The Insecurity of Charging for Authentication And How It Relates To "Decentralized Identifiers" (DIDs)

ID2020 Designshop

Greg Slepak May 22, 2016

The false assumption that digital security is or should be expensive

A frequently voiced thought during ID2020 was the notion that the process of verifying data associated with "DIDs", or "Decentralized Identifiers"[1], had a meaningful cost, and that this cost was somehow proportionally related to the authenticity of that data.

This is a totally incorrect misconception.

It is on the basis of this misconception that Certificate Authorities were able to maintain and expand their business of selling people insecurity at high cost, sometimes charging upwards of $300 or more per year in order to get websites to display a shiny lock icon.

Today, thanks to projects like Let's Encrypt, many people know that they can get this same lock in their web browser for $0.

Did anything fundamentally change during the years that we did not have Let's Encrypt? Did Let's Encrypt invent anything fundamentally new that did not exist before? The answer to these questions is a resounding **NO.**

The only thing that Let's Encrypt managed to accomplish was a change in the politics of Internet security.

There is literally *no need* for **Certificate Authorities** when it comes to securing Internet connections. The *only* valuable thing these companies can do is act as an entity that verifies and attests to the existence of paperwork that somebody provided to them (a Driver's license, a business license, etc.).

[1] A DID is a "worthless" identifier (long "random"), valuable precisely for the reason that it can be used to represent an identity over its entire lifetime without attracting contention over its ownership.

In fact, **Certificate Authorities are the source and primary cause of the Internet's insecurity.**

TOFU, or "Trust-On-First-Use", the principle behind the "super secure software" known as Signal, is incredibly cheap (literally $0), and incredibly secure. This principle of authenticating a connection provides vastly superior security to the one that's provided by CAs, and is already implemented in browsers via the HPKP standard.

There is zero need for CAs.

Similarly, there is zero need for the "Verifier" or "Inspector" aspect of the DID architecture as a separate entity.

The function that this component performs, the "verification" of the data that's associated with a DID, can and should be performed by the user's own device, i.e. a cellphone, at zero effective cost through the use of thin client technology. Outsourcing this task to anyone else is to compromise the security of the system by introducing a totally unnecessary trusted third-party.

Furthermore, just like with CAs and Let's Encrypt, **if the implementation of this component involves any cost,** then it suggests that people are being ripped off by some dishonest company for no reason.

The architecture for DIDs already exists

DIDs already exist. On Ethereum they are the address of a smart contract.

The management of keys, revocation, and recovery of a DID is fairly trivial to program on Ethereum, perhaps only a few dozen lines of code.

The "verification" or "inspection" of a DID is done by every Ethereum node, and in the future will be done by cellphones using thin clients for approximately $0.

Anyone selling you an expensive identity architecture is probably ripping you off and compromising your security

Just like CAs compromise the security of HTTPS, anyone offering to sell you a DID architecture is not only ripping you off, but they are most likely compromising your security as well as the security of everyone that uses their system.

These architectures charge $ to act as a central authority for managing other people's identities. They are in a business they shouldn't be, and the fact that they act as a central authority that manages identities turns them into a single point of failure that can be taken advantage of, hacked, or coerced into compromising your and everyone else's identity.