DCC DIGITAL CREDENTIALS CONSORTIUM

Digital Credentials Enabling Mobility and Verification of Educational Achievements

Brandon Muramatsu, MIT
Willem van Valkenburg, Delft University of Technology

DCC DIGITAL CREDENTIALS CONSORTIUM

Today

- A brief intro to the Digital Credentials Consortium
- Two case studies
  - GDPR and Digital Credentials, Delft University of Technology
  - Open Source Learner Credential Wallet, MIT

DCC DIGITAL CREDENTIALS CONSORTIUM

Digital Credentials Consortium

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.

DCC DIGITAL CREDENTIALS CONSORTIUM

DCC Founding Members

Delft University of Technology (The Netherlands)

Georgia Institute of Technology (USA)

Harvard University (USA)

Hasso Plattner Institute, University of Potsdam (Germany)

Massachusetts Institute of Technology (USA)

McMaster University (Canada)

Tecnológico De Monterrey (Mexico)

Technical University of Munich (Germany)

University of California at Berkeley (USA)

University of California, Irvine (USA)

University of Milano-Bicocca (Italy)

University of Toronto (Canada)

DCC DIGITAL CREDENTIALS CONSORTIUM

DCC Guiding Principles

Learners

- **Learners retain primary control over their credentials.**
- Learners' consent is required for issuance of digital credentials.
- Learners decide to whom they grant access.
- Barriers to receiving and managing credentials are minimal to enable broad participation.

Issuers

- Issuers control to whom they issue credentials, the particular achievement that the credential represents, and which credential options are available to the learner.
- Issuers can revoke credentials according to their institution's policies.
- Barriers to issuing credentials are minimal to enable broad and diverse participation.

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.**

DCC DIGITAL CREDENTIALS CONSORTIUM

How does DCC do its work?

- Consortium of members with alignment to guiding principles, and each working in similar ways on digital credentials
- DCC does its work through open standards organizations primarily the **W3C Verifiable Credentials for Education (W3C VC-EDU) Community Group**
  - Coordinates with IMS Global on Comprehensive Learner Record and Open Badges v3 specifications
- Shared technical work through a Technical Working Group made up of DCC members
- Implementing **Verifiable Credentials (VC)** and **Decentralized Identifiers (DID)** specifications
  - Meet key DCC guiding principles of learner control

DCC DIGITAL CREDENTIALS CONSORTIUM

What is a Digital Credential?

DCC DIGITAL CREDENTIALS CONSORTIUM

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.

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

Individual members continue to focus on the document within the envelope.

DCC DIGITAL CREDENTIALS CONSORTIUM

Key Terminology

The **learner** is the individual that has lifelong learning experiences that may be represented by a credential.

The **issuer** is an entity issuing credentials to the learner.

A **credential** is a set of claims (attributes about a learner) made by an issuer.

A **verifiable credential** is a tamper-evident credential where the authorship can be cryptographically verified.

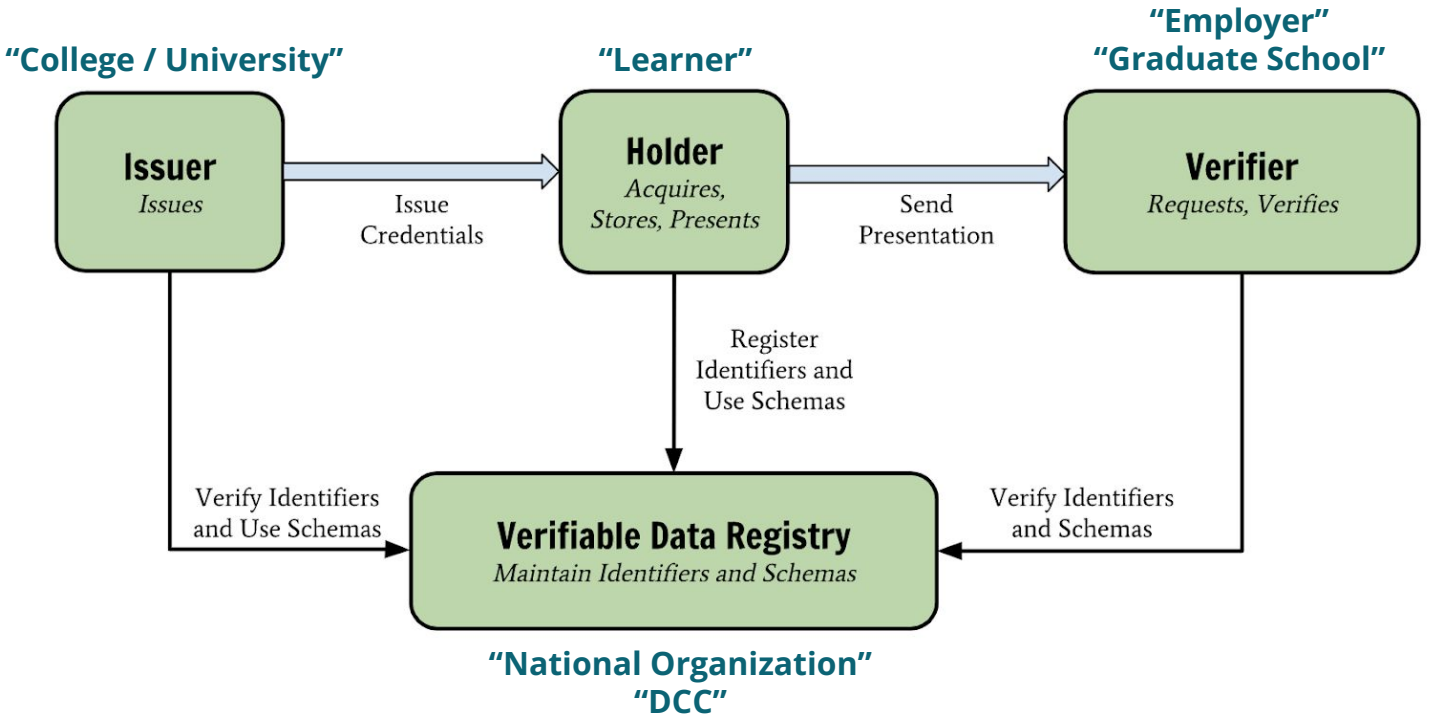
The **relying party** is any organization or person with whom the learner chooses to issue a credential.

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

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

DCC DIGITAL CREDENTIALS CONSORTIUM

Verifiable Credentials Ecosystem



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

Delft University of Technology

General Data Protection Regulation and Blockchain

General Data Protection Regulation (GDPR)

The European Union's General Data Protection Regulation become binding in May 2018.

Goal of GDPR:

1. to facilitate free movement of personal data between EU members states
2. to establish a framework of fundamental data rights protection.

The legal framework creates a number of obligations resting on *data controllers* (entities determining the means and purpose of data processing)

The legal framework creates a number of rights to *data subjects* (the natural persons to whom the personal data relates) to be enforced by data controllers. E.g. Article 16 GDPR – right to rectification, Article 17 GDPR – right to erasure (‘right to be forgotten’)

Leading principles of GDPR

Lawfulness, fairness and transparency	organisations need to make sure their data collection practices don't break the law and that they aren't hiding anything from data subjects.
Purpose limitation	Organisations should only collect personal data for a specific purpose, clearly state what that purpose is, and only collect data for as long as necessary to complete that purpose.
Data minimisation	Organisations must only process the personal data that they need to achieve its processing purposes.
Accuracy	The accuracy of personal data is integral to data protection. The GDPR states that "every reasonable step must be taken" to erase or rectify data that is inaccurate or incomplete.
Storage limitation	Organisations need to delete personal data when it's no longer necessary.
Integrity and confidentiality (security)	Personal data should be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
Accountability	The controller shall be responsible for, and be able to demonstrate compliance with the above principles

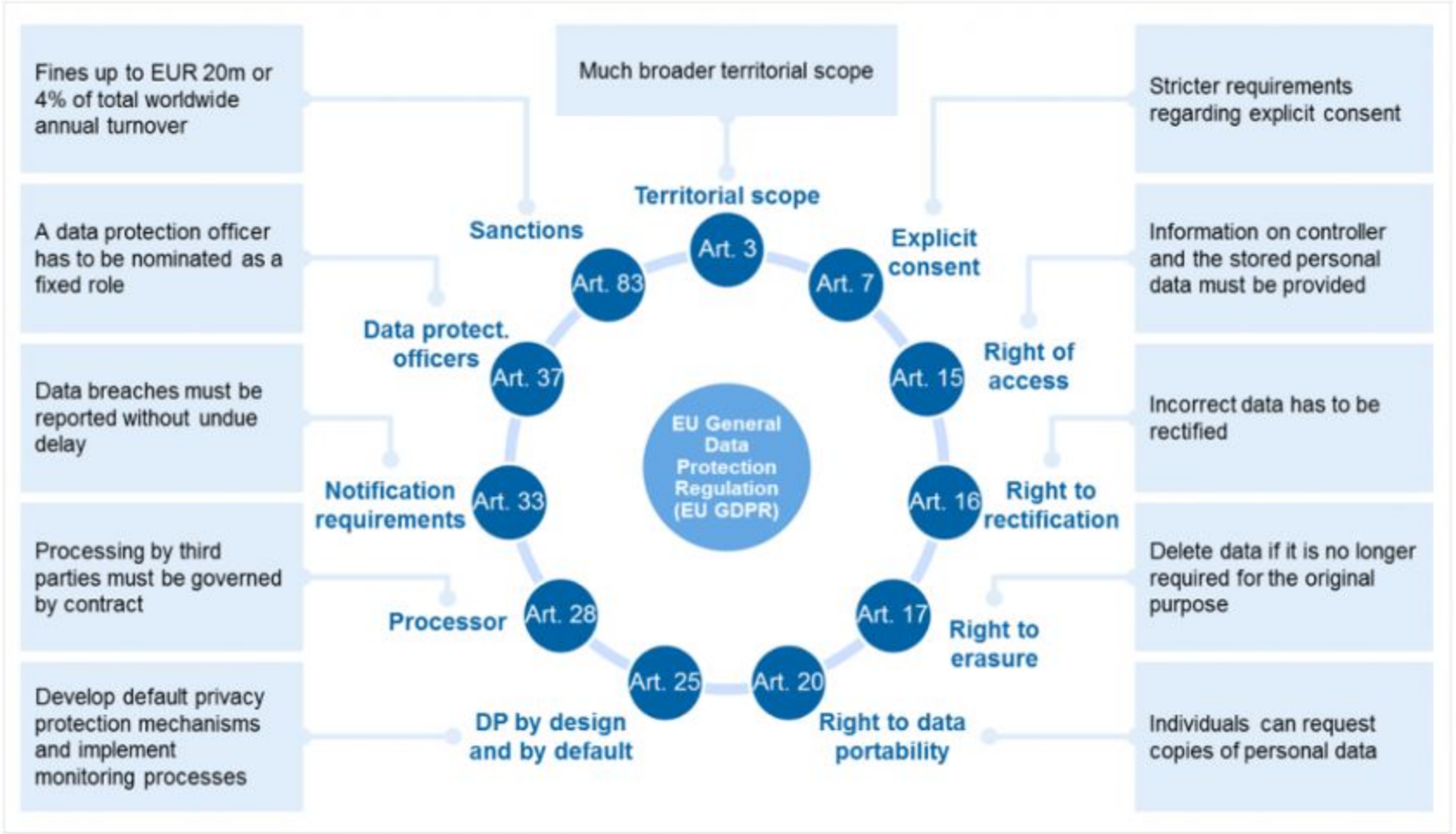


Figure 1: Major requirements of GDPR (summary)

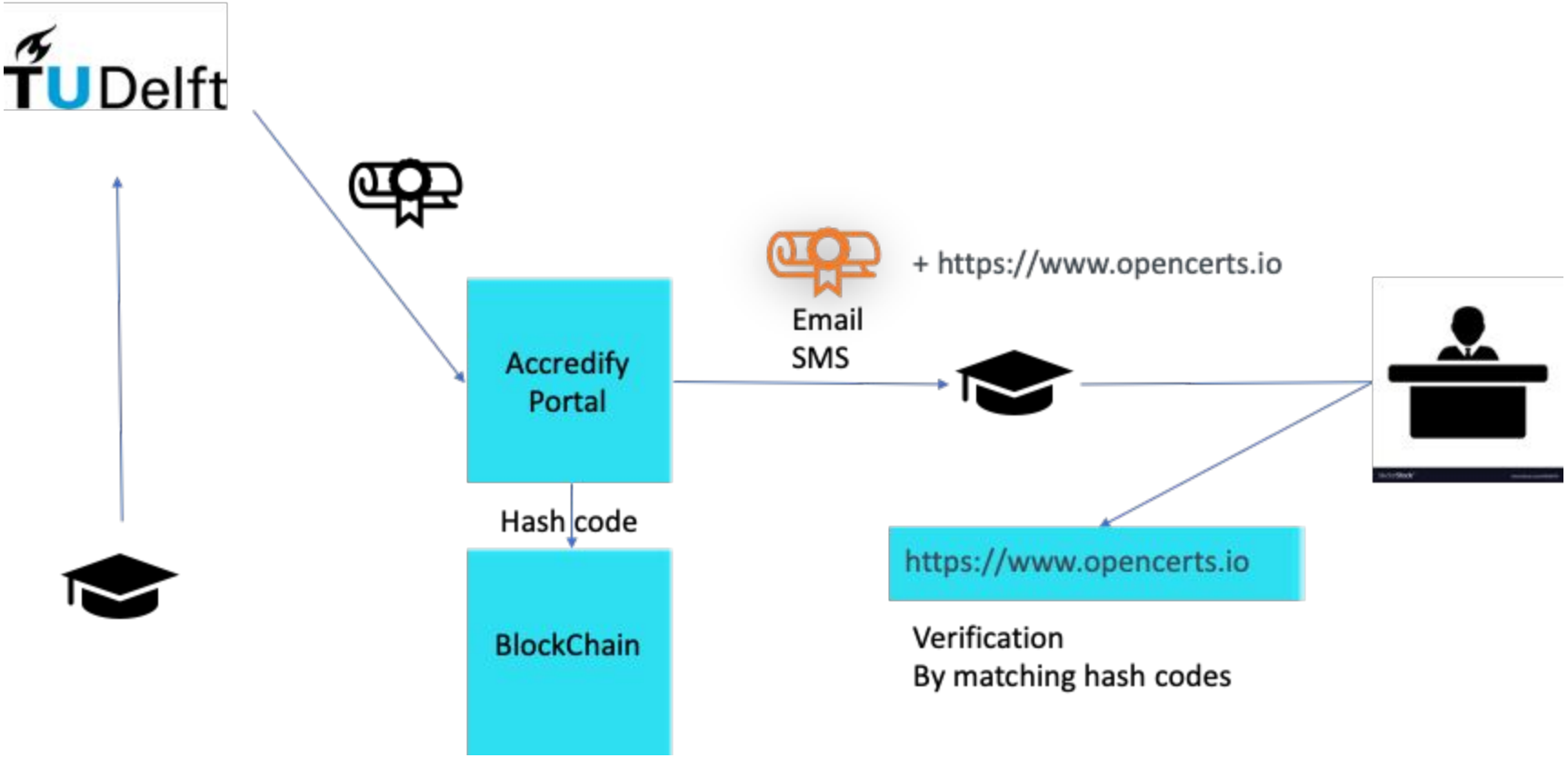
Source:https://www.bankinghub.eu/banking/finance-risk/gdpr-deep-dive-implement-right-forgotten

GDPR and Blockchain

The GDPR is based on assumptions that creates tension with blockchain.

GDPR	Blockchain
in relation to each personal data point there is at least one natural or legal person – the data controller – whom the subjects can address to enforce their rights under EU Data protection law.	decentralizes to many actors and allocation of responsibility and accountability is burdensome.
data can be modified or erased where necessary to comply with the legal requirements of GDPR Article 16 (right to rectification) and 17 (right to erasure (‘right to be forgotten’)	Modification and erasure of data is made onerous to ensure data integrity and increase trust in the network.

What does this look like in practice?



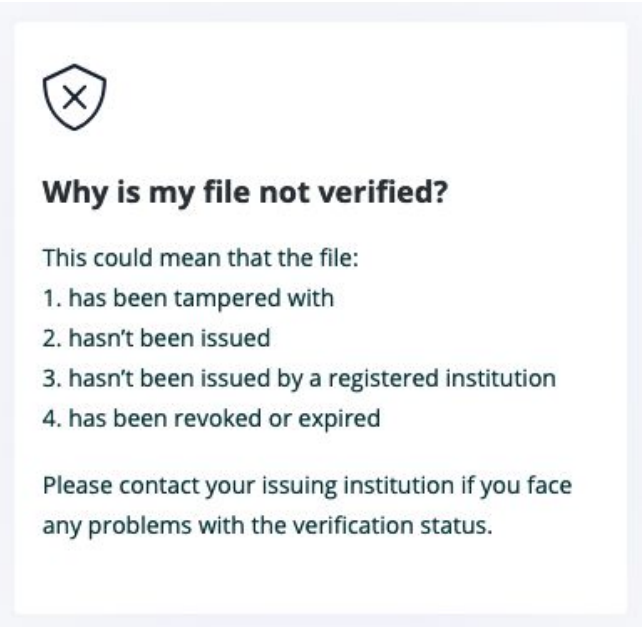
Personal data on the Blockchain?

In the pilot we explored the following:

- Is data that is encrypted or hashed/ ‘anonymized’ still quality as personal data as per the GDPR requirements of anonymisation?
- How is the right to erasure/right to be forgotten dealt with in the pilot?

The right to be forgotten is not an absolute right

- if a learner requests to be forgotten, Accredify deletes their personal data. The learner is the one who should contact institutes where they have personally shared their opencert file which could be still verified.
- What happens now is that Accredify deletes personal data from their system which is GDPR complaint. This is because the right to be forgotten does not extend to all the institutes where the learner shared their file.
- If a certificate is revoked and cannot be verified in the future that doesn't say much – so it is good to add an explanation.



Hashing, salt and peppering of personal data

- As long as the hash relates to something it is not anonymised.
- This is the current conflict within blockchain and GDPR and the interpretation of what is considered as anonymous.

Open Source Learner Wallet
MIT

MIT Team
Brandon Muramatsu
Philipp Schmidt
Gillian Walsh
Dmitri Zagidulin

About the Open Source Learner Wallet Project

- A key missing ingredient in a digital credential infrastructure
  - Prioritizes learner agency
  - Enables trust
  - Supports diverse institutions
- A **learner credential wallet specification** (May 2021)
- An open source learner wallet **mobile app, eduWallet**
- A **pilot** with U.S. institutions:
  - College Unbound, Georgia Tech and San Jose City College
  - MIT xPRO and University of North Texas / Concentric Sky

Details on eduWallet
An Open Source Learner Wallet

- Both Android and iOS versions
  - Going into pilot testing December 2021–January 2022
- Key features
  - Login to secure wallet
  - **Add verifiable credentials** via deep link (direct and QR Code) and via QR code
  - **Display credentials locally**—Issuer, issuer logo, credential name, issuance date
  - **Select and share credentials** as JSON-LD via operating system sharing mechanisms (copy to clipboard, save as file)
  - Delete credentials, backup and restore from file

Demo

- Login to a LMS or student portal
- Prompted to install eduWallet from Apple or Google Play app stores
- First time setup of eduWallet
- (Simulated) Access credential via LMS / QR Code / Deep Link
- (Not demonstrated) Authenticate before receiving credential
- View credentials (and share them)

DCC DIGITAL CREDENTIALS CONSORTIUM

Questions?

Brandon Muramatsu
mura@mit.edu

Willem van Valkenburg
w.f.vanvalkenburg@tudelft.nl

MIT | Open Learning