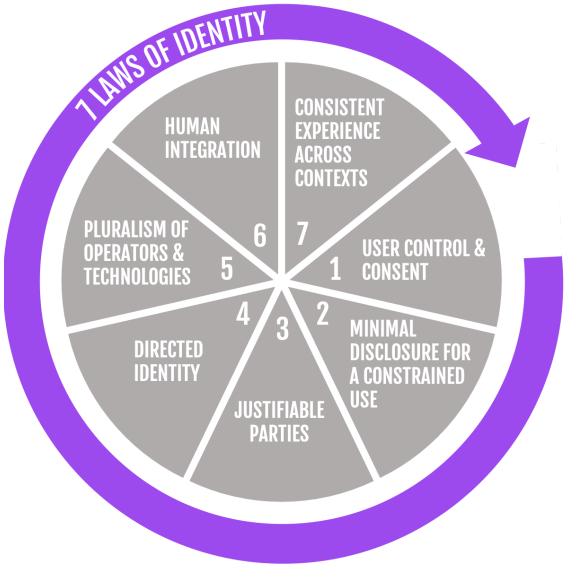
Convergence.Tech

Digital Credentials and the Laws of Identity

By Kim Cameron, Chief Identity Officer, Convergence.Tech

As I wrote in The Laws of Identity (2005), "the Internet was built without a way to know who and what you are connecting to". This resulted in "a patchwork quilt of identity one-offs". There has been considerable progress since then, but digital identity remains a problem in dire need of a better solution.



Today none of us has our own "digital identity". Instead, we end up with a jumble of so-called "identities" (mostly usernames and passwords) different for each website we visit, and identifiers controlled by our employers, our governments, and Internet giants like Google and Facebook. In other words, the patchwork quilt of identity one-offs, each usable only within its own realm, remains the norm.

Yet there is exciting news. *A new technology that provides a better solution has been approved as a world standard by the W3C – the main international standards organization for the World Wide Web.*

The technology, called "Verifiable Credentials", is one of the most important to arise since the birth of the Internet. It is driven by new needs arising from economic and social changes on many fronts. People are increasingly mobile. Workplaces are becoming dependent on 'gig' workers hired on short term contracts so companies can adapt quickly to ever-changing circumstances. The rapid changes people experience in location and employment force them into new contexts – where others do not know them or what they have achieved. This means even physical interactions have come to take on more characteristics of digital ones, where we are "without a way to know who we are connecting to". Both the workplace and the marketplace have changed – becoming increasingly 'virtual'.

All of this has created the need for a reliable (verifiable) way to communicate who we are and what we have done. Verifiable Credentials answer this need by providing proofs about our identity, entitlements, capabilities, and qualifications. As companies and governments take advantage of verifiable credentials to simplify their service offerings, each of us will be drawn into their use. And when we do, we will find ourselves in a world where we *"actually know who we are connecting to".*

Any technology can create problems at the same time it solves them. Because Verifiable Credentials will have such a strong impact, we need to be extraordinarily vigilant that they are not used in ways that break the Laws of Identity. Specifically:

1. *Control and Consent*: First and foremost, people must be in **full control** of the Verifiable Credentials that describe them, determining when credentials are shared, with whom, and why.
2. *Minimal Disclosure for a Constrained Use*: People must only be asked to present a credential for a specific purpose, and the credential should only reveal information necessary for that purpose.
3. *Justifiable Parties:* When a credential is presented, only the requestor and the user should know about it.
4. *Directed Identity:* The technical identifiers and keys of a credential presented in one context *must not correlate* with those used in any other.
5. *Pluralism of Operators and Technologies:* A minimal Verifiable Credential provided by any provider should be able to be stored in any standardized wallet produced by any entity. Yet some credentials and wallets may offer additional capabilities appropriate for specific use cases.
6. *Human Integration:* Providers must ensure that people using wallets understand *why* a credential is being requested and *what* it reveals so they can decide whether to release it for a given purpose.
7. *Consistent experience across contexts:* Technology providers and operators should attempt to create an ecosystem where the actual experience of obtaining, storing, recognizing, viewing, approving and presenting credentials is similar enough across providers and contexts that people will immediately understand what is going on. An analogy with automobiles may help: interiors and layouts of controls are different, yet drivers can easily recognize how to drive one car rather than another.

We are early in the process of deploying Verifiable Credentials on a world scale. **Convergence.Tech** is committed to working with organizations using the technology to deeply understand the many cases where it solves problems. Together we will produce white papers that explore the benefits and challenges of verifiable credentials in real-world situations. We will draw conclusions about best practices and find ways to fine tune the technology. And we will evaluate the compliance of different solutions with the Laws of Identity.

Please join us in this endeavor. Let's work together to finally solve the problem of digital identity.
