**January 20, 2015**

**Anonymous Credentials:**

**A Report from the Internet2 NSTIC Pilot work in Scalable Privacy**

**Context:** The Internet2 Scalable Privacy Initiative, funded in the original NSTIC pilot round, is an attempt to distill and adapt the leading edge efforts in identity within the R&E community to a broader citizen centric context. The particular focus of the work has been privacy at scale. With complex online interactions, numerous interactions per user per day, and the user’s desire to “just have it do the right thing about privacy,” rolling out effective, resilient, scalable, and cost-­‐effective privacy infrastructure will be difficult. Privacy needs to scale with the growing number of users, scale with the number of services users need to manage, and types of applications in which privacy must be managed.  Moreover, there is a growing diversity of users and personal attitudes towards privacy that should be accommodated. These challenges have lead us to focus on foundational elements that are essential to scale and currently missing from the Identity Ecosystem. The Scalable Privacy work, led by Internet2 staff, draws heavily on the expertise of the Internet2 community in identity management, privacy and federation and examines a set of missing components that the identity ecosystem needs for deployment at scale. Many those involved in the work have had long and productive engagements with federal identity work over several decades. Deliverables have included critical software (MFA management for the leading open source federation software, certificate management tools, etc.), business and deployment plans, identification of key schema for inclusion in citizen-centric uses, evaluation of anonymous credential deployment at scale, and end-user consent management tools.

**Background:**

The NSTIC Scalable Privacy activity at Internet2 committed to an investigation of anonymous credentials. Anonymous credentials represent a small set of small intellectual properties, currently implemented in proprietary code, that provide unique capabilities identified in the NSTIC guiding principles – unobservability and the ability to provide assertions without revealing PII.[[1]](#footnote-1) Unobservability refers to the capability of a credential being used without the issuing authority knowing of its use. Providing assertions without revealing PII is exemplified by the ability of anonymous credentials to respond to assertions (e.g., “user is over 21”) without revealing the actual age. While the anonymous credential technology goes back over ten years to a Ph. D. thesis by Stefan Brands at Eindhoven University and work done under the leadership of Ron Rivest of MIT[[2]](#footnote-2), a number of factors have hindered the widespread deployment. This analysis highlights those factors and our efforts to address them.

The original intent of this activity was to deploy some basic anonymous credential capability and integrate it into an enterprise-oriented architecture. That ambitious goal was quickly tempered by challenges in the relationships with Microsoft, the owners of the uProve version of the capability, and the rudimentary state of the Idemix software we received from IBM. As a result, the pilot readjusted its goals to focus on identifying the barriers we faced.

**Terminology:**

Both the phrases “zero knowledge” and “anonymous credentials” have become blurred in the marketplace. [[3]](#footnote-3) There are now several companies that use the phrases, or variants, in corporate names and or tag lines.[[4]](#footnote-4) It is often difficult to discern the technologies under these corporate hoods and what compromises on classic unobservability they may have made. The particular software systems we worked with – from IBM and MS – have IPR lineage directly to the original uses of the words and provide some measure of unobservability.

**Methodology:**

The project leads for anonymous credentials, Ken Klingenstein and Steven Carmody, have a combined forty years of experience in PKI efforts within the leading edge R&E community. The project engaged with Anna Lysyanskaya[[5]](#footnote-5) of the Brown University Computer Science Department on the state of the art in anonymous credentials. That led to conversations with the two principal owners of the intellectual property Microsoft and IBM. (The IBM work involved the Alexandra Institutet, A/S of Denmark.) The conversations with Microsoft found common interest around the PrivacyLens UX we have been developing as part of the NSTIC grant, but never gained traction as responsibilities for the technology within Microsoft shifted

With IBM the engagement has been sustained, and productive to some degree. The IBM code base has been provided, generally in alpha state of a new version. New versions are delivered on an irregular schedule, and associated libraries follow later. We have been able to install a working system recently, to generate credentials that can respond to queries. The current version could best be described as an early prototype.

* It can only be used from the command line; you run a script that does a series of about a dozen queries to various services, and eventually types out a “yes” or “no”.
* There are no tools for creating or managing credentials. It currently cannot be used with a web browser (a requirement for most users).
* It is unfortunately far from a widely deployable product able to support a variety of needs, with facile credential creation, etc.

In addition, we’ve engaged in conversations with the principal European Commission effort – ABC4 trust. ([www.abc4trust.eu](http://www.abc4trust.eu)) They are in the process of a yearlong study about what are the barriers to anonymous credential deployment. They have reviewed this paper and will include it in their analysis.

**Findings:**

*1. Having an open source implementation of anonymous credentials would be of value.*

Whether that is through a renewed effort to change how current approaches are licensed or creation of a new code base, a large segment of the potential early adopters, such as R&E, require open source. It is unclear whether creation of a new code base would face legal issues. It is worthwhile to explore this further, and if feasible, promote some effort in developing such an open source.

A corollary of this is to encourage web browsers to use the open source to develop, and bundle in, plug-ins to process anonymous credentials. Without the modules, mass adoption is unlikely.

*2. Characteristics of, and requirements for, unobservability should be reconsidered.*

New requirements for credentials may present challenges in preserving unobservability. These considerations include mobility, a variety of devices and operating systems, informed consent, accessibility, etc. To the degree that these capabilities would involve third-party sources of information, name translation, etc. would possibly produce observable behaviors.

Revocation remains a difficult issue for any static credential. That said, there are use cases for which revocation is so unlikely as to be unimportant, and simple periodic renewal of the credential is sufficient. [[6]](#footnote-6)

When unobservability is required, the lack of anonymous credentials has led to workarounds that are problematic. Double blind portals and gateways are difficult to do right[[7]](#footnote-7) and are one-offs due to a lack of a marketplace as well.

*3. Hybrid architectures are likely the best approach to real world deployability*

It is likely that a deployable environment will need to use a hybrid architecture where some of the unobservability needs are met with a legal and policy approach rather than pure technology. This will be true with cloud-based approaches for mobility, for example, where the use of a credential may be observable to the cloud provider holding it.

4. *An enterprise-centric implementation would address gaps*.

The enterprise would hold credentials for users rather than at the desktop. This would enable a host of capabilities, from mobility to support of informed consent, but at some cost of unobservability, which might need to be managed via policy rather than pure technology. Our goal was to implement this hybrid approach, but we did not get there. The code only provides very early stage functionality, and could never be given to an actual end user. And, for it to work at all and provide unobservability, a user would have to run a set of services within their desktop machine. That would have to be installed by whoever provided the desktop operating system.

1. Work funded by Department of Commerce NIST Cooperative Agreement 70ANB12D300 (CFDA 11.609)

 See NSTIC [↑](#footnote-ref-1)
2. http://people.csail.mit.edu/rivest/ [↑](#footnote-ref-2)
3. Interestingly, neither of the extensive discussions of the two terms in Wikipedia cites the other – see <http://en.wikipedia.org/wiki/Privacy-enhancing_technologies> and <http://en.wikipedia.org/wiki/Zero-knowledge_proof> [↑](#footnote-ref-3)
4. See, for example, <https://spideroak.com/zero-knowledge/> for a cloud based password store, and <http://emergentchaos.com/archives/2007/06/whatever-happened-to-zero-knowledge-systems.html> for the use of zero knowledge to describe a TOR-like service. [↑](#footnote-ref-4)
5. http://cs.brown.edu/~anna/ [↑](#footnote-ref-5)
6. Examples include an institution issuing an electronic diploma and [↑](#footnote-ref-6)
7. Among the challenges that a gateway presents are the security of the gateway itself, securing portal applications from each other, and effecting attribute release to per application. [↑](#footnote-ref-7)