



1
2 **PCTF Authentication Conformance Profile**

3 Document Status: Final Recommendation V1.1

4 In accordance with the [DIACC Operating Procedures](#), Final Recommendations are a
5 deliverable that represents the findings of a DIACC Expert Committee that have been
6 approved by an Expert Committee and have been ratified by a DIACC Sustaining
7 Member Ballot.

8 This document has been developed by DIACC's [Trust Framework Expert Committee](#). It
9 is anticipated that the contents of this document will be reviewed and updated on a
10 regular basis to address feedback related to operational implementation, advancements
11 in technology, and changing legislation, regulations, and policy. Notification regarding
12 changes to this document will be shared through electronic communications including
13 email and social media. Notification will also be recorded on the [Pan-Canadian Trust
14 Framework Work Programme](#).

15 This document is provided "AS IS," and no DIACC Participant makes any warranty of
16 any kind, expressed or implied, including any implied warranties of merchantability, non-
17 infringement of third party intellectual property rights, and fitness for a particular
18 purpose. Those who are seeking further information regarding DIACC governance are
19 invited to review the [DIACC Controlling Policies](#).

20 IPR: [DIACC Intellectual Property Rights V1.0 PDF](#) | © 2023

21

22

23

24

25

26

27

28

29

30

31

32

33

34

35

36

37

38

39

40

41

42

43

44

45

46

47

48

49

50

51

52

53

54

55

Table of Contents

1. Introduction to the PCTF Authentication Component Conformance Criteria	3
1.1 About PCTF Conformance Criteria.....	3
2. Authentication Conventions	4
2.1 Conformance Criteria Keywords	4
3. Authentication Risks	5
4. Authentication Component Conformance Criteria	15

56

57 **1. Introduction to the PCTF Authentication** 58 **Component Conformance Criteria**

59 This document specifies the Conformance Criteria of the PCTF Authentication
60 Component, a component of the Pan-Canadian Trust Framework (PCTF). For a general
61 introduction to the Pan-Canadian PCTF, please see the PCTF Model Overview. The
62 PCTF Model Overview provides the PCTF’s goals and objectives, a high-level model
63 outline of the PCTF, and contextual information.

64 Each PCTF component is made up of two documents:

- 65 1. **Overview** – Introduces the subject matter of the component. The overview
66 provides information essential to understanding the Conformance Criteria of the
67 component. This includes definitions of key terms, concepts, and the Trusted
68 Processes that are part of the component.
- 69 2. **Conformance profile** – Specifies the Conformance Criteria used to standardize
70 and assess the integrity of the Trusted Processes that are part of the component.

71 The Conformance Criteria specified herein can be used to assure the on-going integrity
72 of login and authentication processes such that they result in the representation of a
73 unique Subject at a Level of Assurance that it is the same Subject with each successful
74 login to an Authentication Service Provider.

75 **1.1 About PCTF Conformance Criteria**

76 The PCTF promotes trust through a set of auditable business and technical requirements
77 for various processes.

78 A process is a business or technical activity (or set of such activities) that transforms an
79 input condition to an output condition – an output on which other processes often
80 depend. Conformance Criteria are the requirements and specifications that comprise a
81 standard for these processes. They can be used to assess the integrity of a process. In
82 the PCTF context, a process is designated a Trusted Process when it is assessed and
83 certified as conforming to Conformance Criteria defined in a PCTF conformance profile.

84 The integrity of a process is paramount because many Participants—across
85 jurisdictional, organizational, and sectoral boundaries and over the short-term and long-
86 term—rely on the output of that process. Conformance criteria are therefore central to
87 the trust framework because they specify the requirements that ensure process integrity.
88

89 **Note:** PCTF Conformance Criteria do not replace or supersede existing regulations;
90 organizations and individuals are expected to comply with relevant legislation, policy and
91 regulations in their jurisdiction.

92 2. Authentication Conventions

93 Each PCTF component includes conventions that ensure consistent use and
94 interpretation of terms and concepts appearing in the component. **The**
95 **PCTF Authentication Component Overview provides conventions for this**
96 **component.** These conventions include definitions and descriptions of the following
97 items that are referred to in this conformance profile:

- 98 • Key terms and concepts
- 99 • Abbreviation and acronyms
- 100 • Roles
- 101 • Levels of Assurance
- 102 • Trusted Processes and associated conditions

103

104 **Note:**

- 105 • Conventions may vary between PCTF components. Readers are encouraged to
106 review the conventions for each PCTF component they are reading.
- 107 • Defined Terms – For purposes of this conformance profile, terms and definitions
108 listed in both the PCTF Authentication Component Overview and the PCTF
109 Glossary apply. Key terms and concepts described and defined in this section, or
110 the PCTF Authentication Component Overview, or the PCTF Glossary are
111 capitalized throughout this document.
- 112 • Hypertext Links – Hypertext links may be embedded in electronic versions of this
113 document. All links were accessible at time of writing.
- 114 • All references to the term ‘credential within this document refer to an
115 ‘Authentication Credential’. The shorter version is used herein to improve
116 readability.

117 2.1 Conformance Criteria Keywords

118 Throughout this document the following terms indicate the precedence and/or general
119 rigidity of the Conformance Criteria and are to be interpreted as noted below.

- 120 • **MUST** means that the requirement is absolute as part of the Conformance
121 Criteria.
- 122 • **MUST NOT** means that the requirement is an absolute prohibition of the
123 Conformance Criteria.
- 124 • **SHOULD** means that while there may exist valid reasons in particular
125 circumstances to ignore the requirement, the full implications must be understood
126 and carefully weighed before choosing to not adhere to the Conformance Criteria
127 or choosing a different option as specified by the Conformance Criteria.

- 128 • **SHOULD NOT** means that a valid exception reason may exist in particular
- 129 circumstances when the requirement is acceptable or even useful, however, the
- 130 full implications should be understood and the case carefully weighed before
- 131 choosing to not conform to the requirement as described.
- 132 • **MAY** means that the requirement is discretionary but recommended.
- 133

134 **Note:** The above listed keywords appear in **bold** typeface and ALL CAPS throughout
135 this conformance profile.

136 3. Authentication Risks

136a	Type of Risk	Threat category	Threat scenario / Vulnerability	Additional info	Threat Agent	Impact	Proposed safeguards (e.g., input to conformance requirements)
136b	Information security → harm to Holder, harm to Relying Parties	Product or service quality risk	Product or service contains software vulnerabilities	Accidental or malicious intent	<ul style="list-style-type: none"> • Hacker/attacker • Unintended consequences of software flaws 	<p>Harm to ecosystem participants:</p> <ul style="list-style-type: none"> • Trust in ecosystem • Reputational risk of ecosystem as a whole <p>Harm to Holder:</p> <ul style="list-style-type: none"> • Identity theft • Financial harm • Loss of privilege/access/use • Reputational harm <p>Harm to Relying Parties:</p>	<ul style="list-style-type: none"> • Product or service undergoes a certification process, and as appropriate, re-certification process, and has a Trustmark proving implementer follows standard industry practice product development processes throughout entire lifecycle. • Considerations for supply chain integrity validation, security in the SDLC, 3rd party security assessments, vulnerability management process

Pan-Canadian Trust Framework
PCTF Authentication Final Recommendation V1.1
DIACC / PCTF03

						<ul style="list-style-type: none"> • Financial harm • Loss of privilege/access/use • Reputational harm • Privacy harm 	
136c	Information security lifecycle management → user inconvenience	Product or service quality risk	Product or service is no longer supported and is obsolete	<ul style="list-style-type: none"> • Unpatched flaws • Lack of interoperability/utility 	<ul style="list-style-type: none"> • Malicious actors targeting unpatched software • Unusable software (incompatible) 	<ul style="list-style-type: none"> • Holder is unable to perform required transactions • Credential or access compromised 	<ul style="list-style-type: none"> • Product and/or service should be updated or replaced with a compatible and/or more secure replacement and a patch management regimen should be maintained
136d	Information security → harm to Holder	Product or service provider integrity/supply chain risk	Malicious actors provide product or service with intent to harm customers	Malicious actors provide product or service. This may resemble a well-known product or service.	Malicious product or service provider	<ul style="list-style-type: none"> • Impersonate Holder • Privacy harm to Holder • Reputational harm to Holder 	Customer properly assesses product or service providers; Customers may rely on certifications and/or Trustmarks
136e	Information security lifecycle management → user inconvenience.	Product or service quality risk	Product or service does not implement, or conform to, industry standards	Product or service is unable to interoperate with applications or other systems	Product or service provider	<ul style="list-style-type: none"> • Denial of Service to the Customer • Holder is unable to perform required 	<ul style="list-style-type: none"> • Product or service implements industry standards as proved by an appropriate certification program or Trustmark

Pan-Canadian Trust Framework
PCTF Authentication Final Recommendation V1.1
DIACC / PCTF03

					<p>transactions</p> <ul style="list-style-type: none"> • Issuer unable to issue • Verifier not able to verify 	<ul style="list-style-type: none"> • Verify interoperability with recognized industry standards such as X.509, TOTP, SAML, OIDC family, W3C Verifiable Credentials, etc. 	
135f	Information security → harm to Holder.	Product or service quality risk	Product or service has inadequate technical security controls or management practices	Implementation of product/service was not appropriately monitored	Hacker	System is easily compromised, which could expose data, or allow a sophisticated attacker to issue unauthorized Credentials or to bypass access controls	<ul style="list-style-type: none"> • Product or service provider undergoes a certification process and has a Trustmark proving conformance to standard industry practices. • Considerations for supply chain integrity validation, security in the SDLC, 3rd party security assessments, vulnerability management process
136g	Information security: key management → harm to Subjects	Unauthorized data access risk	Operating environment does not support required security functions for specific/target LOA(s)	Standard industry key management tools and processes are not used, or not used effectively	Malicious actor (local or remote)	Compromised keys/privacy breach/identity theft/unauthorized data access	<ul style="list-style-type: none"> • Product or service provider explicitly supports adequate/evaluated key management capability <p>Note:</p> <ul style="list-style-type: none"> • This includes key management functions & high-impact security functions managed on

Pan-Canadian Trust Framework
PCTF Authentication Final Recommendation V1.1
DIACC / PCTF03

						product or service infrastructure and/or end-user equipment <ul style="list-style-type: none"> • “Adequate” (FIPS for hardware, NIST for software) will depend on LOA
136h	Information security: key management security → harm to Subjects	Backup and recovery risks/key management risks	Product or service has inadequate backup and recovery controls	Malicious actor steals secret keys using backup/recovery mechanism	Malicious actor (local or remote)	Compromised keys/unauthorized data access/privacy breach/identity theft <ul style="list-style-type: none"> • Backup and recovery processes to be defined for the corresponding LOA and assessed as part of the certification process • Backups must have same LOA protections as the original or “live service” protections
136i	Information security: key management security → harm to Subjects	Infrastructure, software or device-related security risks/key management risks	Product or service does not support required security functions for specific/target LOA(s).	<ul style="list-style-type: none"> • Product or service software does not have adequate key management protections. • Malicious actor steals secret keys 	Malicious actor (local or remote)	Compromised keys/unauthorized data access/privacy breach/identity theft <ul style="list-style-type: none"> • Product or service uses adequate/evaluated key management software and/or hardware with non-exportable keys • Note: “adequate” (NIST for software) will depend on LOA

			(e.g., steals key from memory, cracks white box crypto, power analysis)			
136j	Information security: data analytics → harm to Subjects	Data analytics in the Product or Service	Product or service allows (or does not properly disallow) sharing of sensitive information. (e.g., Sensitive information being passed in data analytics collection)	Unintentional or intentional	Malicious actor or insufficiently trained workforce	<ul style="list-style-type: none"> • Sensitive data leakage in analytics data • Privacy breach/identity theft <ul style="list-style-type: none"> • If sensitive data required in analytics, ensure anonymized, or tokenized and encrypted before being sent - including before saved to local storage in offline modes and backups • Trust mark to ensure privacy risk assessment is completed when adding/modifying data analytics - where assessment includes risk of unintended use of analytics data • Trust mark to ensure access control requirements on access to analytics data • Training of workforce with

Pan-Canadian Trust Framework
PCTF Authentication Final Recommendation V1.1
DIACC / PCTF03

						standard data privacy practices	
136k	Information security: environment security → harm to Subjects	Insider security risks	Product or service provider personnel are compromised	Social Engineering	Unauthorized data access/Non-Subject Access	Privacy breach/identity theft	<ul style="list-style-type: none"> Product or service provider to check for known vulnerabilities on launch, notifies Subjects/Customers of specific vulnerabilities and required corrective actions prior to product or service use LOA driven requirements
136l	Information security: environment security → harm to Subject	Insider security risks	Credential holder is compromised	Social Engineering	Unauthorized data access/Non-Subject Access	Privacy breach/identity theft	<ul style="list-style-type: none"> Product or service provider to check for known vulnerabilities on launch, notifies Subjects/customers of specific vulnerabilities and required corrective actions prior to product or service use LOA driven requirements
136m	Information security: Binding and authentication → harm to Subject	Unauthorized use of the product or service	Authenticator compromise	When users share devices, authenticators without proper access controls could allow others to share the	<ul style="list-style-type: none"> Hackers Acquaintances Family Members 	Assertions are made on the behalf of the user without their consent	<ul style="list-style-type: none"> Include specific language in the EULA to ensure authorized users understand their responsibility. Provide authentication experiences that do not depend exclusively on possession and

			information of the authorized holder without their consent			control of a single device. <ul style="list-style-type: none"> Apply additional Anti-Spoofing and Liveness Detection Techniques (ISO-30107) 	
136n	Privacy → user tracking	User tracking	Identifying information correlation without notice or consent	Product or service uses common identifiers across multiple verifiers	Invasion of privacy	<ul style="list-style-type: none"> Linking of identifiers across Verifiers User tracking Data aggregation 	<ul style="list-style-type: none"> Product or service uses standard unique identifiers technologies such as: <ul style="list-style-type: none"> URI (e.g., various DID methods) UUID GUID
136o	Privacy → oversharing	Oversharing	Product or service does not support data minimization	Subject provides more information to Verifier than appropriate	<ul style="list-style-type: none"> Rogue Verifier targeting user of specific Product or Service that does not offer data minimization capabilities Unintended Verifier that receives more information 	<ul style="list-style-type: none"> Holder provides more information to Verifier than appropriate Privacy breach/identity theft Verifier privacy regulation non-compliance for receipt of data it did not have a business need for 	Product or service to support data minimization capabilities (e.g., selective disclosure, ZKP)

				than it asked for/needs	<ul style="list-style-type: none"> Inability for government Verifier use as government may not have authority to receive additional information not asked for 		
136p	Privacy → oversharing	Oversharing	End-user choice of Credential and/or claims may result in disclosure of information not strictly required	Incomplete, unclear, or ambiguous notice	<ul style="list-style-type: none"> Product or Service provider (introduces threat) - quality issue Rogue Verifier targeting user of specific Products or Services that do not offer proper notice 	<ul style="list-style-type: none"> Holder provides more information to Verifier than they would have otherwise agreed to; Decisions being made by Verifier on that information could have negative impact to that user Holder not able to accurately 	<ul style="list-style-type: none"> Product or service effectively discloses information to be shared to Holder and allows Holder to control Data that may not be 'understandable' (i.e., encoded data) should be described in plain language

Pan-Canadian Trust Framework
PCTF Authentication Final Recommendation V1.1
DIACC / PCTF03

						ly assess risk of information disclosure	
136q	Privacy → oversharing	Oversharing	Product or service collects more claims than are strictly required	Subject provides more information to Verifier than appropriate. Incomplete, unclear, or ambiguous notice	Product or service provider puts additional information at risk	Holder not able to accurately assess risk of information disclosure	<ul style="list-style-type: none"> Product or service effectively limits information it collects Product or service provides full and complete notice to the Holder.
136r	Compliance → privacy	Privacy	Product or service does not conform to PCTF Privacy component	N/A	N/A	Privacy non-compliance	Trustmark to ensure PCTF Privacy Component compliance as part of product or service certification
136s	Accessibility	User experience	Product or service does not conform to industry accessibility standards	N/A	N/A	<ul style="list-style-type: none"> Holder is unable to use product or service due to disabilities; Subject vulnerable population to alternate processes or tools that may carry different 	Product or service implements industry standard accessibility capabilities

Pan-Canadian Trust Framework
PCTF Authentication Final Recommendation V1.1
DIACC / PCTF03

					<ul style="list-style-type: none"> risks to privacy Abandonment; reputational risk Lack of service; Over-sharing of data 		
136t	Usability	User experience	Product or service instructions are not clear	<ul style="list-style-type: none"> Product or service instructions are not clear to the Holder Notice is unclear or ambiguous Poor user experience 	N/A	<ul style="list-style-type: none"> Holder uses product or service in an unintended way that results in harm to the Holder Release of PII to unintended recipient (accidental privacy breach; phishing) 	<ul style="list-style-type: none"> Product or service uses plain language and has consistent look and feel Robust product or service design: Prevent access to, or sharing from, without validating the entities information is being exchanged with
136u	Information security: data registry security → harm to Subject	Governance	Product or service relies on (trusts) a credential authority that is not (or no longer) appropriate	Product or Service trusts public key of malicious actor	Malicious actor that establishes a rogue data registry or registry entry	<ul style="list-style-type: none"> Users make unintentional/uninformed sharing decisions. Privacy breach/i 	Product or service authenticates Data Registry as Trusted; where, authentication implies a capability to ensure “is legitimate” or “is suitable for the defined purpose”

					identity theft		
136v	Information security: channel compromise → risks to Subject	Missing authentication	<ul style="list-style-type: none"> • Authentication channel is insecure or compromised. (i.e., Attacker in the Middle) • Insecure session management or session hijacking 	N/A	Malicious 3rd party	<ul style="list-style-type: none"> • Unauthorized data access, privacy • Identity theft • Unauthorized actions 	<ul style="list-style-type: none"> • Product or service implements appropriate controls to meet the selected LoA • Product or service has the controls it has implemented audited and/or actively tested for effectiveness
136w	Information security: stored information compromise	Compromised keys	Credential Storage: Insecure storage of Credentials can lead to unauthorized access if the stored data is compromised	<ul style="list-style-type: none"> • Secure backup • Secure key storage 	Malicious 3rd party	<ul style="list-style-type: none"> • Privacy breach • Identity theft • Authorized access to data and/or activity 	<ul style="list-style-type: none"> • Product or service implements appropriate controls to meet the selected LOA • Product or service has the controls it has implemented audited and/or actively tested for effectiveness

137 **4. Authentication Component Conformance**
138 **Criteria**

139 The following sections define Conformance Criteria that are essential requirements for
140 the Trusted Processes of the Authentication Component. The Authentication Trusted
141 Process are:

- 142 1. Credential Issuance
- 143 2. Authentication
- 144 3. Authenticated Session Initiation
- 145 4. Authenticated Session Termination
- 146 5. Credential Suspension
- 147 6. Credential Recovery

- 148 7. Credential Maintenance
149 8. Credential Revocation

150 Conformance criteria are categorized by Trusted Process and profiled in terms of Levels
151 of Assurance. Conformance Criteria are grouped by topic within each category. For ease
152 of reference, a specific conformance criterion may be referred to by its category and
153 reference number. Example: “**BASE-1**” refers to “Baseline Conformance Criteria
154 reference No. 1”.

155
156 **Note:**

- 157 • Baseline Conformance Criteria are also included as part of this conformance
158 profile.
- 159 • Conformance Criteria specified in other PCTF components of may also be
160 applicable to Authentication Trusted Processes under certain circumstances.
- 161 • Notification Conformance Criteria specified in this conformance profile represent
162 only those notifications specific to processes in the context of the
163 PCTF Authentication Component. See the PCTF Notice and Consent Component
164 for additional notification-related Conformance Criteria.
- 165 • LOA 4 is out of scope for this version. Reference is retained as a placeholder for
166 future development.
- 167 • Further guidance on policy and operational controls supporting the Authentication
168 Conformance Profile can be found in the PCTF Infrastructure (Technology &
169 Operations) Conformance Profile.

170

170a

170b

170c

170d

170e

170f

170g

Reference	Conformance Criteria	Level of Assurance (LOA)			
BASE	Baseline	LOA1	LOA2	LOA3	LOA4
EVENT LOGGING					
1	Credential use events MAY be logged and retained for a predefined period of time as evidence.	X			
2	Credential use events SHOULD be logged and retained for a predefined period of time as evidence.		X		
3	Credential use events MUST be logged and retained for a predefined period of time as evidence.			X	
4	Credential management and use event logs MUST be: <ul style="list-style-type: none"> • Traceable back to a specific Credential and include the result and date and time of the logged event. 		X	X	

Pan-Canadian Trust Framework
PCTF Authentication Final Recommendation V1.1
DIACC / PCTF03

		<ul style="list-style-type: none"> Protected by access controls to limit access only to those who require it (see NIST Special Publication 800-92 for recommendations concerning computer security log management). 				
170h	5	Credential management and use event logs MUST have a tamper-detection mechanism to detect unauthorized modifications.		X	X	
170i	6	Personal information and authenticator secrets (e.g., passwords, OTP values, security questions, security answers) MUST NOT be logged within the service.	X	X	X	
170j	INFORMATION SECURITY					
170k	7	The Credential Service Provider/Authentication Service Provider MAY ensure i) the integrity, ii) the confidentiality, and iii) the availability of the service by adhering to a set of information security guidelines and controls (e.g., CSEC ITSG-33) that support these efforts.	X			
170l	8	The Credential Service Provider/Authentication Service Provider MUST : Ensure i) the integrity, ii) the confidentiality, and iii) the availability of the service by adhering to a set of information security guidelines and controls (e.g., CSEC ITSG-33) that support these efforts.		X	X	
170m	9	The Credential Service Provider/Authentication			X	

		Service Provider MUST have an independently audited control report to demonstrate adherence to a set of information security guidelines and controls.				
170n	IT SERVICE MANAGEMENT					
	10	The Credential Service Provider/Authentication Service Provider SHOULD have a documented service management practice for all aspects of the service it provides related to PCTF Authentication Component Trusted Processes.	X			
170o	11	The Credential Service Provider/Authentication Service Provider MUST: Establish and maintain a documented service management practice for all aspects of the service it provides related to PCTF Authentication Component Trusted Processes.		X		
170p	12	The Credential Service Provider/Authentication Service Provider MUST: <ul style="list-style-type: none"> • Establish and maintain a documented service management practice for all aspects of the service it provides related to PCTF Authentication Component Trusted Processes. • Have a documented and independently audited service management practice for all relevant aspects of the service it provides related 			X	

Pan-Canadian Trust Framework
PCTF Authentication Final Recommendation V1.1
DIACC / PCTF03

		to PCTF Authentication Component Trusted Processes.				
170q	13	The Credential Service Provider/Authentication Service Provider SHOULD adhere to an industry standard service management framework (e.g., ITIL).	X	X		
170r	14	The Credential Service Provider/Authentication Service Provider MUST adhere to an industry standard service management framework (e.g., ITIL).			X	
170s	MONITORING					
170t	15	The Credential Service Provider/Authentication Service Provider SHOULD have controls to detect misuse or compromise of the Credential.	X			
170u	16	The Credential Service Provider/Authentication Service Provider MUST have controls to detect misuse or compromise of the Credential.		X	X	
170v	17	The Credential Service Provider SHOULD initiate the Credential Suspension process, the Credential Maintenance process, or the Credential Revocation process when it finds actionable indications of Credential misuse or compromise.	X			
170w	18	The Credential Service Provider MUST initiate the Credential Suspension process, the Credential Maintenance process, or the		X	X	

Pan-Canadian Trust Framework
PCTF Authentication Final Recommendation V1.1
DIACC / PCTF03

		Credential Revocation process when it finds actionable indications of Credential misuse or compromise.				
170x	PRIVACY					
170y	19	The Credential Service Provider/Authentication Service Provider SHOULD adhere to the privacy risk management practices of the PCTF Privacy Component and any relevant PCTF Profiles applicable to the digital ID service.	X			
170z	20	The Credential Service Provider/Authentication Service Provider MUST adhere to the privacy risk management practices of the PCTF Privacy Component and any PCTF Profiles applicable to the digital ID service.		X	X	
170aa	21	The Credential Service Provider/Authentication Service Provider MUST adhere to privacy risk management practices that are accepted by and applicable to all parties participating in the digital ID service.		X	X	
170ab	NOTIFICATIONS					
170ac	22	The Credential Service Provider MAY notify the Subject without delay (e.g., immediate notification by email, text, or as prescribed by a CSP's policy) of any changes to individual Credential information (e.g., password update, adding or removing Authenticators).	X			

Pan-Canadian Trust Framework
PCTF Authentication Final Recommendation V1.1
DIACC / PCTF03

170ad	23	The Credential Service Provider MUST notify the Subject without delay (e.g., immediate notification by email, text, or as prescribed by a CSP's policy) of any changes to individual Credential information (e.g., password update, adding or removing authenticators).		X	X	
170ae	CDIS	Credential Issuance	LOA1	LOA2	LOA3	LOA4
170af	BINDING SUBJECT					
170ag	1	The Credential Service Provider SHOULD enforce that the Credential is only bound to one Subject.	X			
170ah	2	The Credential Service Provider MUST enforce that the Credential is only bound to one Subject.		X	X	
170ai	3	The Credential Service Provider MAY document, or have a documented process for demonstrating, the Level of Assurance of the Subject's identity when the Credential was issued.	X			
170aj	4	The Credential Service Provider MUST document, or have a documented process for demonstrating, the Level of Assurance of the Subject's identity when the Credential was issued.		X	X	
170ak	5	The Credential Service Provider MUST make information available to Authentication Service Providers to verify the current state of any Credentials it has issued unless privacy constraints prohibit the sharing of this information (e.g., if a credential is an "Inaccessible Credential" or	X	X	X	

Pan-Canadian Trust Framework
PCTF Authentication Final Recommendation V1.1
DIACC / PCTF03

		a “Revoked Credential”, the minimum necessary status information must be available to Authentication Service Providers if allowable.)				
170al	BINDING AUTHENTICATORS					
170am	6	The Credential Service Provider MAY provide the ability to bind an Authenticator provided by the Subject to the Credential.	X	X	X	
170an	7	The Credential Service Provider MUST bind at least one Authenticator to the Credential. (e.g., password, Q&A, or OTP).	X			
170ao	8	The Credential Service Provider MUST bind two or more Authenticators to the Credential. (e.g., password, Q&A, or OTP).		X	X	
170ap	9	At least two different Authenticators SHOULD be bound to the Credential such that recovery of one authenticator (e.g., from loss or theft) is possible using another Authenticator (e.g., an authenticator account could be recovered with a one-time-use recovery code).		X		
170aq	10	At least two different Authenticators MUST be bound to the Credential such that recovery of the primary Authenticator (e.g., from loss or theft) is possible using another Authenticator (e.g., an authenticator account could be recovered with a one-time-use recovery code).			X	

Pan-Canadian Trust Framework
PCTF Authentication Final Recommendation V1.1
DIACC / PCTF03

170ar	11	Additional Authenticators, which could be used for recovery purposes, MUST be the same or higher LOA as an Authenticator to be recovered.		X	X	
170as	12	The Credential Service Provider MAY document, or have a documented process for, demonstrating the Level of Assurance of the Subject's identity when the Credential was recovered.	X			
170at	13	The Credential Service Provider MUST document, or have a documented process for, demonstrating the Level of Assurance of the Subject's identity when the Credential was recovered.		X	X	
170au	AUTHENTICATOR CREATION					
170av	14	When the Authenticator is created (e.g., hardware OTP device OR software OTP), the creator MUST have an auditable quality management system and control processes		X		
170aw	15	When the Authenticator is created (e.g., hardware OTP device OR software OTP), the creator MUST have an Independently auditable quality management system and control processes.			X	
170ax	16	When the Authenticator uses information embedded by a manufacturer (e.g., hardware OTP device OR software OTP), the Credential Service Provider MUST ensure that there is an auditable security management control process that protects that		X		

Pan-Canadian Trust Framework
PCTF Authentication Final Recommendation V1.1
DIACC / PCTF03

		information from compromise beginning from manufacture time through delivery to the Credential Service Provider.				
170ay	17	When the Authenticator uses information embedded by a manufacturer (e.g., hardware OTP device OR software OTP), the Credential Service Provider MUST ensure that there is an Independently Audited security management control process that protects that information from compromise beginning from manufacture time through delivery to the Credential Service Provider.			X	
170az	CREDENTIAL STORAGE					
170ba	18	The Credential Service Provider/Authentication Service Provider MUST enforce access controls to prevent unauthorized access to Credential information.	X	X	X	
170bb	19	Any secrets bound to the Credential MUST be either stored as a salted hash or stored encrypted.		X	X	
170bc	20	Any Credential attributes containing personal information that are stored within the service MUST be secured (e.g., encrypted and/or hashed).	X	X	X	
170bd	21	Backups of Credential information MUST be encrypted prior to being transferred to long term storage and MUST remain encrypted while in storage.		X	X	
170be	22	Cryptographic modules MUST meet an industry		X	X	

Pan-Canadian Trust Framework
PCTF Authentication Final Recommendation V1.1
DIACC / PCTF03

		recognized Validation standard (e.g., <u>FIPS 140-2</u>).				
170bf	AUTH	Authentication	LOA1	LOA2	LOA3	LOA4
170bg	AUTHENTICATORS					
170bh	1	<p>The Authentication Service Provider MUST require at least a single Authenticator of the following types:</p> <ul style="list-style-type: none"> • Something the Subject knows; • Something the Subject has; or, <p>Something the Subject is or does.</p>	X	X		
170bi	2	<p>If only a single Authenticator is required, that Authenticator MUST be of an Authenticator Type that is either "something the Subject knows" or "something the Subject has".</p> <p>The "something the Subject is or does" Authenticator Type MUST only be used as secondary Authenticators.</p>		X		
170bj	3	<p>The Authentication Service Provider MUST require at least two different Authenticators that:</p> <ul style="list-style-type: none"> • Provide different Authentication Factors; and <p>Are not susceptible to the same threat vectors.</p>			X	
170bk	4	<p>Of the different Authenticators required by the Authentication Service Provider by the AUTH criteria:</p> <ul style="list-style-type: none"> • One of the Authenticators MUST be of the type 			X	

		"something the Subject has"; and The other Authenticator(s) MAY be an Authenticator Type that is either "something the Subject knows" or "something the Subject is or does".				
170bl	5	The Authentication Service Provider MUST consult any information made available by the Credential Service Provider to determine the current state of a Credential.	X	X	X	
170bm	6	A biometric SHOULD NOT be used unless it is demonstrably necessary and is the best mechanism to meet a specific authentication need considering the commensurate potential loss of privacy.	X	X	X	
170bn	AUTHENTICATOR TYPE					
170bo	6	Any Authenticator Type MAY be used.	X			
170bp	7	The Authentication Service Provider MUST use an industry standard or best practice for authentication (e.g., standards and practices developed and approved by Kantara, W3C, IETF or FIDO Alliance).		X	X	
170bq	8	The Authentication Service Provider MUST use Authenticator Types that are resistant to the threats listed in the THREAT MITIGATION criteria for LOA3.			X	
170br	THREAT MITIGATION					
170bs	9	The Authentication Service Provider MUST have effective control processes	X			

Pan-Canadian Trust Framework
PCTF Authentication Final Recommendation V1.1
DIACC / PCTF03

		<p>to prevent, detect and recover from at least the following types of attacks:</p> <ul style="list-style-type: none"> • Authenticator secret guessing; and • Replay attacks. <p>This MAY be included in the scope of the guidelines described in the BASE criteria.</p>				
170bt	10	<p>The Authentication Service Provider MUST have effective control processes to prevent, detect and recover from at least the following types of attacks:</p> <ul style="list-style-type: none"> • Authenticator secret guessing; • Replay; • Eavesdropping; and • Session hijacking. <p>This MUST be included in the scope of the controls described in the BASE criteria.</p>		X		
170bu	11	<p>The Authentication Service Provider MUST have effective control processes to prevent, detect and recover from at least the following types of attacks:</p> <ul style="list-style-type: none"> • Authenticator secret guessing; • Replay; • Eavesdropping; • Session hijacking; • Impersonation/phishing; and • Man-in-the-middle attacks (e.g., using mutually authenticated TLS). 			X	

Pan-Canadian Trust Framework
PCTF Authentication Final Recommendation V1.1
DIACC / PCTF03

		This MUST be included in the scope of the independent audit process required by the BASE criteria.				
170bv	ADAPTIVE RISK					
170bw	12	The Authentication Service Provider MAY provide the ability to perform Adaptive Risk Authentication.	X			
170bx	13	The Authentication Service Provider SHOULD provide the ability to perform Adaptive Risk Authentication.		X		
170by	14	The Authentication Service Provider MUST detect and mitigate interactions that represent high risk, based on information from the context of the authentication (such as transactions that originate from an unexpected location or channel for a Subject, or that indicate an unexpected hardware or software configuration) -or- The Authentication Service Provider MUST treat every interaction as one that represents high risk.			X	
170bz	CRYPTOGRAPHIC MODULE					
170ca	15	Any cryptographic modules used in client-side authentication MUST meet an industry recognized Validation standard (e.g., <u>FIPS 140-2</u> or equivalent).		X	X	
170cb	AUTHENTICATION RESULT					
170cc	16	The Authentication Service Provider MUST return a	X	X	X	

Pan-Canadian Trust Framework
PCTF Authentication Final Recommendation V1.1
DIACC / PCTF03

		success result only when the Subject has successfully completed their authentication attempt.				
170cd	17	The Authentication Service Provider MUST return a failure result to an authentication attempt when the presented Credential is suspended or revoked, or Credential misuse or compromise is detected.	X	X	X	
170ce	18	The Authentication Service Provider MUST provide a mechanism that: <ul style="list-style-type: none"> • Confirms that the authentication result was originated by the Authentication Service Provider; • Was not tampered with in transit; and Is only usable by the Relying Party.		X	X	
170cf	19	The authentication result MUST be valid for a maximum period of time that is: <ul style="list-style-type: none"> • Specified by the Authentication Service Provider; and Known to the Relying Party.		X	X	
170cg	INSE	Authenticated Session Initiation	LOA1	LOA2	LOA3	LOA4
170ch	INITIATE SESSION					
170ci	1	The Authentication Service Provider SHOULD provide the ability to maintain a Session binding with all Relying Parties, where Authenticated Session Initiation is a supported process.	X			

Pan-Canadian Trust Framework
PCTF Authentication Final Recommendation V1.1
DIACC / PCTF03

170cj	2	The Authentication Service Provider MUST provide the ability to maintain a Session binding with all Relying Parties, where Authenticated Session Initiation is a supported process.		X	X	
170ck	3	If a Subject authenticates at a given LOA, the resulting Session MUST be considered to be the same LOA (e.g., if the Subject authenticates at LOA2, the Session must be considered LOA2), where Authenticated Session Initiation is a supported process.	X	X	X	
170cl	RE-AUTHENTICATION					
170cm	4	The Authentication Service Provider SHOULD require the Subject to re-authenticate after a predefined period of time or event as determined by a risk-based approach (e.g., when a single sign-on attempt is made to another Relying Party in a federation).	X			
170cn	5	The Authentication Service Provider MUST require the Subject to re-authenticate after a predefined period of time or event as determined by a risk-based approach (e.g., when a single sign-on attempt is made to another Relying Party in a federation or when a Relying Party requests re-authentication).		X	X	
170co	6	The Authentication Service Provider MAY extend Session timeouts.	X			
170cp	7	If the re-authentication is LOA2 or LOA3, the Session timeouts MAY be extended		X	X	

Pan-Canadian Trust Framework
PCTF Authentication Final Recommendation V1.1
DIACC / PCTF03

		but MUST match original LOA and meet all authentication criteria listed above.				
170cq	TESE	Authenticated Session Termination	LOA1	LOA2	LOA3	LOA4
170cr	SESSION TIMEOUT					
170cs	1	The Authentication Service Provider SHOULD enforce a maximum Session time to force re-authentication in a federated single sign-on scenario after the predefined Session time, where Authenticated Session Termination is a supported process.	X			
170ct	2	The Authentication Service Provider MUST enforce a maximum Session time to force re-authentication in a federated single sign-on scenario after the predefined Session time, where Authenticated Session Termination is a supported process.		X	X	
170cu	3	The Authentication Service Provider SHOULD enforce a maximum Session inactivity time to force re-authentication in a federated single sign-on scenario after the predefined Session time, where Authenticated Session Termination is a supported process.	X			
170cv	4	The Authentication Service Provider MUST enforce a maximum Session inactivity time to force re-authentication in a federated single sign-on scenario after the predefined Session time, where Authenticated		X	X	

Pan-Canadian Trust Framework
PCTF Authentication Final Recommendation V1.1
DIACC / PCTF03

		Session Termination is a supported process.				
170cw	5	Maximum Session time and maximum Session inactivity values at LOA3 SHOULD be shorter than for those for LOA2.			X	
170cx	6	A Session timeout due to exceeding maximum Session time or maximum Session inactivity time at LOA3, MAY result in either a Session termination, or a downgrade to a LOA2 Session.			X	
170cy	7	In the case of a Session downgrade: <ul style="list-style-type: none"> The Authentication Service Provider MUST notify all Relying Parties associated to the LOA3 Session; and <p>The Session timeouts due to exceeding maximum Session time or maximum Session inactivity time MAY be extended to their LOA2 values (minus the time which has already passed).</p>			X	
170cz	TERMINATE SESSION					
170da	8	The Authentication Service Provider SHOULD notify all Relying Parties that the Session has been terminated.	X			
170db	9	The Authentication Service Provider MUST notify all Relying Parties that the Session has been terminated.		X	X	
170dc	CRSP	Credential Suspension	LOA1	LOA2	LOA3	LOA4
170dd	SUBJECT INITIATED					
170de	1	The Credential Service Provider SHOULD provide	X	X	X	

Pan-Canadian Trust Framework
PCTF Authentication Final Recommendation V1.1
DIACC / PCTF03

		the ability for a Subject to initiate Credential suspension.				
170df	ADMINISTRATOR INITIATED					
170dg	2	The Credential Service Provider MAY provide the ability for authorized personnel to suspend the use of an Credential.	X	X	X	
170dh	3	The Credential Service Provider SHOULD enforce access controls to ensure only authorized personnel have access to this process.	X			
170di	4	The Credential Service Provider MUST enforce access controls to ensure only authorized personnel have access to this process.		X	X	
170dj	5	The Credential Service Provider MUST require authorized personnel to provide a LOA3 or higher Credential in order to suspend the use of an Credential.			X	
170dk	CRVY	Credential Recovery	LOA1	LOA2	LOA3	LOA4
170dl	SUBJECT INITIATED					
170dm	1	The Credential Service Provider SHOULD provide the Subject the ability to request the recovery of a suspended Credential, where Credential Recovery is a supported process.	X			
170dn	2	The Credential Service Provider SHOULD require the Subject to authenticate with a LOA equivalent to that of the Credential being recovered, where Credential Recovery is a supported process.	X			
170do	3	The Credential Service Provider MUST provide the Subject the ability to request		X	X	

Pan-Canadian Trust Framework
PCTF Authentication Final Recommendation V1.1
DIACC / PCTF03

		the recovery of a suspended Credential, where Credential Recovery is a supported process.				
170dp	4	The Credential Service Provider MUST require the Subject to authenticate with a LOA equivalent to that of the Credential being recovered, where Credential Recovery is a supported process.		X	X	
170dq	ADMINISTRATOR INITIATED					
170dr	5	The Credential Service Provider MAY provide the ability for authorized personnel to initiate Credential Recovery on behalf of the Subject.	X	X	X	
170ds	6	The Credential Service Provider SHOULD enforce access controls to ensure only authorized personnel have access to this process, where Credential Recovery is a supported process.	X			
170dt	7	The Credential Service Provider MUST enforce access controls to ensure only authorized personnel have access to this process, where Credential Recovery is a supported process.		X	X	
170du	8	The Credential Service Provider MUST require authorized personnel to provide a LOA3 or higher Credential in order to recover a Credential, where Credential Recovery is a supported process.			X	
170dv	SYSTEM INITIATED					
170dw	9	The Credential Service Provider MAY provide the ability to automatically recover a suspended	X	X	X	

Pan-Canadian Trust Framework
PCTF Authentication Final Recommendation V1.1
DIACC / PCTF03

		Credential (e.g., automatically reactivate a Credential previously suspended due to too many failed login attempts).				
170dx	CRMA	Credential Maintenance	LOA1	LOA2	LOA3	LOA4
170dy	SUBJECT INITIATED					
170dz	1	The Credential Service Provider SHOULD provide the ability to update the Authenticators bound to the Credential where possible (e.g., password change, bind a new Authenticator).	X			
170ea	2	The Credential Service Provider SHOULD provide the ability to allow Credential attributes (e.g., password, Q&A, recovery codes) to be modified.	X			
170eb	3	The Credential Service Provider MUST provide the ability to update the Authenticators bound to the Credential where possible (e.g., password change, change of PIN, refresh face image on file with more recent image, change of private key).		X	X	
170ec	4	The Credential Service Provider MUST provide the ability to allow Credential attributes (e.g., password, Q&A, recovery codes, cryptographic keys, biometrics, aliases, DIDs) to be modified.		X	X	
170ed	5	The Credential Service Provider MUST require authentication at a LOA equivalent to or greater than the LOA of the Credential attribute (e.g., password, Q&A, recovery codes, cryptographic keys,		X	X	

Pan-Canadian Trust Framework
PCTF Authentication Final Recommendation V1.1
DIACC / PCTF03

		biometrics, aliases, DIDs) being modified. For example, a Subject logged using a single-factor password should not be able to modify recovery codes, OTP values.				
170ee	ADMINISTRATOR INITIATED					
170ef	6	The Credential Service Provider MAY provide the ability to allow authorized personnel to update the Authenticators bound to the Credential (e.g., remove an Authenticator or initiate a password change).	X	X	X	
170eg	7	The Credential Service Provider MAY provide the ability to allow authorized personnel to update Credential attributes.	X	X	X	
170eh	8	The Credential Service Provider MUST enforce access controls to ensure only authorized personnel have access to this process.	X	X	X	
170ei	9	The Credential Service Provider MUST require authorized personnel to provide a LOA3 or higher Credential in order to perform Credential maintenance.			X	
170ej	10	The Credential Service Provider SHOULD require the Subject to complete any administrator initiated Credential activities (e.g., an administrator cannot change the Subjects password only initiate a reset).	X			
170ek	11	The Credential Service Provider MUST require the Subject to complete any administrator initiated Credential activities (e.g., an		X	X	

Pan-Canadian Trust Framework
PCTF Authentication Final Recommendation V1.1
DIACC / PCTF03

		administrator cannot change the Subjects password only initiate a reset).				
170el	SYSTEM INITIATED					
170em	12	The Credential Service Provider SHOULD enforce Authenticator control and protection requirements (e.g., Q&A complexity requirements, password updates, OTP updates) appropriate to the Authenticator (see NIST Special Publication 800-53 (Rev. 4) and Government of Canada Password Guidance for examples and references).	X			
170en	13	The Credential Service Provider MUST enforce Authenticator control and protection requirements (e.g., Q&A complexity requirements, password updates, OTP updates) appropriate to the Authenticator (see NIST Special Publication 800-53 (Rev. 4) and Government of Canada Password Guidance for examples and references).		X	X	
170eo	CRVX	Credential Revocation	LOA1	LOA2	LOA3	LOA4
170ep	SUBJECT INITIATED					
170eq	1	The Credential Service Provider SHOULD allow a Subject to revoke their own Credential.	X			
170er	2	The Credential Service Provider MUST allow a Subject to revoke their own Credential.		X	X	
170es	ADMINISTRATOR INITIATED					
170et	3	The Credential Service Provider MAY have the ability to allow authorized	X			

Pan-Canadian Trust Framework
PCTF Authentication Final Recommendation V1.1
DIACC / PCTF03

		personnel to revoke a Credential.				
170eu	4	The Credential Service Provider MUST have the ability to allow authorized personnel to revoke a Credential.		X	X	
170ev	5	The Credential Service Provider MUST enforce access controls to ensure only authorized personnel have access to this process.	X	X	X	
170ew	6	The Credential Service Provider MUST require authorized personnel to provide a LOA3 or higher Credential in order to revoke a Credential.			X	

171 **Table 1. PCTF Authentication Component Conformance Criteria**

172 _____

173 **Revision History**

	Version	Date of Issue	Author(s)	Description
173a	.01	2018-04-10	TFEC	Initial working draft
173b	.02	2018-07-31	DIACC Editor	Suggested changes to address outstanding review comments.
173c	.03	2019-04-30	DIACC Editor	<ul style="list-style-type: none"> • Formatting edits • Updated links to referenced standards
173d	.04	2019-07-08	DIACC Editor	<ul style="list-style-type: none"> • Standardize priority of requirement terms • Update PCTF model image
173e	.05	2019-10-21	TFEC and PCTF Editing Team	Revised content based on discussion draft comments.
173f	1.0	2019-10-30	TFEC	Approved as Draft Recommendation V1.0
173g	1.1	N/A	PCTF Editing Team	Updates per comments received during draft recommendation review period.
173h	1.0	2020-05-11	PCTF Editing Team	Final Recommendation V1.0
173i	1.1	2023-11-15	PCTF Authentication Design Team	Updates made to address feedback received through PCTF alpha testing

Status: Final Recommendation

Pan-Canadian Trust Framework
PCTF Authentication Final Recommendation V1.1
DIACC / PCTF03

173k

			and deferred comments from earlier iterations.
1.1	2023-12-01	PCTF Authentication Design Team	TFEC approves as Final Recommendation V1.1

174