“Encryption” de-confusion (mini video)

Script

Let’s clear up some confusion around the term “encryption” as it relates to Authenticity.

In the Authenticity infrastructure there are two very different types of encryption. One is of direct interest to users; the other occurs behind the scenes in the PKI “back room,” so we’ll set that one aside for now.

The type of encryption of interest to users is the familiar process by which a piece of data is scrambled to protect it from unauthorized users, then later unscrambled by an authorized user.

The mathematical “key” that scrambles the data is the same key that unscrambles it. Because the same key encrypts AND decrypts, this is called “symmetric encryption.” As you might expect, making sure the key doesn’t fall into the wrong hands is a critical security issue. In fact, one of the three essential processes performed by PKI is ensuring that your description key is delivered ONLY to the intended person. In Authenticity discussions, when you hear “key management” or “decryption control”, THIS is the key we’re talking about – making sure it’s received by the right person. PKI can do just that.

As for the other type of encryption used behind the scenes – the only reason to say anything about that is because you may have heard something about it. But it’s important to understand that this backroom type of encryption is an internal tool used in Authenticity – it’s NOT a user-facing feature of Authenticity, and it’s NOT necessary to know anything more about it than this:

In our documentation about PKI, we describe this type of encryption in terms of making and solving digital puzzles. The encryption key (making) and decryption key (solving) are different – we call them the PEN and the PCN. In classic PKI terminology, they are called the private key and the public key – and because they are different, this is called “asymmetric encryption” It’s the brilliant mathematical invention from half a century ago that is just now coming into play as the solution to our online security mess. It’s happening all the time, every time a digital identity is used in a process.

[Last scene retreats behind the “back room” door.]

So, to summarize – THIS is what we ordinarily mean when we talk about encryption: Encrypting user data for security, and making sure ONLY the right person gets the key to decrypt it.