2 – The Public Authority Component

Question 2 *Reliable digital identity certificates, professional licenses, and occupancy permits call for a reliable source of issuing public authority that is independent of any geographic jurisdiction. Where do we find such a source of duly constituted global public authority?*

Answer 2 The Public Authority Component

On March 7, 2005, the City of Osmio was chartered at the Geneva headquarters of the oldest international governance body in the world, the International Telecommunication Union. Osmio's Vital Records Department is a certification authority that limits its practice to creating, maintaining, and protecting identity certificates. Osmio's Professional Licensing Department will issue licenses that allow architects, contractors, and building inspectors to sign plans for facilities and occupancy permits. Osmio's authority is strictly limited to those who choose to accept it, and its governance is as participatory as that of a small New England town.

Back to Identity Certification

When it comes to Internet identity, single sign-on seems to get the bulk of the attention. The benefit is clear: one username and password log you in to thousands of sites. And isn't that what we all need? An end to rampant password proliferation? Especially if the single sign-on system includes a way to prevent nosy marketers and governments from tracking that ID.

But as with everything, there's a right way and a wrong way to do it. In principle, an identity that is provided by any single sign-on provider will let you sign in to thousands of other sites. Kim Cameron, an identity expert who knows all about single sign-on, explains the popular OpenID single sign-on system in a video on his Identity Weblog[46].

OpenID is an Internet Single Sign-On standard that is supported by Google and Yahoo and Facebook and hundreds of other OpenID identity providers. In fact, the Osmio Vital Records Department is an OpenID identity provider.

Kim Cameron's blog shows what's good about OpenID — fairly universal single sign-on — as well as something that's not so good: it is quite vulnerable to phishing attacks. When successful, an attack leaves what he calls the "evil site" with everything its owners need to log in to all your sites that accept OpenID. When that happens, and your OpenID is compromised in one place, it's compromised everywhere.

Kim then introduces something that he feels fixes the OpenID problem: The Information Card and the CardSpace infrastructure of which an Information Card is part.

46 http://www.identityblog.com/wp-content/images/2008/02/OpenID/Normal/OpenIDPhish.html.

Well, an Information Card is a digital certificate. Kim's point is that OpenID's vulnerability calls for a solution, and that solution is a version of PKI.

And of course we agree. PKI done right fixes the problem not only with OpenID but with similar single sign on systems. CardSpace and its Information Cards purportedly fix the problem with OpenID.

But does it really?

The claim in the video is that "information cards employ advanced cryptography, so using an Information Card at an evil site gives away nothing that compromises your access to legitimate sites." And that is true. Information Cards has the right idea.

But let's parse that statement, "Information cards employ advanced cryptography..." (mmmm, Advanced Cryptography...sounds impressive....)

Advanced cryptography is good. You use it every time you go to a site that starts with HTTPS://. Advanced cryptography builds an SSL/TLS tunnel between your computer and a site. And it's true, no one can get into the middle of the tunnel.

But wait.

Suppose all your personal information were kept in a physical room with a super-advanced lock on the door, impossible to pick. Secure, right?

But who has the keys?

Kim Cameron is a distinguished identity professional who happens to work for Microsoft. CardSpace and Information Cards are Microsoft products. Not that there's anything wrong with Microsoft. It's just that...who keeps the keys? Microsoft?

And wait. This is all about certificates and certification. After all, what is an InfoCard but a certified identity credential? An InfoCard is based upon a digital certificate, and any certificate, whether on paper or on bits, consists of authority attesting to a claim.

A birth certificate is authority attesting to the circumstances of your birth. Public authority, that is; the official record of your birth is not made and certified by a commercial enterprise. The very notion is preposterous.

Authority in the context of identity credentials also should mean public authority.

As in city hall. Where policies are a matter of law, not some corporation's whim. And where public officials can administer oaths that carry the penalty of perjury.

For attestation to be worth anything, it must be done by duly constituted public authority.

Fungible Authority

Authority, particularly public authority, has a reputation for being bureaucratic, for being about forms and procedures. Some forms of authority, however, are available more or less on demand, and for a price, much like a commodity. They can be brought to bear on a situation in as flexible a manner as ordering up some building materials for a construction project. "You need 24 kilograms of Type 4 authority? I'll have it delivered tomorrow afternoon."

The authority of attestation professionals — CPAs and chartered accountants, court reporters, signing agents, justices of the peace, and notaries — is similarly available on demand. Their authority is well-defined, consistent, and duly constituted by a governing body. As a result, this authority is the same, no matter which individual professional provides the authentication service to you. As independent professionals, they serve clients in the same manner as any professional service provider.

Q: Is authenticity a producible product?

A: Yes, absolutely.

Authenticity may be produced at various levels of quality. The raw materials that go into it are

- Assertions (claims) of individuals
- Attestations from public authority
- Authenticity conveyance infrastructure (PKI)

The foundational assertion and attestation, the one that all others are built upon in a village, whether it's a village of 700 people or a global village of 7 billion people, is that of identity. And the first and essential meaningful attestation is by duly constituted public authority. Attestation by others simply augments that.

One problem with most PKI implementations is that very little attestation is done by public authority. That's one of the first things that the Quiet Enjoyment Infrastructure version of PKI sets out to fix.

The Authenticity Institute provides support to organizations that have chosen to implement the principles, methods, and procedures of the Quiet Enjoyment Infrastructure. The slogan of the Authenticity Institute and its licensees, both commercial and noncommercial, is, "Identity is the Foundation of Security."

Really, that's shorthand for "Public Authority is the foundation of Reliable Identity, which is the Foundation of Authenticity, which is the Foundation of Security and Accountability and Manageability and a whole lot of other good things."

Identity is manifested in digital identity certificates, PKI-based credentials that are technically identical to the digital certificates that attest to the ownership of websites. The difference is that an identity certificate attests to a person's identity rather than a site's ownership.

Recall from Chapter 8 that a digital certificate and its corresponding PEN (private key) solve the big problem with digital identities: a hacker can capture all the bits that go back and forth when you authenticate yourself to a site, but unlike a password or other digital identity credentials, those bits will do him no good. He will not be able to impersonate you.

Unlike an account password, your PEN is never transmitted but rather just solves puzzles presented to it to prove that you are you. Furthermore, if the whole system is

designed properly, you can be anonymous and accountable at the same time. Your privacy is protected.

Who Sez?

So your digital identity certificate says that your claim of identity is valid, that you are indeed you. But who issues the certificate? If a PKI includes something called a "certification authority," then who is the authority?

What is authority? Over millennia human society has developed superb answers to that question. But lately we seem to have forgotten the answers. Lately what I call collegial attestation has been put forward in a number of forms, letting "good people" attest to the validity of each other's claims. That can work for a while, as long as substantial money, power, and reputations are not involved. We'll go into the collegial attestation initiatives after describing how the relationship between trust and authority developed historically.

A Brief History of Trust

While we tend to think of science and technology as a steady march forward to better solutions to harder problems, sometimes the march is in the opposite direction. Sometimes new products suffer from problems that already have been solved. Solutions can be forgotten; technology sometimes goes backward.

If you visit a 200-year-old New England home you'll see shallow little fireplaces that jut out into just about every room. They look useless, as though they'd just fill the room with smoke. Because of the work of Benjamin Rush and other early researchers in fluid dynamics, a system of flue baffles provides reliable draft in those old fireplaces, drawing smoke away even on windy days, while the positioning of the fireplace radiates the most heat possible into the room. Compare those old fireplaces to the big, deep, ineffective smoke belchers in new homes and you have one example of technology gone backward.

And so it is with the methods and procedures of the production of authenticity.

As we noted earlier, PKI is old. It's been around for decades. Yet the fundamental principles behind the production of Authenticity are much older, going back centuries and even millennia.

Conveying Trust Without Electrons or Photons

If you follow the contemporary debate about security you can find yourself tacitly assuming that before the Internet the world had never encountered security problems; that people never had to know whether to trust or distrust strangers and their documents and assertions.

But of course human society has needed trust systems for millennia, and has instituted systems of trust that were effective in the absence of systems of communication. If a stranger presented you with a document purporting to be an offer from Napoleon to sell the mid-section of a continent for $15 million, you couldn't just pick up a phone

and call around to find out whether it was real. The document itself, along with the circumstances of its presentation, had to convey the information for judging its authenticity.

Making matters more difficult was the widespread illiteracy even among people of means. How would you engage in a transaction with someone just a few hundred miles away if you couldn't read and had no means of communication other than paper carried by a courier on horseback? How could you even know the details of the contract, let alone trust it?

The Tabellio

The Roman Empire developed elaborate and workable systems of property ownership, governance, and commerce throughout its vast and multi-lingual provinces. A significant part of the answer was a well-developed system of trust that depended upon attestation professionals: the scribes and tabelliones[47].

The term tabellio referred to a Roman officer who put into writing the necessary forms, agreements, wills, and other instruments, and witnessed their execution. Some of their responsibilities were judicial in nature, and there were no appeals from their judgments.

Notaries were the clerks of the tabelliones. The notarius, essentially a trusted public stenographer, listened to a description of the agreement of parties, reducing it to short notes. The resulting legal instruments then were written in extenso, which was done by the tabelliones on wax tablets. The workings of Roman society depended upon the integrity of the tabellio.

Imagine the challenge of transporting accurate copies of those wax tablets to interested parties, in a confidential and accurate and timely manner, without the aid of any communication technology more effective than a box on a horse drawn vehicle. That challenge, it would seem, is much more difficult than securing spaces that are accessed via the Internet.

Over the years, other offices have been instituted with similar responsibilities. The office of Justice of the Peace originated in 1195, when England's Richard the Lionhearted commissioned certain knights to preserve the peace in regions of unrest. Directly responsible to the king, they were designated custodes pacis, keepers of the peace, changed to Justices of the Peace in 1361 under Edward III. Eventually the police duties were left to constables, and the office of Justice of the Peace became much like that of the ancient tabellio.

The office of the notary also has evolved over time. In most jurisdictions it has been promoted from that of trusted clerkships to attesting officers to the attesting officers themselves.

---

47 Lectric Law Library Lexicon, 2001, and *The Future Needs You: The Notary Public In The Digital Age*, PKI Press, 2004.

More recently other attestation professions have appeared. Chartered accountants and certified public accountants, certified court reporters, commissioners of deeds, consular documentary officials, and others each provide some elements of a trust network.

For centuries the notary public had a role in just about all dealings among strangers. In some jurisdictions, the public office of notary is still strong and respected, with high qualification standards required. In India, for example, only licensed attorneys who have practiced continuously for 10 years without a significant blemish on their record may be considered for the position. (The Indian form of affirmative action reduces that to eight years for women and members of the lower castes.) India has 1,570 notaries serving a population of more than a billion people.

In contrast, to become a notary public, an appointed public official, in Massachusetts, you'll need $50, four signatures on a form, and a trip to the State House. If you can't get to the State House, other arrangements can be made. As long as you can come up with the fifty dollars.

I myself am a notary in Massachusetts. Theoretically, my background was thoroughly checked before I was appointed a public official. In reality there is no background check, no fingerprinting, not even a social security number, required.

According to the National Notary Association there are 4.5 million notaries in the United States.

In general, notary qualification standards are much higher in Latin law countries than in common-law jurisdictions. They also tend to be high in regions where conditions resemble those of the Roman Empire, with poor communication infrastructure, widespread illiteracy, and commerce conducted in many languages.

But the variation in those standards is not the end of the story. Every notary public in every jurisdiction is a public official. Malfeasance in office is not just a matter of exposure to possible litigation; any notary anywhere who knowingly attests to a falsehood in the performance of official duties is subject not only to litigation, but also to criminal prosecution.

Any notary anywhere may administer an oath, which puts the affiant (the person taking the oath) under penalty of perjury. (Actually anyone at any time may put themselves under penalty of perjury, but without the notarized affidavit they later may just as easily deny or disclaim that act.) There's more to this apparatus of trust than the demonstrated good character of the notary or other attestation official.

Theoretically, notaries have a built-in strong incentive to do their job with great diligence. Unfortunately, the universality of the legal basis of the office of the notary means little if the holders of the office in some jurisdictions are so unqualified as not to understand it. How many of the four and a half million U.S. Notaries would immediately quit if they understood they could go to jail for doing the job improperly? Therein lays a big problem with any attempt to bring authenticity to a wired world that desperately needs it.

There is, however, no universal, worldwide designation for notaries, and therein lies a big problem with any attempt to bring authenticity to a wired world that desperately needs it. Of all things, the telephone is responsible, in my opinion, for the problem.

The Collapse of the Notary Profession in the Telephone Century

Through the centuries and around the world, the environment in which systems of trust has had to function changed little. Even the Renaissance and the Enlightenment brought only the recording of contracts on paper instead of wax. It wasn't until the deployment of the telegraph and telephone that trust systems started to change.

What happened to the notary profession in 20th century North America?

People got phone calls that went like this: "Harry, this is Mary. I just talked to an old acquaintance named Fred who has a deal on a gross of frammets that I can't take advantage of. I know you're in the market for them so I suggested he call you. He's a good guy, always delivers. So how are the kids?"

Or, just as likely, "Hi Nancy, what's up? Yeah, I did business with that guy. No, forget terms, with him you need to get cash. He shows up with a letter of credit but ends up not using it, it's probably no good. I had to wait five months to get paid. Be careful of him."

The proliferation of telephones created a vast referral network that could be used to calibrate the trustworthiness of strangers. References, contacts, the straight story on other people were as available as your phone. Referrals tended to come from networks of existing relationships where at least one member knew the new contact, and they had a very important aural cue to their authenticity: you recognized the voice of your acquaintance on the telephone.

Conveying Trust *with* Electrons and Photons

We have come full circle, back to the 19th century, where anybody can be anybody. People show up on your online doorstep with all sorts of offers and ideas, and you have no idea whom to trust.

After being briefly marginalized, the role of attestation from public authority is back, as vital in the 21st century as it was in Roman times.

Wax seals and PKI serve the same purpose: they exist to convey authenticity. They may both be considered authenticity conveyance infrastructures.

The quality of the authenticity conveyed by a wax seal is not the same as the quality of the seal itself. If the seal die is issued carelessly or if it is kept in a space where anyone can use it, then it makes no difference how much care was taken to make the seal irreproducible. In precisely the same way, if a PKI certification authority issues digital certificates carelessly, or if its certification and certificate verification processes are vulnerable to intrusion, then it makes no difference how much care was taken in choosing the PKI technology.

In fact we do have companies selling all sorts of server certificates and identity certificates and code signing certificates, all using tried and tested technology. They publish their certification practice statements, in the hope that stating their intentions with rigorous precision will make up for the absence of the one raw material not available to them in the manufacture of those certificates. But the missing ingredient, of course, is authority.

The certification "authorities" issuing the vast majority of certificates simply lack, well, authority. They are commercial enterprises that can be bought and sold, and in fact the largest one, VeriSign, was sold in 2010. The buyer happened to be a legitimate enterprise (Symantec) but there's absolutely nothing to prevent some sketchy and disreputable global conglomerate from buying certification "authority."

In Chapter 6 we predicted that an online organized crime group will purchase one or more small banks, getting past the obstacles to laundering money. The purchase of a respected certification authority business would complete its process of metastasizing into an inseparable part of the global economic body. Then we'll all be back in the role of the prehistoric farmer, required to hand over our geese and pigs and autonomy and money to the global protection racket gangsters just to stay alive.

Certificates issued by such commercial certification "authorities" simply are not reliable. While it may be too glib to say that trust cannot be bought and sold, it is true that authority cannot be bought and sold. Authority just is. Authority may be applied to a process for a price, but authority's only asset value exists in the fact that it means something.

What is Authority?

Trust Management Engineer Matt Blaze:

"A commercial certification authority protects you from anyone whose money they refuse to take."

Take a moment to think about this quote from Matt Blaze who, like Moxie Marlinspike, often finds himself in the important role of the boy who calls attention to the digital emperor's lack of clothing. Let's take a look at how the certification "industry" is stark naked. We'll put technology aside for the moment, because certification really has little to do with technology. Paper certificates and digital certificates both fulfill exactly the same function.

A Certificate Is Authority Attesting to a Claim

A certificate consists of a source of authority attesting to an assertion or claim made by someone other than that authority. Historically a certificate took the form of a seal or signature on a paper document. As we have learned in our discussion of PKI (puzzle kit infrastructure), a digital certificate can serve the same purpose more reliably, because while a signature or a seal on paper is not that hard to fake, it is impossible to fake a digital certificate that corresponds to a well-protected PEN (private key) of sufficient length.

That is, impossible to fake if the certificate was issued properly. But here's where the system falls apart. The PKI construction materials are solid, even brilliant. But the completely nontechnical job of checking out the claims being attested to is often done very sloppily and casually.

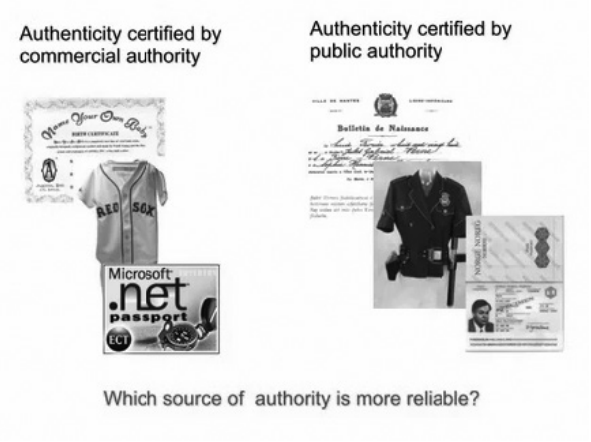
And why not? Companies in the certification industry assume none of the criminal liability that public officials, such as notary publics, take on when they put their good names and seals on a document. Making matters worse, there is also very little civil liability involved. The inevitable result is that digital certificates are sold in the marketplace. It seems so obvious that it shouldn't be worth noting. But as long as we leave security to the experts, the best we can hope for is good technology applied using bad practices.

Recall the message that if you are not a security expert then you know more about how to establish security than a security expert does. In the Never Never Land of security on the World Wide Web, if the subject isn't technology, then the subject is not even perceived. Authenticity and authority? What kind of app is that?

So just push technology aside for a moment while we address a very important question.

Who should certify?

Well, anyone can claim authority and attest to anything. Whether the attestation is worth anything is another matter. If you're the president of your comic book collectors' club, you can certify that someone is a member. If you're the maker of Cabbage Patch dolls, you can issue Cabbage Patch birth certificates.



But can you imagine what life would be like if the local pawn shop and payday loan outfit were able to issue real birth certificates, passports, and drivers' licenses? Consider the attestations in this illustration. Top left is a birth certificate for a Cabbage Patch; top right is a real birth certificate.

A uniform isn't a certificate, but a uniform does constitute a form of certification. Here are a couple of uniforms. Pay a little extra and get a baseball uniform that is indistinguishable from that of a genuine (certified) professional athlete. But don't try faking the uniform on the right. It's a form of certification by public authority.

Then there are passports – a Microsoft .net Passport identity credential and a real passport. Use whatever name you want for the one on the left, but don't try that with the one on the right.

Generally speaking, certification by public authority is in an entirely different category of quality from certification by a private party[48].

The vital records department of your city or country attests to the information claimed on your human birth certificate. The U.S. Department of State, the U.K. Home Office, or a similar office of state in your country of citizenship attests to your claimed right to travel, as evidenced by a certificate called a passport. Your police department commissions officers to apply public authority in the enforcement of law. The professional licensing departments of your state, province, or municipality attest to the claims of architects, contractors, and building inspectors that they are qualified to practice their professions.

The manufacturer of Cabbage Patch Dolls is the appropriate authority to certify the circumstances of a doll's "birth." Officers of organizations apply the authority of the organization when they sign the minutes of a board meeting. But in the other examples, certification must be done by duly constituted public authority. No other authority is appropriate or adequate.

To illustrate why that's the case, imagine if the physical world worked like this:
In fact, this is exactly how certifications of authenticity are sold online.

This is what protects the integrity of the world's information infrastructure. Certification is packaged and sold like bags of garden fertilizer. Which is appropriate, considering what commercial certification amounts to. Where on earth did we get the idea that some corner check-cashing and payday loan outfit should be issuing certificates?

How can an industry whose only product is authenticity fail to pay attention to the need for authenticity? The answer is simple: It never occurred to them that authenticity is what they are supposed to be producing. They think they're all about "selling certificates." The whole business seems hard for non-IT people to understand. Outsiders chalk it up to the opaqueness of technology, when they should instead listen to their instinct telling them it's just plain nuts.

---

48 A signature by an officer on a corporation's document might be cited as a certification by private authority with real consequence. Note, however, that if the certification attests to something that is found to be fraudulent, the consequences are very different if the corporation is public, that is, regulated by a public securities regulator such as the SEC, or private. Public authority wields criminal sanctions; it is authority with teeth.

A quick look at the accepted definition[49] of "certificate" and "certification authority" should tell you that something is seriously wrong:

> **Certificate**
> A token which underpins the principle of trust in SSL-encrypted transactions. The information within a certificate includes the issuer (the Certificate Authority that issued the certificate), the organisation that owns the certificate, public key, the validity period (usually one year) of the certificate, and the hostname that the certificate was issued in respect of. It is digitally signed by the certification authority so that none of the details can be changed without invalidating the signature.
>
> **Certification Authority**
> An organisation which is used to confirm the relationship between a party to the https transaction and that party's public key. Certification authorities may be widely known and trusted institutions for Internet based transactions (see third party); where https is used on companies internal networks, an internal department within the company may fulfil this role (see private certification).

So let's apply the same lexicographical methods to come up with a definition of the paper version of a certificate and the paper certificate version of a certification authority:

> **Certificate**
> A piece of paper made from cellulose fibers that has been treated with sulfuric acid and other substances, turning it into vellum or parchment paper, upon which three things appear: 1) permanent printed writing, 2) the handwritten name of one or more individuals, and 3) an embossed insignia.
>
> **Certification Authority**
> An organization that produces certificates.

Rather misses the point, no?

What else can be said about this ridiculous gap between the substance of certification, whether on paper or bits, and the completely vacant use of the concept in information technology practice? And we have all just bought this stuff, hook, line, and sinker? Simply astounding.

Let's Step Outside For a Moment

Most of the merchandising — yes, merchandising — of commercial certificates is aimed at owners of websites rather than at the bankers and health-care administrators and managers who could benefit from identity certificates. That's mostly because if you leave

49 Netcraft SSL Survey Glossary, https://ssl.netcraft.com/ssl-sample-report/glossary.

out the costly authenticity ingredient, site certificates are enormously profitable. Identity certificates, not so much.

Site certificates are digital certificates that attest to a site's legitimacy, that is, they attest that the site or its domain is in fact owned and controlled by the organization that claims to own and control it. When you buy something at https://qualitystuff.com, its site certificate assures you that it's really the site of QualityStuff, Inc., and not some impostor's phishing site angling to capture your credit card information.

That is, it's supposed to assure you of that. But when you see that https://, or when you see the further assurance of a green address bar that's supposed to signify an even higher level "extended validation" of certification, do you really know anything about how the certification "authority" checked out the claims of the site owner?

The Quiet Enjoyment Infrastructure is about authenticity that starts with individual identity, so why are we discussing site certificates instead of identity certificates? Well, it's true that web sites exist only in the great outdoors; QEI is about indoor spaces. And among other things, indoor spaces call for the digital signatures of professionally licensed individuals, not some amorphous corporate entity whose fundamental character can change with the next change in ownership or leadership. Authenticity starts with individual accountability, and so we need to focus on the individual identity certificates from which all authenticity in the Authenticity Economy emanates.

But the site-certificate "industry" is also the primary issuer (merchandiser) of identity certificates, and so we need to illustrate the dubious practices of the site-certificate "industry" to show why reliable identities call for different practices.

Let's start with the whole notion of a certificate industry. While I am a free enterprise enthusiast, I nevertheless must ask: Whose crazy idea was it that certification should be done by commercial enterprises?

Wherever the idea came from, it gains legitimacy from the "best practices" syndrome.

> best practices, [best-prăktəsɪz], N, the term used when a decision maker neither understands the technology involved in a decision nor cares to take the time to learn about it, and needs a CYA euphemism for "we'll just do what everyone else is doing; that way I won't stand out too badly when the stuff shows itself to be garbage."

In order to make clear what's wrong with the certification practices we all rely upon, we should look where most certification is currently done: certification of web sites. Let's learn from the abuses committed under the guise of certification so that when identity certification becomes mainstream we won't repeat them.

Site Certificates, i.e. Cabbage Patch Certificates

The absence of rational thought that characterizes "best practices" has left the world believing that certification is mostly about technology, that when we examine the prac-

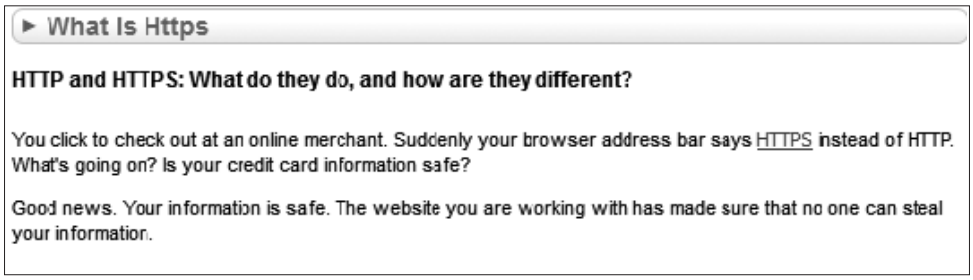
tice of site certification we should focus on how the tunnel is constructed rather than on questions such as

Who has the authority to certify?
Where did they get that authority?
What is their professional liability?
How exacting are the standards by which the certification was performed?
What standards govern the design and operation of the certification servers?
What governing body makes those standards?
How are those governed involved in governance?

...because, well, until recently SSL/TLS technologists had never been asked to deal with those issues and they're neither lawyers nor public policy people so please don't start bringing them up now. Please just trust that it's all about technology. Sooner or later the phishers and predators will get tired of being bad and just go away, right?

Let's tell the story of contemporary site "certification" in pictures, with some juxtaposition of real site certification advertising with parodic images from another context.

First, there is the story that the certificate merchandisers tell users, as opposed to site owners, about the significance of https, as in this lullaby from certificate merchandiser[50] Comodo:



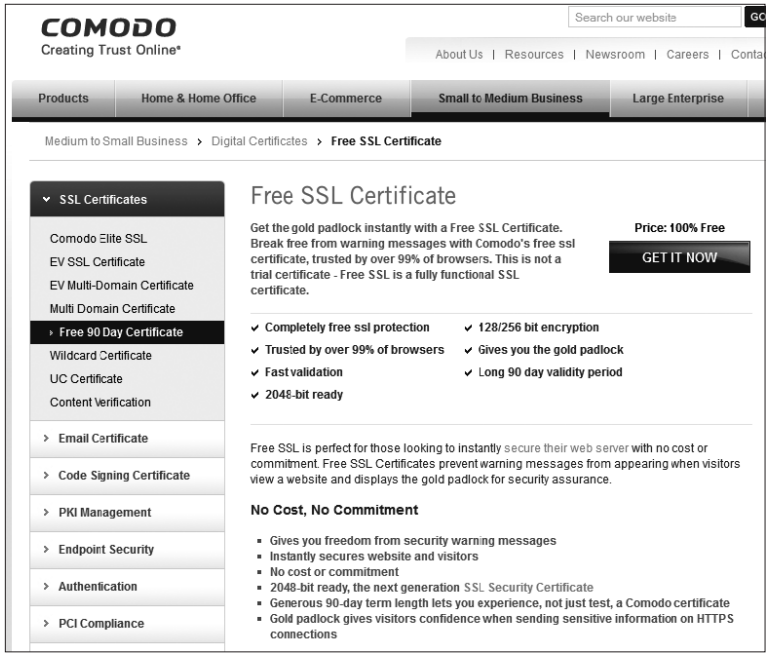
Ah, "your information is safe." No equivocation there. In order to offer that assurance, Comodo must require site owners to pass a very thorough and rigorous procedure before bestowing a site certificate. So let's see how Comodo sternly lays down the law to site owners[51].

Are they selling certificates or office carpeting? No, wait, carpeting wouldn't be free.

And if you're too blatant about your intention to set up a bank phishing attack site and even Comodo somehow manages to turn you down, the company has a network of resellers, er, "registration authorities," who have proven to be much more accommodating.

50 http://www.instantssl.com/https-tutorials/what-is-https.html, October 2011.

51 http://www.comodo.com/business-security/digital-certificates/free-ssl.php, October 2011.



This wanton fudding of terminology has serious consequences. A real PKI registration authority is not a reseller but rather has specific legal responsibilities. A Comodo "registration authority" is no more a registration authority than is a convenience store selling snacks and lottery tickets.

The makers of browsers are complicit in this problem, as they get to decide what certification authorities are sufficiently legitimate to have their root certificates included in the browser's certificate store. If they had that determination to do over again they would probably apply their late discovery that certification involves more than technology, and make different choices. But for reasons explained by Steve Kalman, a well-known CISSP trainer in his blog, Posterous[52], they are stuck with their choices:

> **Comodo fake certs**
>
> One of the several dozen trusted CAs was hacked recently.
>
> The Browser vendors will not remove Comodo from your trusted certificate list (and to be fair, the vast majority of certs are still trustworthy). They won't do it because it would lead them into expensive litigation from Comodo and from the trustworthy sites that would be blocked.

We shouldn't just pick on Comodo. Here's how the market leader, VeriSign, now a unit of Symantec, merchandises the confidence of unsuspecting users. Is there any reason why the term "confidence racket" should not be applied to this?

52 http://techauthor.posterous.com/.

Here's a banner aimed at site owners from the Thawte unit of Symantec:

Issued within minutes! The exclamation point is more telling than their copywriter intended, emphasizing that there is no way to do an adequate job of evaluating a claim of site ownership in minutes.

Thawte, like GeoTrust, is a unit of VeriSign (now itself a unit of Symantec), although it keeps that under wraps as much as possible. Can you imagine a municipality, state, or nation concealing the fact that it is owned by another entity? We allow commercial enterprises to do things like that because, well, authenticity in the public arena is the business of duly constituted public authority rather than commercial enterprises. Commercial enterprises have implicit license to sling the BS in ways that public authority may not. Caveat emptor.

Speaking of GeoTrust and merchandising partners masquerading as registration authorities, here's an ad for "GeoTrust Resellers" (yes, they actually use words like "reseller"):


GeoTrust

INTRODUCING...

An Exciting **NEW PRODUCT** for GeoTrust Resellers

the **Registered Member Program** with **Verified Domain™ Site Seals**

GeoTrust Registered Member
GEOCODE 1 2 3 4 5 6
CLICK

Address a highly profitable market that has yet to be tapped -- with Verified Domain Site Seals from GeoTrust.

In today's increasingly networked environment, everyone wants to rely on the web for information. But it's hard to know which sites can be trusted -- and which sites may be fraudulent.

For customers doing online transactions, you already know how to sell the security of GeoTrust SSL certificates. **But, what about the 50 million web sites that don't conduct e-commerce?** Now, any verified web site can become a GeoTrust Registered Member, and display the Verified Domain Site seal that indicates they are a trusted web site.

THE BENEFITS ARE CLEAR
We want you to help make the Internet more secure by encouraging your customers to become members and display this seal on their sites. A more trusted environment benefits everyone.

And of course, we want to help you make additional revenue from each customer you host. The Registered Member Verified Domain Site seal retails for $49.00 (with multi-year discounts available). **Your Pay-As-You-Go price is only $30.00 -- allowing you to make a sizeable profit!** Include it as part of your packaged hosting products or as a stand alone product. Everyone will benefit!

VERIFIED SITE SEAL

FOR MORE INFORMATION, CALL YOUR GEOTRUST SALES REP TODAY!
Call 1-866-273-7355 (press 4)
or email partners@geotrust.com

Registered Member Verified Domain™ Site seals are ideal for:

- Customers using a shared SSL certificate for e-commerce
- Organizations, non-profits and other public institutions
- Professional services such as lawyers, real estate agents, insurance agents, doctors and consultants
- Media outlets such as newspapers, magazines, radio stations and television stations
- Blogs
- Any of the 50 million legitimate informational web sites

Sorry, I should have warned you to wear your boots before entering this chapter. More GeoTrust:


GeoTrust

Q: How are you taking advantage of the **multi-billion dollar** mobile computing market?

A: With **Power Server ID™** the most universally recognized and powerful SSL certificate yet.

Find out how you can increase your margins by as much as 400%,
while helping your customers address the growing mobile computing market
Download our **FREE** QuickSELL Guide for Resellers

So let's see, the relatively young and highly profitable site-certificate industry might have something to teach other old hidebound certification organizations. Let's show those old fogeys the possibilities:

Act today, and take advantage of our special low price bundle of Professional Architect and Structural Engineer licenses!

With these two certifications, you're well on your way to breaking ground on your first 50-story office building! And be sure to ask about our specials on building permits, occupancy permits, and building inspector professional licenses!

Is it not blatant on the face of it that the "digital certificate industry" is as fraudulent a confidence racket as the no-doc mortgage securitization and CDO business?

At least the slingers of mortgage BS weren't trying to foist their stuff as something official. That's because they didn't think to invoke magic intimidation words like "cryptography" and "secure sockets layer" to aid them in their obfuscatory mission. Simple lack of imagination I suppose.

It Took a Village

A few isolated voices in the wilderness have tried for years to call attention to the craziness implicit in relying on the outdoor information infrastructure for commercial

"certification." The voices were pretty much ignored…until 2011. Comodohacker. Massive issuance of fraudulent certificates by an Iranian hacker. One CA waiting 10 days before notifying relying parties of the breach. The disaster that had to happen, happened.

Since then, at least a few have started to question the way certification is performed. It's unfortunate that relying parties were harmed, but the attention is welcome.

Let's now take a look at two sets of responses: the collegial certification response and the QEI response.

Collegial Attestation and Collegial Certification

The subject of the quality of certification was completely missing in discussions of PKI when the first edition of this book came out in 2004. The fact that it's getting lots of attention today is a hopeful sign.

However, it seems to be getting attention from people who have faith in the notion of what I call "collegial attestation." Let's look at a few of those.

The Original Collegial System: Pretty Good Privacy (PGP)

The original PKI-like form of collegial attestation was Phil Zimmerman's PGP — Pretty Good Privacy. Actually, PGP was a complete system providing both attestation of the identity of the people using it and a very well thought out way to build communities of encrypted information exchange. In many ways PGP is like our InDoors Infrastructure, but without the occupancy permits and other elements that depend upon public authority as opposed to collegial authority. The original system, now referred to as a protocol, defines standard formats for the exchange of public keys and symmetric keys, the signing of messages and files, encryption, and (mutual) certification.

The original PGP has split into commercial and noncommercial versions, with the noncommercial version, OpenPGP, having become a standard governed by the Internet Engineering Task Force (IETF). OpenPGP and its OpenPGP Alliance are responsible for the vast preponderance of the world's encrypted email.

OpenPGP has added a more formalized system of trust certification to the ad hoc certification methods of the original PGP. The system specifies three levels of trust certification:

Level 0	key is valid, but no attestation to identity of its holder
Level 1	key may be used to issue Level 0 "signatures"
Level 2	enables its holder to act like a certification authority

Since OpenPGP is an IETF standard, this level of trust mechanism is further explained in its RFC[53]:

53 IETF RFC 4880, http://www.ietf.org/rfc/rfc4880.txt

```
5.2.3.13. Trust Signature
(1 octet "level" (depth), 1 octet of trust amount)
Signer asserts that the key is not only valid but also trust-
worthy at the specified level. Level 0 has the same meaning as
an ordinary validity signature. Level 1 means that the signed
key is asserted to be a valid trusted introducer, with the
2nd octet of the body specifying the degree of trust. Level 2
means that the signed key is asserted to be trusted to issue
level 1 trust signatures, i.e., that it is a "meta introduc-
er". Generally, a level n trust signature asserts that a key
is trusted to issue level n-1 trust signatures. The trust
amount is in a range from 0-255, interpreted such that val-
ues less than 120 indicate partial trust and values of 120 or
greater indicate complete trust. Implementations SHOULD emit
values of 60 for partial trust and 120 for complete trust.
```

PGP presents an excellent algorithm for conveying trust and then establishing confidentiality. All it needs is a reliable source of authenticity to establish that trust in the first place. The assumption is that trust can be crowdsourced.

Philip Zimmerman's 2001 essay[54] , "Why OpenPGP's PKI is better than an X.509 PKI," presents the case for collegial certification as opposed to authoritative certification:

> In the minds of many people, the phrase "Public Key Infrastructure" has become synonymous with "Certificate Authority". This is because in the X.509 world, the only PKI that we usually encounter is one built on a centralized CA. Matt Blaze made the cogent observation that commercial CAs will protect you against anyone who that CA refuses to accept money from. These CAs are "baked into" the major browsers, with no decisions by the users to trust them.
>
> Throughout this discussion, we refer to the IETF OpenPGP standard instead of PGP, which is a single company's implementation of the OpenPGP standard.
>
> There is indeed an OpenPGP Public Key Infrastructure. But what we call a PKI in the OpenPGP world is actually an emergent property of the sum total of all the keys in the ser population, all the signatures on all those keys, the individual opinions of each OpenPGP user as to who they choose as trusted introducers, all the OpenPGP client software which runs the OpenPGP trust model and performs trust calculations for each client user, and the key servers which fluidly disseminate this collective-knowledge.

54 The OpenPGP Alliance, http://www.openpgp.org/technical/whybetter.shtml.

PGP has flourished for many years without the need to establish a centralized CA. This is because OpenPGP uses a decentralized system of trusted introducers, which are the same as a CA. OpenPGP allows anyone to sign anyone else's public key. When Alice signs Bob's key, she is introducing Bob's key to anyone who trusts Alice. If someone trusts Alice to introduce keys, then Alice is a trusted introducer in the mind of that observer.

If I get a key signed by several introducers, and one of these introducers is Alice, and I trust Alice, then the key is certified by a trusted introducer. It may also be signed by other introducers, but they are not trusted by me, so they are not trusted introducers from my point of view. It is enough that Alice signed the key, because I trust Alice.

It would be even better if the several introducers of that key includes two or more people that I trust. If the key is signed by two trusted introducers, then I can be more confident of the key's certification, because it is less likely that an attacker could trick two introducers that I trust into signing a bogus key. People can make mistakes, and sign the wrong key occasionally. OpenPGP has a fault tolerant architecture that allows me to require a key to be signed by two trusted introducers to be regarded as a valid key. This allows a higher level of confidence that the key truly belongs to the person named on the key.

Of course, a clever attacker could trick two or more unsophisticated introducers into signing a bogus public key. But that does not matter in the OpenPGP trust model, because I don't trust unsophisticated introducers that can be so easily fooled. No one should. 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.

If only untrusted introducers sign a bogus key, no one will be fooled in the PGP trust model. You must tell the OpenPGP client software which introducers you trust, and the client software uses that knowledge to calculate if a key is properly certified by an introducer that you trust by looking for signatures from one of the trusted introducers. If the key lacks any signatures from introducers that you've told the client software that you trust, the client software does not regard they key as certified, and won't let you use it (or at least will strongly urge you not to use it). Everyone gets to choose who they trust as introducers. Different OpenPGP users will have different sets of trusted introducers. In many cases, there will be overlap, because some introducers become widely trusted. They may even sign a great many keys, on a full time basis. Such people are called CAs in the X.509 world.

There is nothing wrong with having CAs in the OpenPGP world. If many people choose to trust the same CA to act as an introducer, and they all configure their own

> copies of the OpenPGP client software to trust that CA, then the OpenPGP trust model acts like the X.509 trust model. In fact, the OpenPGP trust model is a proper superset of the centralized trust model we most often see in the X.509 world. There is no situation in the X.509 trust model that cannot be handled exactly the same way in the OpenPGP trust model. But OpenPGP can do so much more, and with a fault tolerant architecture, and more user control of his view of the OpenPGP PKI.

Phil Zimmerman is certainly right in citing Matt Blaze's famous comment about commercial certification authorities. Our existing certification infrastructure is rotten, for exactly the reason cited by Blaze. It's a problem that must be fixed.

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 John Edwards's campaign staff or a group of characters from Michael Lewis's chronicles of Wall Street to conspire to convince a PGP key holder that a particular individual is someone whom 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 global web of trust.

I have been to PGP key signing parties, so I have seen the trust given to strangers firsthand. It may not be quite the Blanche DuBois level but a few people with fake IDs putting on a show of trust among each other could easily pwn everyone at the event. The first step would be to observe who seems to know what they're doing in checking IDs and who does not, and start with the latter.

In a worldwide faculty club where not much money is at stake, collegial attestation can work. But collegial environments don't have major inauthenticity problems to solve. In the wider world where fraud and theft have become common business practices, pwning the PGP network would happen as soon as a few hundred thousand dollars could be gained by doing so.

Wikipedia's entry under PGP notes that

> The problem of correctly identifying a public key as belonging to a particular user 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.
>
> No fully satisfactory solution is known?

Then we need to make known the Authenticity Infrastructure portion of the Quiet Enjoyment Infrastructure. We claim that it is indeed a fully satisfactory solution. In

fact, one eighth of it consists of a collegial certification component, defined not just in the mechanics of its operation but also in terms that are tied to networks of people as they exist in the real world. For example, a social network for children should require that its members' identities be validated by an administrator in a child's school, with the administrators themselves having been properly enrolled using face-to-face notarial procedures.

We'll go into the details of the six components of the Authenticity Infrastructure shortly, but first let's keep examining the various approaches to collegial certification.

Gnu Privacy Guard (GPG)

GPG is another example of an encryption and signing infrastructure that is built upon collegial certification. Although they came from different origins, PGP and GPG have evolved into very similar infrastructures. The current version of the GNU Privacy Guard program implements the RFC 4880 specifications that define OpenPGP, licensed under the GPL.

GPG is an implementation of PGP that complies with the principles and standards of the GNU Project. (GNU is a self-referential acronym, GNU's Not Unix). Founded and guided by Richard Stallman, the organization exists to build and deploy software that provides "four freedoms" to its users: freedom to run a program for any purpose, freedom to access the source code, freedom to redistribute copies, and freedom to improve and change modified versions for use by anyone. These freedoms are preserved in the distribution license, which itself must be included in every copy of any source code that is derived from the original received distribution.

Next we will look at two newer versions of collegial attestation, The Perspectives Project and Convergence. But because of their unfortunate choice of terminology, let's first revisit that important word "notary."

The "Notary" Web of Trust

Years ago some of the commercial certification authorities came to concede that the dreadfully untechnical, labor-intensive, and difficult-to-leverage process of performing face-to-face verification of identities of individuals might actually be necessary to give Internet users confidence in the identities of the people they deal with.

One would think they would start with notaries public, who are chartered with the authority of the state to do exactly that job. In fact, some of those certification authorities did use the term "notary," except that they seem to treat it as a term with no particular legal meaning, indeed as a term that they coined.

Thawte, a unit of VeriSign (now Symantec,) even had a formal process for chartering "notaries." The following easy steps published by Thawte would have you "notarizing" people and documents in no time! In its own words its "Web of Trust" was

A unique, community-driven certification system based on face-to-face ID validation on a peer-to-peer basis. It's a "bottom-up" CA, compared to traditional "top-down" CA systems. You can be notarized, and then you in turn can act as a notary and certify the identity of your friends!

To join the web of trust you need to be enrolled in the free Thawte Personal Certification System. You can join the web of trust today by finding a Web of Trust Notary near you in the Directory of Notaries, or signing up to be notarized directly by a Thawte employee on one of our Notarization Tours.

Web of Trust in Brief:

- You can include your name in your cert once you reach 50 points
- You can become a notary at 100 points
- New notaries can certify you up to 10 points
- Experienced notaries can give you up to 35 points

The wonderful thing about being a Thawte notary was that it totally dispensed with this messy little detail that comes with being a real notary. If you knowingly attest to a falsehood while acting in your official capacity as a notary, you may be sent to jail. If you do that as a Thawte notary, they may say nasty things about you in the Web of Trust café. No problem, just get another identity and start over.

The Thawte notary didn't even need to be insured! If one of the Web of Trust "notaries" notarized someone at Leavenworth Federal Penitentiary — you know, where they send people convicted of identity theft — then that person could "notarize" all of his fellow inmates. Even before they get out of prison they could go around the Internet, with the validity of their stolen identities attested to by the Web of Trust certification authority.

Imagine what would happen if Thawte had called its security policy consultants "lawyers" and its security monitoring people "police officers!" They'd get to see what real live lawyers and police officers look like up close, and they'd get a serious lesson, with heavy tuition, in the semantics of authority. Misuse of the term "notary" is theoretically a greater criminal offense than misuse of the term "lawyer," as "notary" denotes a public office.[55]

Fortunately, Thawte realized the error of its ways in November 2009 and discontinued its "Notary Web of Trust." Perhaps Michael Baum of Thawte's parent company, Symantec/VeriSign, reminded them that a notary public is a human being whose actions as a public official carry the consequences of criminal and civil liability.

One would think that the Thawte experience would have put an end to the misuse of the word "notary." Guess again.

55 Yes, lawyers, you are at times an Officer of the Court, a public office.

The Perspectives Project

Here is the Carnegie Mellon University Perspectives Project introducing itself[56]:

> Perspectives is a new approach to helping computers communicate securely on the Internet. With Perspectives, public "network notary" servers regularly monitor the SSL certificates used by 100,000s+ websites to help your browser detect "man-in-the-middle" attacks without relying on certificate authorities.

Not only is a notary not a public official, it's not even a person. It's a machine!

If a Perspectives "notary" fraudulently certifies, do they put the server behind bars? Can someone who's damaged by a server's careless performance of its duties sue the server?

The Perspectives introduction continues:

> Because anyone can run a network notary server, you get to choose who you trust to validate SSL certificates, a powerful concept indeed! You can try it out using our Firefox Extension.
>
> **The Problem**
>
> …The root of the problem is that with the CA model, browsers blindly trust a group of 600+ corporate and government parties (ref) to validate SSL certificates. You as a web browser user have little or no choice about who to trust and essentially no visibility into whether these organizations deserve your trust.
>
> **How Perspectives Helps**
>
> Perspectives takes a different approach to how the web browser determines if an SSL certificate is valid. Instead of requiring browser users to trust an anointed group of certificate authorities, Perspectives gives users the ability to pick a group they trust (e.g., the EFF, Google, their company, their university, their group of friends, etc.) and trust no one else.
>
> How is this possible? Perspectives has a decentralized model that let's anyone run one or more "network notary servers". A network notary server is connected to the Internet and regularly monitors websites to build a history of the SSL certificate used by each site. Notary servers or groups of notary servers may be operated by public organizations, private companies, or even individuals.
>
> Rather than validating an SSL certificate by checking for certificate authority approval, with Perspectives the browser validates a certificate by checking for consistency with the certificates observed by the network notaries over time. With network notary servers spread around the world and keeping a history of data, it is VERY hard for an attacker to launch a man-in-the-middle attack (see our academic paper for a full security analysis)…

56 http://perspectives-project.org/.

Perspectives, like its derivative called Convergence, seem to deal only with site certificates rather than identity certificates or code-signing certificates. If you haven't guessed by now, our solution is to have them both signed not only by a responsible institutional authority but by an individual responsible person, a signing officer of the organization represented by the site or the code.

Companies are bought and sold all the time. Companies have business units and subsidiaries that can be quite autonomous and whose management can change at any time. It makes no difference whether an outside authority is collegial or institutional; as long as a site certificate does not carry the same legal weight as, say, a corporate charter, there is no way an outside authority can confidently attest to its legitimacy.

The digital signature of a legally responsible and liable signing officer from within the organization operating the site is a completely different matter from that of an outside authority. Would you make yourself legally liable for the content of your employer's current site? You'd probably want to spend a day or two examining it first, particularly if your hard-earned Signing Officer's professional license were at stake. When the marketing VP wants to add some "optimistic" product claims, he or she would know that any edits to the site would have to be signed with your PEN in order for your digital signature on the site to continue to validate when a user clicks on its icon.

Signing Officers will have a lot of responsibility. And they will need to be compensated accordingly.

TIM

The Trustworthy Internet Movement was formed in March 2012 as a nonprofit, vendor-neutral organization whose goal is to bring together a number of SSL-related methods and technologies to bring about a more secure Internet. One of its first projects is SSL Pulse, a database of ratings of sites using TLS/SSL and the various providers of all parts of the TLS, including certification authorities. Presumably site owners would look to the SSL Pulse database before "buying a site certificate," as the process is accurately and dreadfully characterized.

Site owners will shop for the best CA rather than the cheapest certificate? Good luck with that.

Moxie Marlinspike's Convergence

Besides being on the board of TIM, Moxie Marlinspike has put forward his own collegial certification system called Convergence. Convergence purports to solve the problem of an unreliable system of certification authorities with collegial certification. Convergence has been characterized[57] as a "crowdsourced approach to improving SSL security."

In Marlinspike's own words,

57 "New SSL Alternative: Support Grows for Convergence," by Mathew J. Schwartz, Information Week, September 30, 2011, http://www.informationweek.com/news/security/management/231700001.

> Convergence allows you to choose who you want to trust, rather than having someone else's decision forced on you. You can revise your trust decisions at any time, so that you're not locked in to trusting anyone for longer than you want.

This will work, as PGP has worked. That is, it will work for people who are willing to put effort into managing trust relationships, and who are not engaging in transactions that are big enough to attract skilled fraudsters.

Consider how a decision to move to a new town implies that same choice of whom to trust. By establishing a residence in a municipality, you are accepting its ordinances, its building codes, the authority of its city hall, the authority of both the municipality and its state or province, including the duly constituted public authority of the notaries who are commissioned to practice in that state or province.

A sensible person might take a really good job in a place with a notoriously corrupt and repressive government, as the quality of governance is only one part of the consideration. But who would join an online community if its source of authority were corrupt and repressive?

Can you use Marlinspike's Convergence to declare your trust in one certification authority whose authority is embodied in the city hall of an online municipality? Of course; Convergence would support that nicely. There is no conflict between the Convergence view of trusted authority and the QEI view, as both are built upon the user's voluntary granting of trust to a particular source of authority.

The conflict between Convergence and the Quiet Enjoyment Infrastructure is about the use of the term "notary." If a real notary performs a fraudulent notarization, there is criminal as well as civil liability.

> An alternate approach to vetting SSL certificates is gaining steam. Notably, security firm Qualys said it will finance and support two notary servers for Convergence, a still-in-beta project developed by security researcher Moxie Marlinspike as a way to crowdsource certificate authenticity.
>
> "Moxie advertises the project as a way of dispensing with certificate authorities ('An agile, distributed, and secure strategy for replacing Certificate Authorities')," said Ivan Ristic, director of engineering for Qualys, in a blog post.
>
> "You get a browser add-on (only Firefox for the time being) that, once activated, completely replaces the existing CA infrastructure," he said. "Whenever you visit an SSL site your browser will talk to two or more remote parties (notaries) and ask them to check the site's certificate for you. If they both see the same certificate you decide to trust the site."

> Convergence removes browsers from the "who should I trust?" equation. That's a crucial development, since if a CA issues bad certificates, the only current way to revoke them from browsers or applications is for developers to update their code, which is a slow, cumbersome approach. In addition, Convergence creates a backend—the notary servers—that handles trust decisions. "The approach is great in its simplicity: if you can see the same certificate from several different locations you conclude that it must be the correct certificate," Ristic said…
>
> Convergence isn't the only potential SSL alternative. Another possibility—which could be used with Convergence—is to sign domains using the DNSSecurity Extension, which enables a browser to ensure that the DNS infrastructure it's using is secure…
>
> Google, however, hasn't endorsed Convergence, and said it has no plans to add it to Chrome. "Although the idea of trust agility is great, 99.99% of Chrome users would never change the default settings," said Google security analyst Adam Langley in a blog post, earlier this month.
>
> "Given that essentially the whole population of Chrome users would use the default notary settings, those notaries will get a large amount of traffic. Also, we have a very strong interest for the notaries to function, otherwise Chrome stops working," he said. "Combined, that means that Google would end up running the notaries."
>
> Furthermore, Convergence had yet to address how internal servers or captive portals—often seen used at Wi-Fi hotspots as a way to force someone to agree with terms of service or authenticate before they're granted access—would be secured. "These two problems, captive portals especially, are the bane of many an idea in this area," he said.
>
> Still, when it comes to overhauling SSL, fruitful discussions are finally underway. "We mustn't rush," said Ristic. "We've just been given the ability to choose whom to trust, and it's too soon to settle on any one implementation. I am far more interested in experimenting with different approaches, to see what works and what does not."

"99.99% of Chrome users would never change the default settings." Well of course. Imagine that upon moving to a new town you were presented with a choice of which city hall you would accept as the source of authority over your domicile; which set of ordinances you want to be held to.

Duly constituted public authority was invented to replace competing claims of authority, also called competing protection rackets, as exemplified by the competing gangs of thugs that extorted geese and pigs from peasant farmers in our world history lesson. Do we want to go back to that? Is that where we're headed?

Most people are going to assume that the default is put there by people who have some kind of authority and accountability and liability. Or are people left to do their own analysis of authority and construct their own authority model?

History shows that the smartest leader of the toughest gang of thugs will win that one. I wonder what absolute monarchy will look like in the post-digital age. Perhaps the monarch will be a bot. How do you put the Hope Diamond on the head of a bot?

No, you want a default, the source of services provided and ordinances to be observed.

The Dot-Secure TLD

Supposedly ICANN is greatly expanding the number of top-level domains (TLDs), although doing so will likely involve much more difficulty than it had anticipated.

If the expansion does in fact happen, a group led by The NCC Group plc of the U.K. plans to establish and serve as registrar for the .secure TLD under the name The Artemis Group.

.secure would bring together a number of elements of security, starting with a requirement that every site make use of DNSSEC zone signing. Also required would be Domain Keys Identified Mail (DKIM) and TLS tunnels for every session.

So basically .secure is an attempt at building codes for the World Wide Web and for email.

Now if they add DSRIE (digital signatures from reliable identities everywhere) and professional licensing (which can't exist without measurably reliable identities) and… well, the rest of QEI, then they will have solved the problem.

For now, .secure is a structured and formalized version of collegial attestation.

Demosthenes' View of Collegial Attestation

PGP, Perspectives, Convergence, TIM, dot-secure, and other forms of collegial attestation and certification are reminiscent of the attitudes and philosophies of the counterculture of the '60s and early '70s.

I was there. I was one of them. I drank the Kool Aid, at least the figurative version of it.

Then an incident taught me a valuable lesson about the fallibility of trust in collegial groups.

In my second year at Hanover College my roommate and I decided to set up a bar in our dorm room, serving beer, wine, and bourbon to trusted friends. (Whoever coined the term "sophomoric" did not choose an age group at random.) Caught after about the fourth customer, I was marched off to the Dean of Students, who offered me a deal: Be his eyes and ears in the dorm and he would let this one go.

What the dean didn't know, or so my furtive little mind thought, was that I had joined the staff of a new "alternative" and very countercultural campus newspaper. What

a wonderful story this would make: Dean of Students Tries to Recruit Stooges! Gleefully I wrote it up, eagerly anticipating the administration's attempt to deal with the resulting campus-wide outrage. Any attempt to discipline this earnest reporter would just intensify the furor, right?

Alas, it turned out that the publisher of our little rag was himself best buddies with the dean. The paper existed as a way to attract and identify malcontents. The story never saw the light of day, and I was very lucky not to have been thrown out of school.

That incident illustrates what Demosthenes had in mind when he articulated[58] his famous view of trust:

"There is one safeguard which all sensible men possess by nature...It is distrust. Guard this possession and cleave to it; preserve this, and you need never fear disaster."

Demosthenes would not be a fan of collegial attestation or collegial certification.

Gather any group of friends and friends-of-friends, depend upon the mutual trust of the group for some meaningful purpose, especially a purpose that involves money, power, or reputations, and eventually you will be disappointed. The bigger the group, the higher the probability that some incident, some source of jealousy or resentment, some innate psychopathology, or some opportunity for personal gain, will cause an incident where the mutual trust is betrayed. The rarity of such incidents will not lessen their effect among members of the group whose mutual trust is the very reason for its existence.

If your mutual certification system assumes that its members are special, that they are uniformly and always trustworthy, the system will sooner or later be subverted. It's just too ripe an opportunity for the little inner psychopath that sits dormant in some people until opportunity arises.

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."

Whenever possible, in the "accountability" part of the formula, the one who steps forward and accepts responsibility for the main attestation should be subject to criminal liability.

Collegial certification may work for a while when not much of consequence is at stake among those who rely upon the certification. When real money or power is added to the mix – forget it.

A combination of duly constituted public authority, professional liability, and clearly defined personal accountability is not a perfect solution. But it's a pretty good one.

TIM's on the Right Track but He's Missing Something Essential

Moxie Marlinspike comes at the problem of certification from the right place. As a countercultural live-off-the-land type, he would have been right at home with my crowd in the 1960s. (Yes, I was in the Air Force then. Someday someone will chronicle the story of us hippies in the military.) An article of faith among us was that we should "question

58 Demosthenes (383-322 BC), in the *Second Phillipic.*

authority." That's always good advice for everyone, hippies and suburban suits alike.

But while we must constantly question authority and never assume it can be left alone to do its job without our scrutiny, authority is necessary. Certainly if you have an authenticity system with an important component called a "certification authority," it needs to be DCPA. Duly Constituted Public Authority.

We are accustomed to seeing authority in bad examples: power-hungry bureaucrats, self-serving governments, lawmaking bodies corrupted by industry lobbies, irresponsible regulators and auditing firms…Wall Street!

Those abusers obscure the quiet, unobtrusive counter-examples: the vital records departments, the bureaucracies that issue passports and drivers' licenses. They're not perfect but they tend to be effective and fair in doing their job.

Governance, Not Government

That old and largely forgotten distinction between state and government we discussed points the way to effective authority. In most places state and government have become practically synonymous, but a few holdouts illustrate the distinction.

When British prime ministers are elected, they must present their credentials to the queen before they may "form a government."

Form a government? The expression has always struck Americans among others as a bit bizarre. But in a constitutional monarchy, continuity is provided by an institution that simply exists, and whose only responsibility is to deem other things to exist. The word "real" in "real estate" means "royal." Another institution called "government" exists when the head of state — the monarch — says it exists.

What would happen if the queen refused to accept the credentials of an incoming prime minister? That might be the end of the monarchy, because of course British government is powerful in a way that British monarchy is not.

But it's not power we're talking about. Authority is not the same thing as power.

State ≠ Government

Here's another way of looking at it. It occurs to me that state gathers and applies public **authority**, while **government** gathers and applies public **money**.

State tends to charge a fee for the service of applying public authority, such as when you pay for a passport or a certified copy of a birth certificate.

Government tends to charge taxes for…well, government tends to charge taxes.

State simply attests to claims in order to define what's real, as in a notary's attestation to a signature's genuineness and validity, or a passport's attestation to citizenship.

Or attestation in a birth certificate to a claim of parents and hospital staff that a person came into existence at a certain time and place.

The economics of state tends to be like the economics of a service business: we pay a fee for the application of public authority to attest to our claims. Government, by con-

trast, does things. Government initiates. Government builds roads, fights wars, educates children, attempts to solve social problems, and collects taxes to pay for it all.

$State_1$ = $State_2$

Now compare this use of the term "state" to its use in computer technology, and compare the role of government to that of an operating system. The operating system does things, while the recording of state in a browser or anywhere else is just a set of protected records that keep track of what's what. E Web Programmer defines "stateful"[59] as

> The property of an object such that it contains information that is maintained across method calls.

And so if some software entity has business with that object, it can refer to its state to know how to deal with it.

The function of the system of state in a computer is to attest to what exists, in a way that makes it difficult for a user to claim otherwise. Have you authenticated to this site? Server and client operating systems can't rely on any old user claim for the answer; some authoritative attestation of state will guide the operating system. The operating system is powerful; the computer's state department is authoritative, or should be. The computer's state department should provide authoritative attestation to the rest of the system.

In non-PKI information infrastructures, objects sometimes define their own states. Objects that interact with each other simply keep track of each others' states in order to know what to do.

In PKI, the state of certain objects is defined by authority. In the Building Codes Component of the Quiet Enjoyment Infrastructure, for example, a facility cannot be accessed via InDoor methods unless it carries an occupancy permit, which can only be issued by authority.

Similarly, if an entity in physical space (person, organization, etc.) has business with another entity, it may refer to a property that was designated by public authority: a duly chartered corporation, a legal immigrant, a licensed driver, a professionally licensed architect.

In QEI we merge both forms of state. If state1 is the computer meaning of "state" and state2 is the governance meaning of "state," then in many ways state1 = state2. The city's Vital Records Department and Buildings Department are agencies of state (the computer term) and state (the public authority term). The certification authority is City Hall.

---

59 ´http://www.ewebprogrammer.com/ejb-architecture-session-beans/ejb-architecture-sessionBeans-glossary.jsp.

Certification in QEI

If you apply authority properly, PKI goes from being difficult to deploy to being quite straightforward in its application to real life. Add authority to the existing superb technology of PKI and the solution is at hand. When it comes to available resources with which to build a trust infrastructure and solve our security problems, we have it so much easier than the Romans did.

If the Romans could make their system work, it should be easy for us. But first we must have the essential ingredient of the Roman trust system. We need a ready supply of high-quality attestation authority.

The Rebirth of Professional Attestation

In recent years Florida and Alabama took steps to adopt a few of the institutions of Latin law as opposed to common law. They joined Louisiana (the only Latin law jurisdiction in the United States) in commissioning civil notaries, essentially the same thing as Latin notaries.

In many ways, the contemporary Latin notary is the equivalent of the Roman tabellio. The concept of a Latin notary is foreign to most people in the United States. In the 49 U.S. common-law states there is one kind of lawyer, an advocate. And the fact that all lawyers are advocates means that the practice of law is adversarial.

Latin, or civil, notaries are lawyers, too, but unlike the usual lawyer, they represent the public in effecting deeds among private parties. Latin notaries are not advocates. They are interested only in executing legal instruments designed to reduce the possibility of litigation, and they bring the authority of the commissioning jurisdiction to bear in making that happen.

There are two sources of resistance to Latin law. One is the belief that the British system of common law is superior and sufficient; the other is the tendency of Latin law to order things at the start of a business or personal relationship so as to minimize disputes later, and to manage the disputes in order to come to a resolution as quickly and simply and inexpensively as possible. Any reasonable person can see that a combination of common and Latin law is the best legal foundation for society, even though it reduces the opportunity for litigators to earn huge contingency fees. But in some circles English Common Law is practically a religious ideal, and any suggestion that it is not completely sufficient is heresy.

Call me a heretic, but we cannot continue to invite people to launch relationships upon defective agreements so that the ensuing litigation will give the courts fresh supplies for their inventory of precedents. More importantly for our present purposes, in the global village identities must be established with the kind of authoritative basis one tends to find in Latin law jurisdictions.

That is not to say that the Attestation Officers must be Latin notaries. They don't have to be lawyers. But we need to place responsibility for trustworthy attestation with qualified, commissioned individuals.

Under the Latin law, the messy business of deciding just who at Arthur Andersen actually abrogated their duties would mean looking no further than the Enron annual report, to see which CPA signed the statements and took responsibility for the whole mess.

But if things were done that way there might not have been a mess to begin with. What CPA would have signed his or her good name to the Enron or WorldCom or HealthSouth income statements, or the Merrill Lynch balance sheet?

And so, beyond the benefit to Internet users, bringing back individual professional accountability to areas where it has been lacking would reduce the common level of BS[60] in the land of litigation.

The not-so-hidden agenda of Quiet Enjoyment goes way beyond Internet problems. We're here to start the process of lifting society out of this big pit of BS.

Authenticity Calls for Digital Signatures Everywhere

The next chapter will give details about enrollment procedures, but it will be helpful to briefly illustrate here how the Enrollment Component works within the context of the Public Authority Component.

In the Authenticity Infrastructure, everyone gets at least one key pair at enrollment. We call the key pair a puzzle kit. The puzzle kit consists of two keys, two mathematically related numbers, though there is no need to know what's in the puzzle kit. Your computer takes care of all the key stuff; it's invisible to the user.

One key in the pair is designated private, and you keep it in a secure place such as a smart card. The other is your public key, which you can share with anyone.

You can use the resulting credential online or offline to prove identity.

Actually that foundational, archival key pair is used to generate other key pairs that are used on a day-to-day basis but for now, to keep things simple, we'll pretend there is just the one key pair.

We digitally sign things like documents, messages, images, etc., using the tools of PKI. Digital signatures from privacy-protected reliable identities are essential to the Authenticity Infrastructure portion of the Quiet Enjoyment Infrastructure.

We'll oversimplify for a moment to convey the basic idea behind digital signatures. If you'd like a little more detail there's a short video on that at quietenjoyment.net.

To establish authenticity using this simplified method, you encrypt a message or document with your private key.

Anyone on earth can decrypt it with your public key and see that it was encrypted by you and has not been altered.

That's the essential idea behind a digital signature. To keep it simple we've left out some technical steps; you don't need to understand those to make use of digital signatures. In practice your computer does almost everything in the background.

60 n., abbr. from Latin: *Blandior Subjectio, Bovis Sordes,* or *Bellus Sclestus.*

Really, this is the heart and soul of authenticity: Digital signatures from reliable identities, with privacy protection. When we have spaces where that's the rule, we will have solved massive numbers of problems. Especially if those online spaces include a way to prevent others from tracking you by tracking your signatures.

Note that authenticity does not imply confidentiality. If confidentiality is what you're after, you encrypt the message or file with your recipient's public key. Then the recipient is the only person on earth who can decrypt and read it.

If you're familiar with PKI you know I've oversimplified things here. For example, encryption in the real world is almost always done with old-fashioned symmetric cryptography, where the encryption key and decryption key are the same. But that symmetric key is created using PKI keys. I don't want to confuse you with these details, but you know... we do need to be authentic here...

While encryption of your files may be important to you or your business, our message is about authenticity and privacy rather than confidentiality of files. And authenticity calls for digital signatures...from reliable identities...with privacy protection.

So for our purposes here, encryption is only important as it is involved in digital signatures. Actually, encryption of files is easy; the hard part is managing who has what keys to which files when, and where those keys are kept. If you want to learn more about encryption of your files, one of the Authenticity Alliance enterprises, that is, one of the licensees of The Authenticity Institute, can help.

The Certification Authority

The digital signature on a file or message shows that it is authentically from the person who signed it. So recipients know that the file has not been altered since the signature was made. But how do they know that it was actually signed by the person who purported to sign it and not by an impostor's PEN (private key)?

Our reliable enrollment process gives us a level of certainty about who the key pair was issued to. But when the user presents that credential, how does the relying party know about the enrollment process? Indeed, how does the relying party know that the identity can be relied upon?

This is the role of the certification authority. Invisibly, and in a split second, the relying party's computer sends a message using the Online Certificate Status Protocol (OCSP) to the certification authority, the public authority that signed the public key, asking, “Is this a legitimate credential that has not expired or been revoked?” The authoritative answer, yes or no, can be relied upon. The subject's public key is signed by the certification authority.

We showed how identity certificates are like site certificates, and how identity certificates and their corresponding private keys can be used to produce meaningful digital signatures. Why shouldn't all secure sites be digitally signed by an individual, by the signing officer of the organization that owns the site? That would certainly improve au-

thenticity on the Web — especially if signing officers carried professional licenses issued by public authority.

Perhaps you're wondering how signing officers will feel about attaching their name and reputation to a site. Here's a hint: licensed professionals are typically paid well for accepting professional responsibility.

Our certification authority takes the form of a vital records department of an online municipality. Like any community, our Villages® must have a source of public authority if we want there to be order, productivity, and progress. In democracies, republics and dictatorships, in strong central governments and loose federations of cities and provinces, there are always keepers of the physical or virtual seal who apply public authority — the authority of the state or municipality — in private matters.

Beware

Before we go into some detail about the Osmio Vital Records Department, we need to look into the ways the term "digital signature" is misunderstood and misused, often by legislatures. In some jurisdictions a simple image of a written signature is legally considered to be a digital signature. My sister Barbara, an appraiser, points out how this has proven to be disastrous in the appraisal community, and that is not the only example.

When you get involved with our initiative — and I do hope you will get involved — you can help us educate lawmakers and organizations about what makes a real digital signature reliable, and why other things calling themselves digital signatures are not reliable.

We've illustrated how digital signatures work, and how digital signatures from reliable identities can bring authenticity to the spaces – online spaces but also physical spaces – used by the people who choose to depend upon them. Surely you'll want to be part of one or more of the communities that use such spaces — or be the one to bring your existing community into a space that has the benefit of the Authenticity Infrastructure.

Our Source of Duly Constituted Public Authority

The Authenticity Institute serves as a combination of licensor and incubator to a collection of commercial and noncommercial organizations called The Authenticity Alliance. Each is, or will be, led by an entrepreneur who is knowledgeable in its target market.

The Authenticity Institute provides the use of intellectual property, training, methods and procedures, support, business models, a chart of accounts and accounting system, and basic business services needed by licensees to help them deliver authenticity to their particular target audience or to other Alliance member organizations.

We bring one more very important asset to our licensees, and that's a very special relationship. Let me explain. I am a free-enterprise enthusiast, but in this case the job of attestation must be done by the people who issue genuine birth certificates and licenses. For attestation to be worth anything, it must be done by DCPA: Duly Constituted Public Authority.

We need a noncommercial participant in our network of authenticity organizations, a source of duly constituted public authority.

Its authority must apply in the required jurisdiction, which covers this turf:

…because packets of information on the Internet know nothing about national boundaries or national laws. And there will always be some country that views spam and identity theft and online crime as a productive part of its national economy.

A Legitimate Source of Global Authority

We have established a rigorous set of standards for our enrollment professionals, and have provided for a licensing organization that will identify, recruit, train, equip, and supervise people who meet those standards. We have called upon many sources of authority in the process.

But the Public Authority Component is still not complete. We still have not identified the entity that has the proper authority to serve as certification authority to the whole thing, signing the certificates of the attestation professionals.

In 2002, as I was writing the first edition of this book, I was introduced to a group at the International Telecommunication Union that was planning something very similar to my Quiet Enjoyment Infrastructure. It was called the World e-Trust Initiative.

The special asset that we bring to our licensees is our relationship with the International Telecommunication Union in constituting a source of legitimate public authority.

The ITU was founded in 1865 to resolve conflicting national laws regarding encryption of telegraph messages. (Yes. National governments regulating encryption technology – in 1865.) This, the oldest international governance body in the world, it sets standards for cross-border telephone and network switching, broadcast frequencies, signal strength — any situation where signals cross national boundaries. Like the U.S. State Department and its passport agency, the ITU has earned its position of authority over many years through trustworthy service combined with the absence of any commercial

agenda. In fact, the X.509 digital certificate standard that everyone, including us, uses is a product of the ITU.

The ITU created its World e-Trust Unit originally to serve as the root authority for certificate issuance, to enable e-commerce in the developing world. A few of us have encouraged the World e-Trust Unit to include the developed world as well, and to include in their vision service not only to e-commerce applications but to all of the purposes mentioned in this book.

The ITU is our noncommercial source of duly constituted public authority for the World City Hall, the Authenticity Alliance member organization, the City of Osmio.

World e-Trust Memorandum of Understanding (MoU)

The Authenticity Institute, which is the company that is responsible for bringing the Quiet Enjoyment Infrastructure to potential partners, is a signatory (through a predecessor company) to the document that sets forth the standards and purposes for the ITU's World e-Trust Unit. If digital certificates are to mean something, this source of trust is essential. The world needs this source of trust.

Following are excerpts from the World e-Trust Memorandum of Understanding:

1. CONSIDERING that the International Telecommunication Union (hereinafter referred to as "ITU"), having its Headquarters at Place des Nations, CH-1211 Geneva 20, Switzerland, is an international organization where Member States and Sector Members cooperate to attain ITU's purposes, in particular, the development of telecommunications and the harmonization of national telecommunication policies;
2. CONSIDERING that the Telecommunication Development Bureau (hereinafter referred to as "BDT") is the executive arm of the Telecommunication Development Sector of the ITU (hereinafter referred to as "ITU-D"), whose main responsibility is to foster telecommunication development in developing countries through policy advice, provision of technical assistance, mobilization of resources and initiatives to extend access to under-served communities;
3. CONSIDERING that pursuant to the provisions of the Valetta Action Plan (hereinafter referred to as "VAP") adopted by the World Telecommunication Development Conference held in 1998 (hereinafter referred to as "WTDC-98"):
    - BDT should work closely with the private sector to ensure the successful implementation of its Action Plan (VAP), and ITU should make efforts to encourage the private sector to take a more active part through partnerships with telecommunication entities in order to help close the gap in universal and information access (Res. 6);

- ITU-D should be the intermediary, facilitating development partnerships among all parties, e.g. by encouraging regional telecommunication projects, to promote transnational partnerships of knowledge-based enterprise incubators and emerging companies in the telecommunication sector, involving Developing Countries (Res. 13);
- Providers of telecommunication equipment and services should make new technologies and know-how available to their customers in Developing Countries, and international organizations and donor countries are requested to assist Developing Countries in exploring ways and means of improving the transfer of technology, including technical and financial assistance (Res. 15);

4. CONSIDERING the need for a cost-effective approach to assist Developing Countries in their transition to the digital economy; The Signatories to this Memorandum of Understanding (hereinafter referred to as "MoU") hereby agree to voluntarily cooperate, according to their respective roles and competencies, as follows:

Objective

To leverage on the potentials of Internet Protocol (IP), digital mobile and other new technologies to provide sustainable e-services, the security and trust concerns 2 related to the use of public networks must be addressed. By identifying the requirements for secure e-services, a cost-effective approach is to build a common platform on which specific sector-based applications (interoperable with the common platform) can be run to provide the desired e-services. This approach takes advantage of economies of scale in reducing the overall deployment cost without any impact on the security requirements. The objective of this MoU is to establish an inclusive, technology-neutral and technology independent framework for contributions towards a beneficial, non-exclusive, cost-effective and global development and deployment of highly secure infrastructure and applications for value-added e-services in Developing and Least Developed Countries worldwide. Through value-added e-services, various sectors in developing countries will participate in the development, investment and use of new technologies thereby stimulating the development of the telecommunication infrastructure, creating socio-economic benefits and contributing towards building a truly global information society. From this broad and neutral platform, ITU aims to create an environment that will encourage Member States, Sector Members, industry partners, intergovernmental and other international organizations and all other interested entities to make various types of voluntary contributions aimed at the development of effective, useful of infrastructure and applications

for value-added e-services by collaborating and coordinating their activities within their respective areas of competence in the spirit of this MoU, towards the objective (Paragraph 1.) established under this MoU.

The Municipal Charter of the City of Osmio

On March 7, 2005, we held the Quiet Enjoyment Infrastructure meeting at the Geneva headquarters of the ITU, to start putting together a source of appropriate worldwide duly constituted public authority[61] .

A year later the ITU elected Hamadoun Touré, the head of the ITU division that put forth the World e-Trust Initiative, as its Secretary General. Dr. Touré then appointed me to the High Level Experts Group of the ITU's Global Cybersecurity Agenda.

A short clip from my address in that capacity to the UN's World Summit on Information Society may be seen at http://www.youtube.com/watch?v=e3hViw833so.

Osmio's Vital Records Department, operating under a Certification Practice Statement established by the Osmio Certification Practices Commission, signs public keys establishing identity certificates, but only when requisite evidence of identity is provided to it by an Attestation Officer acting on behalf of an authorized enrollment authority.

Presently, that means our Authenticity Alliance member organization Reliable Identities, Inc.

In traditional PKI parlance, Reliable Identities is a registration authority. Reliable Identities is licensed by the City of Osmio to supervise the gathering of evidence supporting a claim of identity and the submission of certificate signing requests to the Osmio Vital Records Department.

The more rigorous set of enrollment procedures are performed by an attestation officer (a specially qualified signing agent notary, who among other things, knows how to check ID) in a face-to-face process that involves an oath, an affidavit, and a jurat. The legal effect of a notarial action is to apply public authority to a document by means of a face-to-face procedure[62] , unlike some commercial certification authorities that improperly and perhaps illegally use the term “notary” to apply to individuals with no public authority.

That produces our Digital Birth Certificate, Osmio's more rigorous and costly set of enrollment procedures, for more demanding relying party situations. If a more lightweight identity will suffice, you can avoid a trip to a notary with our alternative to the Digital Birth Certificate, called ReliableID. ReliableID enrollments are performed remotely.

61 You can see the current version of the Municipal Charter of the City of Osmio at http://osmio.ch/cityhall_charter.html.

62 In July 2012 the Commonwealth of Virginia introduced a procedure that allows a notarization to take place over an audio-video link. Osmio makes use of the Virginia procedure in a special class of Digital Birth Certificates.

In both enrollment procedures, Digital Birth Certificate and ReliableID, a key pair is generated under the supervision of Reliable Identities.

Let's assume your situation calls for the higher identity quality of a Digital Birth Certificate. Reliable Identities will send you to a web site where you'll fill in a form that generates an Affidavit of Identity. You'll print the affidavit and take it to a signing agent, our specially qualified notary, who will check your ID and administer an oath.

After that our Attestation Officer will help you generate your private and public key, and submit the public key and the Attestation Officer's attestation that your assertion of identity has been properly validated. If all is in order, the public key will be signed by the Osmio Vital Records Department.

For the ReliableID enrollment, the less rigorous and less costly alternative, there are two options. For one type of ReliableID enrollment you'll need to be reachable at a telephone number that is published under your name or at your place of employment. A still less rigorous and less costly ReliableID enrollment requires you to prove identity using what we call PII corroboration, which is similar to knowledge-based authentication.

In between the face-to-face Digital Birth Certificate procedure and the ReliableID procedure is the "Virginia Digital Birth Certificate" procedure, which takes advantage of a 2012 Virginia law enabling notarizations to take place over an audio-video link. You need not actually be in Virginia; you can be anywhere.

Regardless of which enrollment procedure is used, our patent-pending Identity Quality Assurance system yields an identity quality score based upon specific criteria. Identity Quality Assurance provides a way of knowing that an identity assertion is appropriate, as measured in each of eight categories.

Each of the eight Dimensions of Identity Quality is measured on a scale of 0 to 9, with 0 being the lowest rating. Thus the highest quality ID will carry a score of 72. With that one you can buy an office building on another continent while sitting in your den.

International Governance Is Not World Government

Governance through international organizations tends to make some people nervous. The prospect of a Josef Stalin gaining control of a technology-empowered United Nations is beyond scary and not beyond the realm of possibility. The comforting thing about the United Nations is that unlike a national government, it is truly a loose assortment of agencies, few of which have any tight accountability to the Secretary General or the General Assembly. The ITU regulates telecommunications across boundaries; the UPU regulates the relationships among national postal services. Each is an affiliate of the UN but neither really takes orders from the UN. That's the way it should be.

Ambitious demagogues hoping to use the UN as a platform for world despotism are deprived of the one thing ambitious leaders have always called upon: invoking The Enemy. Until the Earth is attacked by alien invaders, we are safe from that most effective path to despotism.

Nevertheless, it's true that Internet packets know nothing about national boundaries. We have seen that attempts by nations to proxy the Internet, restricting citizens to a filtered view of the world, do not work. Proxies can be circumvented. When it comes to the Net as a whole, national boundaries don't need to be circumvented. They largely don't exist.

Some ambitious gangs of thugs have indeed come forth to vie for the role of world government. We've mentioned Lulz Security, TeaMp0isoN, Anonymous, and others.

Here are some other gangs that blatantly belie the "do no evil" ethic when they break into our second homes, steal our property, that is, our personal information, and put it onto their balance sheets: Google, Facebook, DoubleClick, Yahoo, etc. Will one of them prevail against LulzSec to become the government of the world?

Or will we prevent world government by carefully building a system of international governance?

Commercial Services Support Public Authority

Public authority regularly depends upon commercial contractors to support its work. Vital records departments don't manufacture the certificate paper stock and embossing seals that are used in the application of their public authority; they purchase those things. For example, Giesecke & Devrient is a German company that prints currency for many nations and also produces PKI token technology. The key ingredient in its product — authority — is imported in its entirety from its client country's treasury. Giesecke & Devrient is trusted by Treasury people to treat that authority very carefully.

The operations of the Osmio Vital Records Department are managed on contract by a privately-held commercial certification authority enterprise, StartCom Ltd63 . StartCom provides the certification authority management expertise; the City of Osmio provides the duly constituted public authority.

StartCom competes successfully and profitably, steadily gaining market share against other CAs. Most importantly, StartCom has distinguished itself as an organization that knows how to do certification right, as reflected in its performance in the infamous Comodo hacker incident that brought down DigiNotar and prompted the whole collegial certification movement.

Here's how InformationWeek reported64 on that performance:

InformationWeek
THE BUSINESS VALUE OF TECHNOLOGY

63 Full disclosure: The author is a stockholder in StartCom Ltd.

64 "How StartCom Foiled Comodohacker: Four Lessons," by Mathew J. Schwartz, *Information Week*, September 08, 2011, http://www.informationweek.com/security/attacks/how-startcom-foiled-comodohacker-4-lesso/231601037.

How StartCom Foiled Comodohacker: 4 Lessons

Comodohacker claims to have exploited six certificate authorities including DigiNotar—yet he failed to break into at least one. Here's how StartCom's approach to security worked.

Based on the boasts of "Comodohacker," he's compromised six certificate authorities (CAs) this year, including Comodo in March and DigiNotar in July. He's also claimed to have exploited at least four more, including GlobalSign.

But the Comodohacker also said that he was unable to hack into StartCom Certification Authority… In other words, StartCom successfully defended itself, while — at least by ComodoHacker's count — a half-dozen similar businesses got hacked.

Asked about what exactly tripped up Comodohacker, Eddy Nigg — founder, COO, and CTO of StartCom — said via email that he didn't want to reveal too much. "That's the way he experienced it, [but] from the technical point of view it's obviously a bit different. But I don't want to spoil it and provide unnecessary information, as you might understand."

Every year, StartCom submits itself to the WebTrust Extended Validation audit. Just as important, StartCom has distinguished itself as a leader in the effort to clean up the certification business. As web site owners worry about browser software makers taking action against the more egregious commercial certification authorities, rendering their site certificates useless, StartCom puts itself at the other end of the scale.

Although the volume of site certificates issued by the industry vastly dwarfs the volume of identity certificates, StartCom takes identity certification seriously. StartCom personnel know how to perform remote verification of identity, the heart of the ReliableID enrollment process, on a global basis.

StartCom is contracted to build and manage our certification from public authority. But certification policy and oversight come from Osmio's Vital Records Department and its Certification Practices Board.

Meaning, of course, that it comes from you, the involved resident of Osmio with a background in PKI or public records management or other relevant experience — and of course with a demonstrated record of integrity.

Together, the City of Osmio, Reliable Identities, Inc., and StartCom form our Authenticity Factory. Other Authenticity enterprises take the output of the authenticity factory to their target markets, with each one backed up by The Authenticity Institute.

Osmio and Cross Certification

Cross-certification is a process by which a certificate signed by one root is accepted in a PKI using a different root. Certification schemes built to serve entities within bound-

aries have a built-in hurdle to cross-certification. If the boundary is geographical and political, then all jurisdictions in the world must either cross-certify or else the world must stop shrinking; people from one place may not have a basis for authentic communication with people from another.

In other words, certificates issued by any jurisdiction must be honored by every other, regardless of differences in certification practices and standards. Digital certificates must become like notarizations.

But notarizations are used in a human context, with human beings looking at documents and the people who present them. Digital certificates are looked at and checked out by algorithms. Algorithms understand only logical contexts, not all the subtle visual and other cues that support a paper notarization.

The only root authority that can serve as the ultimate root authority is worldwide duly constituted public authority. The ITU has taken on this responsibility in its World e-Trust Initiative's root-of-roots for certification. But the ITU's constituency is limited to member organizations, i.e., companies in the technology and telecommunication industries, and the telecommunication ministries of sovereign nations.

We need an international organization that can apply the global, duly-constituted public authority of the ITU but whose constituency is the people it serves. We need an organization that is governed with not just the consent of, but with the participation of, those it serves.

That is the City of Osmio, a municipality that has no physical jurisdiction but whose logical jurisdiction encompasses all who choose to accept its governance.

Osmio, SAS 70 Certification, and WebTrust Audit

The Osmio Vital Records Department is subject to an AICPA audit of service organizations called SAS 70, and in particular the version for certification authorities called the WebTrust audit. In the AICPA's own words, here is what such an audit does:

> Statement on Auditing Standards (SAS) No. 70, Service Organizations, is an internationally recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA). SAS 70 is the authoritative guidance that allows service organizations to disclose their control activities and processes to their customers and their customers' auditors in a uniform reporting format. A SAS 70 examination signifies that a service organization has had its control objectives and control activities examined by an independent accounting and auditing firm. A formal report including the auditor's opinion ("Service Auditor's Report") is issued to the service organization at the conclusion of a SAS 70 examination.
>
> SAS 70 provides guidance to enable an independent auditor ("service auditor") to issue an opinion on a service organization's description of controls through a Service

Auditor's Report (see below). SAS 70 is not a pre-determined set of control objectives or control activities that service organizations must achieve. Service auditors are required to follow the AICPA's standards for fieldwork, quality control, and reporting. A SAS 70 examination is not a "checklist" audit.

Own Your Identity and Its Issuer

Let's address some FAQs about Osmio. First, who is Osmio? Who owns Osmio? The answer is the same as the answer to the question, “Who owns the city or town where you live?”

Why, you do. Cities and towns are owned by their residents. When you establish a second home in one of Osmio's residential neighborhoods, you become an owner of the City of Osmio. That means you own its departments, which include the City of Osmio Vital Records Department. So you own the certification authority.

And Then Get Involved

“How is Osmio governed?” might be your next question. As with any city, the involvement of its citizens affects the quality of its governance. So we hope that after you set up a home in Osmio you'll get involved in the town's governance.

Osmio uses a system of governance called Optimocracy, named after the engineering process of optimization. Optimocracy is enabled by the existence of reliable identities, and is explained by the answer to the next question, “Who governs Osmio?”

The answer here is similar to the answer to the ownership question. Participation in the governance of Osmio via one of its boards or commissions is open to any resident who can demonstrate both a willingness to keep up with the issues before the board, by participating in its real-time and threaded deliberations, and an ability to comprehend those issues by periodically answering some objective questions about them. The top administrative officer of the City of Osmio is its Chief Moderator, who is elected by the members of Osmio's boards and commissions.

If you're particularly interested in privacy, you might want to join the board of privacy standards and practices. There's also the professional licensing board and many other opportunities for participation. If you're knowledgeable about PKI or if you're a vital records professional, you can apply for one of the seats on its Certification Practices Board.

Think the keeper of the keys to your private life should be a company like Microsoft? If so, try applying for a position on Microsoft's Certification Practices Board. Just get in touch with Steve Ballmer or his successor, whoever that might be. I'm sure the CEO of Microsoft would love to get you involved.

While you're waiting for a response, consider joining the World Trust Signatories Association, whose goal is to bring the support of individuals to the latest version of

what used to be called the World e-Trust Initiative. Since the ITU's charter limits its constituency to national governments and sponsoring companies, this separate group exists to bring the voices of individuals like you and me together to urge the adoption of the building blocks of Authenticity. To learn more about the World Trust Signatories Association, go to trustsig.org. Read its Memorandum of Support, and if you agree with its principles and intent, get yourself a certified identity and sign it.

Our solution to the problems of the world's information infrastructure, and to many other problems, is built upon the historic fact of achievable authenticity.

One person must recuse himself from participating in most parts of Osmio's governance, and that is this author. Directly and through The Authenticity Institute, Inc., I have invested resources "on spec" in the building of Osmio, and expect to get compensated for that effort when Osmio is successful. But it's up to Osmio's administration to issue the payment, and it would be a conflict of interest for me to be part of that process.

Next anticipated question: "By what authority is Osmio chartered?"

There is no provision in existing national or provincial law for the chartering of municipalities that don't exist as a physical space on the earth's surface. But that is changing, through the same process that saw the first municipal charters of cities.

There was a need to fill a void in existing law, and so it was filled. Simple as that. Most of the nations of the world were established with much less authority than was applied in the chartering of the City of Osmio in the Quiet Enjoyment Infrastructure meeting at the Geneva headquarters of the International Telecommunication Union on March 7, 2005.

Next FAQ: "Can other online communities and social networks benefit from Osmio's ability to bring authenticity to online spaces?"

Well, okay, that wasn't exactly a frequently asked question but we do have an answer. Osmio also can serve as administrative capital for communities such as social networks, which are typically not owned by their residents.

Perhaps you have a social network, a community, that could benefit from the Quiet Enjoyment Infrastructure by adopting Osmio as its administrative capital. Just let Osmio's Standards Adoption Board know that you want to adopt QEI standards and they'll get you started.

And if you don't have an established social network for your existing community of interest, our Authenticity Enterprise Global Villages, Inc. will be happy to set up a Village® Authenticity-Enabled Social Network for your group.

Duly Constituted Public Authority Is Part of Every QEI Component

Duly Constituted Public Authority is an important ingredient in each component of the Quiet Enjoyment Infrastructure. The source of public authority for QEI takes the form of a municipality. We have introduced the City of Osmio and its Vital Records Department, which serves as the certification authority for the identity credentials in the Identity Reliability Component.

The main source of Osmio's public authority is the same as the source of public authority everywhere: The acceptance of its authority by its citizens. While there is no precedent for the chartering of a municipality that exists only in cyberspace, that needn't stop us.

Besides its Vital Records Department, Osmio's other departments are designed to provide a source of duly constituted public authority for areas where it is needed:

- Vital Records
- Standards
- Professional Licensing
- Privacy Protection
- Buildings
- Public Works
- Vehicles
- Planning and Zoning
- Law Enforcement
- Judiciary
- Municipal Charter Commission

The All-Important Certification Practice Statement

The City of Osmio is the global source of public authority for the various certifications in QEI. Every certification authority, and every certification offered by it, is governed by its certification-practice statement. We won't reproduce all of that here, and in fact the very important professional licensing CPSs await the involvement of the yet-to-be-convened governing boards.

The City of Osmio has Certification Practice Statements for its identity certifications, professional licensing certifications, and building and occupancy permits, and will be adding more. They are long, and so they've been removed from this volume to save space. You may see them in their entirety at http://osmio.org.

The Ultimate Authority

We've invoked many sources of authority in our infrastructure so far, but there is one we have left for last. Recall that the second O in (E&O)2 stands for "oath."

In some jurisdictions, an affidavit may attest to the witness of either an oath or an affirmation, both of which are verbal statements made by the affiant (the person taking the oath or affidavit), both invoking the same legal sanction. In other words, the affidavit is made under penalty of perjury; the affiant is subject to criminal prosecution if it is later determined that the statement is untrue.

As contrasted with an affirmation, an oath includes an element that may be seen by some as old-fashioned and even irrelevant: It is an attestation before a Supreme Being. Obviously the perception of the consequences of lying with this sanction is personal,

and in some cases there is a perception of no consequences at all.

In the land where separation of church and state is for some reason taken to mean separation of Supreme Being and state, it is perceived as unconstitutional not to provide a secular alternative to the oath. But some jurisdictions will not, or may not, honor an affidavit backed only by an affirmation and not an oath. This could present a problem for our Public Authority Component, which needs to have worldwide viability.

So as a workaround, one may substitute "That Which Created Me" for the word "God" in the verbal statement and the affidavit.

But enough theology, let's get down to the practical and tangible. Let's take a look at the procedures and the equipment Attestation Officers will use to perform their job.