



Digital Identity Priority Stream Joint Councils

25 September 2019

Sophia Howse, BC
Alexandre Bourque, TBS

Joint Councils - Digital ID Roadmap



POLICY AND GOVERNANCE



PAN-CANADIAN TRUST FRAMEWORK



PILOTS AND PUBLIC LAUNCHES



COMMUNICATION AND COLLABORATION



TECHNOLOGY



Objective

- In February 2019, the JCs approved funds to develop recommendations for the future governance framework for digital identities in Canada
- The ask was to present recommendations back to JCs today

Key Questions

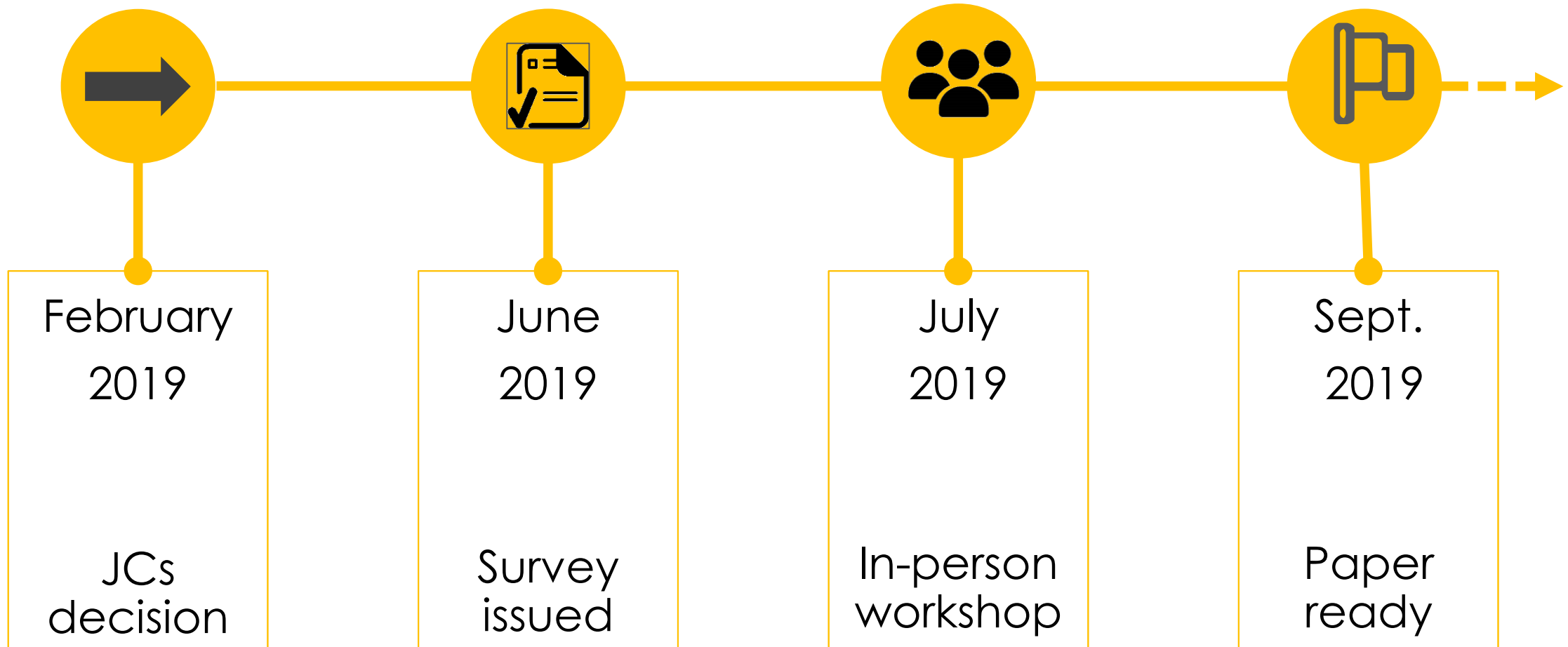
WHAT needs to be governed?

HOW should it be governed?

WHO should govern?

- 1 Identify the elements of the DI landscape that need oversight and governance
- 2 For the elements determined to require governance, identify how they should be governed;
- 3 Determine who is accountable, who should be responsible for the governance. Identify existing or new oversight bodies (public, private, joint, independent)

Approach



Survey: 26 responses

Federal Government

- TBS
- IRRC
- ISED
- ESDC
- CRA
- Public Services and Procurement Canada
- Immigration and Refugee Board of Canada

Provinces & Territories

- Ontario * 2
- Nova Scotia
- British Columbia
- New Brunswick
- Alberta
- Northwest Territories
- Saskatchewan
- Quebec
- Newfoundland & Labrador

Private Sector

- DIACC
- Price Waterhouse Coopers
- Biometric Signature ID
- 2 keys
- Vancouver City Savings Credit Union (Vancity)
- Manulife
- Interac

Other

- VSO - BC
- Canada Health Infoway

Survey

- Survey was broadly distributed to both public and private sector organizations
 - deliberately designed around open-ended questions
 - thoughtful and in-depth responses, providing a rich source of material for the in-person workshop
 - analysis and synthesis of key themes and options; no mathematical reporting of findings
 - summary and detailed report shared with all workshop participants

What should be governed?

8 areas identified

1. Setting the rules for onboarding

Overarching standards & conformance criteria

core standards and criteria for Canadian digital identities

Privacy, notice & consent

authority to collect, record keeping, sharing data

Data management & protection

collecting, compiling, aggregating, storage & retention

2. Recognizing trusted entities

Being an issuer, network provider or service provider

how organizations are recognized as trusted entities

3. Governing the operational processes

Creating a digital identity

Issuance, enrollment and ensuring equal access for all

Using a digital identity

authentication, authorization, attribute exchange, propagation

Managing digital identities

managing the digital identity lifecycle, complaints & revocation

Misuse & breaches

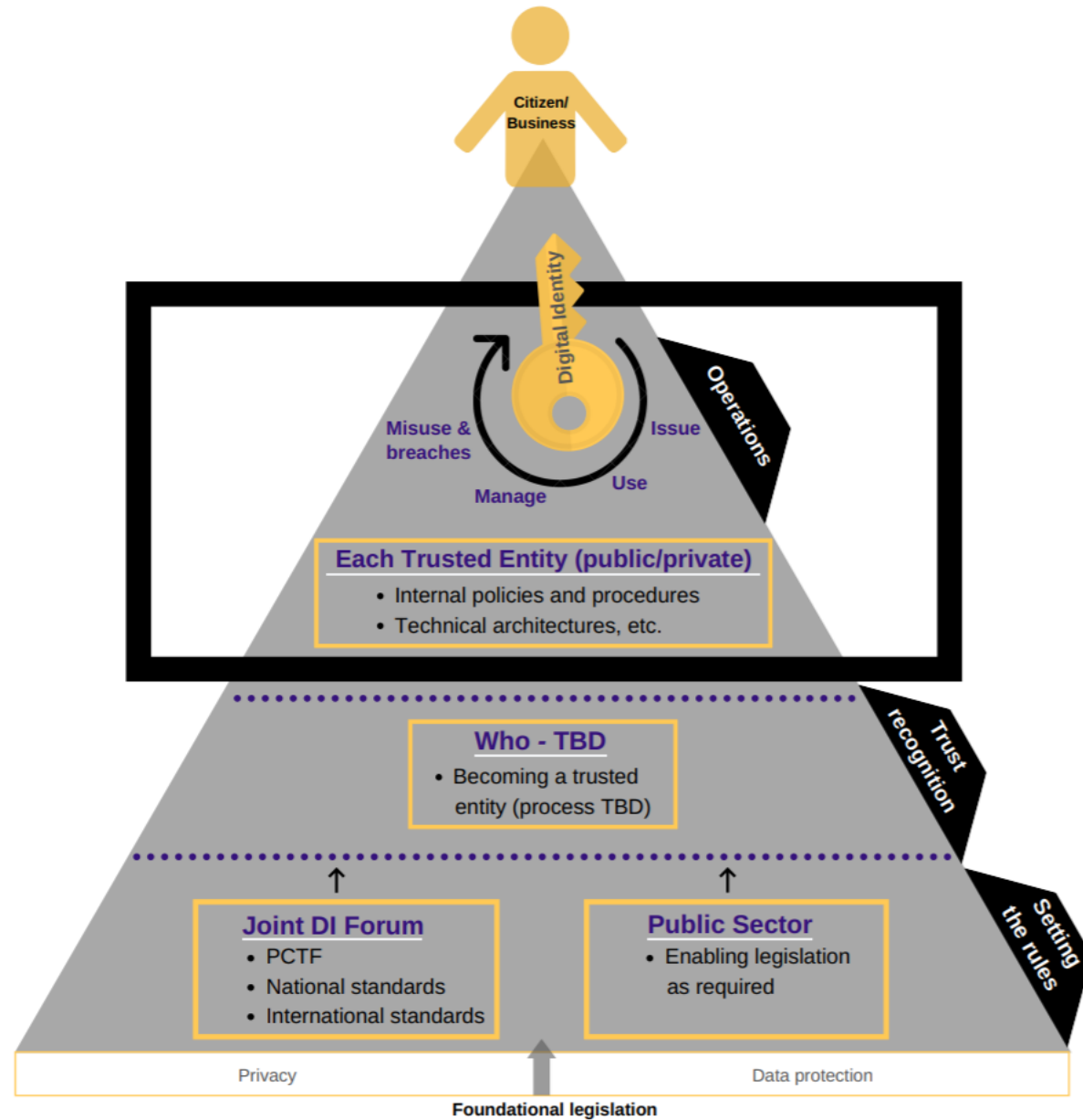
notification, remediation and penalties

Framework design principles

The governance framework should...

- be sufficient to safeguard the integrity of digital identities.
- be a coalition of the willing and be authoritative to those who adopt
- leverage existing frameworks to enable true interoperability
- ensure that individuals are in control of their own data to the limits of the law
- allow service providers to determine who they will trust
- be capable of evolving and scaling
- use clear incentives to drive user behaviour

The governance framework



Summary of key recommended accountabilities

Public Sector

- No change to accountability for privacy and security legislation
- Any enabling legislation required for jurisdictions to issue DIs
- VSOs and IRCC continue to issue foundational identities
- Internal policies, program design and technology and architectural decisions

Joint Public and Private

- Pan-Canadian Trust Framework and other required standards
- Legislative barriers
- Legislation and policy interpretation
- Central registry of trusted entities
- Change management and communications hub
- International standards liaison
- Escalated complaints

Private Sector

- Internal policies, program design and technology and architectural decisions

TBD: Accountability and process for the recognition of trusted entities.
Recommend: Joint Forum discuss and bring back to JCs for decision

Structure recommendations

- Joint Public-Private DI Forum: A refreshed DIACC
 - Revise cost structure to ensure there are no financial barriers to participation and all jurisdictions are able to participate
 - Public sector representatives must also represent Vital Statistics and Driver Licence programs
- Public Sector DI Lead for each jurisdiction: A new jurisdictional focus
 - A designated lead within each jurisdiction with the authority to represent the jurisdiction on digital identity
 - undertake a policy and legislative review to understand how the jurisdiction can become an issuer of digital ID
 - able to represent the jurisdiction with the confidence of the jurisdictions' senior executive
 - responsible for consulting and integrating perspectives from jurisdictional registrar and vital statistics organizations
 - capable of addressing topics such as program delivery models, service delivery models, their enablement in legislation, policy and the logistics
- Public Sector Forum: A reframed IMSC
 - Re-scoped to align with the role of the joint forum
 - Focus on the challenges associated with jurisdictional readiness and ability to be an issuer of Dis
 - Re-constituted with the DI leads as the members

Other recommendations

- Legal Identities
 - VSOs and IRCC pursue issuing digital birth certificates and immigration documents and ensure that each individual only has one identity
- Assessment by Jurisdictions on Readiness to Issue
 - Each jurisdiction conducts an assessment of its readiness to issue digital identities and includes a legislative review to identify the need for changes
- Institute for Citizen-Centred Service
 - ICCS be mandated to lead discussions with DIACC and negotiate changes to the DIACC membership fee structure needs to be revisited to ensure barrier-free access for all jurisdictions
- JCs Declaration on Digital Identity
 - JCs Declaration should be reviewed and updated to reflect this significant step forward
- Continuing In-Person Workshops at this level
 - Joint in-person workshop to be convened every quarter.

Digital Readiness Survey to Inform the Recommendations

- Survey was distributed to JC members.
- Responses were received from 23 jurisdictions (8 federal, 11 provincial/territorial, and 4 municipalities).

Six components assessed:

1. Clear and coherent digital strategy
2. User focus and client engagement
3. Innovative and collaborative culture
4. Workforce development
5. Investment procurement strategy
6. Performance measurement

Definitions:

Maturing- program established and presence is stable.

Developing- some capacity in place but further development expected.

Early- still under development with start-up capacity. Capabilities are underway.

Digital Readiness to advance Digital Identity

2019 Jurisdictional Readiness Results

- **Provinces and territories show the highest maturity in digital government**, followed by federal jurisdictions, then municipalities;
- Overall indication that **jurisdictions have a greater awareness of digital government and better understanding of digital readiness today than in 2016**;
- **Culture, lack of resources, keeping pace with technology, and no clear authority/mandate** were identified as **top risks** in pursuing digital transformation
- **Horizontal integration, governance, enabling legislation, as well as agile procurement** were identified as **top future considerations** for digital transformation

Digital Readiness to advance Digital Identity Implications

- **Further collaboration between all jurisdictions is needed to** increase overall understanding of digital government and **bridge the gap in digital readiness across jurisdictions;**
- **Federal and provincial jurisdictions show greater maturity** in strategy, innovation and collaboration, workforce development, and digital investment **which points to resource capabilities to advancing the Digital ID Governance Framework;**
- **Strong consensus** that **governance is a key consideration to advancing** digital government, including **digital identity**. This reemphasizes the **need for a Digital ID Governance Framework for Canada.**

Next Steps

- Approve the recommended governance framework
- Immediate
 - Direct ICCS to negotiate with DIACC to establish a barrier-free joint forum
 - Encourage each jurisdiction to assign a designated DI Lead (1 month)
 - Request VSO and IRCC to commence work towards issuing digital foundational identities
 - Direct DI priority co-leads to organize an in-person workshop with DI leads to build implementation plan and support assessments, with goal of reporting back at February JCs in-person meeting
- When DI Leads identified
 - Encourage each jurisdiction to conduct readiness assessments
- When DI Leads and re-framed DIACC in place
 - Direct IMSC Co-chairs and DI priority co-leads to re-fresh IMSC ToR



Questions?

Thank you!