# Certification Working Group Meeting

**For discussion only**
**12 December 2023**

ICC Digital Standards Initiative

# Agenda

1. What Are We Creating
2. Progress/Planned to Date
3. Outcome of Consultations and Discussions
4. Initial and Revised Scheme Proposals
5. Discussion
6. Next Steps

ICC Digital Standards Initiative

CONSEIL DE GOUVERNANCE NUMÉRIQUE DIGITAL GOVERNANCE COUNCIL

# 1. What Are We Creating

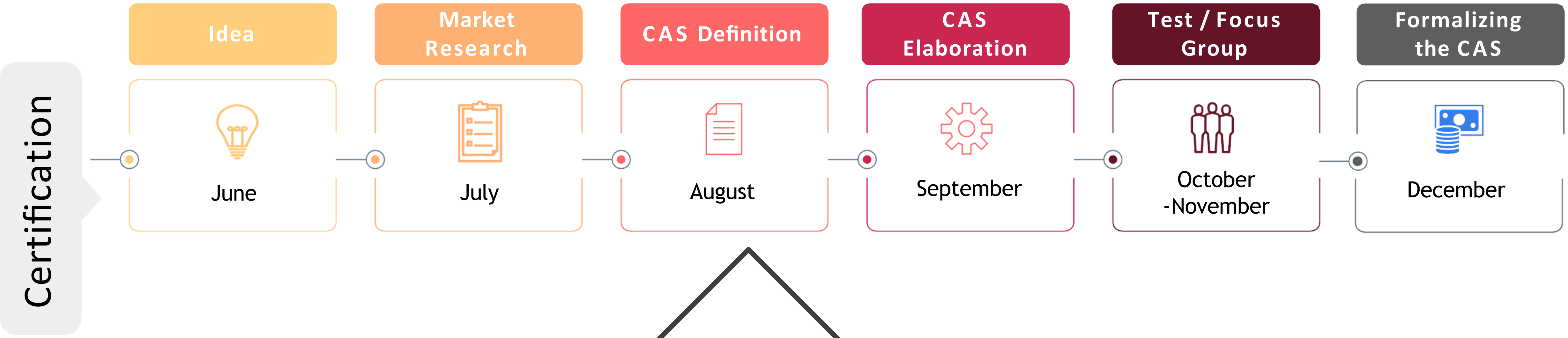
ICC DSI and the Digital Governance Council (DGC) of Canada are collaborating to develop a Conformity Assessment program for systems and services that enable the electronic exchange, management, and interoperation of trade documentation in digital forms.

The scheme is being developed within the DGC’s Digital Trust Conformity Assessment program which brings together standards, assessment methodologies, accreditation programs and communities to engender digital trust that is principles-driven, evidence-based and open-source by design.

# 2. Progress/Planned to Date

- **March-August 2023:**
    - Trust-In-Trade Report Published (March)
    - Kick-Off Meeting (June 6)
- **September -December 2023:**
    - DGC-ICC MOU signed
    - GitHub Repo created (https://github.com/dgc-cgn/CAS-Digital-Trade-Documentation/ )
    - Initial Working Group Meeting (September 12)
    - Second Working Meeting (October 2)
- **January 2024 Planned :**
    - *Prototype*
    - *Test*
    - *Commercialize*

# 3. Outcome of Consultations and Discussions

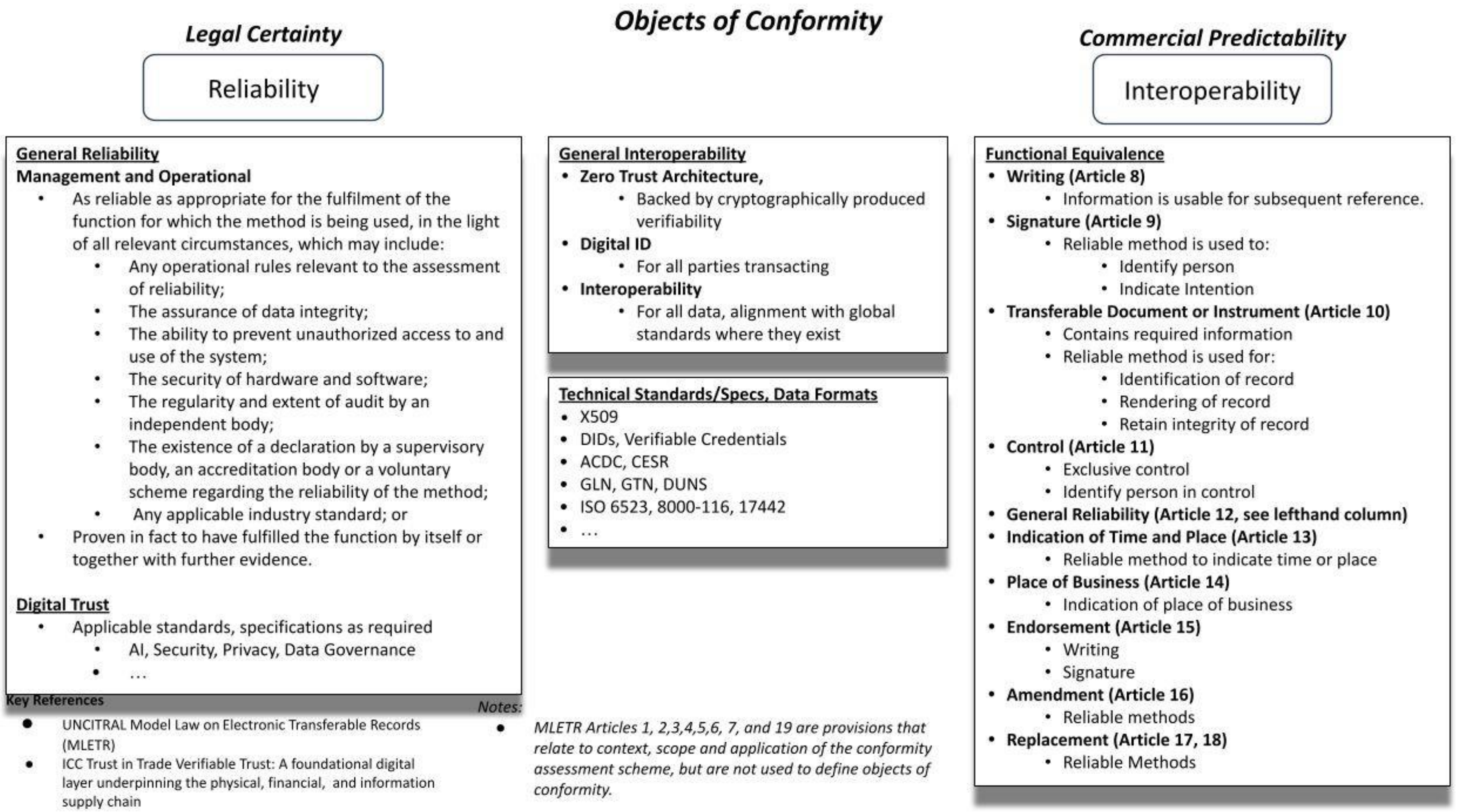


Certification

| Idea | Market Research | CAS Definition | CAS Elaboration | Test / Focus Group | Formalizing the CAS |
|---|---|---|---|---|---|
| June | July | August | September | October -November | December |

- We are approximately 1Q behind the original plan
- Scheme framework developed and presented to working group in Sept 2023
- Subsequent review of documentation, discussions and consultation have resulted in a focused and simplified scheme.

# 4a. Initial Scheme Proposal



*Legal Certainty*

Reliability

*Objects of Conformity*

*Commercial Predictability*

Interoperability

**General Reliability**

**Management and Operational**

- As reliable as appropriate for the fulfilment of the function for which the method is being used, in the light of all relevant circumstances, which may include:
  - Any operational rules relevant to the assessment of reliability;
  - The assurance of data integrity;
  - The ability to prevent unauthorized access to and use of the system;
  - The security of hardware and software;
  - The regularity and extent of audit by an independent body;
  - The existence of a declaration by a supervisory body, an accreditation body or a voluntary scheme regarding the reliability of the method;
  - Any applicable industry standard; or
- Proven in fact to have fulfilled the function by itself or together with further evidence.

**Digital Trust**

- Applicable standards, specifications as required
  - AI, Security, Privacy, Data Governance
  - …

**Key References**

- UNCITRAL Model Law on Electronic Transferable Records (MLETR)
- ICC Trust in Trade Verifiable Trust: A foundational digital layer underpinning the physical, financial, and information supply chain

**General Interoperability**

- **Zero Trust Architecture,**
  - Backed by cryptographically produced verifiability
- **Digital ID**
  - For all parties transacting
- **Interoperability**
  - For all data, alignment with global standards where they exist

**Technical Standards/Specs, Data Formats**

- X509
- DIDs, Verifiable Credentials
- ACDC, CESR
- GLN, GTN, DUNS
- ISO 6523, 8000-116, 17442
- …

*Notes:*

- *MLETR Articles 1, 2,3,4,5,6, 7, and 19 are provisions that relate to context, scope and application of the conformity assessment scheme, but are not used to define objects of conformity.*

**Functional Equivalence**

- **Writing (Article 8)**
  - Information is usable for subsequent reference.
- **Signature (Article 9)**
  - Reliable method is used to:
    - Identify person
    - Indicate Intention
- **Transferable Document or Instrument (Article 10)**
  - Contains required information
  - Reliable method is used for:
    - Identification of record
    - Rendering of record
    - Retain integrity of record
- **Control (Article 11)**
  - Exclusive control
  - Identify person in control
- **General Reliability (Article 12, see lefthand column)**
- **Indication of Time and Place (Article 13)**
  - Reliable method to indicate time or place
- **Place of Business (Article 14)**
  - Indication of place of business
- **Endorsement (Article 15)**
  - Writing
  - Signature
- **Amendment (Article 16)**
  - Reliable methods
- **Replacement (Article 17, 18)**
  - Reliable Methods

# 4b. Revised Scheme Proposal

***System Reliability***

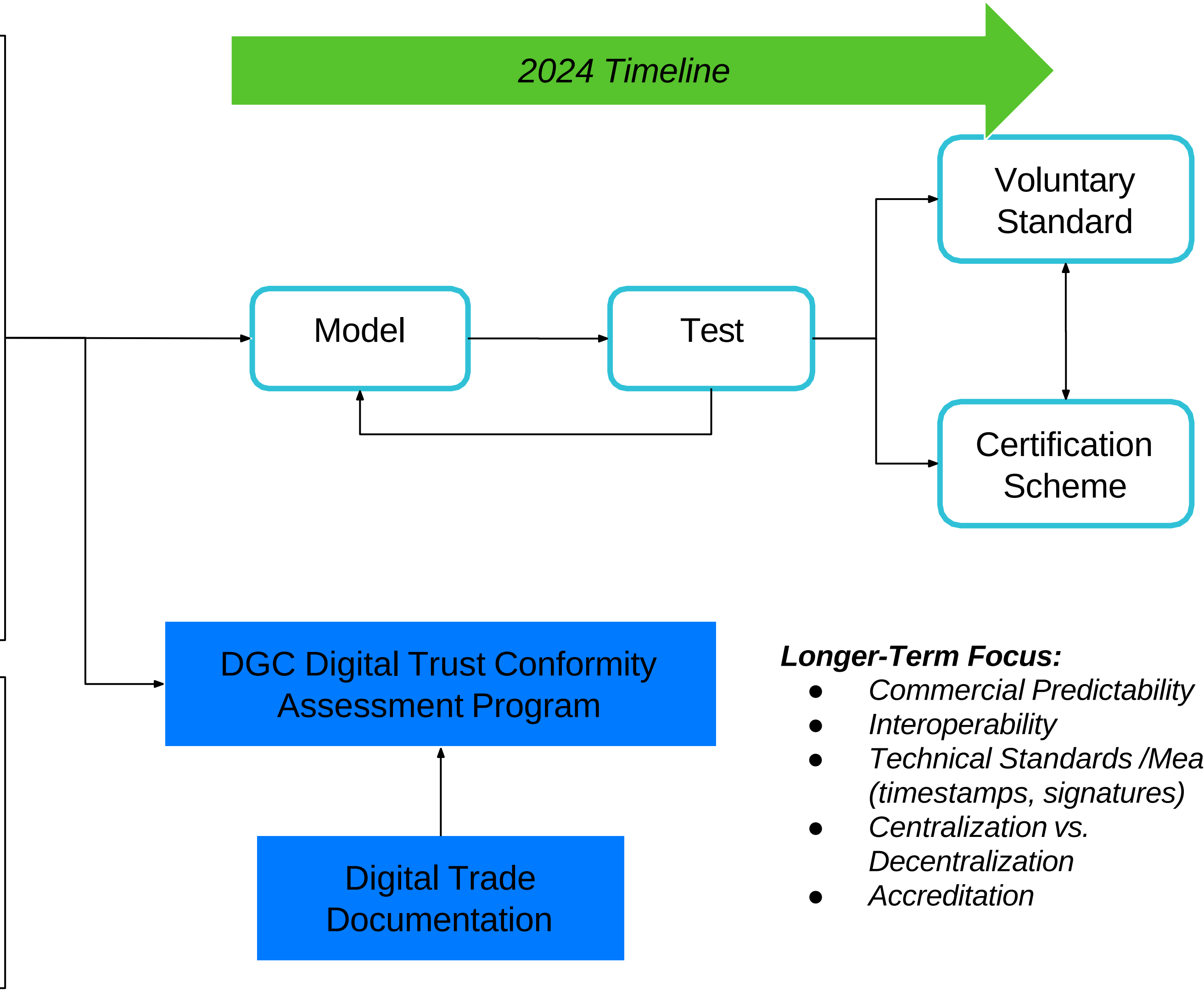
**RELIABLE SYSTEMS ASSURANCE**
Integrity / Singularity / Exclusive Control

**Immediate Focus: Reliability**

- Ensure the reliable transfer of the performance of an obligation embodied in an ETR
- Definition of objects of conformity with accompanying assessment criteria

***Related Initiatives***

DSI DATA MODEL IMPLEMENTATION /
STANDARDS BEST PRACTICE CAPABILITY



*2024 Timeline*

Model

Test

Voluntary Standard

Certification Scheme

DGC Digital Trust Conformity Assessment Program

Digital Trade Documentation

***Longer-Term Focus:***

- *Commercial Predictability*
- *Interoperability*
- *Technical Standards /Measures (timestamps, signatures)*
- *Centralization vs. Decentralization*
- *Accreditation*

https://github.com/dgc-cgn/CAS-Digital-Trade-Documentation/

# WIP Material for Discussion

**Material for discussion can be found at the links below**

Conformity Assessment Scheme: Digital Trade Documentation

a. General Reliability
b. Reliable System
c. Criteria
   i. Integrity
   ii. Singularity
   iii. Control

Example object of conformity: Verifiable Identifier

(Excerpted on next slide)

# Sample conformity approach: Verifiable Identifier

- A **verifiable identifier (VID)** is an address or identifier that is verifiably bound to at least one set of cryptographic keys that are discoverable via an **associated disovery protocol.**
- A VID does not need to change (i.e., can remain the same) when the controller’s key(s) are rotated or network endpoint(s) are updated.
- An **associated discovery protocol** for VIDS allows entities to locate, retrieve, and authenticate public identifiers and system endpoints associated with a particular VID. The discovery protocol ensures the integrity and authenticity of the identifier information through cryptographic proofs and is intended to reduce potential spoofing or fraudulent activities, and to promotes a seamless, secure exchange of information among peers without relying on central authorities or intermediaries.
- VIDs may be issued via a **centralized** or **decentralized** system. This distinction should have no bearing on the assessing the technical format of the VID.
- Decentralizeds VIDs may be further distinguished as **non-autonomous identifiers** or **autonomous identifiers**.
- A VID may be implemented using a variety of schemes, standards and specifications.

**Object of Conformity Criteria**
A VID must have the following characteristics:

1. A VID must be resolvable securely to obtain the current public key(s) needed to verify that the VID owner controls the VID.
2. A VID must be resolvable securely to obtain the current network endpoint(s) for establishing a ToIP connection with the entity identified by the VID.
3. A VID must provide an indication that its keys have changed and the previous keys are no longer valid for new transactions.
4. A VID must support at least one defined **out-of-band (OOBI)** process for initial setup.
5. A VID must support at least one **digital signature scheme**.
6. A VID must support at least one **encryption method**.
7. A VID must support at least one **associated discovery protocol**.

5. Discussion

6. Next Steps

**Feedback from Working Group Members**

ICC Digital Standards Initiative