TEN REASONS WHY PKI HAS FAILED TO GAIN TRACTION

Wes Kussmaul

ABSTRACT

Public key cryptography, in the early years following its invention, offered great promise as the ultimate security solution – but half a century later it is still just a promise. As the powerful construction material now at the core of Public Key Infrastructure (PKI), there have been many failed attempts to put the theory to practical use, and hope is fading that it can ever work in real life. This paper examines the reasons behind PKI's fall from grace to show there is no reason it cannot deliver exactly what it promised.

KEYWORDS

PKI, Authenticity, duly constituted public authority, public authority, City of Osmio, accountable anonymity, Identity Quality Assessment, Reliable Identities, identity certificate, public key cryptography, digital signature, privacy, accountability

1. INTRODUCTION

If PKI is so good, why hasn't it delivered on its promise? In 2006, *MIT Technology Review* said "The Internet is Broken." A decade later, it is *still* broken – and getting worse. Spam brings us phishing attacks that install malware, which in turn builds botnets that steal our money, our identities, and our reputations. Fraud and predation pervade everyday online experience. Identities, cash, and vital records are stolen in *batches*.

While the information security industry assures us "We're working on it," people grow ever more wary of their Internet experience – even as they come to depend on it more and more.

Underneath our security problems are problems of inauthenticity. Our real problem – the *root* problem – is ***inauthenticity***. People are not who they say they are, sites are not what they claim to be, hackers broadcast spam and malware – under *your* name, from *your* computer – from your *thermostat*!

How do we solve problems of inauthenticity? Very simply: We solve the problems of inauthenticity with the proven tools and construction materials of AUTHENTICITY.

Authenticity works where security technology has failed us.

When you solve problems of inauthenticity, you solve other problems as well – security is just one of them. With Authenticity, our information systems will be much more manageable, effective, reliable, and easy to use.

Can we have Authenticity? Yes, absolutely. Mankind has developed – over centuries – a set of methods and procedures to solve problems of inauthenticity, and those methods and procedures fit nicely with today's information technologies.

Historically, an authenticity infrastructure consisted of duly constituted public authority – such as notaries and justices of the peace -- and a means of *conveying* that authority – physical things like notary seals, wax seals, and affidavits.

After all these years, *Authenticity* is still the solution to problems of *inauthenticity*. On the Internet, however, we need a better means of *conveying* Authenticity.

And indeed we have it. We could call it an "authenticity conveyance infrastructure" – or we could call it what its late twentieth century inventors named it: PUBLIC KEY INFRASTRUCTURE, or PKI.

PKI is the ***conveyance of authenticity***.

Conveyance of authenticity was around long before the Internet. The wax seal was a personal "signature," assuring the recipient that the document was authentic and that it really came from the owner of the seal. The wax seal conveyed the *authenticity* of both the sender *and* the document. PKI is the 21st century version of the wax seal. A digital signature conveys the authenticity of both the sender *and* the document.

Recognizing PKI's central role as a conveyance of authenticity, let's introduce an Authenticity Infrastructure, with PKI at the very heart of what makes it work.

So if PKI is so good, why hasn't it solved all our information technology problems? We've identified ten reasons why PKI has not fixed those problems.

2. THE TEN REASONS

2.1. Reason 1: PKI implementations usually omit a vital component.

By definition, PKI cannot exist without private keys. But it has been implemented without specifications and methods for *managing* and *protecting* private keys, especially for identity certificates. PKI has been like a car designed with a body and wheels, but no engine. Is anyone surprised to find out it doesn't work?

The daunting responsibility of managing and protecting private keys, the fear of liability, and general unfamiliarity with the role of private keys in supporting Authenticity – all have contributed to a throwing up of hands when it comes to dealing with this essential element of PKI.

One of the components of the Authenticity Infrastructure is its PEN component – the Personal Endorsement Number – which is all about the creation, protection, and management of what used to be called private keys.

2.2. Reason 2: PKI terminology can be bizarre.

PKI experts have gotten used to saying things like "The user signs the file with his certificate." The poor newcomer who has heard that PKI is good stuff – and is trying to understand how it works – is left scratching his head. As it is now, "certificate" can refer to a signed public key or to a certificate *plus* its corresponding private key.

Suppose you were being introduced to fruit science. Seeing fruit for the first time, you might ask "What *are* these things?"

"This is an apple, and this is an orange" the fruit scientist might say.

"Tell me more about this thing called *apple*."

"An apple? Well – an apple is an apple, plus an orange."

"So what do you think of fruit science so far?"

"I think I'm outta here!"

Remember being introduced in middle school to a useful type of number called an imaginary number? If you can get your "beautiful mind" around *that*, then "a certificate is a certificate plus its private key" might present no problem to you!

But for the rest of us: A ***certificate*** is simply an ***assertion*** signed by an ***authority***. The pen that signs the certificate is NOT part of the certificate. In the Authenticity Infrastructure, the thing

that signs the certificate is called a PEN – a Personal Endorsement Number. It works like the old private key.

The fact that this needs to be clarified says a lot about why PKI has been slow to gain traction. Of all the gobbledygook in information technology, this mangling of the term *certificate* has been among the worst!

2.3. Reason 3: PKI has developed a reputation for being brilliant, but too complex for practical deployment.

Now wait. Every time you go to a secure web page – with the little lock icon and address that starts with "http**s"** – you are using PKI.

You don't need to understand prime number exponentiation or elliptic curve mathematics to do your online banking, or internal combustion engines to drive your car. This undeployability stuff is nonsense. Complex systems are deployed all around us, but designers have found ways to hide complexity beneath a simple and easy user experience. The good news is that your browser and email and other software are set up to use PKI already.

The *not* so good news is that every product handles keys and certificates differently – and very little of it is intuitive.

Back to the *good* news. The developer community for the Authenticity Infrastructure is stepping forward to guide you through the gotchas – particularly when it comes to establishing and using your own identity certificate. We don't care HOW obtuse your software is – we'll get you signing and encrypting. *We* figure it out and make it easy, so *you* don't have to.

But there's another reason why PKI has gained this underserved reputation for complexity*:*

PKI is not particularly complex – it's just BIGGER than technology.

PKI has always been the province of technologists. To a technologist, the very important *certification authority* component of PKI is a piece of technology. But if you're going to do something more complex than build a tunnel between computers whose owners have a business relationship with each other, then real *public authority* is called for.

The certification authority is, first and foremost, a facility where *duly constituted public authority* is applied to documents and procedures. It's much like the vital records department in city hall. Technology experts consider PKI to be complex because this central element:

The establishment and management of DULY CONSTITUTED PUBLIC AUTHORITY

is outside their expertise.

2.4. Reason 4: Reliable identities of users – necessary for effective PKI – have been scarce.

After spending millions of dollars on network security, corporations still have major security problems. Meanwhile, your ATM card allows your bank to dispense cash with confidence from a machine on a city sidewalk.

The technology used by your ATM card is more ancient than the floppy disk! So why are bank ATM networks generally secure, while corporate information networks – in spite of continuous investment in the latest security technology – are barely able to keep ahead of intruders?

The difference is not about *technology* – it's about *assumptions* and *architecture*. Your bank's ATM network starts with the premise that knowing who you are is the foundation of security.

If a trusted co-worker asked you for your network password, what would you say? You'd likely share it. In many companies, collaborative work gets done by sharing access credentials,

despite rules against it. Why shared so freely? It's because that credential protects the *company's* assets – not YOURS! But if that co-worker asked you to share your ATM card and its PIN, THEN what would you say? Of course, they would never ask in the first place! And banks know this.

Banks have known it for decades: *Identity is the foundation of security*. That means *reliable* identity – banks come close to reliable identity through the application of their "Know Your Customer" rules.

The Authenticity Infrastructure makes information resources *secure* and *manageable* by

1. Establishment of *measurably reliable identities*, and
2. Designing and building online spaces upon a foundation measurably reliable identities, PKI, and construction standards and practices.

The Authenticity Infrastructure includes detailed procedures for enrolling individuals either face-to-face or online. The resulting credential is accompanied by a record showing the credential's own reliability, without disclosing any personal information.

This reliability record is a score that measures how likely it is that *this* certificate really represents *this* person.

The reliability score includes – among others – metrics related to how the credential was created and how secure is the physical device where it resides. The credential takes the form of a group of digital identity certificates all identifying the same human being, which is very much like the site certificate of a secure website whose address starts with **https**.

The certificates can be kept in the user's computer or, preferably, in a smart card, USB token, phone, watch, ring, or other device separate from the computer. Most importantly, the credential is designed to be used to establish identity anywhere – including places where it controls access to the user's money, reputation, relationships, and other assets. For an employer, health care provider, bank, or other relying party, this means it will be well-protected by its owner. In other words, you *won't* want to share it with co-workers to access the company network, and you *will* want to keep it as close and guarded as your ATM card.

2.5. Reason 5: Attempts at reliable PKI identity have not adequately protected users' privacy.

Once you've created an identity credential that you can use anywhere, how do you keep nosy organizations from tracking everything you've done with it? Some say we've already lost that battle, that everything we do is tracked by a few powerful organizations – and personal privacy is gone forever.

Indeed, universal identity done *wrong* is a threat to personal privacy. But universal identity done *right* is a fortress of personal privacy, reversing the erosion of privacy we've seen in recent years. The Authenticity Infrastructure accomplishes that elusive goal – long sought by privacy activists – of putting people in real control of the disclosure and use of information about themselves.

More than that, our *reliable identities* add the critical – and until now missing – concept of personal accountability. This combination of privacy plus accountability is the cornerstone of Authenticity.

It's called ***accountable anonymity***. Accountable anonymity is familiar concept older than the Internet. It's like the license plate on your car – anyone can see it, making you accountable for what happens on public roadways. But no one gets to know your identity as driver or owner until something goes wrong, at which point legal authority can unmask your identity and hold you accountable.

License plates work imperfectly in the physical world, but in the digital world we can make them work much better. You see, our identity certificates are standard X509 certificates, except for one thing: They have no information about *you* in them. That's right – like a license plate, they *assert* identity without *disclosing* identity.

2.6. Reason 6: PKI has CONVEYED authenticity without requiring a legitimate SOURCE of authenticity.

How do you *convey* Authenticity without first *establishing* Authenticity?

PKI has been the domain of technologists. If we regard PKI as a set of excellent construction materials – which it is – then those who created it are like materials scientists. Putting well-engineered materials to work requires architects and building inspectors and others whose professional licenses are issued by a public authority and whose actual identity is attested by a vital records department in an agency with duly constituted public *authority*.

But wait – "duly constituted public authority" has that worrisome sound of over-endowed, under-controlled, centralized power. Far from it! It *is* centralized, but for the right reasons and in the right way.

The City of Osmio was founded on March 7, 2005, at the Geneva headquarters of the International Telecommunication Union, to serve as a source of worldwide duly constituted public authority in the certification of identities and in the issuance of professional licenses for the practice of code audit, penetration testing, and other professions.

The seat of this duly constituted public authority is a virtual municipality – owned by those who use the credentials for which it serves as certification authority. It's a global optimocracy – new governance for the Online Age, foundational support for the critical security and privacy challenges of our online communities.

With no connection to any physical political government, it attests to the identity and accountability of *human beings* who sign building permits, building inspections, and occupancy permits for the online spaces where we conduct our lives.

A duly constituted public authority ensures that the word "authority" in the Certification Authority component of every PKI *actually means something*.

2.7. Reason 7: PKI deployments have tried to replace signatures of PEOPLE with signatures of OBJECTS. That doesn't work.

It's true – objects are much easier and less costly to manage than people. You can tell an object what to do, and it does it. But PKI is an authenticity *conveyance* infrastructure, which makes it an *accountability* infrastructure.

How can you make an OBJECT accountable in any meaningful way? You can't. Accountability rests with PEOPLE.

PKI must be built upon individual identity certificates of *human beings*. The notion of an accountable network of *objects* is FOLLY.

2.8. Reason 8: The role of encryption in PKI is confusing.

It's true, encryption plays a central role in PKI. It's also true – sadly – that the type of encryption used in PKI is suitable only for very small files. The world would be a little bit happier if the fundamental laws of mathematics were different and you could send your large document encrypted with your recipient's public key so that they would be the only person on earth with the private key necessary to decrypt it.

Alas, such is not the case, and this is where people understandably get confused. It would help if we explained that a *symmetric* encryption process has to be invoked in most cases in order to share reasonably sized files in confidence. But that makes for a longer story, so the explaining of THAT has tended to be avoided – until now!

An important part of the implementation of The Authenticity Infrastructure is educational. We take the time to show PKI's role in *key management*, which makes encrypted file sharing practical.

PKI uses encryption as a tool to carry out the *processes* of Authenticity, not for encrypting user files. The spotlight really belongs on PKI's work in *conveying* and *supporting* Authenticity, not on its own internal use of encryption in carrying out that work. Fortunately, the files that PKI uses in its work *are* small files, as we will see in the three process descriptions that follow.

Here's how PKI uses encryption to support Authenticity.

Digital signatures – To *ensure the authenticity* of the signer and the file's contents.

Authentication – To *ensure the authenticity* of the person attempting access – such as logging in to a server or using an ATM machine.

File encryption – To *ensure the authenticity* of the person who decrypts the file.

In every case – digital signing, authentication, and file encryption – the role of PKI is the *management of users' key pairs* to encrypt the various small files used in processes that *ensure the authenticity* of people and their files. Even in the third case – file encryption – PKI doesn't use its own (asymmetric) encryption method to encrypt the user's file, but rather uses it to *ensure the authenticity* of the person receiving the decryption key.

Here's how each of these processes works.

First of all, each person has a pair of numbers assigned uniquely to them. The user's PEN (private key) is kept in their personal possession – on a computer, smart card, phone, USB token, watch, or other personal item. The user's PCN (public key) is freely available to any person or process at the other end of an interaction. Either number of this pair can decrypt a file encrypted by the other.

If you're familiar with PKI and public key cryptography, you'll know how these two numbers work as a team to perform *asymmetric* cryptography

2.8.1. Digital signatures

A digital signature simultaneously conveys the authenticity of both a file *and* its signer. It's like a combined "fingerprint" of both the file and its signer, encrypted and decrypted using the signer's key pair. It's actually a condensed and scrambled version of the file – called a "hash" – which is then encrypted with the signer's PEN (private key).

At the receiving end, the signature is decrypted with the signer's PCN (public key), revealing the hash of the original file. The received file is hashed by the recipient, and if the two hashes match, then the file's authenticity is confirmed, and the recipient knows that not a single bit has been changed since the file was signed.

*In this process, the small file encrypted using PKI's asymmetric encryption is the **hash** of the signed file.*

2.8.2. Authentication

The person requesting access sends his PCN to the gatekeeper – the server, ATM machine, access panel, or whatever. The gatekeeper encrypts a small test file using the requester's PCN, and sends it as a challenge to the requester, who decrypts it with his PEN and returns it. If the decrypted file matches the test file, then the PEN must be the correct mate of the PCN, ensuring the authenticity of the requester.

*In this process, the small file encrypted using PKI's asymmetric encryption is the **challenge file** sent by the gatekeeper to the requester.*

2.8.2. File encryption

PKI's asymmetric encryption only works for very small files. On the other hand, single-key symmetric encryption works for *any* size file. But symmetric encryption can't protect the file from decryption by an imposter. So how can we provide the Authenticity protection of PKI's asymmetric encryption for any size file?

The answer: PKI can use its asymmetric encryption to encrypt the symmetric key, because the symmetric key itself *is* a small file. In the case of sending an encrypted file from one person to another, the sender's digital signature *ensures the authenticity* of the sender and the sent file, while the encrypted symmetric key *ensures the authenticity* of the receiver, who is the only person who can decrypt the file.

*In this process, the small file encrypted using PKI's asymmetric encryption is the **symmetric key** that encrypts and decrypts the user file.*

2.9. Reason 9: Old assumptions from the 1980s are driving a ship that's hard to turn – or even challenge.

Imagine telling your building's receptionist "Please determine the intentions of everyone who enters the building, and also determine whether they are good or bad people." If you think that's an unreasonable request, *and* you know how buildings successfully serve us in everyday life, then you are ready to meet the Authenticity Infrastructure that is unencumbered by the flawed assumptions of the security systems that have failed us.

The current practice of information security is mostly about determining the intentions and character of the sender of a stream of bits.

Do you think that's possible?

When it *is* possible, it's because the intruder lacks skills or funding. In other words, existing information security products tend to deter the least threatening attacks – which renders many information security efforts ineffective – or worse, lending a false sense of security. They treat your information facilities as a commando outpost, rather than the online office facilities that they really are.

PKI – *if done right* – offers something better: If you apply reliable identities, building codes, professional accountability, and architecture to PKI, you can build very secure and effective *office buildings* – where you can keep your information and conduct your business in ***quiet enjoyment.***

Quiet enjoyment is an old real estate term that translates elegantly to the world of the online spaces we "occupy." It means you are free to enjoy the property as if it were your own, without intrusion, with the expectation that the property will deliver on all its claims. It is a landlord's assertion – in addition to City Hall's occupancy permit – that the property is *habitable*.

These are very old concepts. Information technologists are not used to relying upon concepts from the 19th century! They involve things that are far outside what information technologists

are used to judging and managing, and they imply a complete departure from today's "examine-the-bit-streams" approach to security – a move that can be seen as risky to a career in IT!

The application of some very *old* concepts to PKI can make it solve *big* problems. If you're a stockholder in a company with an information technology department, you may want to show this message to your CEO.

2.10. Reason 10: PKI, when done right, works TOO well.

Our computers, operating systems, and application software have been designed to let their makers help themselves to information about YOU: your habits, your purchases, your *life*.

The Authenticity Infrastructure puts information about *you* under *your* control. Nosy organizations can no longer help themselves to whatever they want to know about you. And that doesn't make them happy – despite their proclamations about how much they care about your privacy.

The Authenticity Infrastructure also calls for *digital signatures everywhere* while keeping the signer's identity and personal information private. This yields accountability while maintaining privacy – and some organizations seem to be threatened by accountability. Those organizations will tend to lose the ability to snoop, while being held accountable for their own actions.

Suppose your physical home – your house or flat – had been built with secret passageways that you didn't know about. Suppose that every day, various intruders would enter through those secret passageways, open your file cabinets, and place files in your folders. Sometimes they would install devices in your rooms that would report back to them what you're up to.

Those little files left in your online home are called "cookies" – could they have chosen a friendlier or less alarming word than "cookie"?

But those famous – and removable – "cookies" are the *least* sneaky method of tracking you. Flash cookies, beacons, fingerprinting, and other *really* sneaky methods – undetectable and unalterable by you – are infesting your online information home.

That could never happen in your physical home, of course. City Hall's building codes, building inspectors, and occupancy permits would never allow such an obvious breach of the principle of quiet enjoyment in our homes.

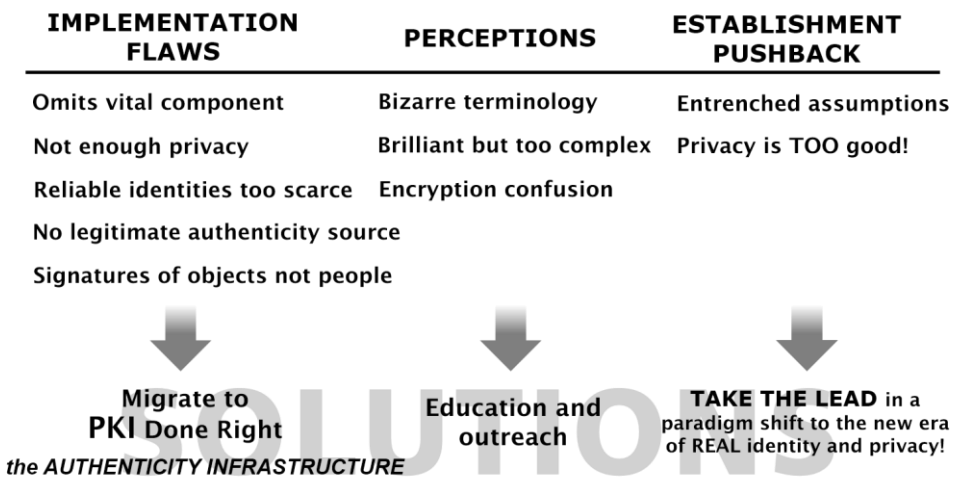
But in that information home – your computer or your phone where you spend more and more of your time – that's exactly how it works.

No wonder data-hungry organizations have been so slow to embrace PKI.

2.11. Ten Reasons Sorted

Let's take a look at how these reasons sort out.

Figure 1. Ten Reasons Sorted



We have **implementation flaws**, **perceptions**, **and institutional pushback**.

What are the solutions? For implementation flaws, we can migrate to PKI done right – which is the Authenticity Infrastructure.

For problems of perception, we can work on education and outreach – like this paper and other documentation and videos.

For institutional pushback, we can take the lead in a paradigm shift toward the new era of *real* identity and privacy.

3. CONCLUSION

As with anything that appears to be at a standstill with no clear path forward, the first step is to clearly identify the obstacles so they can be faced and overcome. Every one of the ten reasons described here has a solution that is not only possible, but has already begun. Work is now underway to clear these hurdles and put PKI to work in solving the exploding epidemic of problems caused directly by the lack of Authenticity in our online world.

Authenticity works where security technology has failed us.

Author

Wes was the sole founder in 1981 of Delphi Internet Services Corporation, which was among the four largest online services along with AOL, CompuServe, and Prodigy. In 1986 he launched a spinoff, Global Villages, Inc., to serve magazine publishers and business clients with their own private-label online service, providing business planning, design, engineering, hosting, management, and promotion services. In response to the need for a regional version of Delphi, Wes launched Local Villages, Inc. Together, Global Villages and Local Villages became known as The Village Group. (Delphi was sold to Rupert Murdoch in 1993 and Global Villages' hosting business to NTT Verio in 1998.)

When, in 1990, the US National Science Foundation dropped its prohibition on the use of the Internet for commerce, disrupting the provision of reliable identities of users, Wes focused on the need for reliable identities of individuals on the Internet, starting with the development of the VIVOS Enrollment Workstation. Designed to be used by notaries with minimal training, VIVOS bound biometrics of the enrollee to digital identity certificates.

While developing VIVOS, Wes was introduced to a group at the International Telecommunication Union who were attempting to implement a world PKI that was similar to the one he envisioned. In 2002 The Village Group became a charter signatory to the International Telecommunication Union's World e-Trust Initiative and is now a Sector Member of the ITU.

In 2008, as a member of the High-Level Experts Group at the ITU's Global Cybersecurity Agenda, Wes introduced the City of Osmio in an address to the United Nations World Summit on Information Society in Geneva. The City of Osmio applies the global public authority of the ITU to the process of identity certification and to other digital certificates.

Wes is an individual adherent to the International Union of Latin Notaries and has been appointed a Notary Ambassador by the National Notary Association. He has written several books about identity, privacy, and PKI, including *Quiet Enjoyment* (2014), *Own Your Privacy* (2013), *Don't Get Norteled* (2015) and *Escape the Plantation* (2015).