J Schlyter, The DNS-based authentication of named entities (DANE) transport layer security (TLS) protocol: TLSA, 2012. https://www.rfc-editor.org/rfc/pdfrfc/rfc6698.txt.pdf
[6] Laurie, B., Langley, A., & Kasper, E. (2013). Certificate transparency (No. RFC 6962).
[7] Solo, D., Housley, R., & Ford, W. (1999). Internet X. 509 public key infrastructure certificate and CRL profile.