Final Report of The CACTI Next-Generation Credentials Working Group

Repository ID: TI.nnn.mm
DOI: TBD
Persistent URL: http://doi.org/TBD
Status: Community Consultation Draft

Authors: Kevin Hickey, University of Detroit, Mercy
Nicole Roy, Internet2

Co-Chairs: Kevin Hickey, University of Detroit, Mercy
Dan Taube, Illinois State University

Publication Date: TBD
Sponsor: Community Architecture Committee for Trust and Identity (CACTI)

Working Group Members:

Chris Phillips	CANARIE
Chris Stucker	Thomas Jefferson University
Christopher Knerr	Baypath University
Dan Taube	Illinois State University
Dmitri Zagidulin	MIT
Drew Capener	Omnibond
Eisaku Sakane	NII
Etan Weintraub	Johns Hopkins University
Gareth Wood	University of Otago
Ian Wat	Bucknell University
James Chartrand	MIT
Jeremy Perkins	Instructure
John Bradley	Yubico
Judith Bush	OCLC
Kerri Lemoie	MIT
Kevin Hickey	University of Detroit-Mercy
Kevin Mackie	Oregon Health and Science University
Kiersten Grover	Baypath University
Margaret Cullen	Painless Security
Mark Jones	UT Health Houston
Naohiro Fujie	OpenID Japan
Nathan Dors	Independent
Nicole Roy	Internet2
Niels Van Dijk	SURF
Rob Carter	Duke University
Samuel Bernardo	LIP
Shigeya Suzuki	WIDE
Stoney Gan	University of South Florida
Waldo Fouche	Australian Access Federation

Table of Contents

Executive Summary

In April, 2023, the Internet2 Community Architecture for Trust and Identity (CACTI[1]), the architectural governance group of Internet2's Trust and Identity Services division, chartered an open working group[2], seeking out global participation from the research and education (R&E) identity and access management (IAM) community, to explore drivers for possible adoption of new technologies in support of the R&E mission.

From the charter[3]:

"The landscape of electronic identity is shifting away from the strongly-centralized model which is used in traditional federated web single-sign-on infrastructures, to one which empowers users (credential holders) to choose what identity they assert, at what time, with what relying party/verifier, and what types of information they disclose. The latter type of user-centric identity ecosystem is known variously as "self-sovereign identity", "verifiable credentials", "wallet-based credentials", etc."

"In order to understand if, why, and how the research and education identity and access management ecosystem needs to grow and adapt to this new environment and set of expectations, we need to understand the use cases and drivers for adoption of these technologies, from the perspective of our diverse user communities: Learners, teachers, researchers, administrators, alumni, etc. It is not possible for CACTI members, in isolation, to

[1] http://doi.org/10.26869/TI.4.1
[2] https://spaces.at.internet2.edu/display/ngcwg/CACTI+Next-Generation+Credential+Use+Cases+Working+Group
[3] https://spaces.at.internet2.edu/display/ngcwg/NGCWG+Charter

derive meaningful or all-encompassing use-cases without the strong participation of a larger community of practitioners and users."

The working group had a relatively short timeframe in which to define for itself the meaning of "next-generation credentials" and then create a call to collect use cases from the InCommon and REFEDS[4] communities. There were 8 total meetings of the group before its deadline to present at the Internet2 Tech Exchange meeting in September, 2023. The first meetings were spent defining terms and building understanding. A number of participants provided input into this process. Working group members collected and documented 31 use cases, and analyzed the first eight use cases in-depth before the deadline. A subset of these were chosen for recommendation for further work, although a follow-on working group should further interpret and refine use cases (with possible additions from a new survey of the community) before using them to define an architecture for future proof(s)-of-concept to meet community needs.

Narrative

The landscape of electronic identity is shifting away from the strongly centralized model which is used in traditional federated web single-sign-on infrastructures, to one which empowers users to choose what identity they assert, with whom they choose to assert it, and what types of information they disclose in a transaction. Efforts at limiting the severe privacy violations which have affected users on the world-wide web over the last 30+ years[5] also necessitate a move away from core web primitives which will become increasingly risky to depend on (as the current InCommon and eduGAIN federation systems do). The Next-Generation Credentials Working Group was chartered to collect a broad range of prospective use cases and drivers for adoption of next-generation credentials from the perspective of as many stakeholders as possible, analyze them for affinity and return on investment (ROI) with the goal of recommending high ROI use cases for proofs of concept (POC).

The working group consisted of 24 individuals from various institutions and organizations and met 8 times beginning June 15, 2023. The group was cognizant of the fact that there are competing theories of design and implementation of next-generation credentials. These technologies are known by several names such as "self-sovereign identity", "verifiable

[4] https://refeds.org/
[5] https://privacysandbox.com/open-web/

credentials", "wallet-based credentials", etc. The group also did not want to reproduce the work of others working in this area. The working group chose to focus on what our community could do.

To develop appropriate use cases, it was necessary for the group to agree upon a common understanding of what would constitute a next generation credential. The group adopted the following working definition of a next-generation credential. It aligns broadly with W3C Verifiable Credentials:

> *A next-generation credential is a machine-verifiable method of conveying information about an entity (a natural person, system, organization, etc.), either self-asserted by that entity, or attested about that entity from an issuer to a verifier by means of a wallet controlled by a holder. It must be secure, privacy enhancing, interoperable, provide a user experience which informs and empowers the user to make meaningful decisions about the release of information under their control, and be revocable.*

Less formally stated, it is a bundle of attributes about a subject such as birth certificate, driver's licenses, or academic credential which can be presented by the owner when required. The critical difference in a next-generation credential ecosystem is that the service provider no longer receives credentials from the issuer but from the user directly. Even though the adopted working definition does not preclude the use of next-generation credentials for authentication, the consensus of the group was that these use cases were not the most interesting or appropriate for the group to consider.

The group recognized that for next-generation credentials to reach their full potential the goals, design, and operation of a next-generation credential ecosystem must be transparent, with four key characteristics considered: interoperability, the trust model, revocability, and user experience.

First, next-generation credentials must be interoperable. Industry tends towards building non-interoperable ecosystems. CACTI should consider participating in existing efforts to standardize in this space as well as pushing for more standardization where it is lacking. Much work is needed in the areas of deployment and testing of models supported by new standards

such as OpenID Federation[6], OpenID4VCI[7] and OpenID4VP[8]. The InCommon community should consider demonstrations or pilots of credentialing systems, wallets, verifiers, issuers and a trust fabric, selecting high-value use cases which demonstrate the value of these new systems in light of the complexity and cost of deployment of the existing credential technologies for many deployers. The community must then be prepared to actively pursue needed extensions or modifications of existing protocols which will support the needs highlighted but as yet unmet. This work must be pursued with an emphasis on international and cross-sector collaboration and compatibility of deployment.

Interoperability with commercial offerings is paramount, but major players like Google, Apple and others have active disincentives to preserve privacy or allow easy portability or interoperability with other ecosystems. Anyone who has ever been ensconced in the “walled garden” of Apple or Google wallets (Apple Pay, Google Wallet, respectively) knows how frustrating this can be when trying to move from one mobile ecosystem to another. Thus, it is important for the InCommon community to work with active global efforts in open wallet standardization, such as the European Commission-funded large-scale wallet pilots for e-citizenship, scholarship and other requirements. An example of this work is the “wwwallet”[9]

Second, next-generation credentials will likely require the adoption of a new trust model, and certainly a new trust infrastructure or infrastructures. Within the current trust model, the end-user may or may not have the ability to consent to disclosure of sensitive information by an identity provider. The current model tries to make this safer, to some extent, with use of SAML entity categories like the REFEDS Research and Scholarship (R&S)[10] category. These categories are monolithic, brittle, and not able to be easily disclosed to users in the context of an authentication/authorization (login) transaction. In this classic model, an identity provider can control what is going to the relying party, including sensitive data, because it is in control of the data. In the next-generation cases, the holder controls the release of information. If the ecosystem is built with privacy as a requirement, especially through means of aggregating actions like revocation checks via systems like low-latency accumulator schemes[11], then the

[6] https://openid.net/specs/openid-federation-1_0.html
[7] https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html
[8] https://openid.net/specs/openid-4-verifiable-presentations-1_0.html
[9] https://wwwallet.org/
[10] https://doi.org/10.5281/zenodo.6832218
[11] https://eprint.iacr.org/2022/1362

issuer will have no visibility into the release of information by a user/holder to a verifier, or the revocation checks that happen at a verifier.

The current deployment model for large-scale SAML-based single sign-on federation is quite brittle and monolithic. Fragile aggregates and non-agile cryptographic processes based upon XML threaten to undermine the long-term viability of the existing ecosystem as deployed. The next-gen model helps alleviate this by enforcing agility and interoperability via standards, building upon lessons learned from decades of experience with SAML and OAuth. Because a heretofore non-existent component plays perhaps the most important role in terms of supporting and enforcing privacy, interoperability (standards/cryptographic primitives) and end-user experience, this component, the wallet, is the core of and perhaps the most substantial piece of work to be done via pilots, standardization, lessons-learned and refinement of work that has gone before.

Third, next-generation credentials must be revocable. Credentials may have a defined lifespan upon issuance or expire upon future conditions agreed upon by both issuer and holder. Revocation is also required in cases where events necessitate reissuance of credentials, and where individual data elements have been invalidated and need to be re-issued. Active, near-real-time revocation and reissuance of an entire credential or data elements within the credential must be supported by issuers, verifiers, and most importantly, wallets. The issue of an offline wallet and/or verifier due to geographic isolation of the user (use of a credential in a wallet to buy supplies at a remote field station with no available Internet access, for example) is an edge-case which may prove challenging. The Pareto principle[12] must be considered when deciding how to optimize our investment of community time and other resources in the pursuit of solutions.

The group's discussions on both trust models and credential revocation identified the need for trust registries. It should be noted that these registries, in some ways, are similar to the trust framework that the InCommon Federation currently operates. This existing trust framework may present an opportunity to utilize lessons already learned as input into a potential future trust model. That said, it is quite likely that support for a new trust registry ecosystem to support these technologies will be greenfield, and must therefore be carefully planned and implemented.

[12] https://en.wikipedia.org/wiki/Pareto_principle

This aspect of ecosystem realization will likely be no less daunting than that of creation of a truly interoperable, secure, and user-friendly wallet or wallets.

Finally, next-generation credentials place a responsibility on users to verify and trust both issuers and verifiers. The user experience must allow for users to easily understand what they are being asked to disclose and by whom, for what purpose, with what scope and constraints, and then flexibly reacting to a user's bona fide and informed decisions to accommodate the user's preferences and decisions. The minimum necessary disclosure required to complete a transaction must be clearly conveyed to the user while also allowing the release of additional attributes if they choose. Support for this type of user experience is incumbent upon all actors in the ecosystem (issuer, verifier, wallet and trust registry) but is perhaps most centrally located and directly presented to the user within the wallet itself.

Pilots should focus on issues which are somewhat unique in the research and education sector: Students, faculty and staff often have very large numbers of groups and roles which need to be used for inter-institutional and intra-institutional authorization. These group memberships rely heavily on real-time revocation for security purposes, and the sheer number of groups often presents challenges to authorization at-scale, aka the "Kerberos PAC field problem"[13]. Another unique need in this sector is support for customized schemas such as eduPerson, voPerson, and SCHAC[14]. The community should investigate how these schemas may be adapted and used within existing open standards in the verifiable credentials space.

The working group collected 31 use cases. One of the more salient dimensions along which use cases differed was the role that R&E institutions would play in each case. In many cases, the institution is an issuer of a credential like a diploma or student identification. In other cases, the institution is a verifier of a credential, perhaps from another academic institution. And, in a few cases, the institution itself would hold credentials. The first two of these categories, the institution as issuer and verifier, seemed to be the most immediately addressable. So, the group attempted to select use cases that best represent those categories.

The working group agreed upon the following three use cases for consideration:

---

[13] https://learn.microsoft.com/en-us/troubleshoot/windows-server/windows-security/kerberos-authentication-problems-if-user-belongs-to-groups

[14] https://refeds.org/specifications

1. A student presents a verifiable credential to a service provider to obtain a service discount only provided to current students without revealing anything more than their current academic status.
2. A university needs to verify a prospective student's high school diploma and/or transcript.
3. An employer needs to verify a prospective employee's college diploma and/or transcript.

Use case one was considered a compelling use case for next-generation credentials. It is simple to understand and clearly exhibits the privacy enhancing potential of next-generation credentials. First, the user need only present their current academic status to the provider while hiding all other information. Second, the issuer of the credential, likely the institution, is unaware the user activated the service discount.

Use cases two and three are similar, but in each case the institution assumes a different role within the ecosystem. In case two, the institution acts as the verifier while in case three it acts as the issuer of an academic record credential. In both cases, interoperability and trust outside of traditional boundaries is a foundational requirement.

Use case three also highlights a security benefit derived from the nature of a next-generation credential. Once an institution has issued a credential, the holder can present the credential directly. There is no intermediary holding the diploma or transcript, thereby adding another potential source of breach. For institutions, the potential reduction in risk due to a smaller attack surface and a more limited breach radius should be compelling.

The working group agreed that use case one best represents the promise and benefits of a next-generation credential ecosystem while remaining simple to understand. The assertion of a person's academic status is a basic function academic institutions perform and is not limited solely to redeeming discounts. Most users are familiar with the use of existing credentialing technologies to prove their academic status. As an existing process both institutions and users are familiar with, it provides an opportunity for a direct comparison between technologies while highlighting the privacy-enhancing capabilities of a next-generation credential.

More work is clearly needed in a number of areas in order to frame a pilot architecture which could support these first, very simple, use cases. The working group recommends follow-on activities which may span the gamut of InCommon's areas of community governance, necessarily creating new working groups to investigate the large-scale architecture, trust model, standards, operational and deployment requirements, global interoperability, and iterative implementation within software.

Conclusions

CACTI, and the InCommon Technical Advisory Committee (TAC) should undertake a shared working group effort starting in the first quarter of 2024 and targeting an end date of the end of September, 2024, to further refine use case(s) for a proof-of-concept, and use that/these use cases to define a high-level architecture and technical requirements for a proof-of-concept deployment of use of verifiable credential technologies within the InCommon trust environment. Use of existing features, functionality, and business processes should be considered, where possible and in alignment with the needs of the community and its requirements. This working group should be tasked with producing a normative document which describes the high-level architecture, as well as normative documentation on software and systems requirements for the proof(s)-of-concept.

Appendix A: Use Cases

These use cases were gathered from the members of the working group and used to form the basis of the findings in this report.

Use Case	Submitter	Description	Classification
1	Kevin HIckey	A faculty member from an existing InCommon member institution, authenticates to Educause using credential(s) stored in a wallet on their personal smartphone.	Authentication used for Authorization (binding an authentication to an issuer)
2	James Chartrand	A student/faculty/staff member collects a Verifiable Credential from InCommon/eduGain that asserts their status (e.g. full-time student, graduated student, tenured faculty). The VC can then be used	Authorization

		autonomously anywhere the status must be proven (like to get a student discount, or to prove that one has a bachelor's degree when getting a visa, applying for a job or to graduate school).	
3		A current student presents their NGC to a service provider in order to obtain a service discount only provided to current students. The anonymous verifiable credential. I am a current student that is all.	Authorization
3b	Nicole Roy	As a student who wants to use an anonymous credential, I need a "giant bucket of centrally-provided revocation status bits" where the revocation status of my anonymous credential can be published alongside many thousands of other such revocation statuses, such that it becomes statistically impossible for a verifier to trace the revocation back to a specific issuer.	Supplemental
4		A financial aid office is processing a request for financial assistance and needs to verify the government-issued identity of an individual to prevent fraud.	Authentication
5		A researcher presents their NGC to a research lab to be verified as qualified to gain entry and access based on their credentials.	Authentication
6	Mark Jones	A person uses a VC issued by their institution to access Google Workspaces	Authentication
7	Mark Jones	A person proves they are 21 years old to enter a club (in the student union)	Authorization
8	Kevin Mackie	As an existing student I need a password reset so I can log into the SIS	Authentication
9	Kevin Mackie	As an existing student I need re-register for financial aid so I can pay for school	Authorization
10	Kevin Mackie	As a prospective I need establish an application account so I can apply to the school	Authorization
11	Kevin Mackie	As an incoming student I need register for classes so I can take classes	Authorization
12	Kevin Mackie	As a former student I need request a copy of my transcript so I can apply for a job at a non-higher ed organization	Authorization
13	Kevin Mackie	As a current faculty I need prove my identity so I can get guest digital access at another institution	Authorization
14	Kevin Mackie	As a recruited faculty I need to provide my cv and credentials so I can apply for a job	Authorization
15	Drew Capener	A parent needs to establish an account with the institution (Ideally somehow asserting the parent relationship)	Authorization
16	Drew Capener	A student/faculty/staff gets a new device and needs to transfer relevant credentials to the new device	Supplemental
17	Drew Capener	A student/faculty/staff needs to be able to use their digital credentials to assert permission to access physical facilities	Authorization

18	Rob Carter	During a local measles outbreak, the University mandates that students show proof of vaccination before returning to campus from winter break. When I matriculated, the university issued me a vaccine VC. As a vaccinated student, I use the credential to prove my status and authorize my return to campus. Later, when I visit a local rec center, I'm able to use the same VC to prove my vaccine status for access to the off-campus facility.	Authorization
19	Rob Carter	As a researcher in the nuclear lab, I'm required to pass annual training offered by a third party in radioisotope safety. The training corporation issues me a VC which I present to an online system at the university each year to maintain my access to the lab facility.	Authorization
20	Rob Carter	The institution's Registrar is asked to provide the DoE with records demonstrating the university's compliance with federal equal opportunity regulations. She is able to use a VC issued by the institution to prove her identity and her status as University Registrar to authorize her submission of records to the Department.	Authorization
21	Niels van Dijk	As a researcher in the (EU based) Elixir Life Sciences VO, I have obtained a VC stating permission from the Elixir Ethical committee to be allowed to access certain medical datasets. The NIH trusts statements from Elixir's Ethical Committee and allows the researcher access to certain dataset based on the VC	Authorization
22	Niels van Dijk	As a researcher in the LIGO collaboration, I have obtained a VC using LIGO's CIlogon platform that grants me access to a dataset of the VIGO collaboration	Authorization
23	Niels van Dijk	As a student I can ask my faculty professor to make some VC statement about me that allows me to enroll in a certain training or course. The training center can validate the professor’s statement without having to trust email or similar	Authorization
24	Niels van Dijk	As a foreign student wanting to attend an education in the US, I can use my digital credentials to prove my identity and provide proof or earlier diplomas and micro credentials	Authorization
25	Niels van Dijk	As a student I self-studied water engineering 101 using the Delft University MOOC. With the VCs I received from Delft University, I can now provide digital proof of this to my US based institution	Authorization
26	Niels van Dijk	As a researcher, my institution has granted me a VC which allows me to use the state's HPC center for 1000 CPU hours	Authorization
27	Niels van Dijk	As a medical professional working in a research hospital, I can now combine credentials from my research institution with my credentials from the ministry of health into 1 credentials set so I do not need to have multiple accounts	Authorization
28	Kerri Lemoie	As an individual who is affiliated with a university, I have been issued a VC that verifies if I am a student, faculty, and/or staff	Authorization
29	Kerri Lemoie	As a graduated student, I must present proof of my graduation to	Authorization

		visa officers in the country where I hope to work.	
30	Kerri Lemoie	As a student I would like to make self-assessments about my abilities & experiences and request that my professors and peers endorse me.	Authorization
31	Kerri Lemoie	As part of the admissions process, student VCs are evaluated for consideration and data from the VCs contributes to admissions reports.	Authorization