

Overview of Certification Systems: X.509, CA, PGP and SKIP

*E. Gerck**
egerck@novaware.cps.softex.br

MCG - Meta-Certificate Group
<http://www.mcg.org.br>

Abstract

Cryptography and certification are considered necessary Internet features and must be used together, for example in e-commerce. This work deals with certification issues and reviews the three most common methods in use today, which are based on X.509 Certificates and Certification Authorities (CAs), PGP and, SKIP. These methods are respectively classified as directory, referral and collaborative based. For two parties in a dialogue the three methods are further classified as extrinsic, because they depend on references which are outside the scope of the dialogue. A series of conceptual, legal and implementation flaws are catalogued for each case, emphasizing X.509 and CAs, which helps to provide users with safety guidelines to be used when resolving certification issues. Governmental initiatives introducing Internet regulations on certification, such as by TTP, are also discussed with their pros and cons regarding security and privacy. Throughout, the paper stresses the basic paradox of security versus privacy when dealing with extrinsic certification systems, whether with X.509 or in combination with PGP. This paper has benefited from the feedback of the Internet community and its expanded on-line version has received more than 50,000 Internet visitors from more than 20,000 unique Internet sites, in 1997/98.

* The author is with Novaware, Av. Albert Einstein 1301, SOFTEX/UNICAMP - Campinas – SP - Brazil;
<http://novaware.cps.softex.br>

Overview of Certification Systems: X.509, CA, PGP and SKIP

*E. Gerck**
egerck@novaware.cps.softex.br

MCG - Meta-Certificate Group
<http://www.mcg.org.br>

Abstract

Cryptography and certification are considered necessary Internet features and must be used together, for example in e-commerce. This work deals with certification issues and reviews the three most common methods in use today, which are based on X.509 Certificates and Certification Authorities (CAs), PGP and, SKIP. These methods are respectively classified as directory, referral and collaborative based. For two parties in a dialogue the three methods are further classified as extrinsic, because they depend on references which are outside the scope of the dialogue. A series of conceptual, legal and implementation flaws are catalogued for each case, emphasizing X.509 and CAs, which helps to provide users with safety guidelines to be used when resolving certification issues. Governmental initiatives introducing Internet regulations on certification, such as by TTP, are also discussed with their pros and cons regarding security and privacy. Throughout, the paper stresses the basic paradox of security versus privacy when dealing with extrinsic certification systems, whether with X.509 or in combination with PGP. This paper has benefited from the feedback of the Internet community and its expanded on-line version has received more than 50,000 Internet visitors from more than 20,000 unique Internet sites, in 1997/98.

Introduction

The Internet is an open system, where the identity¹ of the communicating partners is not easy to define. Further, the communication path is non-physical and may include any number of eavesdropping and active interference possibilities. Thus, Internet communication is much like anonymous postcards, which are answered by anonymous recipients. However, these postcards, open for anyone to read—and even write in them—must carry messages between specific endpoints in a secure and private way.

The solution is to use encryption (to assure privacy) and certification (to assure that communication is happening between the desired endpoints and that it is tamperproof) [MOV97]. This paper deals with the question of certification. The closely related question of encryption is also referred to, in order to set the various certification stages.

The problems that may be caused by false certification or no certification mechanisms can range from a “man-in-the-middle” attack in order to gain knowledge over controlled data, to a completely open situation to gain access to data and resources. It is important to note that these problems do not disappear with encryption or even with a secure protocol such as SSL. If the user is led to connect to a site which appears to be the desired one, as in a spoofing attack [Fel97], the user may have a secure connection to a thief and that will not make it safer.

This paper reviews the three most common certification methods in use today, which are based on X.509 Certificates and Certification Authorities, PGP and, SKIP. These methods are studied from a systemic point of view. The main motivations for this paper are: (i) Conduct a comparative review of the three methods, (ii) Unify a set of references to the most important issues in certification and encryption, as they are related to Internet needs and recent governmental policies, (iii) Provide a basis for the evaluation of other certification solutions available or to be developed, (iv) Identify room for improvements on the current security level of certification, that could be dealt with by other methods, (v)

¹ There are cases in which the identity of the communicating partners is not necessarily relevant. Also, anonymous speech is useful in many circumstances, even when privacy is required. The US historical case of “Deep Throat” disclosing information about the criminal activities of President Nixon is one example of an anonymous though identifiable source, in a private and secure environment. The public release of RC4 algorithm information on the Usenet is an example of an anonymous unidentifiable source, in a public and insecure environment. To assure anonymity is sometimes as difficult as to assure identification. This paper however deals with the commercial relevant cases of identification needs. See [Boh97].

Provide users with safety guidelines to be used when resolving certification issues, and (vi) Access the impact on Internet transaction security due to the security control policy needs of Governments currently actively promoting such policy solutions. An on-line expanded version of this paper [Ger97a] has received more than 50,000 Internet visitors from more than 20,000 unique Internet sites, in one year.

It is important to note that other certification methods which are in development, such as IETF's PKIX [PKIX], are still in a volatile stage and would not be reviewed in this paper in a fair way as compared to the three methods cited above. However, PKIX is a direct derivation of X.509 and the reader will find essentially the same features and problems in PKIX.

1. Certification Methods

Public-key cryptography may give the impression that security can be simply achieved. It seems that one only has to allow the public-key to be distributed at will, there is no need for secrecy, and anyone can receive private and secure messages. The same procedure being applied to each side, sender and receiver, both could immediately engage in private and secure communication.

However, who is at the other side? Is that key really from the sender? Is the key still valid? Questions soon appear and it becomes clear that public-key cryptography has indeed solved the problem of public-key security but not the problems of public-key acquisition, recognition, revocation, distribution, re-distribution, validation and, most importantly, key-binding to an identifier and/or key-attribution to a real-world entity. Communications can be verified neither for origin authentication nor for data-integrity—communications can be private but not secure.

Of course, a private communication with a thief is not secure just because it is private. Clearly, without binding the key to an identifier such as a person's common name, the key is just a byte string and can be yours as well as anyone else's. But, common names or identifiers are oftentimes not enough—where legal capacities must be defined, one needs to have some assurances that the key can be attributed to one well-defined real-world entity such as a person or company.

Certification is needed—i.e., a tamperproof binding between the public-key and some desired attribute, usually the entity's name and/or the entity's real-world confirmed identity. Which still contains all the previous questions, such as certificate acquisition, recognition, revocation, distribution, re-distribution, validation and, most importantly, what are the intended senses or meanings for key-binding to an identifier and/or for key-attribution to a real-world entity. However, certificates introduce tamperproof attributes which can be used as convenient references to differentiate one certificate from another, one key from another and, possibly, one entity from another.

Absolute certification methods are a logical impossibility, because a certificate cannot certify itself. Thus, three main methods have been proposed to deal with this situation, as this paper classifies them:

- Directory methods: X.509 and CA [X509a], [X509b]
- Referral methods: PGP [PGP]
- Collaborative methods: SKIP [SKIP]

Each of the above paradigms deals with the basic certification question in a different way, as analyzed in the following sections. However, for two parties in a dialogue, they share a common ground in that they depend on references which are external to the dialogue between the parties. Hence, they are called extrinsic and share common characteristics, as will be comparatively discussed here. Further discussion on the general characteristics of extrinsic certification as well as the existence proof of two other certification modes, called intrinsic and combined, are presented in [Ger97b].

2. X.509 and CAs

The ITU-T Recommendation X.509 (which has been implemented as a de facto standard) [X509b], describes two levels of authentication: simple authentication, using a password as a verification of claimed identity; and strong authentication, involving credentials formed by using cryptographic techniques. It is this second level that interests us here. It defines a framework for the provision of authentication services, under a central control paradigm represented by a "Directory".

The “Directory” is implemented by Certification Authorities (CA), which are governed by Certification Practice Statements (CPS). The CPS is internally defined by each CA within broad limits and lie outside the scope of X.509, even though X.509 refers several subjects to be defined in the CPS, as discussed in the exposition. There are three main entities which can be outwardly recognized in X.509 certification procedures:

- CA: a general designation for any entity that controls the authentication services and the management of certificates. Also called the issuer. The CA can be public (a bank that issues certificates to allow its clients to access their bank account), commercial (a service provider that sells certificates to other parties, such as Verisign) or private (a company that issues certificates to allow its employees to perform job duties). CAs are in general independent, even in the same country.
- Subscriber: an entity that supplies to the CA the information that is to be included in the entity’s own certificate, signed by the CA. Usually, as defined in CA’s CPSs, the information supplied by the subscriber is “endorsed” by the issuer, where “endorsed” means “copied as received”. This corresponds to “endorsement without recourse”. For example, in English law one can endorse “without recourse” (or, as it used to be expressed, “sans recours”), which passes on the benefit of a bill of exchange without adding any guarantee. In other words, the CA copies the subscriber’s information to the certificate, but neither denotes nor confirms it.
- User: any entity which relies upon the certificate issued by the CA in order to obtain information on the subscriber. Also called the verifier. Users may use any CA or any number of CAs, depending on their location and ease of access. The user should be central to the decision process in all steps, since the user is the party that is relying on the information and is thus at risk.

A further entity is the Naming Authority (NA), which is usually not outwardly perceived but which is the actual entity that defines the naming scheme used by a CA. The CA can double as a NA, but they provide two different functions. Semantically, the CA certificate refers to a name; however it does not denote it—the NA denotes it.

The authentication services provided by CAs are especially relevant in regard to three central questions:

(1) What is a X.509 certificate?

Even though section 3.3.3 of X.509v3 defines a certificate as: “*user certificate; public key certificate; certificate: The public keys of a user, together with some other information, rendered unforgeable by encipherment with the private key of the certification authority which issued it.*”, there are several open questions regarding the contents of certificates and their issuance conditions which need to be discussed, as well as certificate revocation.

(2) What is the naming scheme used in X.509 such that a certificate can be associated with a user?

Section 11.2 of X.509v3, “Management of certificates”, states that the certificate allows an association between a name called “unique distinguished name” or DN for the user and the user’s public-key: “*A certificate associates the public key and unique distinguished name of the user it describes.*”, while Section 7 explains that such DNs are essential to the security design of X.509: “*Authentication relies on each user possessing a unique distinguished name.*” But, how are such DNs assigned? Where are they unique? The DN is denoted by a NA and accepted by a CA as unique within the CA’s domain, where the CA can double as a NA. It is interesting to note that the same user can have different DNs in different CAs, or can use the same DN in different CAs even if it is not the first one to use it in a CA—so, different DNs for different CAs do not necessarily mean different users and vice-versa. Further, a DN may not contain the user’s real-world name or location.

(3) What are the validation procedures for the certified data that is included in a certificate?

X.509 is moot on validation procedures for data included in a certificate such as the user’s name, with the exception of validation procedures for the user’s public-key which are suggested (not mandated) in Section 10 of X.509v3. For example, regarding validation procedures for the user’s identity, Section 11.2.a states that: “*a certification authority shall be satisfied of the identity of a user before creating a certificate for it*”, which means that identity validation procedures are to be satisfied in the CA’s frame of reference by following the CA’s own self-defined rules (the CPS), which can be entirely different for different CAs. Further, in general, commercial CA’s CPSs accept indirect references when issuing certificates, such as using an ID as identity proof, which can be easily subject to fraud and lead to public risks.

Thus, X.509 focuses on defining a mechanism by which information can be made available in a secure way to a third-party—the certificate itself. However, X.509 does not intend to address the level of effort which is needed to validate the information in a certificate neither define a global meaning to that information outside the CA's own management acts.

The main purpose of a CA is to bind a public key to the name contained in the certificate and thus assure third parties that some measure of care was taken to ensure that this binding is valid for both—i.e., name and key. However, the issue whether a user's DN actually corresponds to identity credentials that are linked to a person or simply to an e-mail address—and how such association was verified—is outside the scope of X.509 and depends on each CA's self-defined CPS and on each NA.

Regarding the all-important DN specification denoted by the NA and accepted by the CA, the X.509 DN scheme is based on ITU-T X.500 Recommendation [X500a], [X500b]—but X.500 is not completely defined and, apparently never will be. There is no Internet workgroup, not even ITU-T as its proponent, that currently works on X.500 final naming definitions. This is due to several factors, such as the lack of a centralized world body that would be acceptable to all parties and needs and, most importantly, the perception that global indexes involve strong privacy issues.

Thus, there was ample room for many different readings of the proposed X.509 Recommendation, as different implementations had to ad hoc define how DNs would be used in X.509. Also the X.509 Recommendation depends on many others ISO, ANSI, ITU, and IETF standards, amendments, meeting notes, draft standards, committee drafts, working drafts, and other work-in-progress documents, besides the convoluted language used in some of these specifications, which makes their use difficult by itself, as pointed out by Peter Gutmann [Gut98].

A characteristic of X.509 is that almost all issues that involve semantics or trust are delegated to a CA's CPS—the Certification Practice Statement—which is declared out of scope in relationship to X.509. The CA's CPS is the governing law that the CA presents to potential clients and represents a top-down framework. While some consider the CPS mechanism to be a good way to introduce flexibility in X.509 because each CA can have their own rules for different needs, such mechanism can be considered as X.509's "black-hole" and cannot be directly harmonized for different CAs.

Thus, while this "black-hole" mechanism affords a "solution" to the undefined semantic and trust features in X.509 (as they are declared out of scope and delegated to the CPS), such "laissez faire" attitude leaves ample room for strong differences between CAs and for a biased "take-it-or-leave it" attitude regarding what a CA subscriber can expect.

These problems have caused independent interpretations of X.509 in actual implementations, e.g. as given by Netscape, Microsoft, RSA, etc., and by CAs.

For example, let us consider a protocol called SSL² (Secure Socket Layer, e.g. version 3.0 [SSLa], [SSLb], with an IETF equivalent specification being developed as TLS). If a X.509 Certificate is acceptable by a Netscape SSL product such as the Communicator browser, it does not mean that it will necessarily be acceptable by products from Microsoft or RSA or another vendor. The issue is further confused by a number of ill-defined market names as defined by CAs, such as "Digital-ID" and others, that hide the dependency on X.509 but which nonetheless depend on the same concepts.

Further, lack of CPS harmonization does not allow X.509 to directly scale to a planetary Internet, when different CAs would need to allow for cross-certification (i.e., when subscribers of different CAs are users to one another). Even though cross-certification could work in a parochial Internet where everyone knows what to expect and share a common law and trust system, it is doubtful that it could be successfully applied between competing businesses or different states in a country—much less between different countries, since there is no common world law. There are

² SSL is not a socket protocol as the name might indicate but allows for encryption and certification functionality in a TCP/IP environment. SSL is perhaps the widest used security protocol on the Internet today and implements X.509 certification as interpreted by SSL's proponent, Netscape. There are also other implementations of SSL, such as a free implementation called SSLeay [SSLy] which is export-free and user-friendly—developed by Eric Young and Internet collaborators. SSLeay is widely used with the well-known Apache Web server. The first fully functional version of Apache with SSL support was implemented by Ben Laurie. A full-Java implementation of SSL3.0 called J/SSL is available from Baltimore Technologies.

also subjective and intersubjective aspects of certification and trust which are needed³, but which cannot find a unified global expression—as it would be required for X.509 cross-certification.

Besides, X.509 certificates are not human readable and the user cannot easily see what is being accepted, in fact he has to take it for granted that it is correct—e.g., when a browser presents a readable conversion. However, even experts disagree on basic X.509 issues, as explained above, and there is usually ample room for doubt about what exactly a X.509 certificate is, why it is acceptable or why it is not acceptable. In other words, X.509 certificates have a twilight zone exactly on the most important issue with certification: what has been certified.

Another point is that X.509 certificates need a “Directory” service, provided by a CA, that deals with the users and supplies copies of the certificates—even though the certificate is used off-line with the CA. This means that a CA is needed for two basic reasons: (i) to issue “standard” X.509 certificates that can be interpreted unambiguously and, (ii) to make it possible to have their validity verifiable by a user.

However, who verifies the CA’s validity? The CAs themselves are usually “self-certified” or depend on a CA that is “self-certified”.

The CA paradigm in X.509 is thus, essentially, to rely on an authentication chain that ends in a CA that eventually certifies itself. Therefore, the validity problem is shifted from a local perspective to a global perspective, with the whole chain depending on one final link. At the end, ignorance (and the possibility of fraud) is leveraged to a high degree, in which one weak link may compromise a whole chain of certificates.

What are the causes for weak links? Besides the general issues discussed above, a list of more specific points is presented next—for further details in each item, please see the on-line reference [Ger97a]. The graphical views presented in [GerBoh] can also be useful to better conceptualize the terminology used.

The most important conceptual, legal and implementation flaws that users must be aware of and be able to resolve are:

- (i) Initial decision of trust removed from the user. The server defines which certificates can be accepted.
- (ii) Need to trust untrusted CAs in server-defined certification chains, which implies accepting transitive trust⁴.
- (iii) Certificates expire in domino effect, from the signing CA to the subscribers. Thus, valid certificates may be rendered useless, however without any need per se.
- (iv) Certificates can have very short lifetimes, as short as 4 weeks [Simp97], as defined by their private-key lifetime under attack. However, they are usually issued with a one-year lifetime.
- (v) Certificates need to be multiply provided in order to allow for certificate renewal without service interruption.
- (vi) Protection is an inverse function of worth, because CA root certificates tend to be issued with very long lifetimes, such as twenty-years [Canada].
- (vii) Certificates can be compromised by chain events outside the control of the user or subscriber.

³ Subjective and Inter-Subjective: Subjective means that one needs to take a subjective or personal instance in order to evaluate an object, and Inter-Subjective meaning that this instance can yield different results for objects of the same class. For example, beauty and trust are subjective concepts (“beauty is in the eyes of the beholder” and “trust depends on the observer”) because trust and beauty are abstract objects that cannot be differently instantiated, while a medical diagnosis for a patient is inter-subjective because the diagnosis itself is a particular instance from the class of all diagnosis possible for that patient at that time, each clearly dependent on the patient’s relationship to the physician and different from the other. An inter-subjective concept is overly-variable in reference to a subjective concept, because it also depends on the particular instance of the class’ object. So, even though trust is subjective, trust on a CA certificate is inter-subjective because it cannot be harmonized or harmonizable for all CAs or, even, for all similar certificates issued by a particular CA.

⁴ Trust is not transitive in general—i.e., if you trust your brother it does not mean that you must equally trust the same friends that your brother trusts.

- (viii) Certificates do not include enough direct verification data on the subscriber, that the user could rely upon in order to check them. However, if they do then it would represent a potential violation of the subscriber's privacy rights, which is the basic paradox of security versus privacy in extrinsic certification systems.
- (ix) Certificate revocation lists are a will to revoke, not an actual revocation, and there is no assurance that all certificate copies will be revoked, for a given revoked key.
- (x) Certificates are legally warranted for methods, not for results [UCC], [RSA].
- (xi) Certificate users are not legal relying-parties to the CA, since they are not privy to the subscriber CA contract.
- (xii) Client and S/MIME certificates are issued using insecure on-line protocols in browsers such as Communicator and Explorer.
- (xiii) "Certificate Authorities" and "Certificates" are misnomers. There is nothing "certain" about certificates, the "Authorities" are self-appointed issuers and a "certificate" does not convey any authorization.
- (xiv) "Certificate Authorities" and "Certificates" are actually certified by the users, that must understand that certificates are not magically infused with trust just because they are digitally signed. Certificates are trusted if they are expected to work, not the reverse [Ger98].
- (xv) Commercial CAs disclaim any warranties or fitness to purpose [McCur], because certificates are issued with null semantics:

VERISIGN DISCLAIMS ANY WARRANTIES WITH RESPECT TO THE SERVICES PROVIDED BY VERISIGN HEREUNDER INCLUDING WITHOUT LIMITATION ANY AND ALL IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. VERISIGN MAKES NO REPRESENTATION OR WARRANTY THAT ANY CA OR USER TO WHICH IT HAS ISSUED A DIGITAL ID IN THE VERISIGN SECURE SERVER HIERARCHY IS IN FACT THE PERSON OR ORGANIZATION IT CLAIMS TO BE WITH RESPECT TO THE INFORMATION SUPPLIED TO VERISIGN. VERISIGN MAKES NO ASSURANCES OF THE ACCURACY, AUTHENTICITY, INTEGRITY, OR RELIABILITY OF INFORMATION CONTAINED IN DIGITAL IDS OR IN CRLs COMPILED, PUBLISHED OR DISSEMINATED BY VERISIGN, OR OF THE RESULTS OF CRYPTOGRAPHIC METHODS IMPLEMENTED.

- (xvi) The CA's CPS and warranty disclaimer are generally not visible in the certificate itself, neither X.509 clauses, but merely referenced, so users must be educated on the various issues mentioned above in order to properly deal with the information provided in certificates. Otherwise, it is impossible to prevent against the unknown.

Within the above considerations, what is delivered by a CA in a X.509 certificate? What can a user or subscriber expect? X.509 mandates that a CA must verify (but, still limited in scope by the CPS) that:

- (a) the subject's public-key has a working private-key counterpart elsewhere (but with no warranties, such that the public/private key pair is not artificially weakened, that it is actually in the possession of the named subject and that no one else has obtained a copy of it), and
- (b) the subject's DN is unique to that CA (but with no warranties that such DN contains the actual subject's name, location or that the subject even exists or has a correctly spelled name—as in "Internet Serices" [RSA]).

Further, there are other items in the certificate which have no relationship to the data supplied by the subscriber but which are necessary for the proper use of the certificate, as a secure transport for information in the X.509 model. For example, its serial number, date of issuance, validity, the CA's signature, etc., which usually also carry limited CPS warranties (e.g., disclaimed in the case of fraud, computer viruses, etc.). These other items may further jeopardize the secure use of a certificate, without the user being even aware of it.

Now, having cited Verisign's disclaimer in item (xv), it is important to understand its reasoning and need. The point is not so much that CAs deliver a product with zero warranty (which could be disputed in court even in countries with common-law systems) but that CAs are delivering a product with almost zero content (which any court would accept as

involving almost zero liability)—as it is clearly exemplified in the second and third sentences of the above disclaimer (“...MAKES NO REPRESENTATION ...” and “...MAKES NO ASSURANCES ...”). So, Verisign’s disclaimer does not mean that Verisign has no warranty on their services or that they do not take any liability on them. It only says that Verisign has no warranties and accepts no liability for services that Verisign does not provide.

The fact that Verisign does not provide what perhaps the majority may think they provide is another point altogether. The solution is, perhaps, much more to educate the majority than to expect a company to do what is maybe technically unfeasible in X.509 terms. Thus, in the author’s opinion, Verisign’s CPS is not at all at odds with X.509 or legislation—so, it could very well be an example to be copied. Maybe, it just truly represents the maximum that one could wish for, commercially and technically, in terms of X.509 and with a viable CPS.

Thus, for any generic CA one might expect a similar reasoning. Indeed, if the only thing that a CA does (as per X.509) is to challenge the subscriber’s private-key in order to bind the corresponding public-key with the subscriber’s DN and, if it signs the certificate with a CPS that says that any other data are being copied as received but have not been verified (and have thus no warranty) then the CA has no responsibility for the contents of the certificate—save the positive acknowledgement that the public-key did have a counterpart when it was linked to that DN (where the CPS could further provide exceptions for frauds, virus, MITM attacks, etc.).

One may ask, why are such content limitations and disclaimers necessary for certificates? First, a certificate is not like a car that has a limited liability in space and time (after all, a car is a localized entity that can contain a limited number of people and only one driver). A certificate can be endlessly multiplied and simultaneously presented in a planet-wide area. Certificates are used without limit in a chain of events, which can include other fully unrelated certificates and people⁵.

With the growing attitude of seeking large legal compensation for one’s lack of foresight, the liability pyramid created by a lesser disclaimer could easily extend to the CA’s client’s clients and so on.

Insurance protection may help here, but there are several issues that must be touched upon. The use of insurance always signals lack of knowledge—so it clearly cannot replace it. Further, there is no insurance needed for a sure event and there is no insurance possible for a sure risk. If a user (ie, a CA subscriber) is going to pay for insurance to cover his liabilities and the CA’s liabilities (which is what it amounts to), then responsibility has gone full-circle and is now only in the user’s hands—both to get adequate coverage and to pay for it. While the CA has zero risk and profits as the middleman between the user and the insurance companies. However, that does not solve the risk problem for the user either, because one cannot make the whole world sign up one huge insurance policy—so the user and the CA may be protected by the insurance policy that the user has bought with their names as beneficiaries but that does not protect a third-party (ie, the rest of the world). Last, since CA auditing does not help here, then insurance does not have a reliable risk estimator either, even for the CA subscriber.

Regarding recent legislation efforts, such as in Utah (US) [Utah], Illinois (US) [Ill] and other legislation as reported by Juan Avellan [Ave98], it is clear from the above discussion that demanding broader warrants by law can be self-defeating because CAs may then be forced to reduce the deliverables to zero—instead of coming out and providing for more warranties. There simply is a limit to what X.509 and the CA paradigm can offer regarding legal certificate reliance and—most importantly and often confused with the former—legal certificate content reliance. Law cannot push the technical envelope of X.509.

When confronted with risk situations, a normal business solution is to rely on auditing. However, auditing CA’s certificates is also a difficult, if not impossible, task. This is due to X.509, which allows CA’s practices and policies to be built upon islands of self-regulation exactly on the most important issues of trust and trust management. As publicly declared by Phillip Hallam-Baker [Bak98], a Verisign consultant, not only are the CPSs indeed different and self-made by each CA but they are not designed to be audited, either: *“There is not as yet a defined standard for CA practices against which a company may be audited. In effect each company states their own practices in their Certificate Practices Statement (CPS). The CPS is not a document designed for auditing use however. It describes a ‘specification’, it does not describe details which may be checked by a third party in a systematic manner.”*

⁵ Spoofing chain: A spoofing chain is an operation that tries to obfuscate false data, by giving it a shroud of credibility based on secondary steps that may not be perceived as insecure by a third person. For example, to obtain a false ID a person might begin by obtaining a copy of a true birth certificate of a deceased person, faking mail addresses directed to that name, obtaining secondary IDs such as library cards and working up the ladder to reach a higher level ID and even a SSN. However, because of such frauds, some governments now stamp with “deceased” copies of birth certificates of deceased persons and routinely cross check IDs on a local and national level. This increase in government control of personal IDs is a parallel situation to the current increase of government control of “Internet IDs”—because the public order is at risk.

Last, when one watches for some time the different mailing lists that collect doubts and questions on certification systems from users or, when one reads the majority of the newspaper or magazine articles on the subject, one cannot help but perceive a prevailing feeling in the user community to the effect that a certificate is magically infused with trustworthiness—which is wrong and would imply a deterministic and absolute view of certification. For example, as one user wrote: “Please provide me with a list of all trusted CAs so that I can enter those certificates into my browser”, few understand that trust must be evaluated relative to the user’s own needs—because the user is the party at risk. Thus, the very names Trusted Third Party or trusted CA raise already several questions:

- trusted in relationship to whom?
- trusted by whom?
- trusted for what?
- trusted for how long?
- etc.

How are these questions to be answered? Clearly, by each user (ie, relying party—who is at risk) in its own domain, references and terms. This means that certificates are essentially statements from a CA⁶, not fact, and that meaning and trust on a certificate (like beauty) is in the eyes of the beholder, i.e., must be evaluated by each user.

To conclude, in legal reliance terms, one may trust the confirmation procedures of the CA during certificate reliance, but one cannot rely upon them for other than their value as a representation of the CA’s authentication management act expressed in the CA’s own terms and rules—therefore, a X.509 certificate is neither necessarily meaningful nor valid in a user’s reference frame or for the user’s purposes.

Users and subscribers should then carefully discern the different issues presented here and use their due diligence when relying on Certificates and CAs. Which are not a one-stop security solution but may help provide one more source of information for one’s own trust decisions.

3. PGP

PGP has two parts: certification and encryption. The discussion below is centered exclusively on the certification aspects of PGP [PGP].

First, comparing PGP with X.509 can be very instructive. X.509 is often times spotted as predicating a top-down trust structure (see the CPS discussion above) that is just dictatorially imposed upon the verifier, while PGP would follow a grass-roots approach—thus more Internet-like. However, both PGP and X.509 define their central role to be played by the verifier regarding certificate acceptance, while certificate metrics is defined in both cases without any influence from the verifier (thus, “dictatorially” for both). Further, both are key-transport protocols, and they depend on two types of external references: keys (quantitative) and trust (qualitative). Further still, the web-of-trust in PGP finds its parallel in the X.509 CPS, also when the issuer sets the rules and defines semantic acceptance conditions before certificate signature.

The first main difference is possibly syntactic, in the sense that PGP allows certificates to be stacked up so to say as signatures upon signatures, whereas in X.509 the certificates are linked one to another as in an one-way linked-list (though X.509 could also include PGP syntax). A second main difference is semantic, in which PGP allows an association between keys and real-world persons by web-of-trust rules, but not by transitive trust rules, whereas X.509

⁶ Presumed “certification”: The issuing of a certificate that contains false data—certified or not—gives the impression of credibility to that data, which may be used for a second step in a spoofing chain. Thus it is not acceptable for a certificate to include fields that carry no verification, without explicitly declaring so, as the case with e-mails in current certificates. It is a poor practice to provide a “security” feature that can not be verified or enforced. It gives a presumption of safety to the unwary user. “In California, for example, each drivers license features a photo, several holograms, and a metallic strip for fraud prevention. But this didn’t stop employees of the state’s Department of Motor Vehicles from issuing bogus licenses to anyone willing to fork over the right amount of cash. An estimated 250 DMV employees have issued over 25,000 genuine-looking, but fraudulent licenses in a two year period. Some were paid as much as \$1,000 for such licenses. ‘Ironically, as our documents become more tamper-proof, it’s become more of a problem’, DMV Director Sally Reed admitted to the San Jose Mercury News”, as reported by Nathan J. Muller.

binds keys to names and accepts transitive trust—even though a proper CPS could also forbid transitive trust in X.509 as a function of the CA's policies (again, the analogy between the web of trust rules in PGP and the CA's CPS rules in X.509).

PGP is based on an “introducer-model” which depends on the integrity of a chain of authenticators, the users themselves. The users and their keys are referred from one user to the other, as in a friendship circle, forming an authentication ring—the term ring is not used here to denote a closed structure but as a mathematical set which can at present be loosely modelled as a trusted list—or “web-of-trust”. At the end, you may not know very well the last person that entered the ring, but you hope that someone else in the ring does. Or you may have different rings, with “contact points” which guarantee the referrals. However, the reader should note that no user can know for sure if everyone in his authentication ring has a valid entry. The term “chain” can be used to denote such connected rings, which can also, of course, be multiply connected.

The reader should notice further that the maintenance of this chain—changing, adding or deleting data—is done by the authenticators themselves, in a happenstance pattern. There is no guarantee if and when the chain is up-to-date. Everyone familiar with the classical problem (or need) of file-locking in a multi-user environment will recognize that there is no “file-locking” mechanism here. So, while PGP enforces a model of trust with “trust is not transitive” to setup entries in the web-of-trust, it uses transitive trust in order to upkeep entries, and without allowing for time factors such as lack of synchronism.

There are several other problems and benefits of PGP, which this paper will not address. This is not intended to be a dismissive treatment of PGP, but rather a focus on commercial applications. It is important, however, to note that one of the benefits of PGP is that it can interoperate with a CA fully-trusted by all parties in a domain (such as an internal CA in a company) that is willing to guarantee certificates, as a trusted introducer. Better tools would certainly be necessary for central administration of PGP trust parameters in a corporate system, but the flexibility of PGP makes it a good example of a quasi-decentralized system.

It is important to note that the concept of “central administration of PGP”—which to some might sound even sacrilegious—is a way to guarantee accountability, coherence, dependability and, above all, correct authentication. Of course, within a circle of close friends this is not important.

Because there is no entity responsible if (or when) something goes wrong—not even the user—the use of PGP in a commercial situation is difficult and may not adequately protect the business interests involved, as they usually need to be guaranteed in well-defined contracts with loss responsibilities and fines. Further, PGP does not scale well in size (because of the aforementioned asynchronous maintenance difficulties of the web of trust) or time (because of the same maintenance problems reflected in the so-called certificate revocation certificates, a CRL for PGP certificates). Again, within a circle of close friends this is not important.

4. SKIP

SKIP implements a linked chain of two-sided node authenticators [SKIP]. Each node authenticator derives its information from a type of directory service. Without dismissing SKIP as a valid and interesting protocol, it is important to note that non-repudiation and other security features that depend on certificates will necessarily also depend on data from the application layer. But, as every step of the SKIP authentication process happens at the protocol level (not at the message level), the SKIP protocol needs to be complemented by a second authentication protocol, in a higher layer.

Note that SKIP is transparent to the user, for better or for worse. This means that SKIP lacks user-tunable controls, such as the rejection, revocation, visualization or choice of certificates. Here, also, a type of “directory service” must be used by the node authenticators to obtain information. This is a type of “central administration of SKIP”—which is needed to guarantee accountability, coherence, dependability and, above all, correct authentication. The difficulties of implementing such an administration system worldwide are compounded by the fact that a given packet route will not have a unique path, not even if the same packet route is being used for a series of requests such as produced when a Web site is visited.

The situation is totally different from, for example, a PGP session, where the authentication is done at fixed endpoints and the routing path is not important. Therefore, the user has no practical way to control the process, can not decide

which node authenticator is reliable, can not exclude nodes which have been infected by the enemy, can not choose to choose certificates, etc. The use of SKIP in a commercial situation is thus difficult because the control decisions are totally removed from the user—who is at risk. Further, the system liabilities are ill-defined and responsibilities for fines and losses hard to recover.

5. Certification, Risks and Privacy Rights

As explained in the introduction to this paper, in the Internet encryption is not a luxury, but a necessity. And encryption without certification is an open door to spoofing and other kinds of attack. However, in each of the three methods analysed above the basic certification questions remain: Who is on the other side? Is the certificate valid? Etc.

To try to cope with this situation, which can have national and international impact, governments have proposed several initiatives. Because: (i) certificates depend on some form of encryption (e.g., X.509), and (ii) encryption does not make sense without certification, the two issues—certification and encryption—are inherently present in all proposed initiatives. Before discussing the other aspects of these initiatives, which range from anti-terrorism to politics and beyond, it is important to review the two most important technical issues, as they have been weighed by this work.

First, the issuing of a certificate by a CA can be seen as a public service and thus must be a par with other public services which must be and indeed have been regulated by the government to avoid abuse and misuse. For example, the biscotti paradigm:

If you want to make and eat your own biscotti, fine. If your neighbor wants to eat some of the homemade biscotti you made for your own consumption, this is also usually fine (unless you fear a lawsuit in case of food poisoning). If you want to buy it from someone else for your own private consumption, it is your decision. But if you want to sell it to the general public or to a store, then you must have a seal of approval and must comply with a set of rules.

The same principle applies to a public service that sells services to provide signature keys, public-keys or passwords. They can be subjected to impersonation, falsification, blackmail, etc., all with great potential harm. In other words, because the social order may be disrupted by this service, it must be regulated by the government. The alternative would be for it to be in effect regulated by criminals, which no one would support.

Second, one must take into account the lawful possibility and need to track communications, under court order, to prevent theft, terrorism and all types of crimes, including spying and national security threats. False certificates or too strong encryption can thwart these lawful prerogatives.

These two technical reasons have provided governments both with a reason as well as with an excuse to step in and issue or propose regulations for the Internet on a national as well as on an international level, regarding the issues of certificates and encryption. Much controversy has been going on in the Internet on this theme [EPIC], both pro and con. It is not a purpose of this paper to add to this controversy or to take issue on these subjects, but rather to present and discuss factual data that is pertinent to the technical discussion of the certification question. Besides, this paper focuses on the question of certificates, leaving the issue of cryptography for other efforts.

According to the TTP [TTP97] certification initiative led by the US [NISTa] and being tested as a potential government policy in the UK, as well as its derived Public-Key Infrastructure (PKI) [NISTb] proposal, the certificates issued by CAs and the CAs themselves would be vouched by a complex chain of certificates that would all depend on some government appointed agency—a type of “seal of approval”, which also provides for mandatory key-escrow. Other initiatives, which can work together with TTP-certification, are the so-called key escrow or key recovery schemes [NISTa], the Clipper chip [Gret], GAKware [Shos95] of the type present in the so-called International Cryptography Framework [HPICF], weak cryptography such as using single-DES, or even propositions to cripple cryptography [NISTa]. All these methods, besides the obvious advantages of a legal and centralized control method, provide however a back door into each person’s or company’s private businesses by giving government agencies the possibility of easy

decryption of otherwise private messages. One could add that these methods make a network systems insecure also by design, whereas before they were insecure by accident.

At the least, these methods may eventually represent the end of the Internet as we have it today: a free, essentially self-regulated and uncensored territory, with no visible national borders. While this is justified by some [Den96] as necessary, “*in order to control crime and anarchy*”, for others [Wise95], “*one should avoid the indiscriminate extension of government to the Internet*”⁷.

Adding other political and commercial undertones, the US, the UK, Australia, Belgium, Canada, France, and The Netherlands have tried to or already did impose some kind of restriction on cryptography, authentication or CAs. However, such restrictions are usually mandated by military treaties and alliances, such as NATO, and have no influence on countries which do not have such commitments. A comprehensive survey is being conducted by B-J Koops [Koop98], with data on almost all countries.

While some may consider this solution acceptable, its clear that not everyone and not every corporation want their private correspondence to be written as in an open postcard. Legal requirements, such as client-lawyer secrecy, patent rights and other internationally protected rights such as diplomatic mail and commerce, also need a different solution.

Against the expansion of centralized control, the OECD (Organisation for Economic Co-operation and Development) has issued its Cryptography Policy Guidelines [OECD], that states:

THE FUNDAMENTAL RIGHTS OF INDIVIDUALS TO PRIVACY, INCLUDING SECRECY OF COMMUNICATIONS AND PROTECTION OF PERSONAL DATA, SHOULD BE RESPECTED IN NATIONAL CRYPTOGRAPHY POLICIES AND IN THE IMPLEMENTATION AND USE OF CRYPTOGRAPHIC METHODS. GOVERNMENTS SHOULD CO-OPERATE TO CO-ORDINATE CRYPTOGRAPHY POLICIES. AS PART OF THIS EFFORT, GOVERNMENTS SHOULD REMOVE, OR AVOID CREATING IN THE NAME OF CRYPTOGRAPHY POLICY, UNJUSTIFIED OBSTACLES TO TRADE.

Thus, while it is clear that all the models reviewed (e.g., X.509, CA, PGP, SKIP) do not offer adequate certification per se and actually demand some type of control—in order to avoid crime and anarchy—the consequences of such a control (e.g., TTPs, GAKware or key escrow) as they are being planned today would most probably jeopardize the free use of standard Internet practices, such as PGP mail encryption, SSL-enabled connections, e-commerce, etc.

6. Conclusions

As seen above, X.509 Certificates, CAs, PGP and SKIP need some type of centralized certification control systems in order to be useful in commercial situations. This is the conclusion of each section. There seems to be however a basic systemic conflict between this need and the Internet architecture—which is totally decentralized and very independent in actions as well as in form. While this seems to motivate the eventual uselessness of centralized governmental controls, since we have no centralized world governance or law, how can we provide for the necessary controls in the current environment?

The paper recommends users and subscribers to carefully use their due dilligence when relying on certificates and CAs and provides a series of security considerations, as guidelines to enhance security and privacy in Internet communications. Certificates are not magically infused with trustworthiness just because they are digitally signed. The signature, the contents or both may be totally wrong or revoked.

⁷ Internet access blocking: Some countries block themselves from the Internet, where a sanitized intranet serves the country. The same happens in reverse, when entire countries or domains are or were blocked. In 1997, an entire ISP in Holland has been blocked from the Internet in Germany, because of some www pages published by one of the ISP's clients: in April 11th 1997, the XS4ALL website www.xs4all.nl was censored by the Deutsches Forschungsnetz, the German academic Internet provider. This was confirmed by Dr. Klaus-Eckart Maass, managing director of Deutsches Forschungsnetz in a press release. The pages in question, however, were mirrored in other sites elsewhere in the world and it was thought that it would be near impossible to find and block all such sites. The same situation happened in Canada, with the Homolka case, with the result that it was indeed impossible to block the information spread and access.

One further conclusion is that Governments may need to better adapt control policies to the times at hand. Everyone knows the story of the person that always used a hammer in his work and thus thought that all problems were nails. Modern problems need modern solutions. It is one of this paper's assertion that technology may provide the answer—as well as it did provide the problem—but the answer lies not in an increased control that would be impossible, rather it predicates a paradigm change: “The Internet is at odds with centralized control—thus Internet control must be decentralized in order to be effective”. Note that this principle does not imply the absence of some type of control or “checks and balances” situation—that would be incoherent with this paper and with logic, but indicates that new control types are needed. The new control types can perhaps already be felt in many areas, as a grass-roots development, for example as discussed in the Internet Paradigm exposition by Einar Stefferud [Stef98].

The Meta-Certificate Group – MCG [MCG], an international non-profit open group that includes participants from 26 countries, is currently investigating the Internet certification and security questions. The MCG is drafting a proposal for an open standard-track Internet RFC, describing a layered certification protocol called “Meta-Certificate”, designed to enhance security and flexibility, that should allow either standalone operation or interoperability with current technologies such as X.509, CAs, PGP, SKIP, etc. The present paper was developed as part of the fact finding and modelling work for such effort.

Acknowledgments

The author acknowledges helpful hints and discussions with members of the Meta-Certificate Group, L. Zorzella, L. Machado, Einar Stefferud and Nicholas Bohm MA (Cantab), Solicitor of the Supreme Court of Judicature in England and Wales, also members of the e-carm list, ssl-talk list, ssl-users list, cert-talk list, SPKI list, IETF S/MIME list Usenet newsgroups such as talk.politics.crypto, sci.crypt, comp.security.misc, comp.security.pgp.discuss, and the Internet community. The names herein cited does not mean their endorsement or responsibility in this work, which is the sole responsibility of the author, reflecting his viewpoints—not the viewpoints of any corporation, company, agency or Governments.

* The author is with Novaware, Av. Albert Einstein 1301, SOFTEX/UNICAMP - Campinas – SP - Brazil;
<http://novaware.cps.softex.br>

Copyright © 1997, 1998 by E. Gerck.
All rights reserved, free copying and citation allowed with source and author reference.

References

[Ave98] Juan Avellan “Digital Signatures Links”, in <http://www.qmw.ac.uk/~t16345/>

[Bak98] Phillip Hallam-Baker, public discussion, in <http://www.mcg.org.br/cgi-bin/lwg-mcg/MCG-TALK/archives/mcg/date/article-379.html>

[Boh97] N. Bohm, “Identity”, In MCG Web Page, <http://www.mcg.org.br/identity.txt>, April 1997

[Canada] Canada Post 20-year certificate, in http://www.mcg.org.br/2016_cert.gif

[Den96] Dorothy Denning, “THE FUTURE OF CRYPTOGRAPHY”, in http://www.cypher.net/info/pub/itar/denning_0296_cryptoanarchy.article

[EPIC] “INTERNATIONAL CRYPTOGRAPHY POLICY”, in <http://www.epic.org/crypto/intl/>

- [Fel97] Edward Felten et al., “Web Spoofing: An Internet Con Game”, in 20th National Information Systems Security Conference (Baltimore, Maryland), October, 1997. Also, <http://www.cs.princeton.edu/sip/pub/spoofing.html>
- [Ger97a] E. Gerck. “Overview of Certification Systems: X.509, CA, PGP and SKIP”. In MCG Web Page, <http://www.mcg.org.br/cert.htm>, April, 1997.
- [Ger97b] E. Gerck. “Certification: Extrinsic, Intrinsic and Combined”. In MCG Web Page, <http://www.mcg.org.br/cie.htm>, July, 1997.
- [Ger98] E. Gerck, “The role of trust in certification”, in <http://www.mcg.org.br/augustine.txt>, Feb., 1998.
- [GerBoh] E. Gerck and N. Bohm, “X.509 Certificates: a readable unabridged inside view” in <http://www.mcg.org.br/x509cert.htm>
- [Gret] Ed Grether, “Clipper Chip Information Resources”, in <http://www.northlink.com/~egrether/clipper.html>
- [Gut98] Peter Gutmann, “X.509 Style Guide”, in <http://www.cs.auckland.ac.nz/~pgut001/pubs/x509guide.txt>
- [HPICF] “Hewlett Packard’s International Cryptography Framework”, in <http://www2.hp.com/pressrel/nov96/18nov96c.htm>
- [Illii] “ILLINOIS ELECTRONIC WRITING AND SIGNATURE ACT – Draft with comments”, in <http://www.magnet.state.ma.us/itd/legal/106192.htm>
- [Koop98] Bert-Jaap Koops, “Crypto Law Survey”, in <http://cwis.kub.nl/~frw/people/koops/lawsurvey.htm>
- [McCur] Kevin McCurley, “DigiCrime is now known as root@localhost”, in <http://www.digicrime.com/id.html>
- [MCG] MCG - The Meta-Certificate Group, is an international non-profit open group. The MCG is a fresh exploration of applied cryptography to solve real-world Internet security issues of today, for both individuals, corporations and governments, as represented by the current certificate questions. The MCG Home-Page is at <http://www.mcg.org.br>
- [MOV97] A. Menezes et al., Handbook of Applied Cryptography, CRC Press, New York, 1997.
- [NISTa] “US Cryptography Policy”, in <http://csrc.nist.gov/keyrecovery/policy.txt>
- [NISTb] “NIST PKI Program”, in <http://csrc.nist.gov/pki/>
- [OEDC] “Cryptography Policy Guidelines”, in <http://www.oecd.org/dsti/sti/it/secur/index.htm>
- [PGP] Website at <http://www.pgp.com>
- [PKIX] IETF PKIX, in <http://www.ietf.org/html.charters/pkix-charter.html>
- [RSA] “Internet Services” certificate, in <http://www.mcg.org.br/certspell.gif>
- [Shos95] Adam Shostack, “Response to NAS Crypto Questions”, in <http://www.homeport.org/~adam/NAS.html>
- [Simp97] Ian Simpson, “Modeling the Risks and Costs of Digitally Signed Certificates in Electronic Commerce”, in <http://www.ini.cmu.edu/NETBILL/pubs/certlife/certlife.html>
- [SKIP] Website at <http://skip.incog.com>
- [SSLa] <http://home.netscape.com/eng/ssl3/ssl-toc.html>
- [SSLb] <http://www.netscape.com/newsref/std/SSL.html>
- [SSLy] SSLey, in <http://www.psy.uq.oz.au/~ftp/Crypto/>

[Stef98] Einar Stefferud, “What is the Internet Paradigm? – A Virtual Seminar”, in <http://www.mcg.org.br/paradigm.htm>

[TTP97] “LICENSING OF TRUSTED THIRD PARTIES FOR THE PROVISION OF ENCRYPTION SERVICES”, in <http://www.cl.cam.ac.uk/users/rja14/dti.html>

[UCC] US Uniform Commercial Code, in <http://www.law.upenn.edu/bl/ulc/ucc2/ucc2b296.htm>. See also *Hartong v. Partake, Inc.*, 266 Cal. App. 2d 942, 966, 72 Cal. Rptr. 722, 737 (1968); *Hefferan v. Freebairn*, 34 Cal. 2d 715, 719-20, 214 P.2d 386, 388-90 (1950); *Mariani v. Schonfeld*, 126 Cal. App. 2d 187, 189-90, 271 P.2d 940, 942 (1954).

[Utah] “Utah Digital Signature Program”, in <http://www.commerce.state.ut.us/web/commerce/digsig/dsmain.htm>

[Wise95] Dov Wisebrod, “Controlling the Uncontrollable: Regulating the Internet”, in <http://www.catalaw.com/dov/docs/dw-inet.htm>

[X500a] RFC 1308, in <http://www.cis.ohio-state.edu/htbin/rfc/rfc1308.html>

[X500b] ITU-T X.500, in <http://www.mcg.org.br/mirrors/97x500Rev0.doc>

[X509a] “Summary of ITU-T Recommendation X.509”, in http://www.itu.int/itudoc/itut/rec/x/x500up/s_x509_e_30924.html

[X509b] ITU-T X.509v3, in <http://www.mcg.org.br/mirrors/97x509final.doc>
