PCTF Assurance Maturity Model Draft Recommendation V1.0

This Draft Recommendation has been developed by the Digital ID & Authentication Council of Canada (DIACC) Trust Framework Expert Committee (TFEC). The TFEC operates under the controlling policies of the DIACC. Comments submitted by the public are subject to the DIACC Contributor Agreement.

DIACC expects to modify and improve this Draft Recommendation based upon public comments. The purpose of the open commentary is to ensure transparency in development and diversity of truly Pan-Canadian input. Comments made during the review will be considered for incorporation to the next draft. DIACC will prepare a disposition of comments to provide transparency with regard to how each comment was handled.

Forthcoming PCTF releases will expand, clarify, and refine the content of this document.

Table of Contents

1. Document Conventions
2. Introduction
   - 2.1. The Traditional Approach
     - 2.1.1. The Whistleblower: An Illustrative Use Case
     - 2.1.2. The need for an evolutionary approach
3. The Pan-Canadian Trust Framework Assurance Maturity Model
   - 3.1. Model 1: Traditional Levels of Assurance (Traditional LoA)
     - 3.1.1. Traditional Levels of Assurance and the Whistleblower Example
   - 3.2. Model 2: Discrete Levels of Assurance (Discrete LoA)
     - 3.2.1. Discrete Levels of Assurance and the Whistleblower Example
   - 3.3. Model 3: Vectors of Trust (VoT)
     - 3.3.1. Vectors of Trust and the Whistleblower Example
     - 3.3.2. Interoperability with Model 1 and 2 implementations: PCTF Component Vectors of Trust
     - 3.3.3. PCTF Component Vectors of Trust Explained
       - 3.3.3.1. Authentication (“T”)
       - 3.3.3.2. Verified Person (“H”)
       - 3.3.3.3. Verified Organization (“O”)
       - 3.3.3.4. Credentials (Relationships & Attributes) (“R”)
       - 3.3.3.5. Privacy (“V”)
       - 3.3.3.6. Notice & Consent (“N”)
       - 3.3.3.7. Infrastructure (Technology & Operations) (“S”)
     - 3.3.4. PCTF Component Vectors of Trust and the Whistleblower Example
4. Concurrent Support for all Maturity Models
5. Mapping the Three Models
   - 5.1. PCTF Component Maps
     - 5.1.1. Authentication Map
     - 5.1.2. Verified Person Map
     - 5.1.3. Verified Organization Map
     - 5.1.4. Credential (Relationships & Attributes) Map
     - 5.1.5. Privacy Map
     - 5.1.6. Notice & Consent Map
     - 5.1.7. Infrastructure (Technology & Operations) Map
   - 5.2. New Vectors of Trust Maps
     - 5.2.1. Identity Assurance
     - 5.2.2. Identity Assurance Map
     - 5.2.3. Primary Credential Usage
     - 5.2.4. Primary Credential Usage Map
     - 5.2.5. Primary Credential Management
     - 5.2.6. Credential Management Map
     - 5.2.7. Assertion Presentation
     - 5.2.8. Presentation Assurance Map
6. Risk Evaluation

7. References
8. PCTF Vectors of Trust Standard Specification
    8.1. Trustmark URL
    8.2. Vectors of Trust Component Registry
9. Revision History

1. Document Conventions

In this document, terms that are capitalized and presented *in italics* are terms (e.g. *Credential*) that are defined by the PCTF Glossary V1.0.

2. Introduction

It is essential that *Participants* in a digital ecosystem have a way to evaluate the robustness and trustworthiness of transactions within that ecosystem. In order to do so, *Participants* must share a common vocabulary that describes the level of confidence they can associate with an *Entity* or transaction, as well as a common way in which to determine that level of confidence.

In the Pan-Canadian Trust Framework™ (PCTF), a *Level of Assurance* (LoA) represents the level of confidence an *Entity* may place in the processes and other conformance criteria defined in any given component of the PCTF. *Levels of Assurance* are elemental in creating networks of trust. Levels of Assurance models only work if all *Participants* in a digital ecosystem are able to interpret them consistently. It is therefore critical that all *Participants* in an ecosystem agree upon a minimum set of criteria for each *Level of Assurance*. Only then will a *Relying Party* in that ecosystem be able to properly evaluate the risks inherent in a relationship or transaction, and the *Level of Assurance* that can be placed in *Participants*, *Credentials*, and those transactions. The components of the PCTF describe the detailed conformance criteria that should be used to evaluate such *Levels of Assurance* in the context of a given PCTF component. This document provides guidance regarding how to use those criteria in order to properly classify *Levels of Assurance*.

2.1 The Traditional Approach

When the PCTF was introduced, the most broadly accepted approach to *Levels of Assurance* was as depicted in Figure 1.

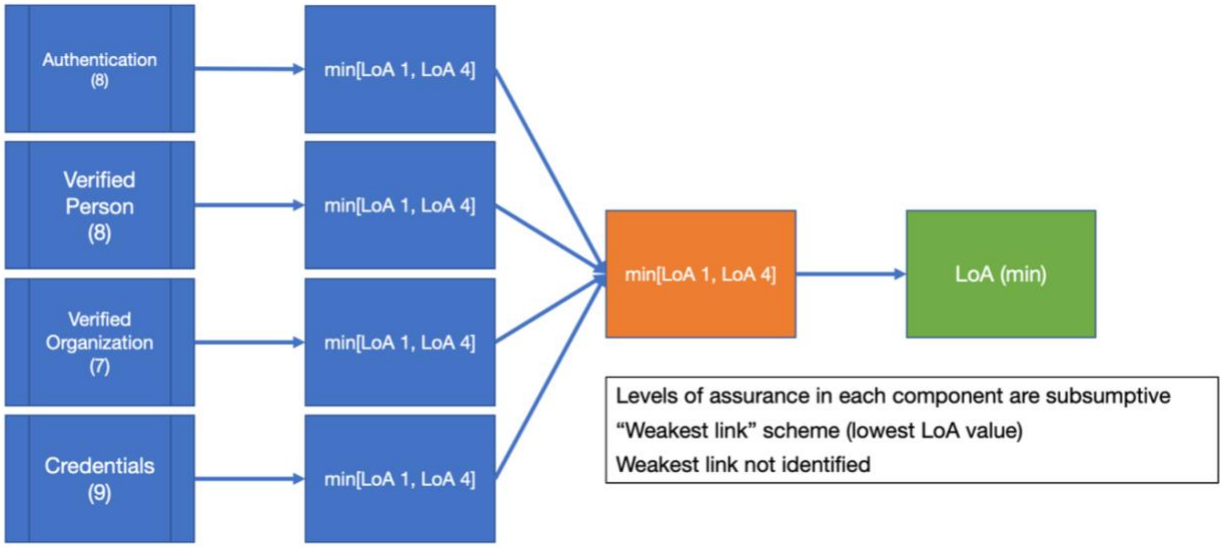

Figure 1: Traditional Levels of Assurance Model

(Note: The number appearing below each component's name in Figure 1 indicates the number of *Trusted Processes* described in that component as of PCTF Version 1.0)

This approach follows a simple, 3-step process to determine a transaction's *Level of Assurance*:

1. Relevant conformance criteria in each component are evaluated to determine which LoA has been achieved for each criterion.
2. The *Level of Assurance* for a specific component is equal to the lowest LoA assessed across all of the relevant criteria for that PCTF component.
3. The overall *Level of Assurance* is equal to the lowest LoA assessed across all of the PCTF components.

This is a weakest link scheme. That is, the highest *Level of Assurance* that can be achieved is that of the weakest of the criteria.

For example, consider a scenario where the relevant criteria are as follows:

- Authentication criteria assessment: Criterion 1: LoA 3; Criterion 2: LoA 3; Criterion 3: LoA 3; Criterion 4: LoA 3
- Verified Person criteria assessment: Criterion 1: LoA 3; Criterion 2: LoA 3; Criterion 3: LoA 2; Criterion 4: LoA 3
- Verified Organization criteria assessment: Criterion 1: LoA 3; Criterion 2: LoA 3; Criterion 3: LoA 3; Criterion 4: LoA 3
- Credentials criteria assessment: Criterion 1: LoA 3; Criterion 2: LoA 3; Criterion 3: LoA 1; Criterion 4: LoA 3

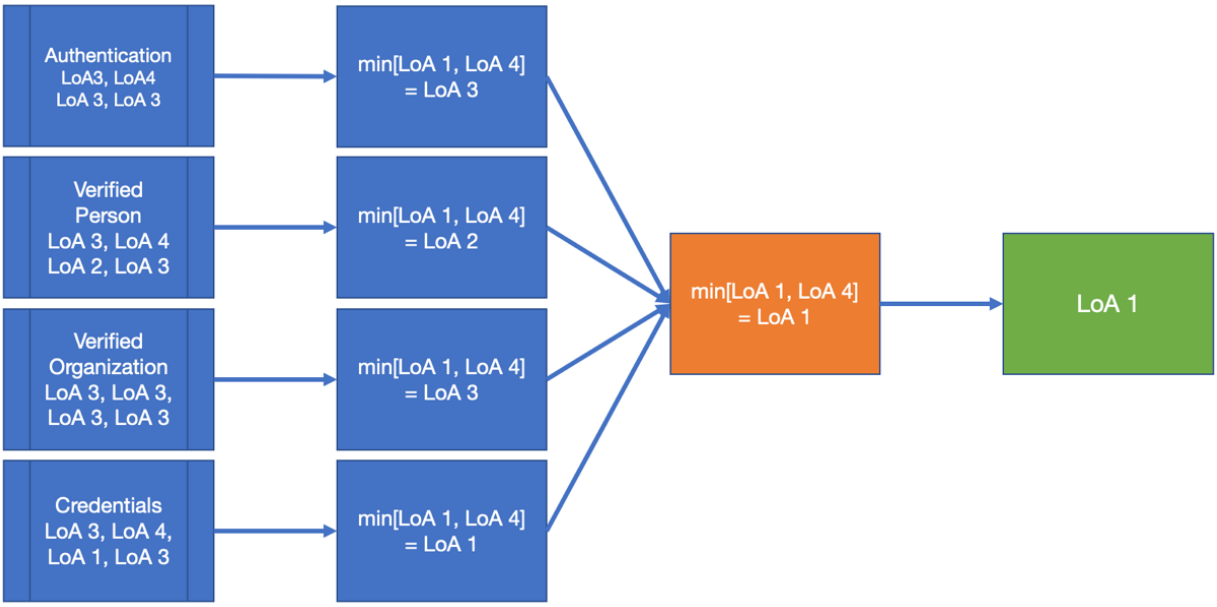

Figure 2: Sample evaluation using the PCTF's inaugural conformance criteria

As shown in Figure 2, given these conditions the *Level of Assurance* associated with the scenario would be LoA 1, which is the level associated with the criterion or criteria that are weakest.

Though this is a weakest link scheme, this approach does not necessitate that the weakest link(s) are identified to the *Relying Party*. Nor are the strongest links identified. This can present challenges to *Relying Parties* attempting to implement a risk-based approach to assurance, as it cannot sufficiently deal with many use cases.

2.1.1 The Whistleblower: An Illustrative Use Case

Consider, for example, the case of a fictitious whistleblower. In our example someone has learned that a group they are a member of is engaging in unlawful, immoral, or even a life-endangering activity. They need to make this activity known in order to preserve the integrity of the group and protect the lives of those impacted. They must remain anonymous. Exposing their identity might result in their dismissal from the group, removing their ability to surface the wrongdoing and, more importantly, preventing them from mitigating the harm it causes. In addition, exposure of their identity may cause irreparable damage to their career or ability to earn income. In extreme cases it might also put their lives, or the lives of their friends and family, in danger.

In a typical digital transaction, a key question is, "Do I know this person (or Entity) and are they whom they claim to be?". However, in this case our *Subject* will never divulge their true identity. Thus, once they have made initial contact and proven their validity as an insider (e.g., by providing verifiable information that proves their provenance) that

question becomes, "Is this the person with whom I have been dealing with previously?". Once we trust them, we need to ensure we can trust things such as whether their account has been compromised, that nobody has assumed their identity, that they are using strong cryptographic authentication, and that the digital activity is not vulnerable to a person-in-the-middle attack.

A digital transaction of this nature might possess the following attributes:

- Identity:
  - Self-asserted, consistent over time
- Credentials:
  - Session cookies
  - Known Device
  - Shared secret
  - Cryptographic asymmetric key
  - Sealed hardware token
  - Full proofing required for every issuance or rotation, revoked when suspicious activity detected
- Assertion Presentation:
  - Signed verifiable assertion, passed through a back channel
  - Assertion encrypted in the *Relying Party*'s key

Even though a transaction with these characteristics is likely sufficiently robust for this whistleblower case, the fact that it uses a self-asserted identity – which the criteria classify as an LoA 1-level identity – will cause the entire transaction to be evaluated as LoA 1 under this assurance scheme. Thus, it would likely be assessed by a *Relying Party* as untrustworthy. Since this scheme delivers a single *Level of Assurance*, the *Relying Party* would have no way of knowing that it is sufficiently robust for the use case, nor would they know why it was assessed as LoA1. They would be unaware that the transaction was authenticated at LoA 3, and it was evaluated overall at LoA 1 solely due to the fact the identity was self-asserted.

2.1.2 The need for an evolutionary approach

There are many use cases where a weakest-link scheme such as this is insufficient. However, weakest-link schemes such as these have been widely adopted and cannot be ignored. Thus, it is clear the PCTF requires an evolutionary approach that offers *Relying Parties* a range of assurance options that enable them to begin with today's widely used models and evolve as needed to address their own risks and requirements.

3. The Pan-Canadian Trust Framework Assurance Maturity Model

The Pan-Canadian Trust Framework Assurance Maturity Model consists of three, interoperable models of maturity:

1. Traditional Levels of Assurance.
2. Discrete Levels of Assurance.
3. Vectors of Trust.

While this represents an evolutionary model, it should be noted that there is no requirement for practitioners to adopt any of the models. Practitioners may begin at any point in the model, may move directly to any other model, and need not have previously adopted any other model.

3.1 Model 1: Traditional Levels of Assurance (Traditional LoA)

The Traditional Levels of Assurance model originally described earlier becomes the basis for maturity Model 1. This represents the most broadly implemented assurance scheme at the time of this writing and provides an on-ramp to the PCTF for those who have currently implemented this scheme.

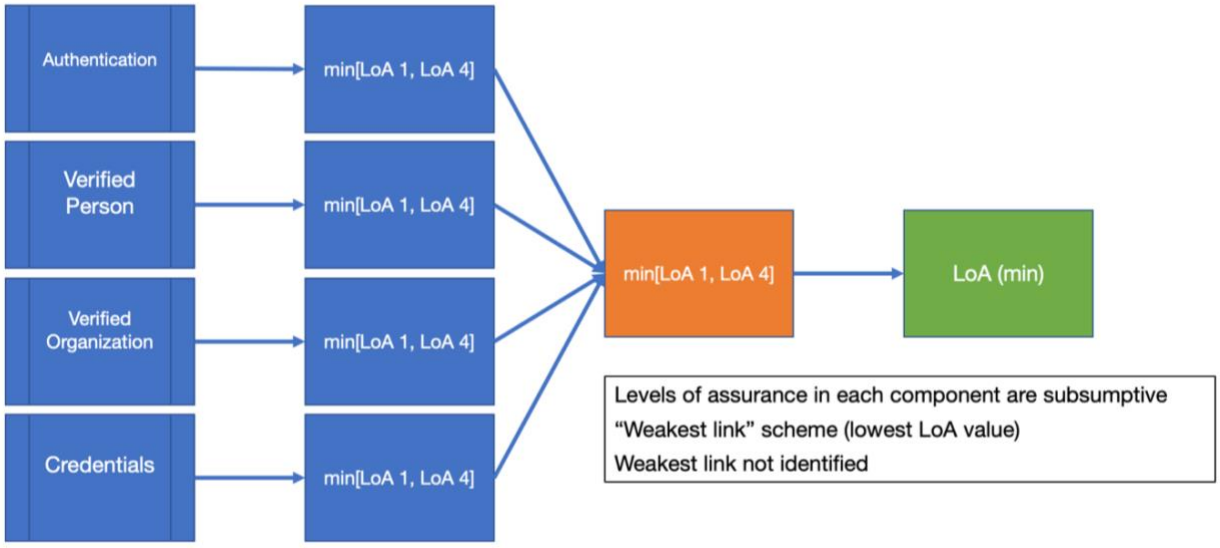

Figure 3: Traditional Levels of Assurance

In this model, *Levels of Assurance* range from "LoA 1", which is least trustworthy, to "LoA 4", which is most trustworthy. LoA 4 typically addresses very high security use cases and is used primarily by public sector practitioners. Most PCTF Version 1 Conformance Profiles do not define conformance criteria for LoA 4. Each *Level of Assurance* is typically subsumptive, and includes most, or all, of the criteria for all of the levels below it (i.e.: those with smaller numbers). In a Traditional LoA scheme, assurance levels are typically broadly characterized as outlined in Figure 4.

Assurance Level	Description
Level 1	• Satisfies all Level 1 Conformance Criteria for the appropriate PCTF component • Little or no confidence required • Little confidence required that an Entity has maintained control over a Credential that has been entrusted to them and that the Credential has not been compromised
Level 2	• Satisfies all Level 2 Conformance Criteria for the appropriate PCTF component • Some confidence required • Some confidence required that an Entity has maintained control over a Credential that has been entrusted to them and that the Credential has not been compromised
Level 3	• Satisfies all Level 3 Conformance Criteria for the appropriate PCTF component • High degree of confidence required • High confidence required that an Entity has maintained control over a Credential that has been entrusted to them and that the Credential has not been compromised
Level 4	• Satisfies all Level 4 Conformance Criteria for the appropriate PCTF component • Very high degree of confidence required • Very high confidence required that an Entity has maintained control over a Credential that has been entrusted to them and that the Credential has not been compromised • **Note**: Most PCTF Version 1 Conformance Profiles do not define criteria for LoA 4.

Figure 4. Assurance Levels (Illustrative)

(Note: The examples in Figure 4 are illustrative. Please consult the PCTF components' Conformance Criteria for the latest information.)

Evaluation of Traditional Levels of Assurance follows a 3-step process:

1. Relevant conformance criteria in each component are evaluated to determine which LoA has been achieved for each criterion.

2. The *Level of Assurance* for a specific component is equal to the lowest LoA assessed across all of the relevant criteria for that PCTF component.
3. The overall *Level of Assurance* is equal to the lowest LoA assessed across all of the PCTF components.

This is a weakest link scheme. That is, the highest *Level of Assurance* that can be achieved is that of the weakest of the criteria.

3.1.1 Traditional Levels of Assurance and the Whistleblower Example

If we carry forward the parameters discussed in our earlier whistleblower example, the fact that the whistleblower presented a self-asserted identity – which meets the criteria for LoA 1 – will result in this entire transaction being assessed at LoA 1.

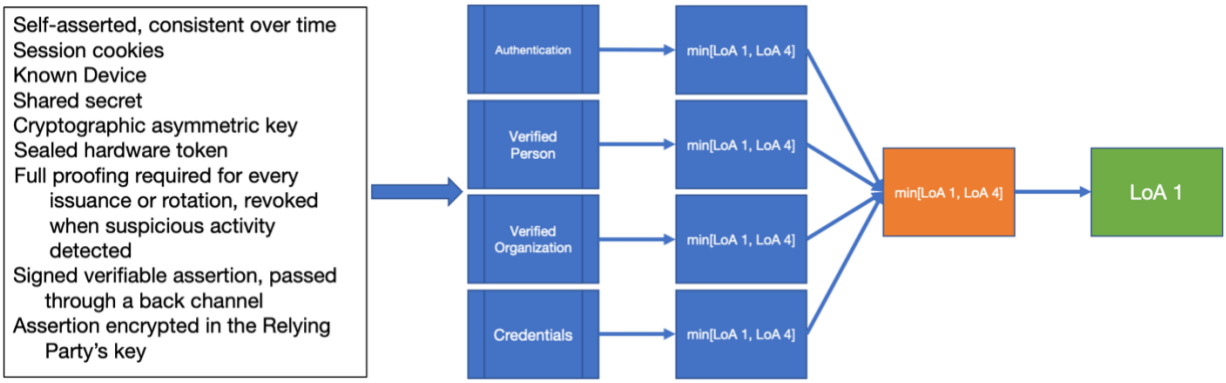

Figure 5: Whistleblower example and Traditional Levels of Assurance (Illustrative)

As demonstrated in the application of the Traditional Levels of Assurance to the whistleblower example, the challenge of a Traditional Levels of Assurance scheme is that it can be difficult, usually impossible, for the *Relying Party* to determine where the weakest link lies, or where there are strengths. *Relying Parties* need a way to independently assess the many different threats present in a Digital Ecosystem such as:

- Whether the *Identity* of a *Subject* is consistent over time.
- Whether it is likely that an imposter is using the Identity.
- Whether the *Credentials* in use are robust or vulnerable.
- Whether the *Credentials* in use are well managed and best practices for *Credential* hygiene are in use.
- Whether the transaction was transmitted robustly and was unlikely subject to spoofing or unintended information disclosure.

The second model of the PCTF Assurance Maturity Model begins to address that.

3.2 Model 2: Discrete Levels of Assurance (Discrete LoA)

Model 2 of the maturity model introduces Discrete Levels of Assurance. Discrete LoA breaks the bonds between the individual components of the assurance scheme and enables independent evaluation of authentication assurance levels (AAL), identity assurance levels (IAL), and credential assurance levels (CAL). It places more emphasis on the *Relying Party*'s requirements through increased attention to threat-risk analysis. It also aligns the conformance criteria with the *Relying Party*'s identified risks and ensures they are evaluated in a manner commensurate with those risks.

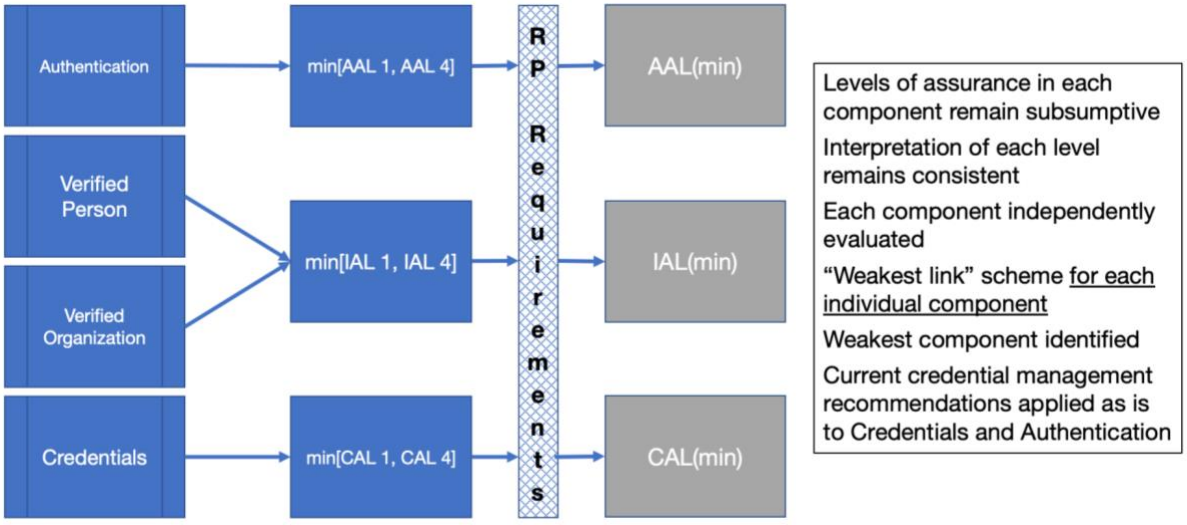

Figure 6: Discrete Levels of Assurance

Evaluation of Discrete Levels of Assurance is as follows:

1. Relevant conformance criteria in each component are evaluated to determine which LoA has been achieved for each criterion.
2. The *Level of Assurance* for a specific component is equal to the lowest LoA assessed across all of the relevant criteria for that PCTF component.
3. The *Level of Assurance* for each component is reported independently.

Characterization of Discrete Levels of Assurance remains consistent with the characteristics outlined in Figure 4, though each individual component is characterized independently of the others. Though it may appear in Figure 6 that assessment of a Verified Person and Verified Organization are combined in the assessment of an IAL, an *Entity* would be either a Verified Person or a Verified Organization, though not both. Thus, only one of those would be applicable to an *Entity* and would be considered during evaluation of its IAL.

Note: Most PCTF Version 1 Conformance Profiles do not provide conformance criteria for assurance at level 4.

The Discrete LoA approach is very similar to the Traditional LoA approach, though possesses some important advantages. It removes the weakest-link approach to *Levels of Assurance* found in the Traditional approach and enables *Relying Parties* to consider the strength and robustness of each component of a digital transaction independently. It also places emphasis on the evaluation of risks in the context of each individual *Relying Party*. To illustrate the differences, let's revisit the whistleblower example.

3.2.1 Discrete Levels of Assurance and the Whistleblower Example

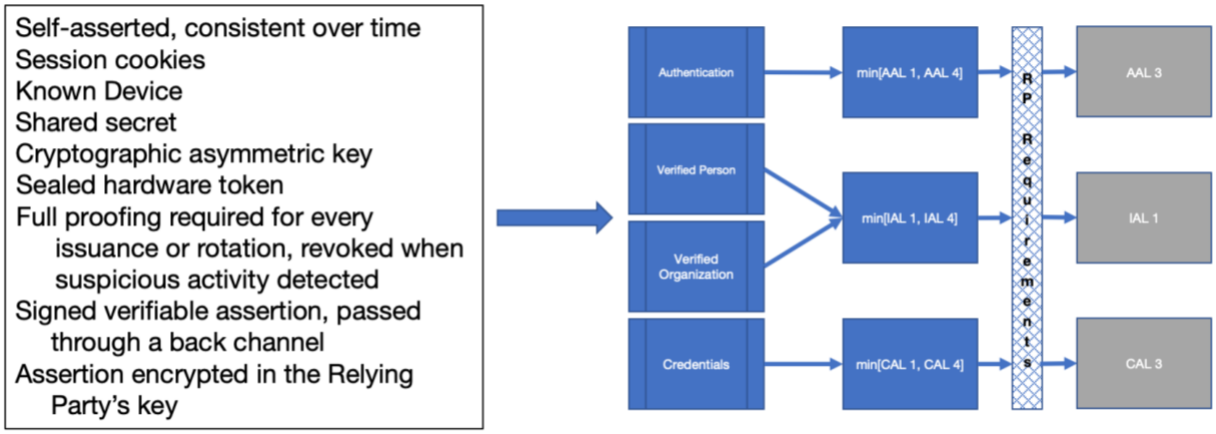

Figure 7: Whistleblower example and Discrete Levels of Assurance (Illustrative)

Using the Discrete LoA approach to evaluate these parameters, the *Relying Party* is now able to understand that, though the identity proofing was evaluated at the lowest *Level of Assurance* (IAL 1), the whistleblower is using a very strong credential (CAL 3) with strong authentication (AAL 3). This provides them with key information to help them to answer the question posed earlier, "Is this the same person I have been transacting with?".

A key advantage of the Discrete LoA approach is that it can be implemented through the assessment of existing PCTF Conformance Criteria. In a sense, it provides better acuity by removing a step from the Traditional LoA approach (i.e.: component aggregation and minimization).

3.3 Model 3: Vectors of Trust (VoT)

Though the Discrete LoA approach provides much more acuity and flexibility than a Traditional LoA approach, like the Traditional LoA scheme it is an aggregate approach that does not specifically identify the rationale for an assigned *Level of Assurance*, the weakest link, nor the specific strengths. For example, even though in our whistleblower

example it provides better information in that the *Relying Party* knows that the AAL and CAL are strong, and that the weakest component is identity, it does not inform the *Relying Party* what aspect of identity is weak. The *Relying Party* may be unaware that the identity is consistent over time, which is an important consideration in the example, and key to answering the question "Is this the person with whom I have been dealing in the past?".

This is just one example of a scenario that illustrates the immediate need for the ability to evaluate different threats independently. The PCTF Assurance Maturity Model addresses this need in its third model of maturity, Vectors of Trust.

The Vectors of Trust approach to assurance provides detailed information regarding each of a transaction's potential threat vectors. This provides the *Relying Party* with information that enables them to better evaluate the risk associated with the transaction, and that is much more actionable.

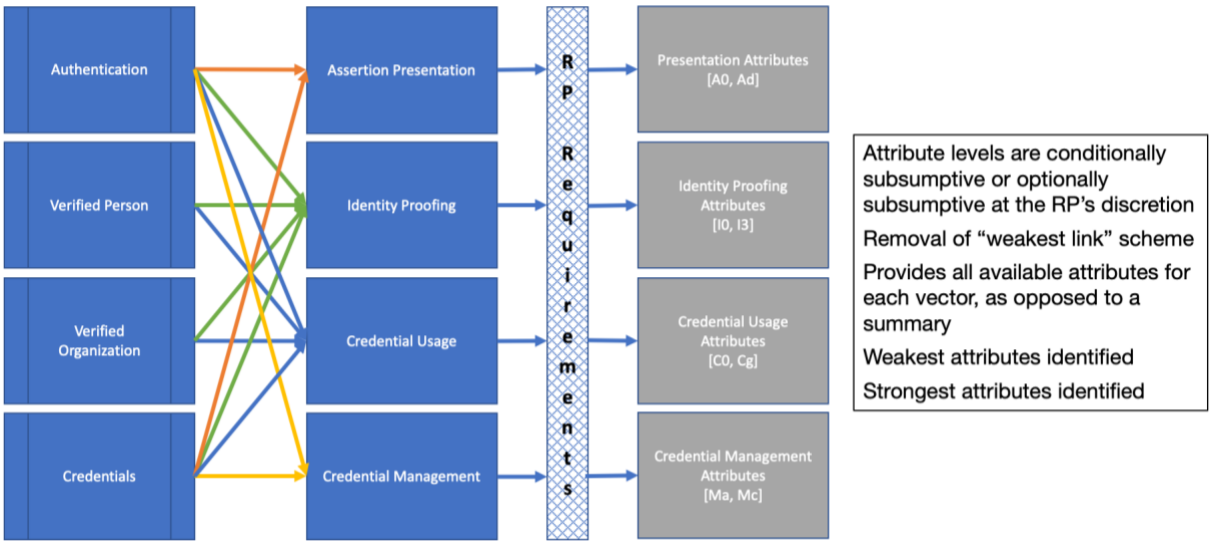

Figure 8: Vectors of Trust Assurance Model

The PCTF Vectors of Trust scheme includes details for four new vector components, as outlined in Figure 9.

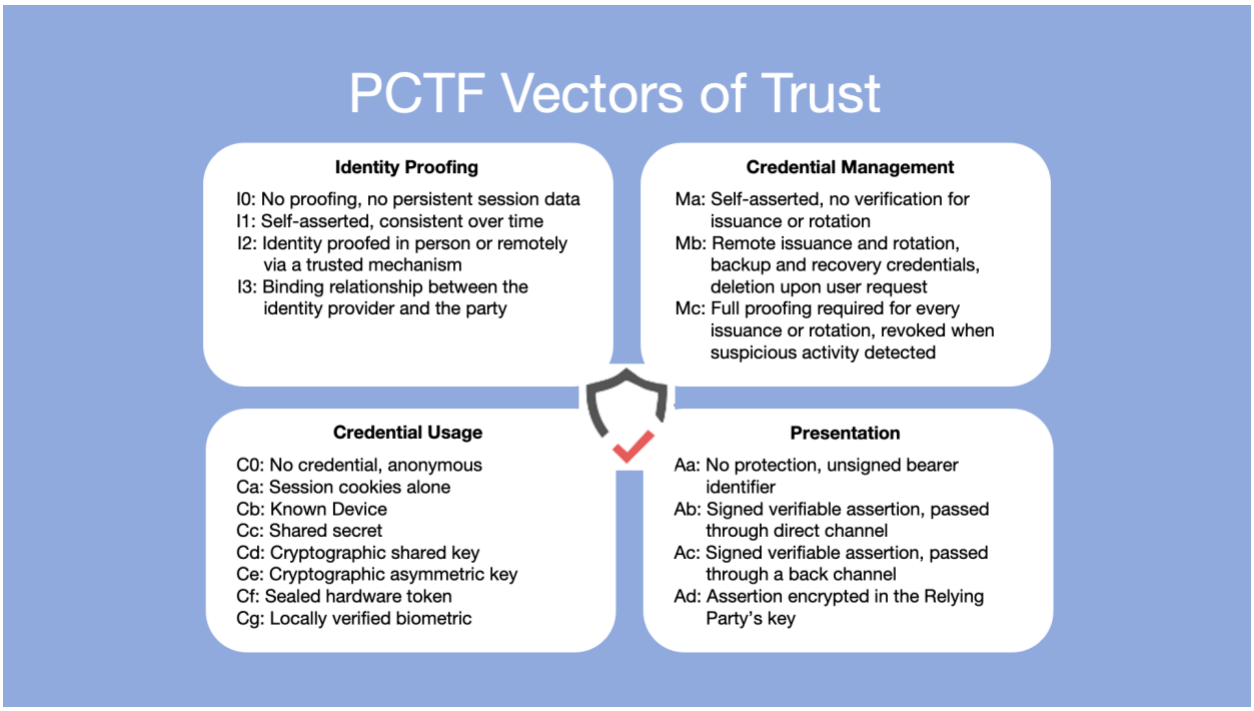

Figure 9: PCTF Vectors of Trust (New)

The Vectors of Trust approach to assurance:

- Enables the *Relying Party* to assess risk with better acuity than Traditional LoA and Discrete LoA schemes.
- Enables *Relying Parties* to decide which components are relevant to their risks or request only the components they need.
- Is flexible in its implementation.
- Can be mapped to Traditional LoA and Discrete LoA schemes for interoperability.
- Is not subject to inconsistencies in evaluation of LoA levels or to LoA level drift.
- Does not require recalibration to account for new technologies and best practices.
- Provides insight into a transaction's specific strengths and weaknesses.
- Is extensible as the PCTF grows.
- Is designed to evolve with new technologies and best practices.

While the PCTF provides a set of baseline vectors and attributes, *Relying Parties* and *Participants* can negotiate specific attributes that best meet their needs and address their specific risks. This may include additional vector components, and some, all, or none of the baseline vector components.

3.3.1 Vectors of Trust and the Whistleblower Example

The Vectors of Trust approach expresses assurance in a much different way that the Traditional LoA and Discrete LoA approaches. Rather than provide a single, composite

LoA measure as in the case of a Traditional LoA scheme, or four composite LoA measures in the case of a Discrete LoA scheme, a Vectors of Trust scheme provides a single vector that contains an expression of every component that is relevant to the transaction. To demonstrate how this works, let's return to our whistleblower example.

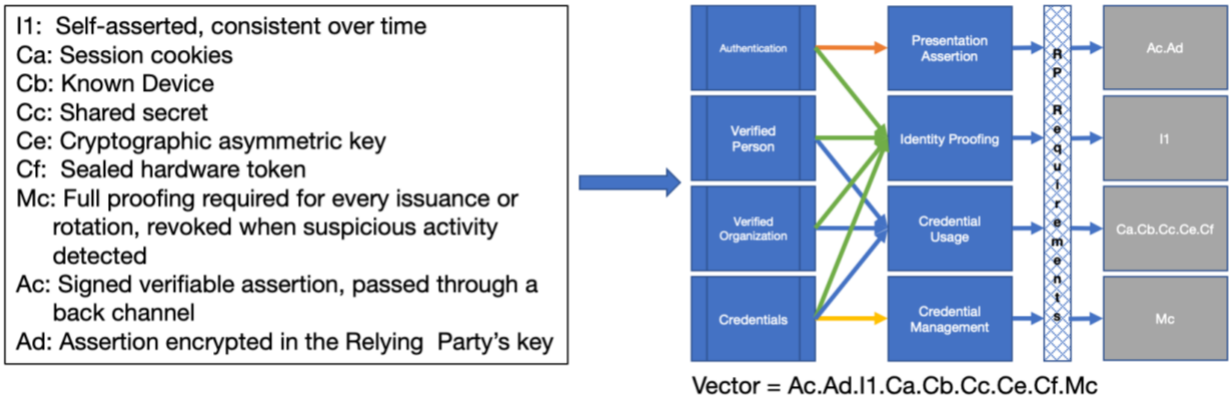

Figure 10: Whistleblower example and Vectors of Trust (Illustrative)

Using a Vectors of Trust approach, the *Relying Party* is provided with the vector "Ac.Ad.I1.Ca.Cb.Cc.Ce.Cf.Mc". This vector is interpreted using the scheme outlined in Figure 10, as follows:

- Authentication:
  - Ac: Signed verifiable assertion, passed through a back channel
  - Ad: Assertion encrypted in the *Relying Party*'s key
- Identity:
  - I1: Self-asserted, consistent over time
- Credential Usage:
  - Ca: Session cookies
  - Cb: Known Device
  - Cc: Shared secret
  - Ce: Cryptographic asymmetric key
  - Cf: Sealed hardware token
- Credential Management:
  - Mc: Full proofing required for every issuance or rotation, revoked when suspicious activity detected

With this level of detail, the *Relying Party* can clearly determine, based upon their own priorities and risk tolerances, whether they can trust this transaction. Thus, they can definitively answer the question, "Is this likely to be the person with whom I have been previously transacting?".

3.3.2 Interoperability with Model 1 and 2 implementations: PCTF Component Vectors of Trust

At the time this document was created Traditional LoA and Discrete LoA were the most commonly implemented assurance schemes, with Traditional LoA being the most commonly encountered model. Since an objective of this maturity model is to enable *Entities* working with all three schemes to collaborate, there is a need for interoperability between those models and PCTF Vectors of Trust. To address this, the PCTF Vectors of Trust scheme also includes seven specific dimensions, each aligned to a component of the PCTF (Table 1).

PCTF Component Name	Demarcator Symbol	Defined Values	Notes
Authentication	T	0, 1, 2, 3, 4	Numeric value corresponds to LoA Achieved via Model 1 or Model 2
Verified Person	H	0, 1, 2, 3, 4	Numeric value corresponds to LoA Achieved via Model 1 or Model 2
Verified Organization	O	0, 1, 2, 3, 4	Numeric value corresponds to LoA Achieved via Model 1 or Model 2
Credential (Relationships & Attributes)	R	0, 1, 2, 3, 4	Numeric value corresponds to LoA Achieved via Model 1 or Model 2
Privacy	V	0, 1	0 = Not conformant; 1 = Conformant
Notice & Consent	N	0, 1	0 = Not conformant; 1 = Conformant
Infrastructure (Technology & Operations)	S	0, 1	0 = Not conformant; 1 = Conformant

Figure 11: PCTF Component Vectors of Trust Dimensions and Defined Values

Use of the PCTF Component Vectors of Trust enable *Entitles* and *Relying Parties* using Model 1 or Model 2 to continue to evaluate and assess risk without modification while providing an additional level of acuity to those using Model 3.

3.3.3 PCTF Component Vectors of Trust Explained

3.3.3.1 Authentication (“T”)

The Authentication dimension of the PCTF Vectors of Trust should express the single value of the lowest LOA assessed against the PCTF Authentication component's conformance criteria. For example, a conformance assessment of LOA 2 against Authentication conformance criteria would be expressed as "T2". The value "T0" may be used to document an assessment that found no conformance with any LOA defined by the Authentication component. If an assessment of conformance against the Authentication component has not been performed, a "T" component must not be included in a vector.

3.3.3.2 Verified Person ("H")

The Verified Person dimension of the PCTF Vectors of Trust should express the single value of the lowest LOA assessed against the PCTF Verified Person conformance criteria. For example, a conformance assessment of LOA 2 against Verified Person conformance criteria would be expressed as "H2". The value "H0" may be used to document an assessment that found no conformance with any LOA defined by the Verified Person component. If an assessment of conformance against the Verified Person component has not been performed, an "H" component must not be included in a vector.

3.3.3.3 Verified Organization ("O")

The Verified Organization dimension of the PCTF Vectors of Trust should express the single value of the lowest LOA assessed against the PCTF Verified Organization conformance criteria. For example, a conformance assessment of LOA 2 against Verified Organization conformance criteria would be expressed as "O2". The value "O0" may be used to document an assessment that found no conformance with any LOA defined by the Verified Organization component. If an assessment of conformance against the Verified Organization component has not been performed, an "O" component must not be included in a vector.

3.3.3.4 Credentials (Relationships & Attributes) ("R")

The Credentials (Relationships & Attributes) dimension of the PCTF Vectors of Trust should express the single value of the lowest LOA assessed against the PCTF Credentials (Relationships & Attributes) conformance criteria. For example, a conformance assessment of CAL 2 against Credentials (Relationships & Attributes) conformance criteria would be expressed as "R2". The value "R0" may be used to document an assessment that found no conformance with any LOA defined by the Credentials (Relationships & Attributes) component. If an assessment of conformance against the Credentials (Relationships & Attributes) component has not been performed, a "R" component must not be included in a vector.

3.3.3.5 Privacy ("V")

The Privacy dimension of the PCTF Vectors of Trust should express that conformance has been assessed against the criteria for the PCTF Privacy component. For example, an assessment of "conforming" would be expressed as "V1". The value "V0" may be used to document an assessment of "not conforming" to the Privacy component. If an assessment of conformance against the Privacy component has not been performed, a "V" component must not be included in a vector.

3.3.3.6 Notice & Consent ("N")

The Notice & Consent dimension of the PCTF Vectors of Trust should express that conformance has been assessed against the criteria for the PCTF Notice & Consent component. For example, an assessment of "conforming" would be expressed as "N1". The value "N0" may be used to document an assessment of "not conforming" to the Notice & Consent component. If an assessment of conformance against the Notice & Consent component has not been performed, a "N" component must not be included in a vector.

3.3.3.7 Infrastructure (Technology & Operations) ("S")

The Infrastructure (Technology & Operations) dimension of the PCTF Vectors of Trust should express that conformance has been assessed against the criteria for the PCTF Infrastructure (Technology & Operations) component. For example, an assessment of "conforming" would be expressed as "S1". The value "S0" may be used to document an assessment of "not conforming" to the Infrastructure (Technology & Operations) component. If an assessment of conformance against the Privacy component has not been performed, a "S" component must not be included in a vector.

3.3.4 PCTF Component Vectors of Trust and the Whistleblower Example

Returning to our whistleblower example, the PCTF Component Vectors of Trust would be evaluated as depicted in Figure 12.

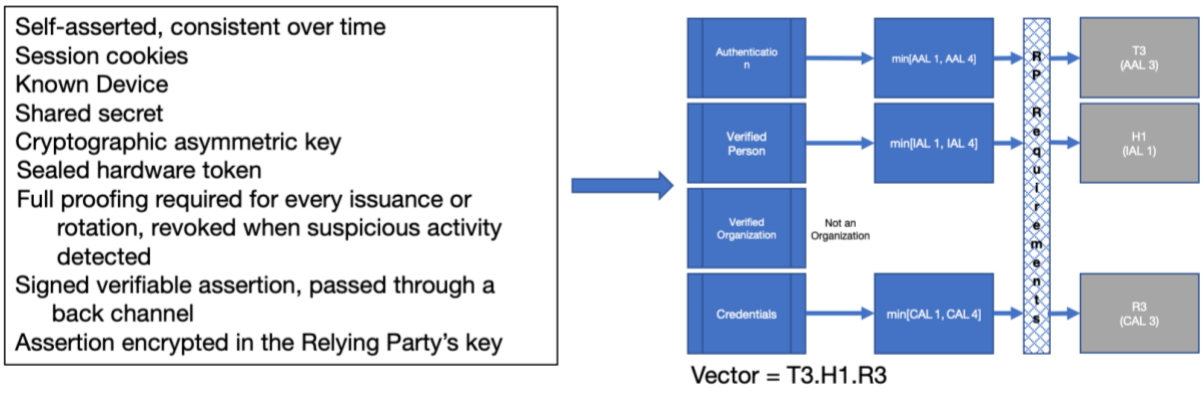

Figure 12: Whistleblower example and Component Vectors of Trust (Illustrative)

Using a Vectors of Trust approach, the *Relying Party* is provided with the vector "T3.H1.R3". This vector is interpreted using the scheme outlined in Figure 12, as follows:

- Authentication:
  - T3: Assessed at PCTF LOA 3 or AAL3 – the system has used strong authentication processes
- Verified Person:
  - H1: Assessed at PCTF LOA 1 or IAL 1 – the system does not know the identity of the person, though assesses it is the same person that was previously transacted with
- Verified Organization:
  - Since there is no organization involved, conformance with Verified Organization was not assessed and was not included
- Credentials (Relationships & Attributes):
  - R3: Assessed at PCTF LOA 3 or CAL 3 – the system has used strong processes to document an attribute (e.g. characteristic or qualifier) of the person
- Privacy:
  - Conformance was not assessed
- Notice & Consent:
  - Conformance was not assessed
- Infrastructure (Technology & Operations):
  - Conformance was not assessed

With this level of detail the *Relying Party* can clearly determine, based upon their own priorities and risk tolerances, whether they can trust this transaction. Thus, they can definitively answer the question, "Is this likely to be the person with whom I have been previously transacting?".

4. Concurrent Support for all Maturity Models

Our ability to carry the whistleblower example through all three models of maturity, albeit with steadily improving results, foreshadows the PCTF's ability to support all three models of maturity concurrently.

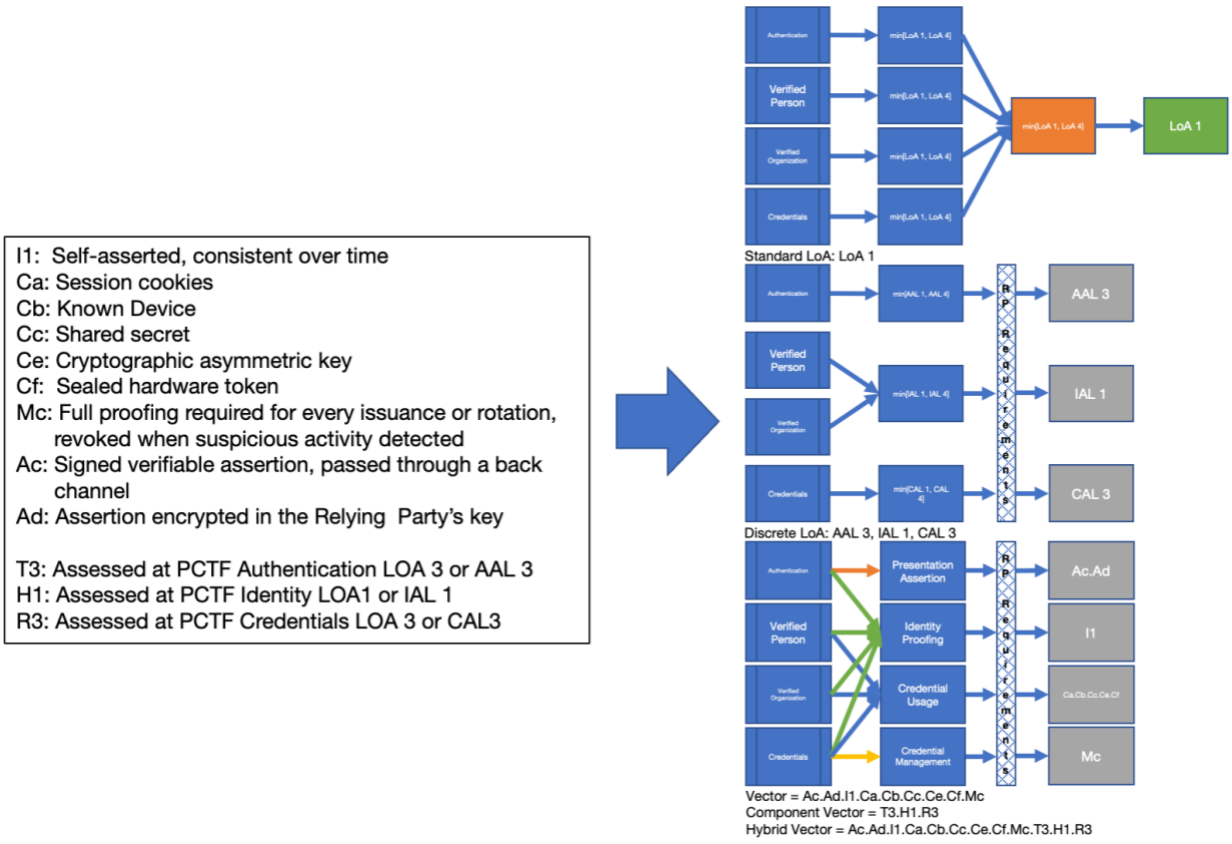

Figure 13: All three models of the PCTF Assurance Maturity Model and the whistleblower example (Illustrative)

The scheme depicted in Figure 13 gives Participants the flexibility to use any one of the three models described in this document. In addition, Participants in an Ecosystem can agree to present and/or receive a hybrid vector which will enable other Participants to evaluate the assurance level of a transaction using any of the three models. For example, the hybrid vector presented in Figure 13 can be interpreted in the following three ways:

1. **Traditional LOA (Model 1): LOA 1** = Min[T3 (Authentication LOA 3), H1 (Identity LOA 1), R3 (Credential LOA 3)]
2. **Discrete LOA (Model 2): AAL 3; IAL 1; CAL 3** = T3(AAL 3).H1(IAL 1).R3(CAL 3)
3. **Vectors of Trust (Model 3): Ac.Ad.I1.Ca.Cb.Cc.Ce.Cf.Mc** = T, H, and R PCTF Component elements ignored

5. Mapping the Three Models

For further clarification a mapping of the three models of maturity follows. Though this mapping will help practitioners to work together, it is ultimately the *Relying Party* who

assesses their own level of risk and who makes the ultimate decision regarding whether they can, or should, trust a transaction.

Note: These mappings are meant as illustrative examples and are not intended to define strict equivalences. The results of any assessment in the context of PCTF should be documented according to the PCTF Assessment Component and may include an expression of assurance according to one or more of the assurance models presented here.

In the tables to follow:

- "Traditional Assurance Model" provides the highest possible assurance level that corresponds to the "Characteristics to Consider".
- "Discrete Assurance Model" provides the highest possible assurance level that corresponds to the "Characteristics to Consider".
- "Vector Component" provides the PCTF Component Vector that corresponds to the "Characteristics to Consider".
- "Characteristics to Consider" documents significant characteristics of the system or transaction that correspond to the values suggested in the other columns of the same row.

As in the example above and in the section describing Model 1, the overall Traditional LoA is calculated by taking the lowest Traditional LoA level evaluated for all assessed components.

Note: Though all of the maps below include a mapping to Traditional LoA 4, not all PCTF components include LoA 4 conformance criteria. Though the result is that it is currently not possible for assessment of a Traditional LoA higher than 3 in those cases, LoA 4 mappings were included to account for future enhancement of those components.

5.1 PCTF Component Maps

5.1.1 Authentication Map

Traditional Assurance Model	Discrete Assurance Model	Vector Component	Characteristics to Consider
None Specified	None Specified	None Specified	• No assessment of conformance to the PCTF Authentication conformance criteria has been made

None Specified	None Specified	T0	• No authentication has been performed that conforms to any PCTF Authentication-defined LoA
LoA 1	AAL 1	T1	• Authentication has been performed that conforms to PCTF Authentication LoA 1 conformance criteria
LoA 2	AAL 2	T2	• Authentication has been performed that conforms to PCTF Authentication LoA 2 conformance criteria
LoA 3	AAL 3	T3	• Authentication has been performed that conforms to PCTF Authentication LoA 3 conformance criteria
LoA 4	AAL 4	T4	• Authentication has been performed that conforms to PCTF Authentication LoA 4 conformance criteria • **Note**: PCTF Authentication Conformance Profile V1.0 does not define conformance criteria for LoA 4.

509 **Figure 14: Authentication Map**

510 ## 5.1.2 Verified Person Map

Traditional Assurance Model	Discrete Assurance Model	Vector Component	Characteristics to Consider
None Specified	None Specified	None Specified	• No PCTF Verified Person conformance criteria assessment was performed

None Specified	None Specified	H0	• No Identity Proofing conforms to any PCTF Verified Person criteria
LoA 1	IAL 1	H1	• Conforms to PCTF Verified Person LoA 1 conformance criteria
LoA 2	IAL 2	H2	• Conforms to PCTF Verified Person LoA 2 conformance criteria
LoA 3	IAL 3	H3	• Conforms to PCTF Verified Person LoA 3 conformance criteria
LoA 4	IAL 4	H4	• Conforms to PCTF Verified Person LoA 4 conformance criteria • **Note**: PCTF Verified Person Conformance Profile V1.0 does not define conformance criteria for LoA 4.

511 **Figure 15: Verified Person Map**

512 ### 5.1.3 Verified Organization Map

Traditional Assurance Model	Discrete Assurance Model	Vector Component	Characteristics to Consider
None Specified	None Specified	None Specified	• No PCTF Verified Organization conformance criteria assessment was performed
None Specified	None Specified	O0	• No Identity Proofing conforms to any PCTF Verified Organization criteria

LoA 1	IAL1	O1	• Conforms to PCTF Verified Organization LoA 1 conformance criteria
LoA 2	IAL2	O2	• Conforms to PCTF Verified Organization LoA 2 conformance criteria
LoA 3	IAL3	O3	• Conforms to PCTF Verified Organization LoA 3 conformance criteria
LoA 4	IAL4	O4	• Conforms to PCTF Verified Organization LoA 4 conformance criteria • **Note**: PCTF Verified Organization Conformance Profile V1.0 does not define conformance criteria for LoA 4.

513 **Figure 16: Verified Organization Map**

514

515

516

517 ## 5.1.4 Credential (Relationships & Attributes) Map

Traditional Assurance Model	Discrete Assurance Model	Vector Component	Characteristics to Consider
None Specified	None Specified	None Specified	• No assessment of conformance to the PCTF Credential (Relationships & Attributes) conformance criteria has been made

None Specified	None Specified	R0	• No trusted processes conform to any PCTF Credential (Relationships & Attributes) CAL
LoA 1	CAL1	R1	• Trusted processes conform to PCTF PCTF Credential (Relationships & Attributes) CAL1
LoA 2	CAL2	R2	• Trusted processes conform to PCTF PCTF Credential (Relationships & Attributes) CAL2
LoA 3	CAL3	R3	• Trusted processes conform to PCTF PCTF Credential (Relationships & Attributes) CAL3
LoA 4	CAL4	R4	• Trusted processes conform to PCTF PCTF Credential (Relationships & Attributes) CAL4

518 **Figure 17: Credential (Relationships & Attributes) Map**

519

520 ### 5.1.5 Privacy Map

Traditional Assurance Model	Discrete Assurance Model	Vector Component	Characteristics to Consider
None Specified	None Specified	None Specified	• No assessment of conformance to the PCTF Privacy conformance criteria has been made

None Specified	None Specified	V0	• The system does not conform to the PCTF Privacy conformance criteria
LoA3	AAL3, IAL3, CAL4	V1	• The system does conform to the PCTF Privacy conformance criteria

Figure 18: Privacy Map

Note: PCTF Privacy does not define levels of assurance. When Privacy is considered in an assessment, a system that does not conform cannot document a conforming level of assurance using the Traditional Assurance Model or the Discrete Assurance Model.

5.1.6 Notice & Consent Map

Traditional Assurance Model	Discrete Assurance Model	Vector Component	Characteristics to Consider
None Specified	None Specified	None Specified	• No assessment of conformance to the PCTF Notice & Consent conformance criteria has been made
None Specified	None Specified	N0	• The system does not conform to the PCTF Notice & Consent conformance criteria
LoA3	AAL3, IAL3, CAL4	N1	• The system does conform to the PCTF Notice & Consent conformance criteria

Figure 19: Notice & Consent Map

Note: PCTF Notice & Consent does not define levels of assurance. When Notice & Consent is considered in an assessment, a system that does not conform cannot document a conforming level of assurance using the Traditional Assurance Model or the Discrete Assurance Model.

5.1.7 Infrastructure (Technology & Operations) Map

Traditional Assurance Model	Discrete Assurance Model	Vector Component	Characteristics to Consider
None Specified	None Specified	None Specified	• No assessment of conformance to the PCTF Infrastructure (Technology & Operations) conformance criteria has been made
None Specified	None Specified	S0	• The system does not conform to the PCTF Infrastructure (Technology & Operations) conformance criteria
LoA3	AAL3, IAL3, CAL4	S1	• The system does conform to the PCTF Infrastructure (Technology & Operations) conformance criteria

Figure 20: Infrastructure (Technology & Operations) Map

Note: PCTF Infrastructure (Technology & Operations) does not define levels of assurance. When Infrastructure (Technology & Operations) is considered in an assessment, a system that does not conform cannot document a conforming level of assurance using the Traditional Assurance Model or the Discrete Assurance Model.

5.2 New Vectors of Trust Maps

Note: Whereas Traditional LOA and Discrete LOA assurance levels are subsumptive (i.e., higher levels are inherently stronger than lower levels and conform to all of the lower levels' criteria), Vectors of Trust are not inherently subsumptive. Thus, higher numeric designators or alphabetically-subsequent alpha designators should not, on their own, be interpreted as an indication of the strength of the element.

5.2.1 Identity Assurance

The primary identity assurance component of this vector definition represents the results of assessment against the Verified Person, Verified Organization, or the lesser LOA of the assessment of both those components. Only one distinct value from this category may be used in a single transaction. This component is intended to align with

the Vectors of Trust Default Component Value Definitions specified in Appendix A, section A.1 of RFC8485. This component may not be included in a vector if no assessment has been done with the PCTF Verified Person or Verified Organization components, or such an assessment has found that no defined *Level of Assurance* has been met (a condition that should be documented as “I0”).

5.2.2 Identity Assurance Map

Traditional Assurance Level	Discrete Assurance Level	Vector ID	Common Characteristics	Vector ID Defining Characteristics
N/A	N/A	I0		No proofing; No persistent session data
LoA 1	IAL 1	I1	Satisfies all Level 1 Conformance Criteria of Verified Person, Verified Organization, or – if both are assessed – both such components. •Little or no confidence required Attributes are self-asserted but consistent over time Potentially pseudonymous	Self-asserted, consistent over time
LoA 2	IAL 2	I2	Satisfies all Level 2 Conformance Criteria of Verified Person, Verified Organization, or – if both are assessed – both such components. •Some confidence required Identity has been proofed either in person or remotely using trusted mechanisms	Identity proofed in person or remotely via a trusted mechanism

LoA 3	IAL 3	I3	Satisfies all Level 3 Conformance Criteria of Verified Person, Verified Organization, or – if both are assessed – both such components. •High confidence required There is a binding relationship between the identity provider and the identified party	Binding relationship between the identity provider and the party

554 **Figure 21: Identity Assurance Map**

555 ## 5.2.3 Primary Credential Usage

556 The primary credential usage component of this vector definition represents distinct
557 categories of primary credential that may be used together in a single transaction. When
558 appropriate, multiple distinct values from this category may be used in a single
559 transaction. This component is intended to align with the Vectors of Trust Default
560 Component Value Definitions specified in Appendix A, section A.2 of RFC8485. This
561 component may not be included in a vector if no assessment has been done with the
562 PCTF Authentication component, or such an assessment has found that no defined
563 Level of Assurance has been met (a condition that should be documented as “T0”).

564 ## 5.2.4 Primary Credential Usage Map

Traditional Assurance Level	Discrete Assurance Level	Corresponding Vector ID	Common Characteristics	Vector ID Defining Characteristics
N/A	N/A	C0		No credential is used; anonymous public service
LoA 1	AAL 1	Ca	Satisfies all Level 1 Authentication	Simple session HTTP cookies (with nothing else)

LoA 1	AAL 1	Cb	Conformance Criteria Little confidence required that an *Entity* has maintained control over Authenticator Validation Data that has been entrusted to them and that the data has not been compromised	Known device, such as those indicated through device posture or device management systems
LoA 2	AAL 2	Cc	•Satisfies all Level 2 Authentication Conformance Criteria •Some confidence required that an *Entity* has maintained control over Authenticator Validation Data that has been entrusted to them and that the data has not been compromised	Shared secret, such as a username and password combination
LoA 2	AAL 2	Cd		Cryptographic proof of key possession using shared key
LoA 3	AAL 3	Ce	•Satisfies all Level 3 Authentication Conformance Criteria •High confidence required that an *Entity* has maintained control over Authenticator Validation Data that has been entrusted to them and that the data has not been compromised	Cryptographic proof of key possession using asymmetric key

LoA 4	AAL 4	Cf	•Satisfies all Level 4 Authentication Conformance Criteria •Very high confidence required that an *Entity* has maintained control over Authenticator Validation Data that has been entrusted to them and that the data has not been compromised	Sealed hardware token / keys stored in a trusted platform module
LoA 4	AAL 4	Cg		Locally verified biometric

565 **Figure 22: Credential Assurance Map**

566 ## 5.2.5 Primary Credential Management

567 The primary credential management component of this vector definition represents
568 distinct categories of management that may be considered separately or together in a
569 single transaction. When appropriate, multiple distinct values from this category may be
570 used in a single transaction. This component is intended to align with the Vectors of
571 Trust Default Component Value Definitions specified in Appendix A, section A.3 of
572 RFC8485. This component may not be included in a vector if no assessment has been
573 done with the PCTF Authentication component, or such an assessment has found that
574 no defined *Level of Assurance* has been met (a condition that should be documented as
575 "T0"). The *Level of Assurance* resulting from the Authentication assessment should be
576 expressed in the same vector with a "T" component.

577 ## 5.2.6 Credential Management Map

Traditional Assurance Level	Discrete Assurance Level	Corresponding Vector ID	Common Characteristics	Vector ID Defining Characteristics

LoA 1	CAL 1	Ma	Satisfies all Level 1 Authentication or Credentials (Relationships and Attributes) Conformance Criteria Little confidence required that an *Entity* has maintained control over Authenticator Validation Data that has been entrusted to them and that the Credential has not been compromised	Self-asserted primary *Authenticator* (user chooses their own credentials and must rotate or revoke them manually); no additional verification for primary credential issuance or rotation
LoA 2	CAL 2	Mb	Satisfies all Level 2 Authentication or Credentials (Relationships and Attributes) Conformance Criteria Some confidence required that an *Entity* has maintained control over a Authenticator Validation Data that has been entrusted to them and that the Credential has not been compromised	Remote issuance and rotation; use of backup recover credentials (such as email verification); deletion on user request

LoA 3	CAL 3	Mc	Satisfies all Level 3 Authentication or Credentials (Relationships and Attributes) Conformance Criteria High confidence required that an *Entity* has maintained control over a Authenticator Validation Data that has been entrusted to them and that the Credential has not been compromised	Full proofing required for each issuance and rotation; revocation upon suspicious activity detection

578 **Figure 23: Credential Usage Map**

579 ## 5.2.7 Assertion Presentation

580 The assertion presentation component of this vector definition represents distinct
581 categories of assertion that are recommended to be used in a subsumptive manner but
582 may be used together. When appropriate, multiple distinct values from this category
583 may be used in a single transaction. This component is intended to align with the
584 Vectors of Trust Default Component Value Definitions specified in Appendix A, section
585 A.4 of RFC8485. This component may not be included in a vector if no assessment has
586 been done with the PCTF Authentication component, or such an assessment has found
587 that no defined *Level of Assurance* has been met (a condition that should be
588 documented as “T0”). The *Level of Assurance* resulting from the Authentication
589 assessment should be expressed in the same vector with a “T” component.

590 **Note:** The PCTF does not currently provide conformance criteria to guide the selection
591 of appropriate values to include for the Assertion Presentation component. An assessor
592 may rely on the set of information security guidelines and controls identified for
593 conformance with BASE 6 and/or BASE 7 in the Authentication Conformance Profile.

594 ## 5.2.8 Presentation Assurance Map

Traditional Assurance Level	Discrete Assurance Level	Corresponding Vector ID	Common Characteristics	Vector ID Defining Characteristics

LoA 1	PAL 1 FAL 1 (NIST)	Aa	Satisfies the criteria in BASE 6 of the Authentication conformance criteria	No protection; unsigned bearer identifier (e.g., HTTP session cookie in a web browser)
LoA 2	PAL 2 FAL 2 (NIST)	Ab	Satisfies the criteria in BASE 7 of the Authentication conformance criteria	Signed and verifiable assertion, passed through the user agent (web browser)
LoA 2	PAL 2 FAL 2 (NIST	Ac	Satisfies the criteria in BASE 7 of the Authentication conformance criteria	Signed and verifiable assertion; passed through a back channel
LoA 2	PAL 2 FAL 2 (NIST)	Ad	Satisfies the criteria in BASE 7 of the Authentication conformance criteria	Assertion encrypted to the *Relying Party*'s key

Figure 24: Presentation Assurance Map

6. Risk Evaluation

Figure 25 contains an enumeration of risks commonly used to assess the *Level of Assurance* required for a specific digital interaction. It should be noted that this table is meant to be illustrative in nature. It is not intended to be exhaustive, nor is it meant to be directive. Accordingly, this table is not presenting additional conformance criteria and does not have to be used as part of an assessment. *Relying Parties* must evaluate the potential risks and harms they are likely to face, and assess the levels of risk they are willing to accept for a specific transaction within their operational context. As such, some of the illustrative criteria uses terminology that is subject to interpretation (e.g., "high", "medium", "low"). This enables practitioners to establish a risk profile that is commensurate with their ministry, department, or type of business. For example, a large financial institution may consider the risk of losing $100,000 as "limited" or "low" whereas a risk of that size may be "severe" or "high" for a small business, startup, or individual.

Since the risk levels are a function of a *Relying Party*'s unique circumstances and any policy, legislation, and/or regulation they are subject to, it is incumbent upon the *Relying Party* to explicitly document their risk tolerance. This will ensure that risk controls are consistently implemented and that they are neither too lenient, nor too stringent regardless of the persons who implement them. It will also ensure the controls are fairly assessed when audited. These risks should also be documented so they are evident to, and clearly understandable by, *Entities* with whom they interact.

Figure 25 contains an illustrative table risks to help *Relying Parties* understand how they can evaluate their own risks and make a determination of the LoA they require.

Impact Category	**Assurance Level Required**			
	LoA 1 or equivalent	**LoA 2 or equivalent**	**LoA 3 or equivalent**	**LoA 4 or equivalent**
Inconvenience, distress, damage to standing or reputation	At worst, limited, short-term inconvenience, distress, embarrassment or damage to the standing or reputation of any party	At worst, serious short-term or limited long-term inconvenience, distress or damage to the standing or reputation of any party	Severe or serious long-term inconvenience, distress or damage to the standing or reputation of any party (ordinarily reserved for situations with severe effects or which affect many individuals)	A severe and permanent inconvenience, distress or damage to the standing or reputation of any party
Financial loss	At worst, an insignificant or inconsequential financial loss to any party, or at worst an inconsequential liability	At worst, a serious financial loss to any party, or a serious liability	A severe financial loss to any party, or a severe liability	A catastrophic financial loss to any party, or a catastrophic liability

Harm to a program or public interest	At worst, a limited adverse effect on organizational operations or assets or government organization, program, asset or the public interest (e.g., mission capability degradation to the extent and duration that the organization is able to perform its primary functions with noticeably reduced effectiveness; minor damage to organizational assets or public interests)	At worst, a serious adverse effect on organizational operations or assets or government organization, program, asset or the public interest (e.g., significant mission capability degradation to the extent and duration that the organization is able to perform its primary functions with significantly reduced effectiveness; significant damage to organizational assets or public interests)	A severe adverse effect on organizational operations or assets or government organization, program, asset or the public interest (e.g., severe mission capability degradation or loss of to the extent and duration that the organization is unable to perform one or more of its primary functions; major damage to organizational assets or public interests)	A catastrophic adverse effect on organizational operations or assets or government organization, program, asset or the public interest (e.g., catastrophic mission capability degradation or loss of to the extent and duration that the organization is unable to perform its primary functions; catastrophic damage to organizational assets or public interests)

Unauthorized release of sensitive personal or commercial information	At worst, a limited release of personal information or commercially sensitive information to unauthorized parties, or breach of privacy, resulting in a loss of confidentiality with a low impact	At worst, a release of personal information or commercially sensitive information to unauthorized parties, or breach of privacy, resulting in a moderate impact	A release of personal information or commercially sensitive information to unauthorized parties, or breach of privacy, resulting in a serious impact	A release of personal information or commercially sensitive information to unauthorized parties, or breach of privacy, resulting in a catastrophic impact
Unauthorized release of sensitive government information	A loss of confidentiality with a low impact	A limited adverse effect on organizational operations and assets due to a loss of confidentiality resulting from the release of sensitive government information to unauthorized parties	A serious adverse effect on organizational operations and assets due to a loss of confidentiality resulting from the release of sensitive government information to unauthorized parties	A catastrophic effect on organizational operations and assets due to a loss of confidentiality resulting from the release of sensitive government information to unauthorized parties

Civil or criminal violations	Private sector: At worst, a risk of civil or criminal violations of a nature that would not ordinarily be subject to enforcement efforts Public sector: Any compromise involving a legal violation is assessed at a minimum of Level 2	A civil or criminal violation that may have minor consequences and that may be subject to enforcement efforts	A civil or criminal violation that may have serious consequences that are of importance to enforcement programs	A violation that may have exceptionally grave consequences that are of special importance to enforcement programs
Personal health and safety	Private sector: At worst, minor injury not requiring medical treatment Public sector: Any compromise health and safety is assessed at minimum of Level 2	Private sector: At worst, moderate risk of minor injury or limited risk of injury requiring medical treatment Public sector: A minor personal injury not requiring medical attention	Private sector: At worst, a low risk of serious injury or death Public sector: A personal injury requiring medical attention	Risk of serious personal injury or death

National interest	(Any compromise involving the national interest is assessed at a minimum of Level 2)	A disadvantage to the national interest	An injury to the national interest	A serious or exceptionally grave injury to the national interest

Figure 25: Risk Evaluation (Illustrative)

7. References

This section lists key external standards, guidelines, and other documents referenced in creation of this PCTF module.

Note

- Where applicable, only the version or release number specified herein applies.

This component of the PCTF leverages the skills, experience, and lessons learned of other organizations working to improve this domain, and has taken into consideration material from the following sources:

- Internet Engineering Task Force (IETF): Request for Comments 8485, Vectors of Trust <https://www.rfc-editor.org/info/rfc8485>
- U.S. Department of Commerce, National Institute of Standards and Technology: NIST Special Publication 800-63-3 Digital Identity Guidelines <https://pages.nist.gov/800-63-3/sp800-63-3.html>
- Government of Canada, Treasury Board of Canada Secretariat: Public Sector Profile of the Pan-Canadian Trust Framework Version 1.1 <https://canada-ca.github.io/PCTF-CCP/>
- TBS Guidelines on Identity Assurance
- World Wide Web Consortium (W3C): Verifiable Credentials Data Model 1.0 <https://www.w3.org/TR/vc-data-model/>

8. PCTF Vectors of Trust Standard Specification

8.1 Trustmark URL

The URL for the DIACC PCTF Vectors of Trust Trustmark is <to be determined>. The value of the vtm field shall be <the same to be determined value>.

8.2 Vectors of Trust Component Registry

This specification adds the following values to the "Vector of Trust Components" registry established by [RFC8485] for use with the DIACC PCTF Vectors of Trust Trustmark.

- Demarcator Symbol: I
- Description: Identity Proofing
- Change Controller: DIACC
- Specification document(s): [PCTF Assurance Maturity Model]
- Demarcator Symbol: C
- Description: Credential Usage
- Change Controller: DIACC
- Specification document(s): [PCTF Assurance Maturity Model]
- Demarcator Symbol: M
- Description: Credential Management
- Change Controller: DIACC
- Specification document(s): [PCTF Assurance Maturity Model]
- Demarcator Symbol: A
- Description: Presentation
- Change Controller: DIACC
- Specification document(s): [PCTF Assurance Maturity Model]
- Demarcator Symbol: T
- Description: Authentication
- Change Controller: DIACC
- Specification document(s): [Authentication Component Overview] and [Authentication Conformance Profile]

- Demarcator Symbol: P
- Description: Verified Person
- Change Controller: DIACC
- Specification document(s): [Verified Person Component Overview] and [Verified Person Conformance Profile]

- Demarcator Symbol: O
- Description: Verified Organization
- Change Controller: DIACC
- Specification document(s): [Verified Organization Component Overview] and [Verified Organization Conformance Profile]

- Demarcator Symbol: R
- Description: Credentials (Relationships & Attributes)
- Change Controller: DIACC

- Specification document(s): [Credentials (Relationships & Attributes) Component Overview] and [Credentials (Relationships & Attributes) Conformance Profile]

- Demarcator Symbol: V
- Description: Privacy
- Change Controller: DIACC
- Specification document(s): [Privacy Component Overview] and [Privacy Conformance Profile]

- Demarcator Symbol: N
- Description: Notice & Consent
- Change Controller: DIACC
- Specification document(s): [Notice & Consent Component Overview] and [Notice & Consent Conformance Profile]

- Demarcator Symbol: S
- Description: Infrastructure (Technology & Operations)
- Change Controller: DIACC
- Specification document(s): [Infrastructure (Technology & Operations) Component Overview] and [Infrastructure (Technology & Operations) Conformance Profile]

9. Revision History

Version	Date	Author	Comment
0.01	2020-09-29	PCTF Editing Team	Initial draft
0.02	2021-01-29	Design Team	Address comments received from initial TFEC review
0.03	2021-05-17	Design Team	Align Vectors of Trust section with current PCTF components and additional updates from Design Team review
1.0	2021-06-09	Design Team	Approved by the TFEC as a Draft Recommendation V1.0