DIACC CCIAN

Decentralized Identity and DIACC PCTF Authentication

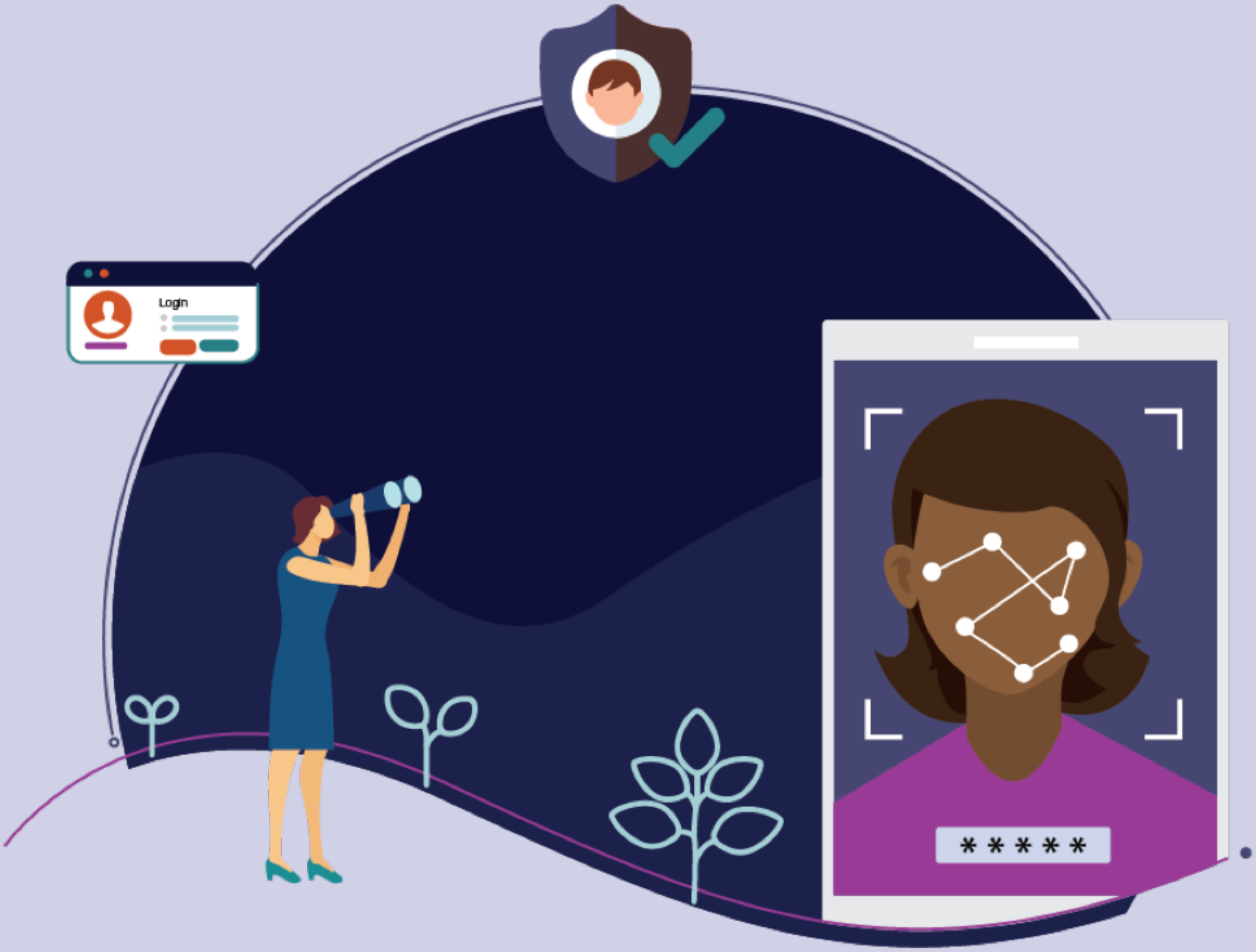


Table of Contents

This paper is a product of a DIACC Innovation Expert Committee innovation initiative. The content of this paper has been supported by DIACC members 2Keys, Applied Recognition, and the Digital Identity Laboratory of Canada with contributions by members of the DIACC's Innovation and Trust Framework Expert Committees.

This paper is a product of a DIACC Innovation Expert Committee innovation initiative. The content of this paper has been supported by DIACC members 2Keys, Applied Recognition, and the Digital Identity Laboratory of Canada with contributions by members of the DIACC's Innovation and Trust Framework Expert Committees.

1. About the DIACC

Created as a result of the federal government's Task Force for the Payments System Review, the Digital ID & Authentication Council of Canada **(**DIACC**)** is a non-profit coalition of public and private sector leaders who are committed to developing a Canadian digital identification and authentication framework that will secure Canada's full and secure participation in the global digital economy.

DIACC innovation papers focus on current issues and opportunities in the digital identity ecosystem. DIACC innovation papers are guided by the DIACC's 10 Digital ID & Authentication ecosystem principles and by the priorities of DIACC members. DIACC papers provide insights to business, legal, and technical audiences in Canada and around the world. DIACC papers are not endorsements and do not represent a qualified organization opinion of the DIACC. DIACC innovation papers are pragmatic and address real-world issues; are open and transparent; vision future opportunities; communicate learning from past projects; are authored by DIACC member domain experts with real-world expertise.

This innovation paper was developed by the DIACC's Innovation Expert Committee (IEC) to address comments received during a public review of the DIACC Pan-Canadian Trust Framework™ (PCTF) Authentication component. This paper shares thoughts as to why the DIACC PCTF Authentication Version 1.0 component is relevant in the context of decentralized or Self-sovereign identity approaches. Version 1.0 will be a bridging document until DIACC delivers the next version of the Authentication component and this paper helps to revise content to properly reflect the emerging model of Decentralized Identity.

This paper is a product of a DIACC Innovation Expert Committee innovation initiative. The content of this paper has been supported by DIACC members 2Keys, Applied Recognition, and the Digital Identity Laboratory of Canada with contributions by members of the DIACC's Innovation and Trust Framework Expert Committees.

2. About the Supporting Members

2Keys: Andrew Johnston is the Vice President, Standards Development and Industry Relations at 2Keys, Co-Chair of the DIACC’s Trust Framework Expert Committee, and member of the DIACC’s Innovation Expert Committee. 2Keys are a national leader in enabling secure digital experiences for Canadian governments, financial institutions and commercial clients.

Applied Recognition: Don Waugh is the Founder and Chief Evangelist for Applied Recognition as well as a member of the DIACC’s Innovation Expert Committee. Applied Recognition is a leader in face recognition for identity and recognition technology that our clients use to build innovative apps, products and services for their customers.

Digital Identity Laboratory of Canada: Pierre Roberge is co-founder and General Manager of the Digital Identity Laboratory of Canada and member of the DIACC’s Innovation Expert Committee. The Digital Identity Laboratory of Canada is an independent not-for-profit entity that offers a full range of evaluation, testing, and certification services for digital identity solutions regarding their compliance and interoperability.

This paper is a product of a DIACC Innovation Expert Committee innovation initiative. The content of this paper has been supported by DIACC members 2Keys, Applied Recognition, and the Digital Identity Laboratory of Canada with contributions by members of the DIACC's Innovation and Trust Framework Expert Committees.

3. Executive Summary

Decentralized Identity is an approach that is emerging to address digital identity problems -- knowing and recognizing people using services delivered through the Internet.

The Authentication component of the DIACC Pan-Canadian Trust Framework™ specifies processes and conformance criteria for service providers. Authentication and credential management services may be assessed against these criteria.

The name “Authentication” may suggest a common “login page” experience – with a username and password form -- and the idea of a “login service provider” – e.g., “login with Google”. However, the conformance criteria of the Authentication component deliberately avoid requiring a particular user experience or technology. Thanks to feedback from public reviews of the Authentication drafts, the component is applicable to service provider relationships that do not require a centralized service intermediary for interoperable online service delivery.

While the Authentication component may have been mostly developed before Decentralized Identity approaches emerged, this document demonstrates that Authentication is applicable in the context of Decentralized Identity systems and encourages service providers not to lose sight of good security practice even in the face of new approaches.

This paper is a product of a DIACC Innovation Expert Committee innovation initiative. The content of this paper has been supported by DIACC members 2Keys, Applied Recognition, and the Digital Identity Laboratory of Canada with contributions by members of the DIACC's Innovation and Trust Framework Expert Committees.

4. Introduction

4.1 Audience for this document

This document may be of interest to members of the DIACC Trust Framework Expert Committee, other members of DIACC interested in the work on the Authentication components, and members of the public who asked questions and provided their thoughts as part of the public reviews of the Authentication Discussion Draft and the Authentication Draft Recommendation.

4.2 Scope

This document will illustrate an alignment between a Decentralized Identity approach with the roles and requirements of the Authentication component of the DIACC Pan-Canadian Trust Framework™ (PCTF). It will also provide a discussion of specific definitions, roles, and requirements that are most relevant to understanding Authentication in the context of Decentralized Identity.

4.3 Terminology

This document uses the term “credential” in the sense defined in the Authentication Component Overview Final Recommendation, section 2.1. The terms “verify” and “verified” are used as in other components of the PCTF, such as Verified Person. Please also see the PCTF Glossary, section 2.2.

This document uses the term “Decentralized Identity” to refer to approaches to digital identity challenges that do not absolutely require a single, central, enabling service provider. The term “self-sovereign identity” is also used to refer to such approaches, normally with greater emphasis on an end-user’s autonomy to use their digital identity credentials. Such approaches have been described as providing users with similar flexibility and agency as physical credentials (e.g., driver’s license, passport) provide. As used in this document, references to “Decentralized Identity approaches” are intended to include “self-sovereign identity approaches”.

Contrast decentralized approaches with federated approaches, where a service provider must be accepted into a federation before users may access its services with their credentials.

4.4 References

This paper is a product of a DIACC Innovation Expert Committee innovation initiative. The content of this paper has been supported by DIACC members 2Keys, Applied Recognition, and the Digital Identity Laboratory of Canada with contributions by members of the DIACC's Innovation and Trust Framework Expert Committees.

For a more comprehensive view of Decentralized Identity and those organizations involved in its continued development, please see the work of the Trust Over IP Foundation, Decentralized Identity Foundation (DIF), the W3C DID Working Group, the W3C Verifiable Credentials Working Group, the W3C Credentials Community Group, and their respective members.

For more on DIACC and its Pan-Canadian Trust Framework™ (PCTF), please visit their website. The Authentication component Overview and Conformance Criteria documents are publicly available.

4.5 Decentralized Identity

Decentralized Identity is an emerging approach that has attracted the attention of service providers looking to improve their online service experiences. The intent of the Authentication component of the DIACC Pan-Canadian Trust Framework™ is to guide service providers to implementations that conform to industry standards and good practices.

Decentralized Identity systems promise to enable digital identity interactions with privacy-preserving characteristics that have been impractical with other approaches to digital identity, such as those that rely on trusted intermediaries. This document will discuss the implications of a Decentralized Identity approach on the DIACC Pan-Canadian Trust Framework™ (PCTF), in support of implementations of trustworthy and accessible digital identity solutions.

5. Purpose of the Authentication Component

The purpose of PCTF components is to support assessments of quality and suitability of processes implemented by a service provider for the information and confidence of the service provider's customers or customer prospects. (See Appendix A for some examples of potential service provider opportunities.)

From the Model Overview, the Objectives (section 2.3) of the Pan-Canadian Trust Framework™ include:

1. Defining participant roles and functions within the ecosystem. [...]
2. Facilitating interactions within the ecosystem by defining requirements and guidelines that establish a level of trustworthiness for processes performed by ecosystem participants. [...]

The Authentication component aims to identify the participant roles in the use of authentication services, and the responsibilities of each participant role with respect to processes required to provide authentication services.

The premise of this paper is that these role definitions, and corresponding process responsibilities, are applicable in the face of the apparently new architectures suggested by Decentralized Identity approaches.

6. Conceptual Elements of Decentralized Identity

There is no accepted definition of "Decentralized Identity", but there are common conceptual components that appear in descriptions of such systems.

Key conceptual elements of a Decentralized Identity system include:

- **Decentralized Registry –** a mechanism to make the Decentralized Identity Documents (DID Documents) of Issuers available to Verifiers
- **Decentralized Identifier (DID)** – "a globally unique persistent identifier that does not require a centralized registration authority" - W3C Decentralized Identifiers (DIDs) v1.0
- ***DID Document*** **–** data that can be used to verify that a Proof contains claims issued by a specific Issuer, and that these claims accurately represent the claims issued as Verifiable Credentials
    - The Authentication component would refer to this as "Authenticator Validation Data"
- **Issuer** – an entity that creates, maintains, and issues Verifiable Credentials, and that publishes at least one DID Document to a Decentralized Registry
- **Verifier –** an entity that accepts and validates Proofs, and retrieves DID Documents from a Decentralized Registry to perform additional validation
- **Subject –** an entity to whom, and about whom, Verifiable Credentials are issued
- **Agent –** a service that accepts Verifiable Credentials on behalf of a Subject, and presents Proofs, derived from Verifiable Credentials, to Verifiers on behalf of a Subject
- **Authorizer** – a service that authenticates a user of an Agent service as the Subject, or an authorized representative of the Subject, of Verifiable Credentials to be used by an Agent to create Proofs
- ***Verifiable Credential*** – a set of one or more claims made by an Issuer about a Subject, for which the authenticity and issuer can be verified, and can be used by Agents to create Proofs

    - The Authentication component would refer to this as a "Credential"
- ***Proof*** – data derived from Verifiable Credentials about a Subject that can be provided by an Agent to a Verifier for validation, for which the authenticity and Issuer can be verified
    - The Authentication component would refer to this as a "Credential"

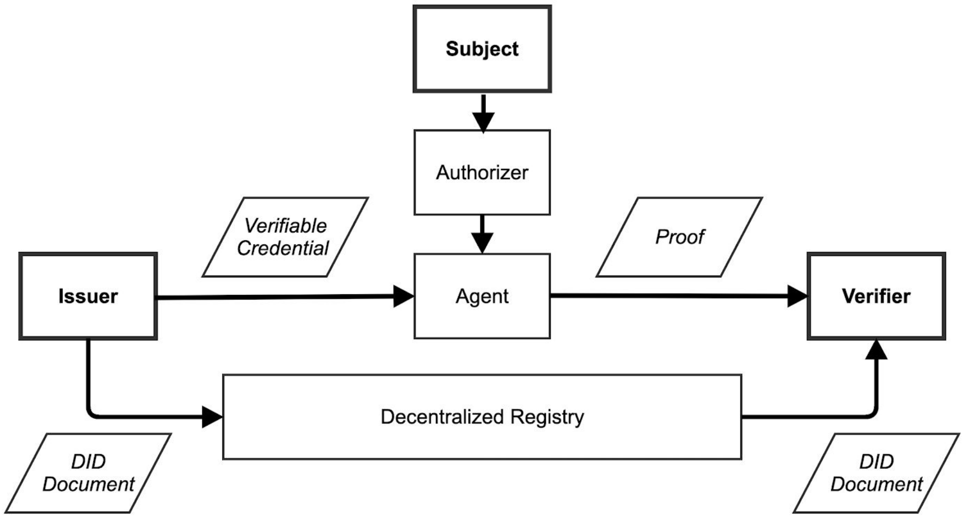


Figure 1: Key conceptual elements of a Decentralized Identity system

The exchange of data, as represented by the arrows in Figure 1, aligns with trusted processes identified in Authentication, particularly Credential Issuance, and Authentication, as Section 5 will illustrate.

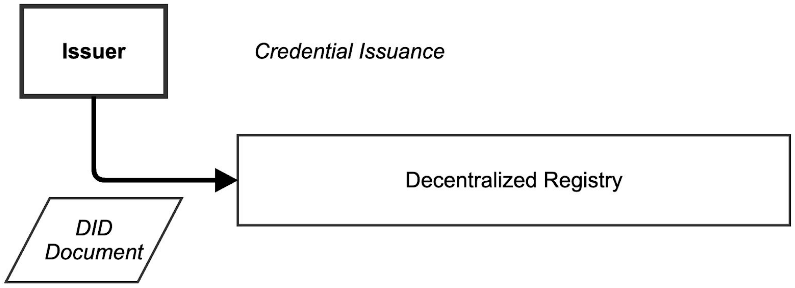
NOTE: This model is a somewhat simplified version of the common model used to describe participants in a Decentralized Identity system. In particular, the idea of a Holder, a person (or business) to whom Verifiable Credentials may be issued on behalf of a different Subject (e.g., parent on behalf of a minor child, or an employee on behalf of a business entity) has been omitted to simplify the arguments presented here; this model assumes that the Holder of a credential – the person (or business) who holds and controls a credential – is the Subject of that credential. Models that include the concept of Holders would still find relevance in the Authentication component for the reasons described here. They may also rely on one or more credentials documenting a recognized or required relationship between a Holder and a Subject.

7. Conceptual Alignment to Authentication Processes

As we look at data and exchanges shown in Figure 1, we can identify alignment to the processes described in Authentication. These steps are intended to identify conceptual processes in a Decentralized Identity system.

NOTE: Appendix B (section 10) identifies and discusses this alignment by relying on specific conformance criteria from Authentication.

7.1 Issuer publishes a DID Document about itself to a Decentralized Registry

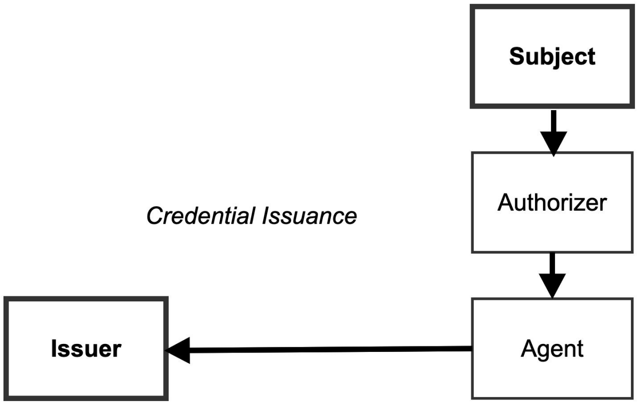


An Issuer creates its own credential, binds an authenticator to that credential, and publishes a DID Document to a Decentralized Registry. This aligns well with the Credential Issuance process, with the slightly unusual characteristic that the Issuer is also the Subject of that credential. (This step would typically be done together with, or entirely by, some authority responsible for admission to a centralized identity system.)

The operators of a Decentralized Registry may be responsible for enforcing policies that may allow them to accept or reject a DID Document registration, in support of the stated goals and interests of the Decentralized Registry. The application of such policies may require an Issuer's identity to be verified. This step would likely depend then on an implementation of the Authentication process.

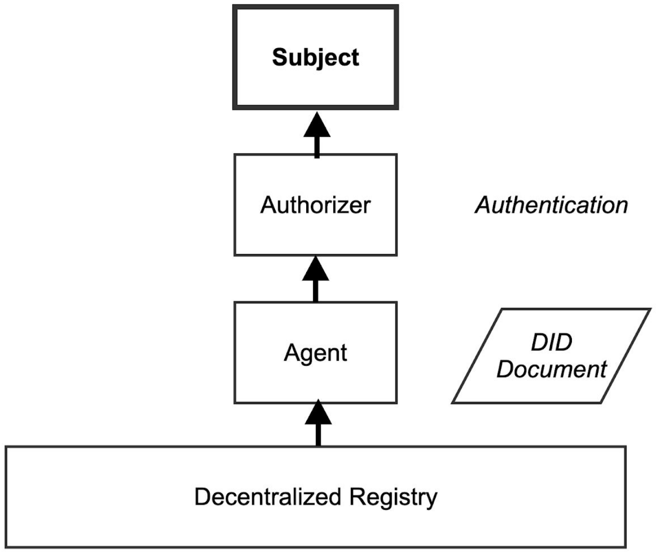
NOTE: The verification of an Issuer's identity also aligns well with processes in other PCTF components such as Verified Person and Verified Organization.

7.2 Subject connects to Issuer via an Agent



A connection between a Subject's Agent and Issuer is established, with the creation of Authenticators (typically private keys) and the sharing of Authenticator Validation Data (typically, corresponding public keys). The Issuers and Agent each bind this data to information about the other party. This aligns to the Credential Issuance process, even though verified identity information may not yet have been exchanged.

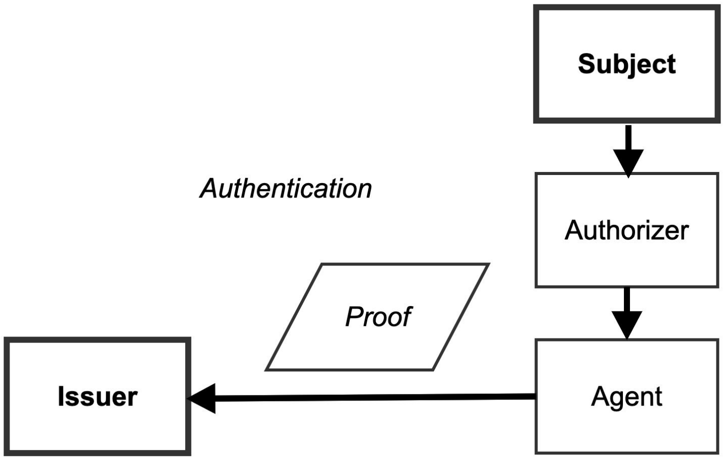
7.3 Subject authenticates Issuer via an Agent



Once such a connection is established, a Subject may choose to verify an Issuer in some trusted context. A Subject's Agent may retrieve an Issuer's DID Document from the Decentralized Registry, or accept a Proof of an Issuer's identity from the Issuer's Agent. This verification would depend on an implementation of Authentication.

NOTE: The verification of an Issuer can be aligned with processes in other PCTF components such as Verified Person and Verified Organization.

7.4 Issuer authenticates Subject

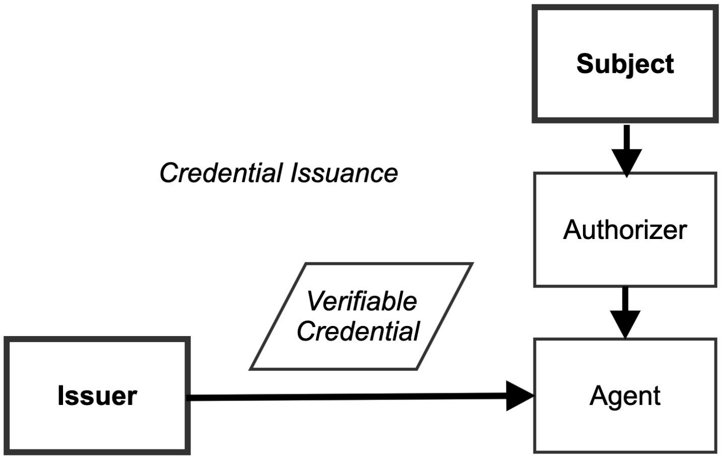


Verifiable Credential to that Subject and ensure that the Issuer's connection is bound to the same Subject. This is another example of an Authentication process implementation.

By performing this verification, an Issuer's Agent depends on an implementation of the Authentication process. This may be done, for example, by accepting a Proof from a Subject's Agent.

NOTE: The verification of a Subject can be aligned with processes in other PCTF components such as Verified Person and Verified Organization.

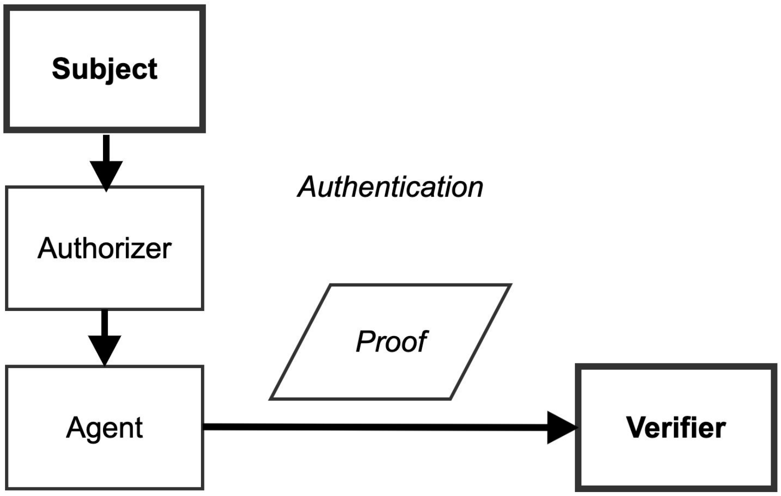
7.5 Issuer provides a Verifiable Credential to a Subject via an Agent



Having verified the identity of a Subject in an appropriate context and confirmed that the provided Authenticator Validation Data – for example, a public key used by a Subject and/or its Agent – is bound to the Subject, an Issuer may issue a Verifiable Credential per the Credential Issuance trusted process.

Note that this Credential Issuance transaction leverages the connection, established in Step 2, to establish a trusted communication session between an Issuer's Agent and a Subject's Agent. This kind of session could be assessed against the conformance criteria of the Authenticated Session Initiation and Authenticated Session Termination processes.

7.6 Subject provides a Proof to a Verifier via an Agent



A Subject may now present a Proof, derived from Verifiable Credentials, to a Verifier as part of an Authentication trusted process.

As with Issuer and Subject, a Subject and Verifier will need to create, as in Step 2, a connection by exchanging authentication information. A Subject's Agent may accept a Proof from a Verifier or its Verifier Agent, another example of the Authentication process.

Note that this Proof transaction leverages the connection to establish a trusted communication session between a Subject's Agent and the Verifier's Agent. This kind of session could be assessed against the conformance criteria of the Authenticated Session Initiation and Authenticated Session Termination processes.

8. Roles and Responsibilities

Authentication defines two roles, and associates specific conformance criteria with one, or the other, or both roles. The trusted processes associated with each role are listed in the table below.

Credential Service Provider	**Authentication Service Provider**
Credential Issuance	
Credential Suspension	Authentication
Credential Recovery	(optional) Authenticated Session Initiation
Credential Maintenance	(optional) Authenticated Session Termination
Credential Revocation	

Table 1: Trusted Processes associated with each Service-Provider Role

The simplest interpretation of the interactions among the conceptual elements from Figure 1 is possible as follows:

- any conceptual element that creates and shares data (DID Documents, Verifiable Credentials, Proofs) may be assessed as a Credential Service Provider;
- any conceptual element that accepts and validates data (DID Documents, Verifiable Credentials, Proofs) may be assessed as an Authentication Service Provider;
- any conceptual element initiating Authenticated Sessions may be assessed as an Authentication Service Provider.

This simple interpretation suggests the roles for conceptual elements in Table 2.

This paper is a product of a DIACC Innovation Expert Committee innovation initiative. The content of this paper has been supported by DIACC members 2Keys, Applied Recognition, and the Digital Identity Laboratory of Canada with contributions by members of the DIACC's Innovation and Trust Framework Expert Committees.

Conceptual Element	**Conceptual Processes**	**Assess in Role**	**Rationale**
Issuer	Credential Issuance, Credential Suspension, Credential Recovery, Credential Maintenance, Credential Revocation	Credential Service Provider	Issues Credentials; Issues DID Documents
Verifier	Authentication	Authentication Service Provider	Verifies Proofs; Verifies DID Documents
Agent	Authentication, Credential Issuance, Credential Suspension, Credential Recovery, Credential Maintenance, Credential Revocation	Authentication Service Provider, Credential Service Provider	Verifies Credentials; Verifies DID Documents; Issues Proofs
Decentralized Registry	Authentication	Authentication Service Provider	Verifies DID Documents

Table 2: Assessment Roles for Decentralized Identity Conceptual Elements

Decentralized Identity systems may involve the frequent issuance and exchange of credentials, Authenticators, and Authenticator Validation Data. Separate Authenticators may be used for almost every exchange in Figure 1, requiring most conceptual elements to implement most of the trusted processes documented in Authentication, and thereby playing both defined roles, as discussed in Section 5.

9. Conclusion

This paper has demonstrated that, as a component of the Pan-Canadian Trust Framework™ designed to support the assessment of a service provider against a set of good practices, Authentication remains applicable in the context of Decentralized Identity systems, by identifying the kinds of services that implement processes from the Authentication component.

The paper advanced a simple conceptual model of key elements of a Decentralized Identity system and showed how those elements aligned with the processes documented in the Authentication component.

We have shown how the Authentication roles of Credential Service Provider, and Authentication Service Provider align with key elements of a simple conceptual model of Decentralized Identity systems. In Appendix A, we have suggested some service provider opportunities in Decentralized Identity.

In Appendix B, we have further documented how specific Authentication conformance criteria might be read in the context of Decentralized Identity systems and highlighted which such criteria may be more or less relevant in a Decentralized Identity service context.

We conclude that Authentication remains as useful and valuable a component as any other in the Pan-Canadian Trust Framework™, in any context, including Decentralized Identity and Verifiable Credentials, where a service provider is enabling or delivering identity services.

Thanks

- The Editor and members of the Authentication editing, drafting, and comment review team.
- Members of TFEC for their review and support of the Authentication PCTF component.
- Members of the public who contributed their feedback during the Authentication Discussion Draft and the Authentication Draft Recommendation review periods.

This paper is a product of a DIACC Innovation Expert Committee innovation initiative. The content of this paper has been supported by DIACC members 2Keys, Applied Recognition, and the Digital Identity Laboratory of Canada with contributions by members of the DIACC's Innovation and Trust Framework Expert Committees.

10. Glossary of Abbreviations

ASP	Authentication Service Provider
CSP	Credential Service Provider
DIACC	Digital ID & Authentication Council of Canada
DI	Decentralized Identity
DID	Decentralized Identifier
DIF	Decentralized Identity Foundation
DLT	Distributed Ledger Technology
DPKI	Distributed Public Key Infrastructure
LOA	Levels of Assurance
PCTF	Pan-Canadian Trust Framework™
PKI	Public Key Infrastructure
SSI	Self-Sovereign Identity
TFEC	Trust Framework Expert Committee
VC	Verifiable Credential
W3C	The World Wide Web Consortium

11. Appendix A: Decentralized Identity Service-Provider Opportunities

In the context of the PCTF Authentication component, service-providers implement trusted processes on behalf of, and as a service to, their customers.

As the business, legal, and technology understanding associated with Decentralized Identity systems continues to evolve, there is likely to be a significant opportunity for service providers to connect participants in the Canadian economy with Decentralized Registries.

11.1 Decentralized Registry Service Provider

A service provider may offer to host and/or manage an element of a Decentralized Registry on behalf of another entity. Decentralized Identity systems built around

This paper is a product of a DIACC Innovation Expert Committee innovation initiative. The content of this paper has been supported by DIACC members 2Keys, Applied Recognition, and the Digital Identity Laboratory of Canada with contributions by members of the DIACC's Innovation and Trust Framework Expert Committees.

distributed ledger technology (DLT) would often depend on the independence of multiple parties to ensure the ongoing integrity of the registry. These parties may choose to depend on a service provider to ensure their contribution to such a registry reflects that independence.

The services provided by a Decentralized Registry Service Provider do not directly or obviously relate to roles documented in Authentication. The policies related to a particular Decentralized Registry, however, may require such a service provider to implement the processes of an Authentication Service Provider and/or a Credential Service Provider as part of the initial set-up, and ongoing maintenance of the service. To that extent a Decentralized Registry Service Provider may be assessed against corresponding Authentication conformance criteria.

11.2 Issuer Service Provider

A service provider may offer to issue Verifiable Credentials on behalf of another entity. One may consider established issuers of paper and plastic credentials as being good candidate customers for such a service, as well as owners of existing authoritative information registries.

The Issuer concept maps well to the Credential Service Provider role in Authentication. To provide an “Issuer service”, a service provider should implement each of the Credential Issuance, Credential Suspension, Credential Recovery, Credential Maintenance, and Credential Revocation processes, and may be assessed against the corresponding conformance criteria.

A service provider implementing an “Issuer service” may also need to implement one or more Authentication processes in support of the service, and to that extent may be assessed against the corresponding conformance criteria.

11.3 Verifier Service Provider

A service provider may offer to retrieve and verify Verifiable Credentials as a service to its customers. This kind of integration service may simplify the introduction of Verifiable Credentials into existing systems and processes.

The Verifier concept corresponds very well to the Authentication Service Provider role in the Authentication. To provide a “Verifier service”, a service provider should implement the Authentication process, and may be assessed against the corresponding conformance criteria.

A service provider implementing a “Verifier service” may also need to implement one or more of the Credential Service Provider processes in support of the service, and to that extent may be assessed against the corresponding conformance criteria.

11.4 Agent/Authorizer Service Provider

A service provider may offer to operate an Agent and/or Authorizer on behalf of a Subject, which may be a person or an organization. Such a service may also be referred to as a “wallet”, or “vault” which is used to hold Verifiable Credentials, to safeguard their use only by an appropriate Subject, or an appropriate representative of such a Subject, to authorize their use in the composition of Proofs, and to compose such Proofs.

Although an Agent service may not be issuing Verifiable Credentials and may even choose not to Authenticate Verifiable Credentials (although this seems like a poor choice), the Agent service may be assessed as an Authentication Service Provider in its support of connections to Verifiers, and may be assessed as a Credential Service Provider in its composition of Proofs.

As a key element in the integrity and the trust in Decentralized Identity systems, an Authorizer service may serve as the “face” – a key provider for user experiences – of such systems. As such, the assessment of an Authorizer service against good-practice criteria like those in Authentication, is a key step in the broad adoption of Decentralized Identity systems. The criteria from the PCTF Privacy component, and the PCTF Notice & Consent component could be seriously considered in the context of an Authorizer.

As a key element in the security and integrity of Decentralized Identity systems, Providers of Agent services may pay particularly close attention to the “Subject Initiated” conformance criteria for the Credential Service Provider role to ensure their service enables its users – Subjects – to play an active role in the management and maintenance of the integrity of Verifiable Credentials. With no single centralized system or service provider with comprehensive insight into activity related to users and their credentials, users of Agent services will need to be enabled, and perhaps encouraged, to take responsibility for the security and integrity of those credentials. Providers of Agents are not absolved of their responsibility to adhere to other criteria but may require unanticipated work related to “Subject Initiated” criteria.

12. Appendix B: Conformance Criteria Context and Commentary

This section documents Decentralized Identity-specific context in select Authentication Conformance Criteria. Some additional comments are offered for consideration in the assessment of some Conformance Criteria in a Decentralized Identity system.

This document uses the reference convention as described in Section 3, paragraph 2 of the Authentication Conformance Profile Final Recommendation to refer to specific conformance criteria (e.g. "The PCTF CDIS 4"). This section presents context and commentary on specific criteria in the order in which they appear in the Authentication Conformance Profile Draft Recommendation.

12.1 Credential Issuance

The PCTF CDIS 4 conformance criterion requires Credential Service Providers (CSP) to make the state of Inaccessible Credentials and Revoked Credentials available to all Authentication Service Providers. A Decentralized Registry may include a "revocation registry" that supports this requirement.

In the case of a Revoked Credential, a Credential Service Provider could use a Decentralized Registry's revocation registry to register the revoked status of a credential. In the case of an Inaccessible Credential, a CSP could likewise use a revocation registry to revoke the Inaccessible Credential and create a new Verifiable Credential for the Subject to replace the Inaccessible Credential.

12.2 Authentication

The PCTF AUTH 5 conformance criterion requires Authentication Service Providers (ASP) to consider the state information made available by an issuing Credential Service Provider about a credential. Assuming the availability and use of a Decentralized Registry's "revocation registry", Authentication Service Providers could use this when verifying a Verifiable Credential in order to satisfy this requirement.

The PCTF AUTH 6, AUTH 7 require Authentication Service Providers not to indicate a successful credential authentication of a credential when the issuing Credential Service Provider has indicated that the credential is inaccessible or revoked.

In the case of Verifiable Credentials, an ASP could perform a check against a Decentralized Registry's "revocation registry" as part of the Authentication process to satisfy this requirement. Note that the Verifiable Credential (VC) may be valid, may be presented with authentic proof that the presenter of the credential is the Subject, or an appropriate representative of the Subject, of the credential, and may be correctly and traceably issued by a trusted Issuer, but if the VC is registered as revoked, the ASP is required to indicate that the VC is not completely authentic. The ASP may choose to share information about the authenticity and state of the credential as part of its service, to allow its customer to make informed risk-management decisions.

The PCTF AUTH 17 requires the use of a standards-based implementation of cryptographic modules used in "client side" authentication. We read this as any authentication that happens on equipment under the physical control of a person, in contrast with authentication that happens on a computer server that typically operates without human involvement. As examples, this could be authentication done via a web browser, or in a mobile app.

This seems most applicable to Authorizer and Agent software and services. FIPS 140-2 certified modules are available for popular mobile platforms like iOS and Android, and in popular open-source libraries such as OpenSSL.

The PCTF AUTH 19 builds on the requirements of AUTH 6 and AUTH 7 to also require an Authentication Service Provider to indicate a failure with an Authentication process in which credential misuse, or credential compromise is detected.

In the context of Verifiable Credentials, misuse may include: a valid Proof from an incorrect Subject; a valid Proof of a Verifiable Credential from an unacceptable Issuer; and a valid Proof with an inappropriate Level of Assurance. Compromise may include a valid Proof of a revoked Verifiable Credential.

12.3 Authenticated Session Initiation

The PCTF INSE 1, INSE 2 conformance criteria require that session bindings are maintained by an ASP with "all Relying Parties". In the Decentralized Identity case, a session is actively maintained between only two parties, so these requirements are likely to be trivial to meet.

The PCTF INSE 5, INSE 6 require a repeated Authentication process in certain circumstances. This requirement could also be satisfied if an Authenticated Session is terminated, and a new Authenticated Session is initiated. The reference to “federation” here is in the context of an example, and not normative.

12.4 Authenticated Session Termination

The PCTF TESE 1, TESE 2, TESE 3, TESE 4 conformance criteria are required only in “federated single sign-on” cases, and do not apply to other kinds of services.

The PCTF TESE 7, TESE 8, TESE 9 require an Authentication Service Provider to notify “all Relying Parties” about session downgrade and session termination events. As noted in INSE 1, INSE 2, in the Decentralized Identity case, a session is actively maintained between only two parties, so these requirements are likely to be trivial to meet.

12.5 Credential Maintenance

The PCTF CRMA 3 conformance criterion requires a Credential Service Provider to allow a Subject to initiate an update to an Authenticator and/or Authenticator Validation Data.

For an Agent/Authorizer, this translates to allowing the Subject to initiate an update to the keys used to protect the connections with each Issuer and Verifier.

For an Issuer, this translates to an Issuer updating that Issuer’s DID Document.

The PCTF CRMA 4 requires a Credential Service Provider to support changes to information bound to a credential.

In the context of Verifiable Credentials, this effectively requires an Issuer to issue a new VC, and as appropriate, revoke the VCs the new credential is intended to replace.

The PCTF CRMA 13 requires, in part, a Credential Service Provider to periodically refresh credential Authenticators and/or Authenticator Validation Data.

As with CRMA 3, its Subject-initiated counterpart, this applies to Agent/Authorizer services, and Issuer services. This may also apply for the successful ongoing operation of a Decentralized Registry. For CRMA 13, however, it is the service that initiates these changes, on an appropriately regular basis.

This paper is a product of a DIACC Innovation Expert Committee innovation initiative. The content of this paper has been supported by DIACC members 2Keys, Applied Recognition, and the Digital Identity Laboratory of Canada with contributions by members of the DIACC's Innovation and Trust Framework Expert Committees.