Collegial Certification Works for Truly Collegial Communities – But What Happens When Real Money and Power Are Involved?

By Wes Kussmaul

What is a certificate supposed to be?

The intended purpose of digital certificates is to be our protection against the nefarious work of scammers, botnet builders, and the growing landscape of fraud, theft, and bad deeds on the Internet. A certificate, whether on paper or in digital bits, consists of *authority* attesting to the validity of an *assertion*. In the familiar world of paper documents, a **driver's license** is authority attesting to the validity of the assertion that an individual is competent to drive. A **passport** is authority attesting to the validity of an individual's legal right to travel abroad. A **birth certificate** is authority attesting to the assertion of an individual's parents and hospital staff to the circumstances of their birth.

In the digital world, a **site certificate** should be authority attesting to the validity of an assertion of site ownership, and an **identity certificate** should be authority attesting to an individual's assertion of who they are.

However, unlike the attestations in the more traditional paper forms of certification – where the source of authority is clear – site and identity attestations all too often come from marketing efforts of commercial enterprises whose aim is to convince the public that they possess authority that, in fact, they do not.

> *Commercial certification authorities protect you from anyone from whom they are unwilling to take money.*
>
> *– Matt Blaze*

In other words, they protect you from no one – since commercial certification authorities are in business to make money and will gladly take it from anyone in exchange for a certificate.

So-called "certification" can be performed by anyone with a server running some software. With no criminal or civil liability – such as that which a notary public takes on when he puts his name and seal on a document – the inevitable result is digital certificates made and sold like the pretend birth certificates shipped with children's dolls, dressed in flashy words like "cryptography" and "secure socket layer."

Collegial certification – sounds good

The consequences of this casual treatment of the concept of "authority" has led some to question the way certification is performed, as evidenced by their creation of a relatively non-technical certification concept that makes sense in some situations. Recognizing it as a workable and valid system for certain types of small communities, we have named this concept **collegial certification**.

In collegial certification, formal certificates are replaced with signatures of acquaintances and colleagues whose personal knowledge of the subject individual allows them to attest to validity of the subject's identity claims. This is a reasonable and valid descendant of the age-old trust concept of village members trusting the word of others they know in the village.

The original PKI-based form of collegial attestation was Phil Zimmerman's PGP — Pretty Good Privacy. PGP was a complete system providing both attestation of identity and a well thought out way to build communities of encrypted information exchange. It defined standard formats for the exchange of public keys and symmetric keys, the signing of messages and files, encryption, and certification. The non-commercial version, OpenPGP, is responsible for most of the world's encrypted email.

OpenPGP uses a decentralized system of trusted "introducers," which are the same as a certification authority, thereby sidestepping the mistrust of centralized authority. Anyone can certify anyone else using this network of introducers, where a trusted introducer can introduce others to *their* trusted introducers. The idea is that it takes two trusted introducers to certify, supposedly providing fault tolerance in case one introducer is corrupted. But where is it written or expected that *any* number of introducers can't be corrupted?

There have been a number of implementations of the collegial certification concept offering an assortment of improvements. But none addresses the underlying flaw in collegial certification: the intrusion of the corrupting influence of money or power, which can sneak in unseen and unexpected.

The unfixable problem

Our existing certification infrastructure is broken for exactly the reason cited above by Matt Blaze. But is collegial certification the answer? Let's look at this statement: "You should only trust honest and sophisticated introducers that understand what it means to sign a key, and will exercise due diligence in ascertaining the identity of the keyholder before signing the key in question." How hard would it be for, say, a few members of a corrupt campaign staff or a group of shady characters to conspire to convince a PGP key holder that a particular individual is someone who he is not? Do that a few times with a few different key holders and voilà, you have a corrupt little weblet of trust that is fully integrated into the network of trusted "introducers."

In a worldwide faculty club where little money is at stake, collegial attestation can work. Wikipedia's entry under PGP notes that the problem of correctly identifying a public key as belonging to a particular user – that is, assuring the integrity of the identity certificate – is not unique to PGP. All public key / private key cryptosystems have the same problem, if in slightly different guise, and no fully satisfactory solution is known.

What is the solution for our "global village" of billions?

Collegial certification is an excellent solution for groups whose members care enough about their information infrastructure to understand how they work and to guide their operation. However, collegial certification does not help solve the issue of certification for the majority of the world's population, who have little or no understanding of certification in the digital realm. How easy would it be for organized scammers and criminals to game a collegial certification system and convincingly portray their certifications as reliable.-

The Authenticity Infrastructure portion of the Quiet Enjoyment Infrastructure specifically addresses the flaws that collegial certification simply cannot resolve because they are rooted in human factors that can't be fixed by technology alone. These elements are the foundation of the new PKI-based Authenticity that we call PKI Done Right:

Duly constituted public authority. The City of Osmio, a root certification authority, is the worldwide version of a City Hall, where birth certificates and other attestation documents are kept. Osmio was chartered on March 7, 2005, in Geneva Switzerland, at the headquarters of the International Telecommunication Union. Its root key signing ceremony was executed and documented on September 12, 2017.

Professional liability. Signers of site certificates, code signers, and others who put their good name on permits and other attestations are professionally liable for the integrity of what they vouch for, just as notaries are for the documents they notarize.

Personal accountability. Identity certificates represent real human beings with measurable certainty, providing complete privacy but for accountability (unmasking) by court order.

Conclusion

If a collegial certification system assumes that its members are special, that they are uniformly and always trustworthy, the system may work for a while. But when real money or power creep in – nearly as certain as rain – the system breaks down. That's why a good system is built not on the naïve "trust, but verify" cliché but rather on "distrust until there is reason to trust, and make sure accountability is built in." A combination of duly constituted public authority, professional liability, and clearly defined personal accountability provides a strong defense.