Digital Credentials
International Collaboration & Interoperable Standards

J. Philipp Schmidt
Kim Hamilton Duffy

DCC | Massachusetts Institute of Technology

digitalcredentials.mit.edu

Outline

- Digital Credentials and the Digital Credentials Consortium
- Relevant Standards
- Themes for Discussion

Digital Credentials and the DCC

What is a Digital Credential?

A combination of two components: a **document** and an **envelope** into which that document is placed.

The **document** is like the diploma a university issues to a graduate, which might contain the name of the recipient as well as a description of the credential they received.

The **envelope** protects the content of the document so it cannot be changed and it reliably communicates the authenticity of its contents.

Digital Credentials Consortium is focusing on the envelope and the system that provides safe delivery and storage of multiple envelopes—similar to the postal service for mail.

DCC Founding Members

Delft University of Technology (NL)
Georgia Institute of Technology (USA)
Harvard University (USA)
Hasso Plattner Institute (Germany)
MIT (USA)
McMaster University (Canada)
Tecnológico De Monterrey (Mexico)
Technical University Munich (Germany)
University of California, Berkeley (USA)
University of California, Irvine (USA)
University of Milano-Bicocca (Italy)
University of Toronto (Canada)

DCC Mission

Our mission is to create a trusted, distributed, and shared infrastructure that will become the standard for issuing, storing, displaying, and verifying academic credentials, digitally.

Download the whitepaper: bit.ly/DCCWhitepaper

DCC Activities

- *Technical Development*
- *Implementation at Member Institutions,*
- *Leadership in Standards Bodies, and*
- *Community Support*

DCC Guiding Principles

Learners

- **Retain primary control over their credentials.**
- Consent is required for issuance of digital credentials.
- Decide to whom they grant access.

Issuers

- Control to whom they issue credentials, the achievement that the credential represents, and which credential options are available to the learner.
- Can revoke credentials.

Trust

- Everyone is able to review how the infrastructure and processes work
- Trust in the integrity of the credentials is established cryptographically
- **Credentials can be verified without consulting the original issuer**

Access

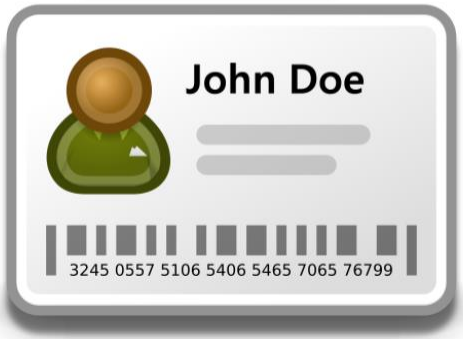
- Barriers to issuing, receiving, and managing credentials are minimal to enable broad and diverse participation.

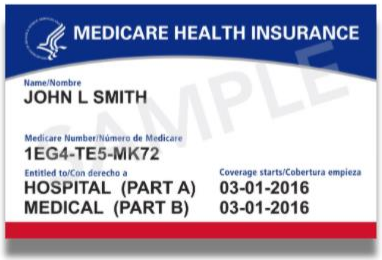
Importance of International Collaboration

- Increasing student mobility across institutions, countries, regions
  - EU-27: ~1.3M international students (2018)
- Higher Education economics are increasingly international
  - ~1M international students in US ($38.7b > U.S. economy)
- Existing frameworks: Erasmus+, EBSI, europass, EQF...
- More complex records of lifelong learning need to support various international experiences
- New emerging standards (no obviously best solution *yet*)
- Needs of institutions & students = interests of technology companies?

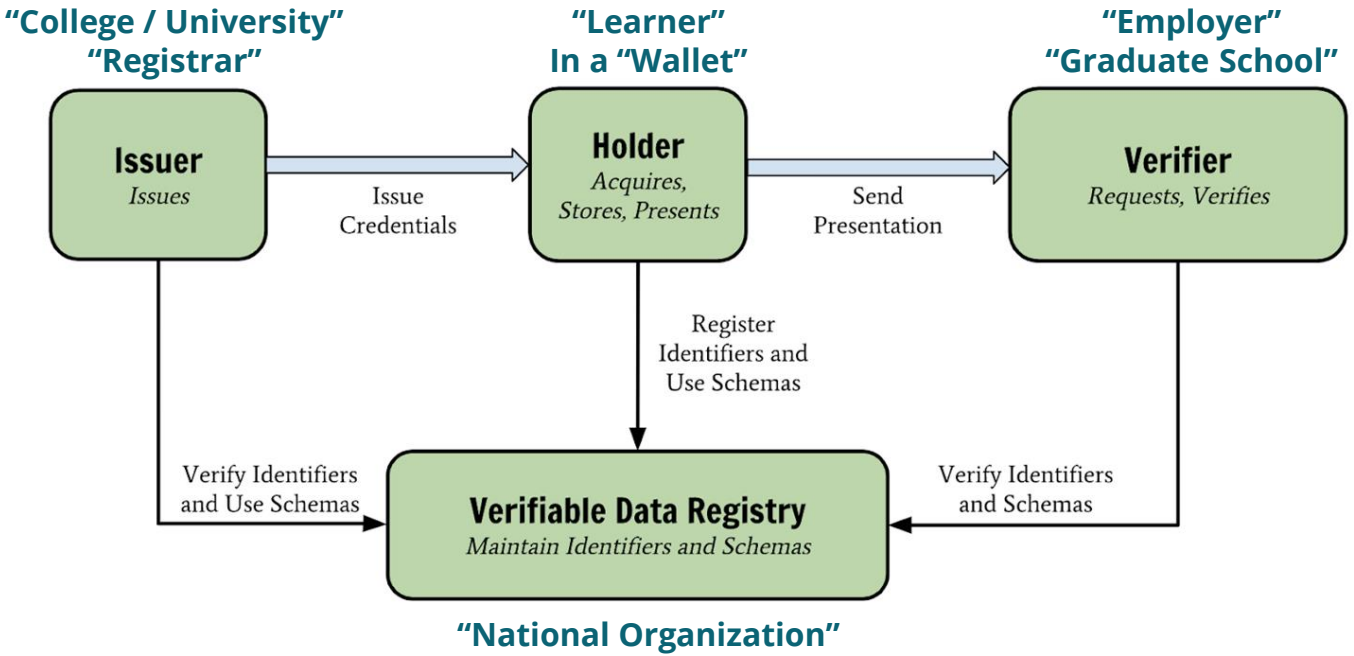
Relevant Standards

What do we mean by “credential”?





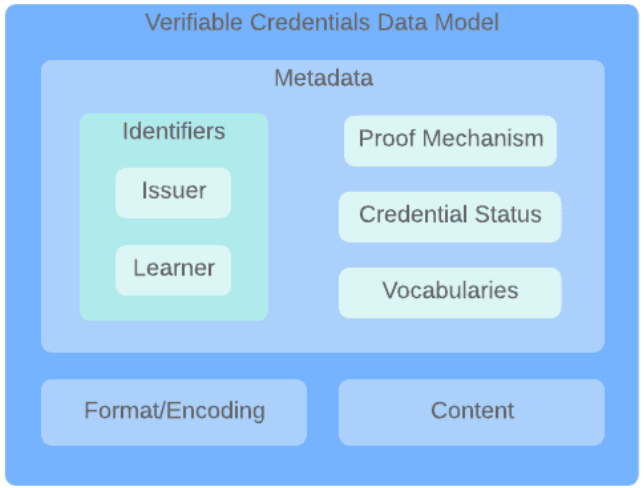
Verifiable Credentials Ecosystem



A **DCC-compatible Credential** is a W3C Verifiable Credential (tamper-evident credential where the authorship can be cryptographically verified) that meets the technical and policy specifications adopted by the DCC.

Generic Structure

- How to verify the credential
- Whether the issuer is authentic
- How to verify the learner
- Credential status information
- Vocabulary/taxonomies used in the credential



Verifiable Credentials

- Portable
- Privacy preserving
- Flexible content, linked data
- Tamper-evident
- Verifiable even when issuer is offline
  - Work well with DIDs as personal identifiers
  - Moves attributes with user control
- Flexible proof schemes (ZKPs)

Key Terminology

Learner - individual that has lifelong learning experiences that may be represented by a credential.

Issuer - an entity issuing credentials to the learner.

Credential - a set of claims (attributes about a learner) made by an issuer.

Verifiable credential - tamper-evident credential where the authorship can be cryptographically verified.

Relying party - any organization or person with whom the learner chooses to issue a credential.

Wallet (aka Envelope) is the software on device or accessible via the web that allows learners to manage their credentials and profiles.

DCC-compatible Credential is a verifiable credential that meets the technical and policy specifications adopted by the DCC.

Decentralized Identifiers

- Identifiers for issuer and subject
- New type of identifier that enables verifiable, decentralized digital identity
- May be decoupled from centralized registries, identity providers, and certificate authorities
- Lifecycle is a first-class concern

did:btcr:xkyt-fzgq-qq87-xnhn

Themes and Discussion

Themes For Today’s Discussions

- Role of Interoperable Standards
- Adaptability
  - One-size-fits-all doesn’t work
  - How do we ensure approach is adaptable to varying regulatory frameworks, institutional processes
  - Layered vs monolithic
- “Trust” is nuanced

Examples of adaptability “dials” and challenges

- VCs bridging to existing, meaningful data standards and vocabs
  - Don’t need to invent new data standards
  - Mapping vs monoliths (conceptual alignment)
  - Tradeoffs, discovery
- Decentralized identifiers / VCs
  - “Pure” SSI bridging to strict legal ID requirements
- **Let’s be explicit about the limitations of technical solutions**
- Working with regulatory bodies, privacy experts
  - E.g., Legal signature requirements, more nuanced discussions of possibilities and limitations of privacy dials
  - “GDPR compliance”

References / Learn More / Get Involved

- W3C Verifiable Credentials for Education Task Force
  - Meets every other Monday. Free, open to the public
  - Join us: https://w3c-ccg.github.io/vc-ed/
- Universal Wallet
  - Spec: https://w3c-ccg.github.io/universal-wallet-interop-spec/
  - Experimental Implementation: https://github.com/w3c-ccg/universal-wallet-interop-spec/
- DCC Resources
  - Website: https://digitalcredentials.mit.edu/
  - White paper: https://digitalcredentials.mit.edu/wp-content/uploads/2020/02/white-paper-building-digital-credential-infrastructure-future.pdf
  - Github repo: https://github.com/digitalcredentials
- Other:
  - Applying SSI Principles to Interoperable Learning Records: https://www.uschamberfoundation.org/sites/default/files/media-uploads/Applying%20SSI%20Principles%20to%20ILRs%20Report.pdf
  - LER Wallet Spec: https://cdn.filestackcontent.com/preview/FeqEJI3S5KelmLv8XJss
  - ILR/LER IEEE Group: https://standards.ieee.org/project/1484_2.html

Contact:
- @kimdhamilton
- kimhd@mit.edu
- https://www.okimsrazor.com/

Thank you!

Appendix

Digital Credentials Consortium

- Committed to standards-based, interoperable, portable credentials
  - Verifiable Credentials
  - Decentralized Identifiers
- Build missing pieces
  - Standards, protocols, learner scenarios
- Primary focus is higher education use cases
  - But part of a broader effort to bridge post-secondary and lifelong learning

Goal: Increase learner agency and promote more equitable learning and career pathways

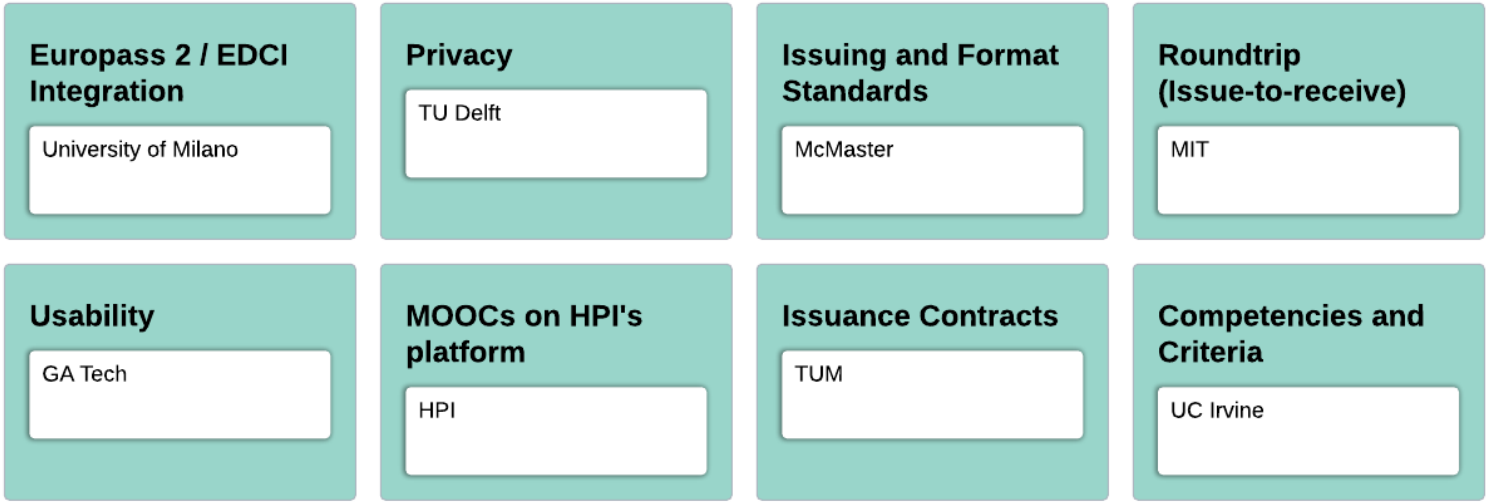
Founding Members

Delft University of Technology (The Netherlands)
Georgia Tech (USA)
Harvard University (USA)
Hasso Plattner Institute, University of Potsdam (Germany)
Massachusetts Institute of Technology (USA)
McMaster University (Canada)
Tecnologico De Monterrey (Mexico)
TU Munich (Germany)
UC Berkeley (USA)
UC Irvine (USA)
University of Milano-Bicocca (Italy)
University of Toronto (Canada)

Pilots Underway

Overview

- Build out technical foundation
- Use-case driven pilots
  - Focusing on different use cases
  - Partnering with different organizations
  - Building out standards, reusable components/libraries
  - Investigating/prototyping more advanced elements



Some examples

- MIT / xPRO digital credentials on course completion
- GA Tech Canvas Integration
- McMaster certification letters

McMaster University

1280 Main St. W.
Hamilton, ON L8S 4L8

February 05, 2021 DLI#: [redacted]

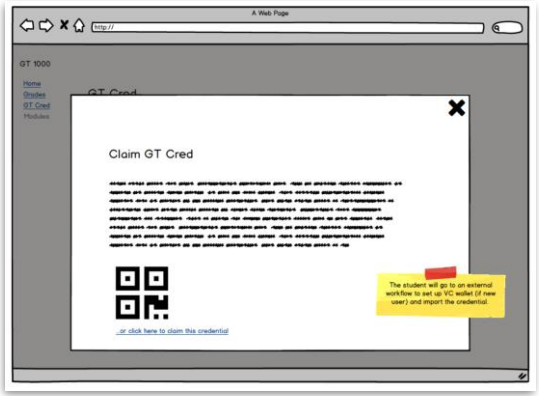
[redacted]

To Whom It May Concern:

This letter confirms [redacted], [redacted] enrolled at McMaster University in the following courses for the 2021 Winter term as a Full-Time student:

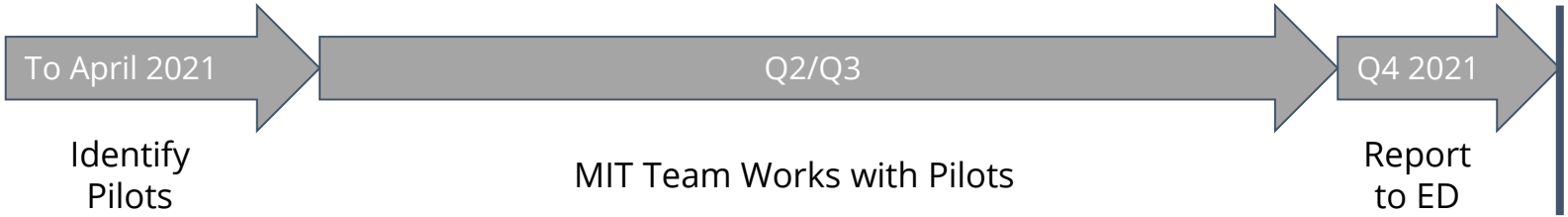
Course Subject	Course Code	Course Description	Status/Reason
POLSCI	2O06B	Political Theory	Enrolled
POLSCI	3Y03	Democratization & Human Rights	Enrolled
POLSCI	3NN3	Stat. Analysis of Primary Data	Enrolled
HLTHAGE	1CC3	Intro to Mental Hlth & Illness	Enrolled
POLSCI	4AA6B	Contemporary Politics	Enrolled

Sincerely,



MIT-ED Digital Credential Project Goals

- U.S. Department of Education contract to MIT to develop an open Student Wallet draft standard and implementation
  - MIT's work builds on DCC activities and is a reference implementation of them
- Deliverables
  - Open Source (Draft) Specification for Student Wallet
  - Reference Implementation
  - 2-3 higher education pilots ("deployments"), support, and analysis



Goals

- Interoperability
- Portability
- Reference implementation, but not “the wallet”
- Facilitate standards compliance for wallet creators
- Learner/individual choice
  - Warning: wallet proliferation