Digital Micro-credentials (DMCs)

By

Anil Ripla

CloudTnT Project

11/07/2024

Contents

Introduction

The purpose of this paper is to provide an introduction to digital micro-credentials (DMCs):

- What they are
- The actors involved
- The digital ecosystem in which they exist

Proposed Definition

A consensus agreement on a standard definition for micro-credentials is proving hard to achieve. There are many views on what exactly is a micro-credential. The views of traditional academic practitioners and those in the Information Technology sector may differ somewhat. The following proposed definition will suit the purpose of this paper.

"A digital micro-credential (DMC) is an electronic file that is issued by an issuer to a holder who has demonstrated competence in a discrete task or set of tasks related to a job."

Actors

The DMC ecosystem is comprised of three principal actors as described below.

Holders

A holder is the individual who earns a DMC.

Issuers

An issuer is an individual or organization who issues a DMC to a holder.

Verifiers

A verifier is an individual or organization, such as an employer, who verifies that the credential presented by a holder was authentically issued by an issuer

Characteristics of Digital Micro-credentials

Discrete Competencies

DMCs are issued to holders who demonstrate competence in a discrete task or set of tasks. These tasks may cover a specific function carried out in a job. For instance, painting a wall, building a website, installing an electrical panel, etc. The competencies should be directly job-related.

Short Time Duration

Holders earn DMCs in a short period of time, from a few hours to a few weeks.

Portable

DMCs are owned by the holders and are portable. They can be stored in a holder's credential wallet and displayed online to verifiers.

Stackable

Individual DMCs can be grouped together to from larger credentials or to cover a wider job function. For instance, a mechanic may stack her individual DMCs in engine repair, automotive electrical and fuel systems as she moves along her career path. This method of stacking DMCs promotes life long learning.

Self-Paced

A holder can take a DMC at any time they desire. The credentials are "on-demand" and can be undertaken by the holder at her own pace.

Accessible

DMCs should be accessible to anyone who has the ability to earn them. There should be no onerous pre-requisites or barriers to a earn a DMC.

Delivery

Informal and Nonformal Education and Training

Many DMCs are currently offered outside the traditional academic education and training system. They predominate in the informal and non-formal sector as described below.

Online Learning

With the rise of the Massive Open Online Courses (MOOCs), there has been a flood of DMCs offered online on websites like Coursera, EdX, Udemy, etc.

Workplace Learning

DMCs can be earned by holders in their place of work, such as in an organization's in-house training or internship system.

Prior Learning and Experience

A holder can present evidence of their workplace competence achieved through prior learning to an issuer to earn a DMC.

Formal Education and Training

DMCs can also be earned in the traditional academic and training system such as:

- Schools and Universities
- Training Intuitions and Vocational Centers
- Formal Apprenticeships

Anatomy of a Digital Micro-credential

Electronic File

DMCs are issued to holders as an electronic file. They can be:

- An Image File (.PNG, .SVG)
- A Text File (.TXT)
- A JSON or JSON Web Token File (.JSON, .JWT)

Data Structure

The electronic file contains the metadata for the credential. The data can be embedded in an image or can be provided in the raw format. The data is structured as a JSON or a JSON Web Token (JWT).

Interoperability Standards

In an effort to standardize the structure of DMCs, there are a number of standards that have been developed. These various standards are described below.

W3C Decentralized Identifiers

The W3C standard for Decentralized Identifiers (DIDs) provides a mechanism to uniquely identity the holder and the issuer of a DMC. It uses cryptography to secure the digital credentials.

W3C Verifiable Credentials

The W3C standard for Verifiable Credentials specifies a data model for the structure of the credential's meta data. It is used in tandem with the DID standard to provide a mechanism to produce a cryptographically secured digital credential.

1Edtech Open Badges Specification

The Open Badges V3 specification builds on the W3C standards to define the requirement for the open badges. The Open Badge is issued as an image file with the credential's metadata embedded in the badge. The badge adopts and expands the W3C specification for data modelling and cryptographic security for the open badge.

Security

DMCs are very secure electronic files. They use asymmetric cryptographic keys to electronically sign a badge. A verifier can be assured that the badge originated from an issuer holding the private key that was used to sign the credential. It is extremely difficult to forge a digitally signed credential.

Trust Model

There is an absence of formal regulation for the DMC in most countries. In light of this, a trust model must be established by the holder, issuer and verifier. The fitness of a credential must be determined by the employers (verifiers) as providing value to their organization. In addition, the verifier must determine if the issuer is a credible individual or organization worthy of their trust. Once verifiers put their trust in issuers and their credentials, holders will be motivated to earn credentials from these trusted issuers. The entire system is be driven by market forces following this trust model.

Electronic Platforms

Issuer Platform

An issuer uses an Issuer Platform to design and issue DMCs to holders. These platforms should comply with the W3C and Open Badges standards to ensure interoperability of credentials.

Holder Wallets

Holders store their DMC in a digital wallet. They can collect credentials, stack them and present their credential collections to verifiers online.

Designing a Micro-credential

Credential Details

The first step in designing a DMC is to define the name and description for the DMC. You should provide enough details so that holders and verifiers can clearly understand what the credential is about.

Criteria

The criteria to earn the DMC must be clearly stated. This is the list of competencies that the holder must demonstrate to earn the credential.

Evidence

The evidence that a holder must produce to demonstrate competence must be listed. For instance, a learner must produce two websites to earn a credential in website design.

Data Model

The credential details, criteria and evidence must be structured to meet the requirements of the W3C and Open Badges standard. The Issuer Platform should automatically format the credential to comply with the standards.

Machine Learning and AI

Machine Leaning (ML) and Artificial Intelligence (AI) can be harnessed to further improve the DMC ecosystem. To implement ML and AI, it is important to ensure the DMC ecosystem produces machine readable data. To this end, the W3C and Open Badges interoperability standards are important tools in producing the big data required for Machine Learning and AI. There are many potentials uses for generative AI solutions in:

- Developing Job Descriptions
- Designing competence-based training
- Identifying training needs for sectors or organizations
- Identifying career paths for employees

CloudTnT Project

In the first phase, the CloudTnT project aims to develop a DMC Issuer Platform that allow issuers to issue credentials that comply with the W3C and Open Badges standards. In addition, an open-source Holder Wallet will be developed that can be hosted by any individual or organization for holders to store and display their credentials. In the second phase, work will be started to develop a Workforce Hub and AI Models for workforce development.