Twelve Reasons Why PKI Has Not Delivered On Its Promise

Wes Kussmaul

Founder and CEO, The Authenticity Institute
AuthenticityInstitute.com

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.

2. The Twelve Reasons

The twelve reasons constitute twelve answers to the question,

"If PKI is so good, why isn't it in use everywhere?"

Following are the twelve reasons behind the misunderstandings, resistance, and slow adoption of this powerful solution:

Reason one: You can't have a working PKI without both public keys and private keys. But the very term "Public Key Infrastructure" covers the specifications for public keys only, leaving the specs for private keys "as an exercise for the reader." It's like providing a car whose engine compartment contains only a notice saying "find a suitable engine and install it here."

Reason two: PKI terminology can be bizarre!

True – the terminology has been carelessly used and badly fuddled. Of all the gobbledygook in information technology, the mangling of the term CERTIFICATE has been among the worst! "Knowledgeable PKI experts will say things like "sign the document with your certificate" – while knowing that the signature is made by the private key, not the certificate! As a result, people who might be interested in putting PKI to work have become confused and discouraged.

Reason three: The conventional wisdom is that PKI is brilliant but too complex for practical deployment.

Translation: PKI is more about non-technology than about technology. Its principal “moving part” is a human being. That makes it “complex” to technologists.

Complex things are all around us, having been made to fit with real life, with the complexity buried behind friendly interfaces. We are surrounded by technologies whose design incorporates their human user. PKI has avoided that.

Reason four: Reliable identities of users – necessary for effective PKI – have been scarce. The high quality technology behind x.509 identity certificates implies high reliability of identity claims. But the rigorous enrollment procedures that will provide measurably reliable confidence in identity claims have been missing.

Reason five: Attempts at reliable PKI identity have not adequately protected users’ privacy. As Reason Ten will illustrate, “Silibandia,” i.e. Silicon Valley plus the broadband and media industries, view genuine individual privacy as a threat to their business model, which relies on the ability to track detail’s of an individual’s life, including their relationships and beliefs.

Reason six: PKI has *conveyed* authenticity without requiring a legitimate *source* of authenticity. When the term “certification authority” was coined, it was defined as “any entity that is able to operate a CA server.” The consequence of that was illustrated when StartCom, a commercial certification authority that was noted for its diligence in verifying the claims of its certification subjects, as sold to WoSign, whose purpose was to issue fraudulent certificates.

The phrase “commercial certification authority” makes as much sense as “commercial vital records department” or “commercial city hall.” A CA cannot be something that can be bought and sold, and certificates cannot be a commodity that’s sold like Cabbage Patch Doll “birth certificates.” A CA must represent DCPA: Duly Constituted Public Authority.

Reason seven: PKI deployments have tried to replace signatures of people with signatures of objects. That doesn’t work. PKI must be built upon identity certificates of human beings, not digital objects. The notion of an accountable object is folly. To serve that intent, the object’s claim must be digitally signed using the private key of an identity certificate. The object’s certificate is just an extension of its responsible party’s certificate, ie the real certificate.

Reason eight: The role of encryption in PKI is confusing.

People who are not involved with asymmetric cryptography tend to think of PKI as an encryption/decryption tool, as it does involve encryption and decryption. But its purpose is to establish authenticity by way of accountability, binding an identifiable human being to their actions.

To further confuse things, the asymmetric key pair is often used to control access to and use of a symmetric key, which is what is really used in the encryption and decryption of useful-sized files.

This is just one of those places where something that is inherently confusing needs to be explained as well and as frequently as possible. Changing the word used to identify the asymmetric pair from “keys” to “numbers” will help. Leave the word “key” to symmetric processes.

Reason nine: Most security technologies are built on an old, fundamentally flawed assumption from the 1960s and 1970s. The flawed assumption is that it is possible to determine the intention and character of the sender of a stream of bits by thoroughly examining it. Until very recently, this “catch the bad guys” mentality has drawn attention away from the real solution, which is about accountability, and which in turn is established by means of true digital signatures everywhere.

“Zero Trust” is a half step toward security built on accountability rather than a cops-and-robbers game.

To illustrate the complete move to accountability we have found success with an office building receptionist metaphor, asking an audience whether they would direct their building's lobby receptionist to identify visitors with bad intentions rather than asking for identity documents in order to establish a measure of accountability.

Reason ten: PKI, when done right, works TOO well!

Companies have become very comfortable and happy with their easy access to personal information. PKI identity certificates may be used by the subjects of the information to control its use. That’s poses a threat to the revenue models of companies that treat stolen personally identifiable information as their own money-making balance sheet asset.

Reason eleven: The assumption has been that PKI’s inherent complexity calls for it to be implemented within one organization, running that organization’s certification authority for internal use only.

In fact, a public PKI with a CA that represents duly constituted public authority *reduces* the complexity of deployment and administration.

To illustrate, imagine a company that chooses to base its employee IDs on company-generated birth certificates rather than birth certificates issued by the vital records department of a public authority. Terminating employees would need their birth certificates revoked, and new employees would need to go through a costly and bureaucratic process for gathering EOI, or Evidence of Identity.

Reason twelve: When PKI was first conceived, the required computing power to handle even 512 bit key pairs would strain the capabilities of the processors of the day. Now of course each of us has a supercomputer in our pocket, which doesn’t even work up a sweat doing2048 bit asymmetric cryptography.

***

To sum up, the impediments to common adoption of PKI may be categorized as implementation flaws, perception barriers, and establishment pushback.

For the implementation flaws, we can migrate to PKI *done right*.

For problems of perception, there is video-based education and outreach.

For establishment pushback, we’re taking the lead in a paradigm shift to a new era of real security, real security, and real privacy.