PKI Done Right

*Companion follow-on to **What Is PKI?***

Video Script

7½ minutes

Video is here:

https://www.taivideos.com/PKI-Done-Right.html

So that's PKI. Pretty remarkable stuff, right? PKI makes a perfect construction material for secure online facilities.

In fact, you use bits and pieces of PKI all the time. Websites that start with httpS:// use bits and pieces of PKI. Blockchain uses bits and pieces of PKI.

But for the same reason that a pile of construction materials is not a building, bits and pieces of PKI do not make a usable PKI facility. A pile of the world's best bank vault construction materials is not a bank vault, right? Overlooking that fact is why PKI has failed to live up to its potential. We're fixing that.

PKIDR stands for PKI Done Right. In order for PKI to be useful it must answer some questions.

For starters, we talk about solving puzzles using this secret large number in your phone to prove that you are who you claim to be, right? The technology is sound. But who established that it's really you with that pair of numbers? Here's Richard Parry, whose Authenticity enterprise serves banks. This excerpt is from his video "Synthetic Identities."

[Excerpt from "Synthetic Identities"]

As you can see, enrollment is important. Anyone who's relying upon your assertion of identity using those two large numbers should know at a glance just how reliable your claim of identity is. How were you enrolled, and by whom? Is this claimed identity backed in some way to real assets of yours? Who else says that this is really you? Your identity should be accompanied by an identity quality score, a number between zero and seventy two, that tells any relying party just how reliable it is so they can make their own determination whether it's sufficiently reliable for their purposes.

But then if you create this measurably reliable credential, you're making yourself eminently trackable. Some would say we've already lost that battle, that Silicon Valley's business model is all about knowing everything about us, and selling that information. Well, let's not settle for that.

Consider your car's license plate. It makes you accountable for what happens on public roadways, but no one gets to know your identity unless there's been an incident. In the same way, your PKIDR credential lets you *assert* your identity without *disclosing* your identity.

You can have multiple personas – think of them as usernames – all tied to one foundational digital certificate. No one gets to know that two of those personas identify the same person unless you allow them to know it, or they get a court order compelling the disclosure.

And who exactly does the disclosing? If there's a central database of identities, isn't it vulnerable to snoops and government spy agencies and hackers? The answer is *no*, the database is not vulnerable. Here's how we can make that claim.

Let's go back to enrollment. In the PKIDR system, enrollment is the responsibility of accountable human beings, specially trained notaries called ***Attestation Officers*** who are legally bound by their commissioning jurisdictions. Even the least costly self-service enrollments produce a record that's under the control of an Attestation Officer. The only record in the central database is what's called a hash number of the person enrolled, and an identifier of the Attestation Officer who is responsible for that record. This is the heart of our patent pending *Internet of People* protocol. If someone demands at gunpoint the name of an enrolled person, all we know is the identity of the Attestation Officer responsible for that particular record.

PKI is an incredible set of construction materials. But construction materials by themselves don't make a building – or a bank vault. Putting PKI construction materials to use properly delivers PKI Done Right, also known as Authenticity. In a nutshell,

Authenticity is ***pervasive accountability with privacy***.
Expanding that a little,

> AUTHENTICITY™ – or PKI Done Right –
> is the condition that exists when we have …
> digital signatures everywhere,
> backed by measurably reliable identity certificates,
> that are owned by their users,
> *– NOT by Facebook, Google, Twitter, or other data harvesters –*
> and which provide ***privacy*** via ***accountable anonymity***.

If anyone tries to tell you that you can't have both security AND privacy, point them to PKIDR.

Linking documents, transactions, and processes to ***accountable human beings*** – using digital signatures of ***measurably reliable identities*** – calls upon time-tested paradigms from the physical world. The crime-friendly, ***unaccountable*** Internet then becomes the ***accountable*** Internet of People.

The solution to the crippling flaws in our digital world has been hiding in plain sight.

PKI Done Right ***works***, where security technology ***has failed us***.