

ICANN 75 KUALA LUMPUR

Digital Identity & Emerging Identifier Technologies

September 21, 2022

Presented By
Jacques Latour
Chief Technology and Security Officer
Canadian Internet Registration Authority

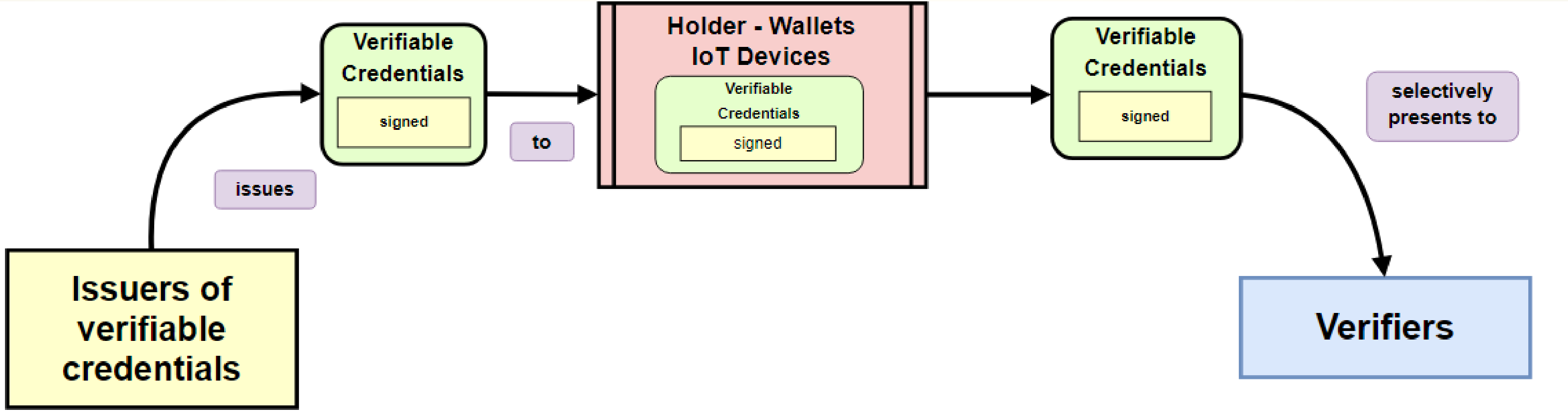


Copyright © 2022 Canadian Internet Registration Authority (“CIRA”). All rights reserved. This material is proprietary to CIRA, and may not be reproduced in whole or in part, in either electronic or printed formats, without the prior written authorization of CIRA.

DIGITAL IDENTITY AND VERIFIABLE CREDENTIALS

Verifiable Credentials, from a driver's license to a university diploma

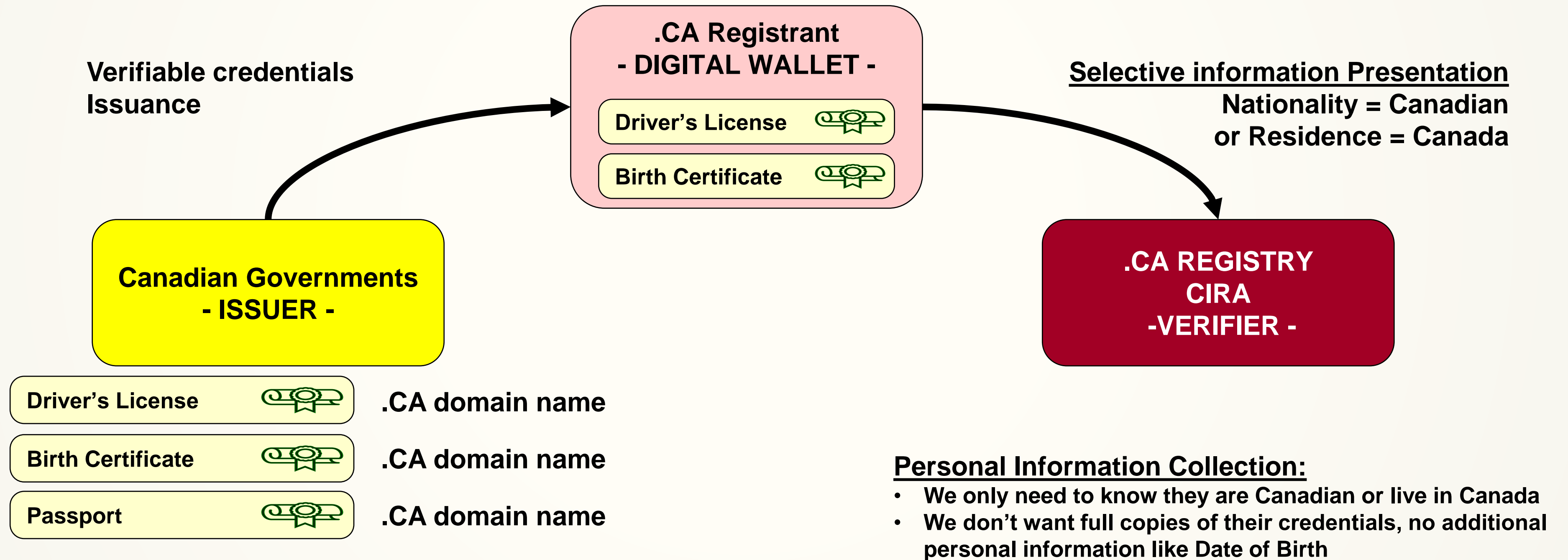
WWW.CIRA.CA



LET'S LOOK AT A REALISTIC USE CASE (IN THE NEAR FUTURE)

CIRA – Canadian Presence Requirement Verification Process

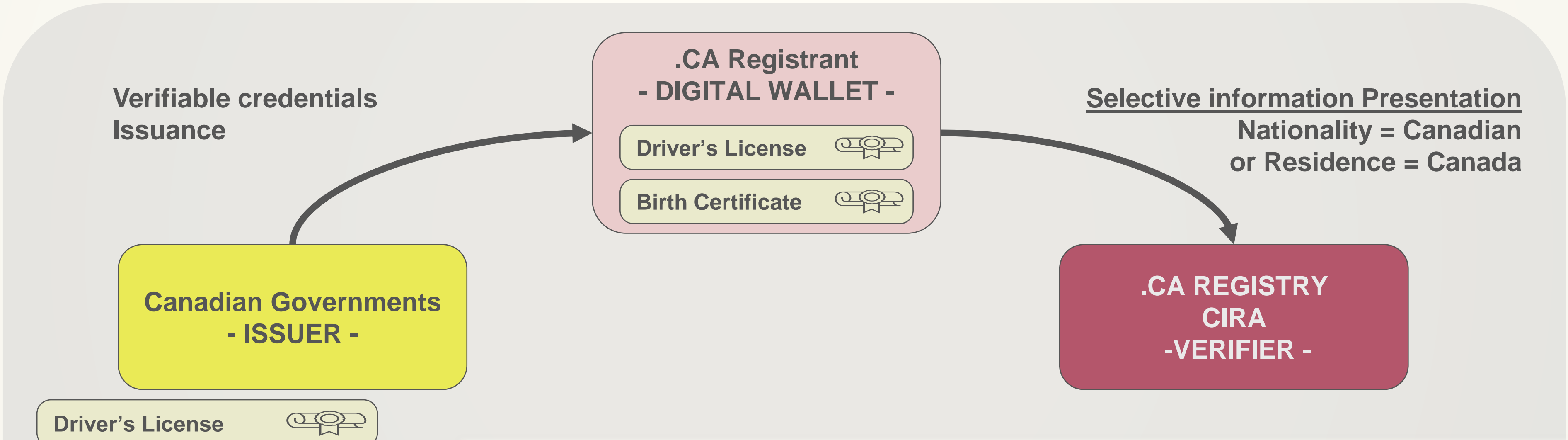
WWW.CIRA.CA



LET'S LOOK AT A REALISTIC USE CASE (IN THE NEAR FUTURE)

CIRA – Canadian Presence Requirement Verification Process

WWW.CIRA.CA



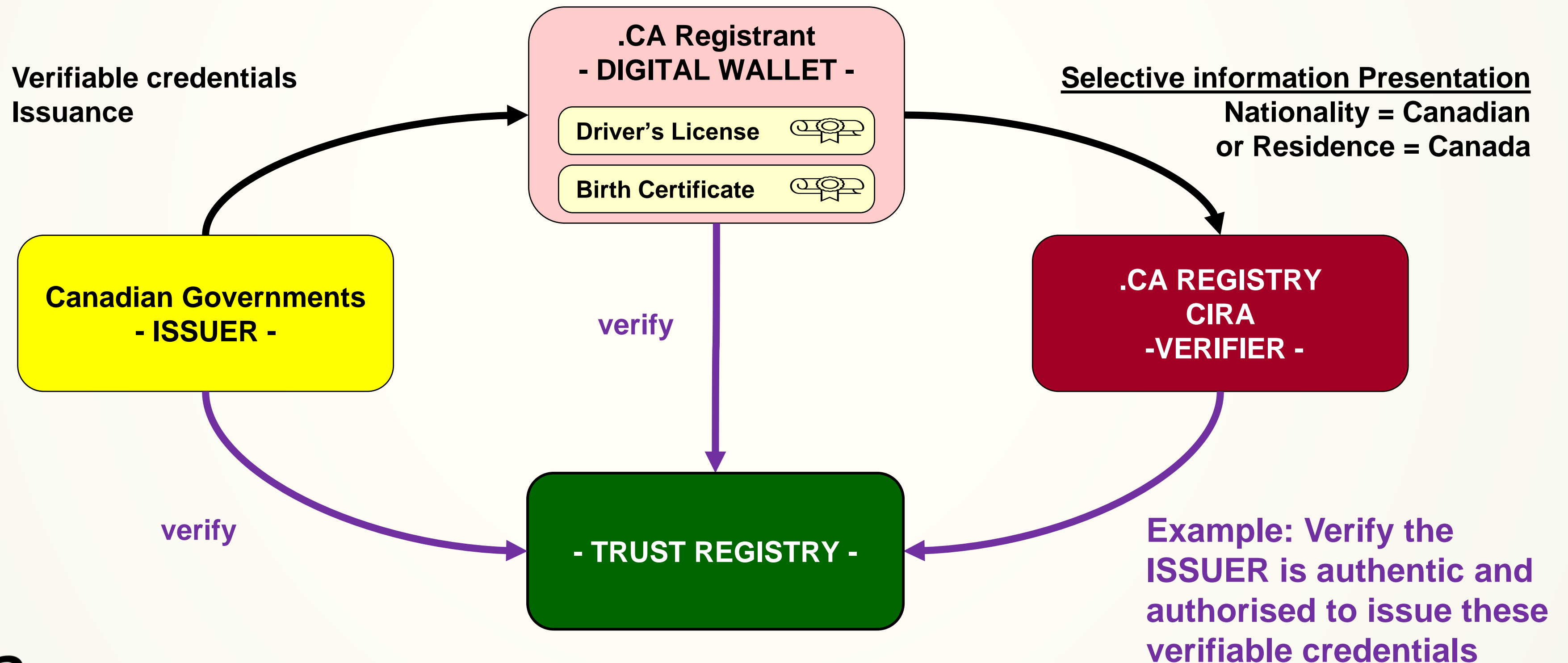
How do you know if the:

- **Issuer** is trusted to **issue** these verifiable credentials?
- **Wallet** is trusted to **hold** these verifiable credentials?
- **Verifier** is trusted to **view** these verifiable credentials?



TRUST REGISTRY

A key component of the digital identity ecosystem



WWW.CIRA.CA

DEFINITION OF A TRUST REGISTRY

Also known as a Member Directory, Repository or Trust Hubs

It's a **network service** that enables the **governing authority** for an ecosystem governance framework (EGF) to specify what **governed parties** are **authorized** to perform what actions under the EGF*

Trust Registry:

- **Defined Scope** (i.e. Ecosystem: **Academia** - Canadian Universities)
- **Governing Authority** (i.e. Canadian University **Certificate/Diplomas** as Verifiable Credentials)
- **Governance Model** (i.e. Canadian Universities **Association**)
- **Governance Model** (i.e. All **accredited** Certificate/Diplomas Canadian Universities)

TRUST REGISTRY

We're going to have 100s of Trust Registries just in Canada...

Canadian Academia
- TRUST REGISTRY -

Canadian Bar
Association
- TRUST REGISTRY -

Canadian Fishing
Association
- TRUST REGISTRY -

Canadian
Certified Electricians
- TRUST REGISTRY -

Canadian
Health Card
- TRUST REGISTRY -

Canadian
Certified Electricians
- TRUST REGISTRY -

Canadian
Medical Association
- TRUST REGISTRY -

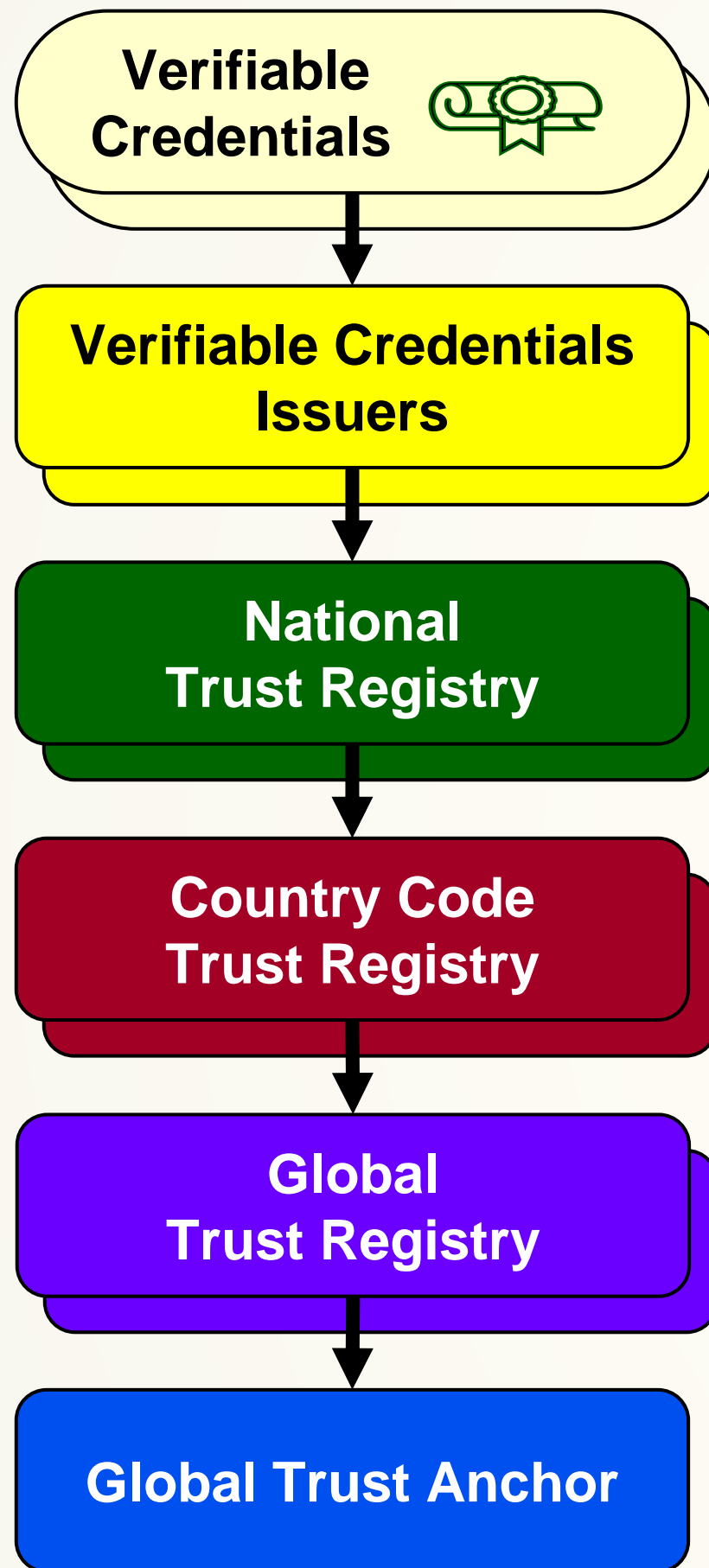
Canadian
Colleges
- TRUST REGISTRY -

Canadian Fundamental
Verifiable Credentials
- TRUST REGISTRY -

EMERGING IDENTIFIERS TECHNOLOGIES

Unique “Digital Identity” identifiers and global interoperability

WWW.CIRA.CA



Now is the time to think on having:

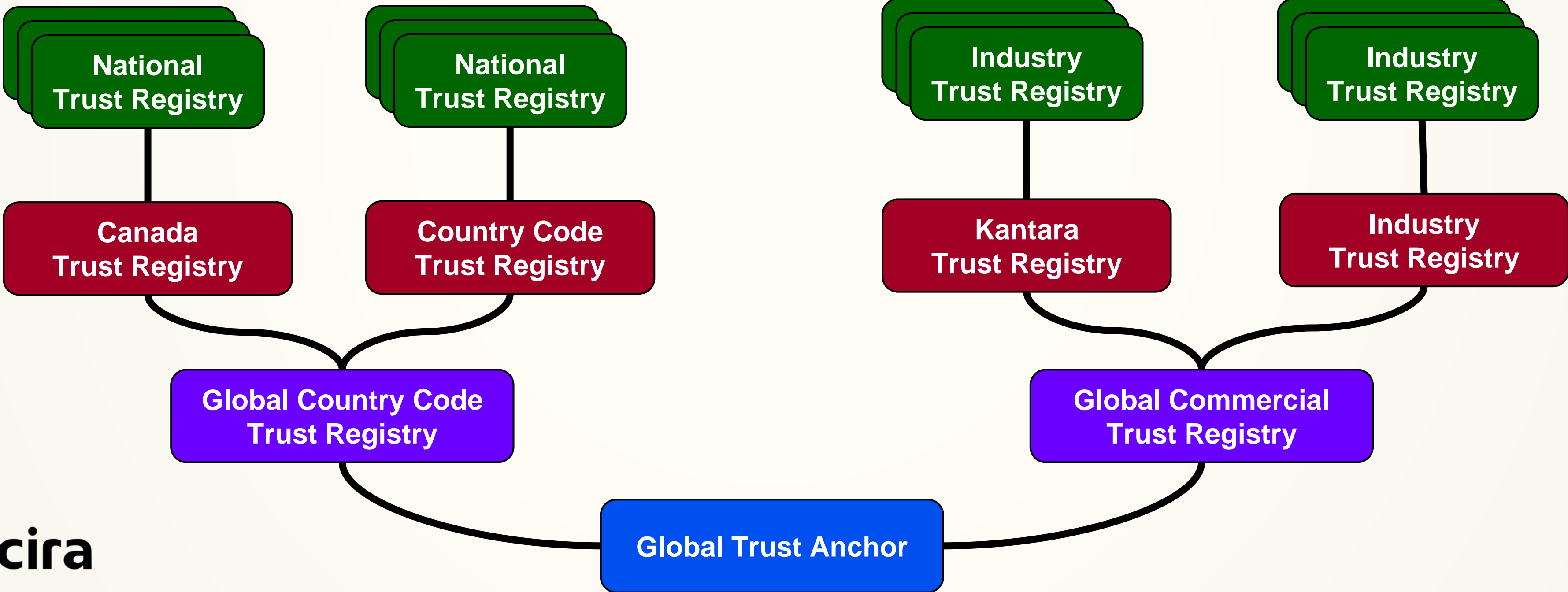
- **A global interoperable identifier structure**
- **Global unique identifiers for verifiable credentials**
- **DNS could be used for the fundamental VC issuers**
 - National ID, Driver’s License, Passport, Health Card
- **Leverage DNSSEC to verify the authenticity verifiable credentials since they have unique DNS domain name**

EMERGING IDENTIFIERS TECHNOLOGIES

This is how we see the future 😊

Leverage the current DNS unique identifier infrastructure!

WWW.CIRA.CA



LEVERAGE DNS & DNSSEC FOR DIGITAL IDENTITY

Ensure Digital Identity Unique Identifiers by using the DNS

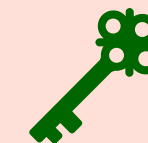
Verifiable Credentials include a Digital Identity Documents (DID) cryptographically **signed** by the issuer and linked to a **Domain Name**

VERIFIABLE CREDENTIALS | **Signed** | Digital Identity Document (DID)

University Diploma Schema



A domain name (i.e. vc.example.ca)



a public key to verify

Need to develop mechanisms in the DNS and DNSSEC to:

- Find the Trust Registry associated to a verifiable credential issuer
- Find if the issuer is registered with a Trust Registry
- Find Digital Identity Document (DID) details from a domain name



Thank You



<https://www.cira.ca>

Supporting Technical Slides For Reference

VERIFYING THE ISSUER AUTHENTICITY

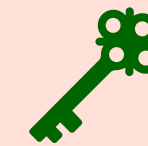
Using DANE TLSA to verify the authenticity the Issuer

VERIFIABLE CREDENTIALS | Signed | Digital Identity Document (DID)


University Diploma Schema



A domain name (i.e. **vc.example.ca**)



a public key to verify

- The public key can be extracted from DNS TLSA queries to verify the **authenticity** of the verifiable credential **issuer**
 - PKIX-TA | CERT | FULL = 0 0 0
 - **vc.example.ca** TLSA (0 0 0) Signer Public Key Certificate 

Authenticate  with 

VERIFYING THE ISSUERS TRUST RELATIONSHIP – STEP 1

Identifying the Trust Registry the Issuer is affiliated with

VERIFIABLE CREDENTIALS | Signed | Digital Identity Document (DID)

University Diploma Schema



A domain name (i.e. **vc.example.ca**)



a public key to verify

- Proposing a method for an **issuer**, a **verifier** or another **trust registry** to **prove** their trust registry **affiliation** via the **DNS**
 - **<TR>** RRTYPE (urg, another...)
- Example:
 - **vc.example.ca TR trust-registry.ca**
 - **vc.example.ca TR academia-trust-registry.ca**
 - **trust-registry.ca TR global-country-code-trust-registry.org**

VERIFYING THE ISSUERS TRUST RELATIONSHIP – STEP 2

Determining if the Issuer is registered with a Trust Registry

VERIFIABLE CREDENTIALS | Signed | Digital Identity Document (DID)

University Diploma Schema



A domain name (i.e. **vc.example.ca**)



a public key to verify

- Proposing a method to verify if an **issuer**, a **verifier** or another **trust registry** is **registered** with a trust registry via the **DNS**
 - **<_trustregistry>** label (yes, just a label !! :-)
- Examples:
 - vc.example.ca._trustregistry.trust-registry.ca** TLSA (0 0 1) <- hash of public key
 - vc.example.ca._trustregistry.academia-trust-registry.ca** TLSA (0 0 1)

PROPOSAL FOR GLOBAL CHAIN OF TRUST FOR TRUST REGISTRIES

From a verifiable credential, you can find the issuer and associated trust registries all the way to a Trust Registry trust anchor in the root zone

```
vc.example.ca. TLSA( 0 0 0 ) signer Public Key
```

```
vc.example.ca. TR trust-registry.ca
```

```
trust-registry.ca. TLSA( 0 0 0 ) signer Public Key
```

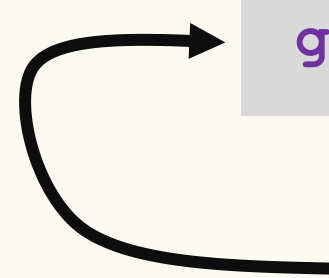
```
vc.example.ca._trustregistry.trust-registry.ca. TLSA( 0 0 1 ) hash of Signer Public Key
```

```
trust-registry.ca. TR global-trust-registry.org
```

```
global-trust-registry.org. TLSA( 0 0 0 ) signer Public Key
```

```
trust-registry.ca._trustregistry.global-trust-registry.org. TLSA (0 0 1 ) hash of Signer Public Key
```

```
global-trust-registry.org_trustregistry. TLSA (0 0 1 ) hash of Signer Public Key
```



This would be a root zone trust anchor for a global trust registry