What is CACTI?

Community Architecture Committee for Trust & Identity (CACTI)

- Comprised of community members
- Provides strategic architectural input to Internet2’s trust & identity projects and activities:
- Charters and manages WGs in support of trust & identity goals
- Manages and evolves community standards
- Fosters relationships and participates with other national or international activities to maintain visibility into developments and trends
- Broadly shares information of relevance to the R&E community in the areas of trust, identity and associated middleware
Current CACTI Members – “Cactitians”

Margaret Cullen, Painless Security
Kevin Hickey, University of Detroit Mercy
John Bradley, Independent
Robert Carter, Duke University
Stoney Gan, University of South Florida
Barry Johnson, Clemson University
Marina Krenz, REN-ISAC
Les LeCroix, Carleton College
Kevin Mackie, Oregon Health & Science
Derek Owens, University of Notre Dame
Jeremy Perkins, Instructure
Chris Phillips, CANARIE

Erik Scott, RENCI
Gareth Wood, University of Otago (NZ)

Liaisons:
Richard Frovarp, CTAB
Rob Gorrell, eAC
Steve Premeau, TAC

Internet2 Staff:
Nicole Roy, Flywheel
Steve Zoppi, Advisor
Call for Nominations

Nominations are open for new CACTI members through October 1st!

• Are you a strategic thinker or architect in the trust & identity space who would like to help us shape the future of Internet2’s trust and identity projects and activities?
  – Please volunteer! Many of us “self-nominated”, and you can, too!
• Do you know someone who would do a good job in this role?
  – Please nominate them!
• Time commitment: 2-hour calls every 4 weeks, preparation for calls, participation in sub-groups or WGs, providing feedback on technical specs, etc.

Nomination Link: https://incommon.org/community/leadership/join-incommon-advisory-committees/

Questions? Please talk to me, Kevin Hickey or Nicole Roy.
CACTI Open Meeting // Next-Generation Credentials Use Cases

Status and Next Steps From The Working Group

Drew Capener, Omnibond
NGCWG Charter

- Identify a broad array of NGC use cases
- Analyze use cases for affinity and ROI
- Recommend high ROI use cases for PoC
- Report and speak on findings of the group
Meetings & Members

- Starting June 15, 2023, the group met 7 times
- 23 individuals from various institutions and organizations
- 6-8 regulars throughout the meeting series
What is a Next-Generation Credential?

A next-generation credential is a \textit{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:

1) \textbf{An issuer} (may be self-issued) \textit{to}

2) \textbf{A verifier} \textit{by means of}

3) \textbf{A wallet} \textit{controlled by}

4) \textbf{A holder} (usually the subject of the attestation)
Assumptions

- Interoperability
- Trust Framework
- Privacy Preserving
Verifiable Credentials

- Verifiable credentials are a bundle of attributes about a subject such as Birth certificates, driver's licenses, academic credentials
- Enhanced privacy - User is in control / data hiding
Use Cases

- A current student presents their verifiable credential to a service provider in order to obtain a service discount only provided to current students without revealing anything more than their student status.
- A university needs to verify a prospective student’s high school diploma and/or transcript.
- An employer needs to verify a prospective employee’s college diploma and/or transcript.
Call To Action

● The working group is continuing on. Please join.
● Send email to: cacti-inquiry@internet2.edu
● Help drive the boat: Join CACTI:
  ○ [https://tinyurl.com/incommonlead](https://tinyurl.com/incommonlead)
  ○ Nominations open through October 1st
● Consider attending Internet2 Community Exchange:
  ○ We’ll have another meeting on this topic
  ○ March 4-7, Chicago