

Le point sur la gestion pancanadienne de l'identité

Conseils mixtes
Le 24 février 2016

Comités sur la gestion de l'identité

Coprésidents du SCGI

Fred Pitt, province de l'Ontario, Secrétariat du Conseil du Trésor

Rita Whittle, gouvernement du Canada, Secrétariat du Conseil du Trésor

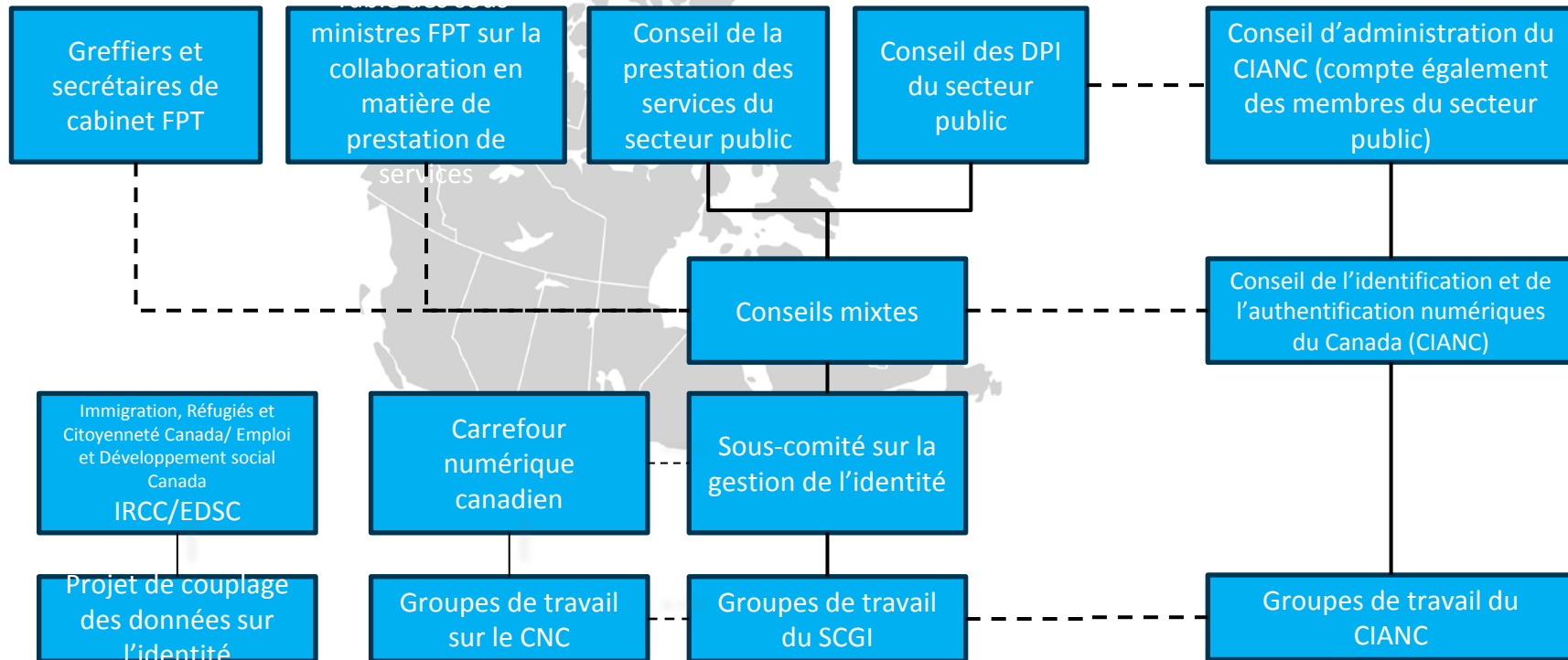
Objectifs

- Donner un aperçu du contexte pancanadien
- Faire le point sur les progrès réalisés relativement à l'établissement du Cadre pancanadien de la fiabilité de l'identité
- Discuter des prochaines étapes

Contexte pancanadien

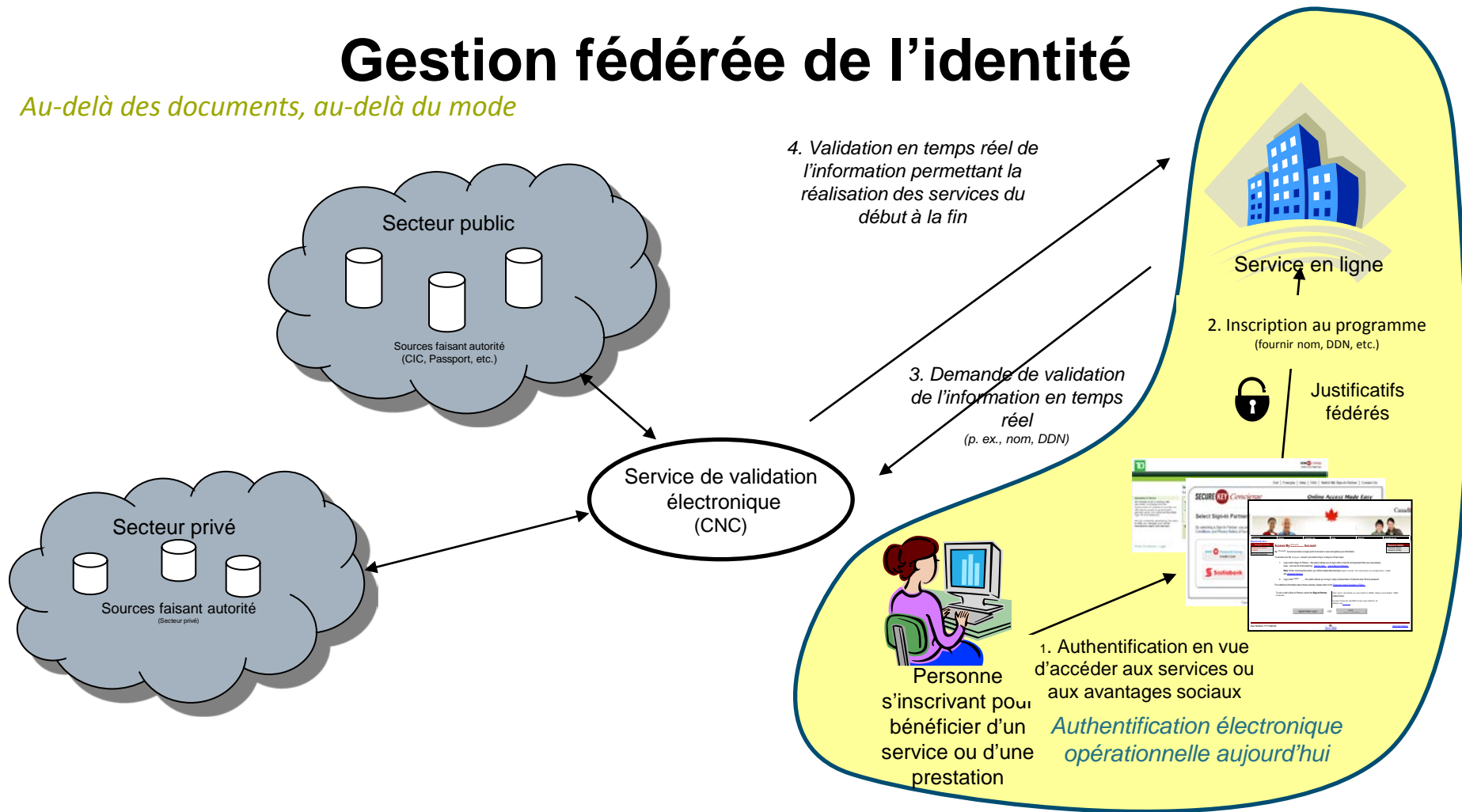
Secteur public

Initiatives du secteur privé et de l'industrie



Gestion fédérée de l'identité

Au-delà des documents, au-delà du mode



Fédération de l'identité : Jalons et initiatives

Jalons/produits livrables

- ✓ 2004 : Voie de communication protégée, y compris le service d'authentification epass, opérationnel
- ✓ 2007 : Rapport du groupe de travail sur la gestion de l'identité et authentification (GIA)
- ✓ 2008 : Rapport d'Auth. élec. sur les exigences futures du gouvernement du Canada
- ✓ 2009 : Directive sur la gestion de l'identité du SCT
- ✓ 2009 : Ligne directrice sur l'authentification du document ITSG-31
- ✓ 2010 : Modèle d'assurance pancanadien
- ✓ 2010 : Norme sur l'assurance de l'identité de la C.-B.
- ✓ 2010 : Norme sur les preuves d'identité de la C.-B.
- ✓ 2010 : Norme sur les justificatifs d'identité et l'authentification électroniques de la C.-B.
- ✓ 2010 : CIC (Programme des passeports) Technologie de reconnaissance faciale, opérationnelle
- ✓ 2010 : Auth. élec. DP 1/DP2/DP3
- ✓ 2011 : Fédération de l'identité pour le gouvernement du Canada : document d'information¹
- ✓ 2011 : Approche pancanadienne de la confiance dans l'identité du CDGI
- ✓ 2011 : Norme sur l'échange de données du Système national d'acheminement des données (SNA)
- ✓ 2012 : Spécifications techniques de l'authentification électronique
- ✓ 2012 : Volets Fiabilité
- ✓ 2012 : Architecture de courtier de la fédération de l'identité
- ✓ 2013 : Justificatifs d'identité fédérés du GC opérationnels
- ✓ 2013 : Norme sur l'assurance de l'identité et des justificatifs
- ✓ 2013 : Rapport de clôture sur l'authentification électronique
- ✓ 2013 : Passeport électronique opérationnel
- ✓ 2013 : Début de la délivrance des nouvelles cartes de services de la C.-B.
- ✓ 2013 : Service Québec maintenant responsable de clicSÉQR
- ✓ 2013 : L'Ontario approuve la politique sur l'identification, l'authentification et l'autorisation (IAA) électroniques
- ✓ 2014 : Norme pancanadienne sur la validation de l'identité
- ✓ 2015 : Norme du GC sur l'assurance de l'identité et lignes directrices connexes
- ✓ 2015 : Norme sur les renseignements sur l'identité de la C.-B.
- ❑ 2016 : Cadre pancanadien de la fiabilité de l'identité

*Leçons
retenues*

*Harmonisation
stratégique*

Initiatives/surveillance

Système national d'acheminement

- 2004-2006 : Projet pilote
- 2006-Présent : En cours de production

Renouvellement de l'authentification électronique

- 2008 : Création du comité des SM sur l'authentification électronique
- 2008-2010 : Consultation et stratégie
- 2010-2012 : Approvisionnement et transition
- 2012 : Services opérationnels : (SecureKey Service de concierge et CléGC)
- 2013 : Conclusion (membres SM intégrés au Comité des SM sur les services et la fédération de l'identité (SFI))

Gestion fédérée de l'identité

- 2010 : Ligne directrice sur la constitution du groupe de travail sur l'authentification
- 2011 : Ligne directrice sur le groupe de travail sur l'authenticité de l'identité
- 2013 : Projets pilotes (personnes/entreprises)
- 2013 : Groupe de travail sur les applications en matière juridique et politique
- 2014 : Carrefour numérique canadien
- 2015 : Projet de couplage des données sur l'identité

Groupe de travail sur l'examen du système des paiements

- 2012 : Recommandation de la création d'un groupe de travail sur l'identification et l'authentification numériques (IAN)

- 2015 : Groupe de travail du CIANC sur le Cadre de confiance

Comités sur la Gestion de l'identité et le Carrefour numérique canadien

- 2012 : Modification de la structure hiérarchique des conseils mixtes
- 2013 : Groupe de travail du SCGI

International

- 2013-2015 : Sommets sur l'identité
- Participation aux normes Kantara, ISO et ANSI

Comité des SM sur les services et la fédération de l'identité (SFI)

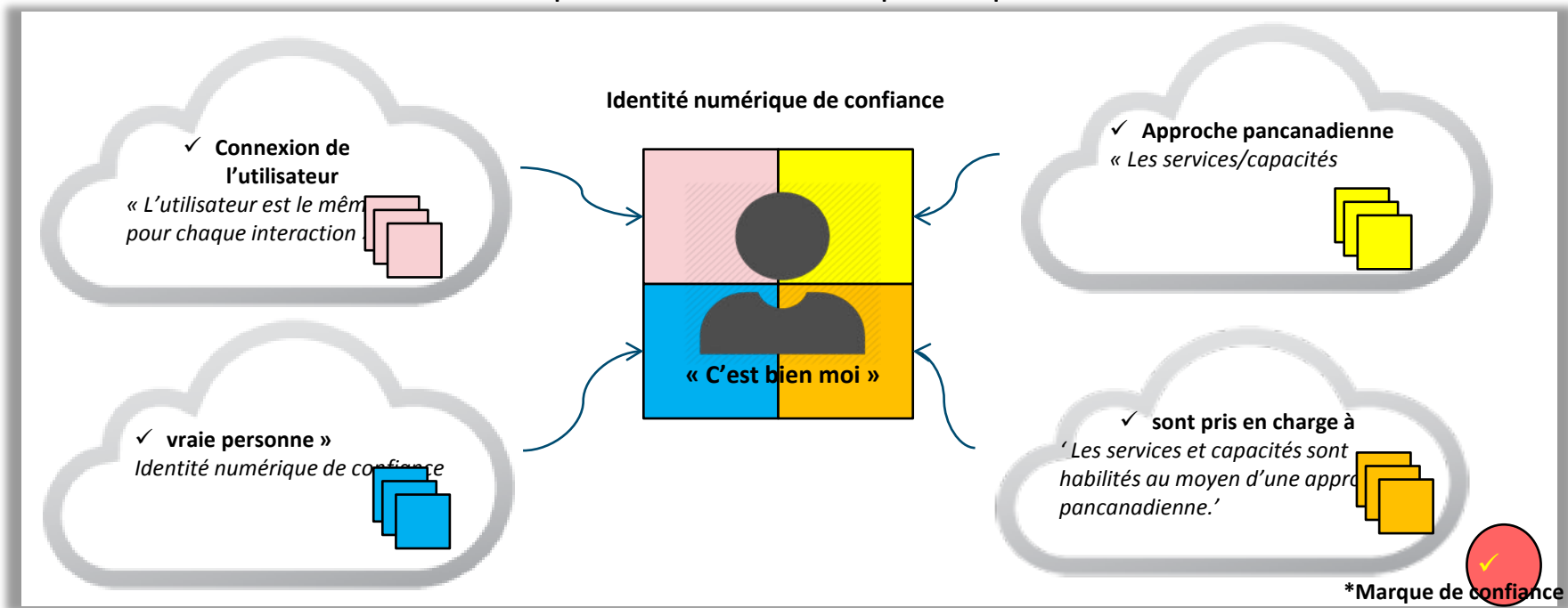
- 2013 : Réunion de lancement

Arrangements et PE connexes

- Validation du certificat de citoyenneté (CIC et provinces)

Objectif : Identité numérique de confiance

‘Une représentation électronique fiable de qui je suis.’
L'identité numérique de confiance comprend quatre volets :



*Marque de confiance

*en cours d'examen

Cadre pancanadien de la fiabilité de l'identité

Identité numérique de confiance

Représentation électronique fiable de ma propre personne



Comprend les considérations liées aux secteurs public et privé

*S'agit-il de la même
personne?*

Volet Connexion d'utilisateur

Ensemble de processus fiables qui garantit qu'un utilisateur est connecté en toute sécurité et agit en son propre nom.

- ☐ Émission d'un justificatif
- ☐ Authentification d'un justificatif
- ☐ Recouvrement d'un justificatif
- ☐ Révocation d'un justificatif

S'agit-il d'une personne réelle existante?

Volet Personne confirmée

Ensemble de processus fiables qui identifie une seule et même personne réelle, qui garantit que les renseignements d'identité sont exacts et à jour et que les demandes et les mesures peuvent être attribuées à cette personne.

- ☐ Résolution de l'identité
- ☐ Établissement de l'identité
- ☐ Validation de l'identité*
- ☐ Vérification de l'identité
- ☐ Entretien de l'identité*

L'utilisateur a-t-il donné son consentement?

Volet Liaison et autorisation

Ensemble de processus fiables qui établit un lien entre la connexion d'utilisateur et la personne confirmée et qui gère l'autorisation (consentement) accordée par la personne.

- ☐ Détermination des justificatifs
- ☐ Établissement de liens pour déterminer l'identité
- ☐ Autorisation du propriétaire

Volet Infrastructure pancanadienne

Normes techniques, spécifications, certifications Protection des renseignements personnels, sécurité, prestation de services, niveau organisationnel

**Le but du Carrefour numérique du Canada (CNC). Est de réaliser ces composantes*

CADRE PANCANADIEN DE FIABILITÉ DE L'IDENTITÉ : CHEMINEMENT CRITIQUE

PARTIE FAISANT AUTORITÉ

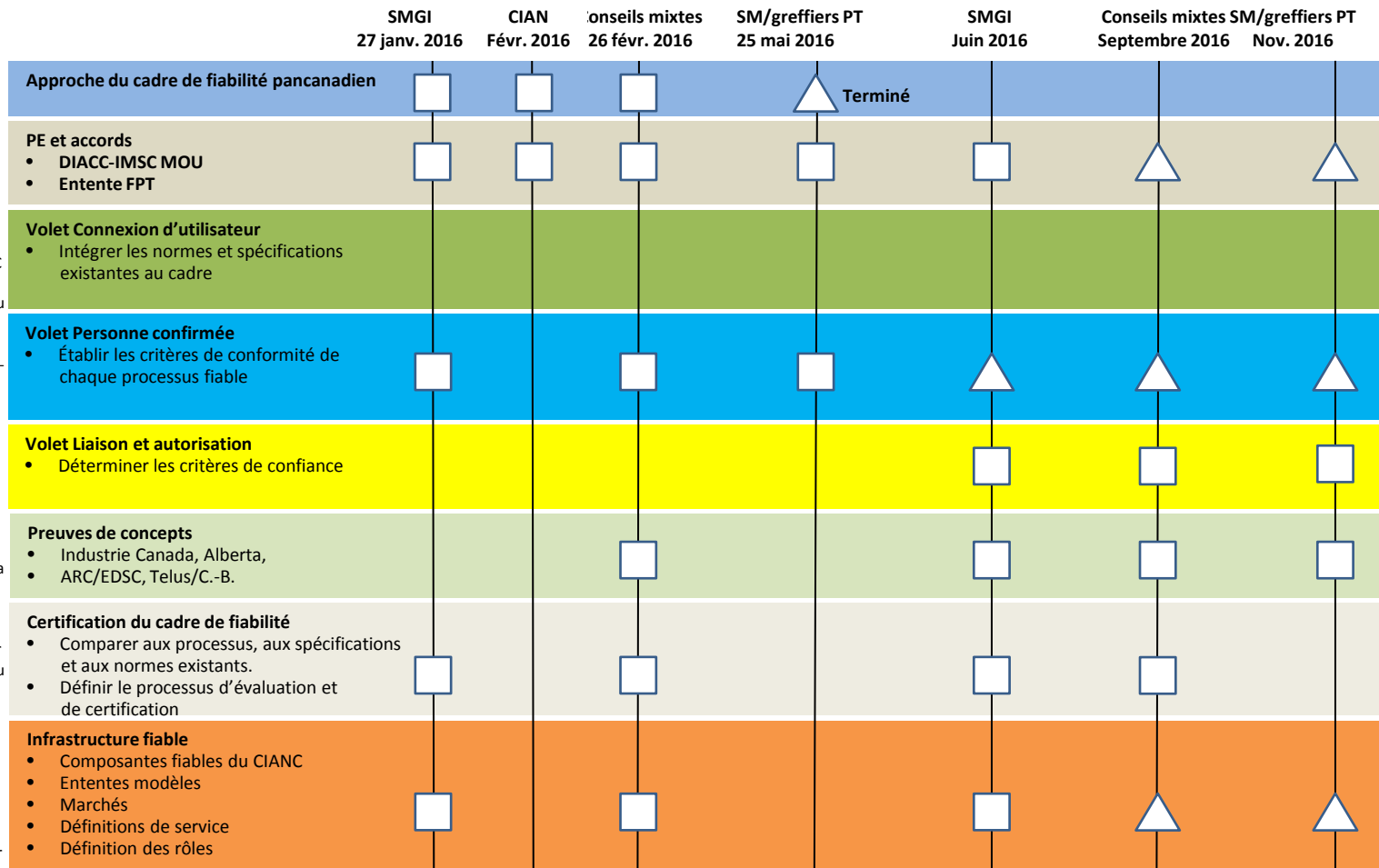
- ✓ 2007 Rapport du GTIGIA
- ✓ 2010 Modèle d'assurance pancanadien
- ✓ 2011 Approche de la confiance dans l'identité du CDGI
- ✓ 2014 Norme pancanadienne sur la validation de l'identité

FPT

- ✓ 2009 Directive sur la gestion de l'identité du GC
- ✓ 2010 Norme sur l'assurance de l'identité du GC
- ✓ 2010 Norme sur les preuves d'identité de la C.-B.
- ✓ 2010 Norme sur les preuves d'identité et l'authentification électroniques
- ✓ 2010 Économie numérique du Canada du GC
- ✓ 2012 STAE 2.1 du GC
- ✓ 2012 Ligne directrice sur la définition des exigences en matière d'authentification du GC
- ✓ 2015 Lignes directrices sur l'assurance de l'identité du GC
- ✓ 2015 Canada numérique 150
- ✓ 2015 Norme sur les renseignements sur l'identité de la C.-B.

CIAN

- ✓ 2012 Groupe de travail sur l'examen des systèmes de paiement



= point/orientation

= décision/approbation

Consulter l'annexe pour obtenir plus de renseignements

Cadre pancanadien de la fiabilité de l'identité

Cadre pancanadien de la fiabilité de l'identité : Progrès réalisés depuis septembre 2015

- **Novembre 2015** : Forum pancanadien sur la fiabilité de l'identité à Ottawa
 - Entente de principe avec CIANC sur l'établissement d'un cadre
- **Décembre 2015** : Établissement du cheminement critique
 - Dates des jalons et des rapports
 - Progrès réalisés à ce jour relativement aux composantes du cadre sur la fiabilité
- **Janvier 2016** : **Élaboration du Cadre de confiance**
 - Ébauche du PE SCGI-CIANC
 - Ébauche de la charte sur le cadre de confiance
 - Mobilisation des groupes de travail du CIANC

Cadre pancanadien de la fiabilité de l'identité

Prochaines étapes...

1. SMGI

- Finaliser le PE CDGI-CIAN et la Charte du cadre de fiabilité
- Cerner les intervenants supplémentaires (par ex. Affaires intergouvernementales)
- Établir les critères de conformité au cadre de fiabilité
 - Connexion de l'utilisateur, personne confirmée, liaison et autorisation
- Faire le point auprès des conseils mixtes (CPSSP/CDPISP) pendant les téléconférences de mars/avril

2. Stratégie sur les services numériques

- Ancrer les efforts relatifs à la gestion de l'identité au pilier de la stratégie en matière de gouvernement/service numérique

3. Table des SM FPT

- Présentation des progrès réalisés relativement au Cadre pancanadien de la fiabilité de l'identité en mai 2016

4. CIAN

- Participer aux réunions mensuelles du conseil
- Participer au groupe de travail sur le cadre de la fiabilité du CIANC


Nous sommes ici.

9 Structure

Vision pancanadienne

Vision pancanadienne (2014) :

Les citoyens et les entreprises peuvent accéder simplement et rapidement, en toute sécurité, aux services offerts de la manière qu'ils choisissent et qu'ils maîtrisent



Valeur opérationnelle

- Favorise une approche pangouvernementale qui permet une prestation de services électroniques transparente.
- Permet une expérience du client améliorée et une commodité accrue pour l'utilisateur en appuyant une approche « une fois suffit ».
- Favorise un climat de confiance à l'égard de l'identité numérique comme solution de rechange à l'identification en personne ou à partir de documents
- Réduit le risque que l'individu ne soit pas celui qu'il prétend être.
- Réduit les frais administratifs liés à l'établissement de l'identité.
- Renforce l'intégrité du programme

Valeur opérationnelle et pour l'utilisateur

La valeur opérationnelle et pour l'utilisateur d'une identité numérique de confiance se concrétise par les participants jouant le rôle de partie faisant autorité, de partie utilisatrice ou de personne (utilisateur).

Responsable du programme gouvernemental



« En tant que partie faisant autorité, nous pouvons fournir une identité numérique de confiance aux fournisseurs de service. »

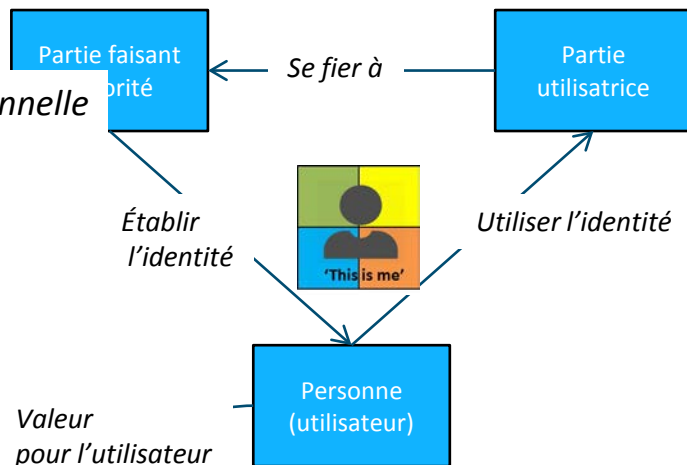
- ✓ **Valeur opérationnelle :**
Occasion d'offrir des services de valeur élevée à l'ensemble de la communauté de la prestation de services

gouvernement



« En tant qu'utilisateur, je peux fournir la preuve de mon identité une seule fois et, avec mon consentement, utiliser mes renseignements d'identité auprès de multiples fournisseurs de services. »

Cadre de la fiabilité de l'identité



Fournisseur de services du



Valeur opérationnelle



« En tant que partie utilisatrice, nous pouvons améliorer et simplifier l'expérience du service en utilisant une identité numérique de confiance qui s'appuie sur des processus fiables. »

- ✓ **Valeur opérationnelle :**
Amélioration de la prestation des services grâce à l'augmentation de l'intégrité, à des gains d'efficience et à la simplification de l'expérience des utilisateurs.

- ✓ **Valeur pour l'utilisateur :** Accès plus facile à des services à valeur élevée de manière fiable, sécurisée et à confidentialité améliorée.

Cadre pancanadien de la fiabilité : Composante 1 – Connexion de l'utilisateur

Processus servant à veiller à ce qu'un utilisateur soit connecté de façon sécurisée et agit en son propre nom

PROGRÈS RÉALISÉS À CE JOUR :

Composante Connexion de l'utilisateur	Secteur public fédéral	PARTIE FAISANT AUTORITÉ
Élaboration de politiques, de normes, de lignes directrices et de spécifications <ul style="list-style-type: none"> ✓ STAE 2.1, ✓ ITSG-31 ✓ Directive sur la gestion de l'identité ✓ Norme sur l'assurance de l'identité et des justificatifs ✓ Volets Fiabilité 	En place	Élaboration
Mise en oeuvre du volet Connexion de l'utilisateur <ul style="list-style-type: none"> ✓ Émission d'un justificatif ✓ Authentification d'un justificatif ✓ Recouvrement d'un justificatif ✓ Révocation d'un justificatif ✓ Volet Processus fiable 	En place	Élaboration
Intégration des normes et spécifications existantes au cadre	Lancement	Lancement

État Non commencé

Lancement

Élaboration

En place

Cadre pancanadien de la fiabilité - Composante 2 – Personne confirmée

Ensemble de processus fiables qui identifie une seule et même personne réelle, qui garantit que les renseignements d'identité sont exacts et à jour et que les demandes et les mesures peuvent être attribuées à cette personne.

PROGRÈS RÉALISÉS À CE JOUR :

Volet Personne confirmée	Secteur public fédéral	PARTIE FAISANT AUTORITÉ
Cadre pancanadien de la fiabilité de l'identité : Définitions des volets <ul style="list-style-type: none"> ✓ Directive sur la gestion de l'identité ✓ Norme sur l'assurance de l'identité et des justificatifs ✓ Volets Fiabilité 	En place (fédéral)	Élaboration
<ul style="list-style-type: none"> ✓ <u>(nouvelles) Lignes directrices sur l'établissement de l'identité</u> 	Élaboration	Élaboration
Volet Personne confirmée <ul style="list-style-type: none"> ✓ Établir les critères de conformité de chaque processus fiable <ul style="list-style-type: none"> - Résolution de l'identité – L'établissement du caractère unique d'une personne au sein de la population d'un programme/service - Établissement de l'identité – La création d'un dossier d'identité faisant autorité dont dépendent d'autres personnes - Validation de l'identité - Confirmation de l'exactitude des renseignements sur l'identité d'une personne établis par une partie faisant autorité. - Vérification de l'identité - Confirmation que les renseignements sur l'identité présentés concernent la personne qui présente la demande. - Entretien de l'identité – Assurance que les renseignements sur l'identité sont exacts, complets et à jour au besoin. ✓ Valider les processus existants (par ex. AB) ✓ Établir les critères de conformité de chaque processus fiable ✓ Établir les nouvelles normes et lignes directrices nécessaires. 	Élaboration	Élaboration

État Non commencé

Lancement

Élaboration

En place

Cadre pancanadien de la fiabilité - Composante 3 – Liaison et autorisation

Ensemble de processus fiables qui relie une connexion sécurisée à une personne confirmée et gère l'autorisation (consentement) accordée par cette personne.

PROGRÈS RÉALISÉS À CE JOUR :

Volet Liaison et autorisation	Secteur public fédéral	PARTIE FAISANT AUTORITÉ
Établissement de politiques, de normes, de lignes directrices et de spécifications (nouveau) Consentement/autorisation de l'utilisateur - Politique sur la diffusion des attributs*	Non commencé	Non commencé
<ul style="list-style-type: none"> ✓ Kantara/IEEE: Accès géré par l'utilisateur (AGU) ✓ OAuth 2.0 	Lancement	Lancement
Opérationnalisation de la composante Liaison et autorisation <ul style="list-style-type: none"> ✓ Détermination des justificatifs ✓ Établissement de liens pour déterminer l'identité ✓ Autorisation du propriétaire 	Lancement	Non commencé
<ul style="list-style-type: none"> ✓ Soutenir les projets pilotes/mises en oeuvre de références ✓ Participer aux consultations sur la gestion du consentement ✓ Établir de nouvelles normes et lignes directrices au besoin ✓ Établir le processus d'inscription aux services, d'inscription au programme ou de gestion des comptes <u>International</u> <ul style="list-style-type: none"> ✓ Étudier les Electronic Identification and Trust Services (eIDAS) – Règlement de IUE 	Lancement	Non commencé

* Réalisé séparément par les programmes, services et administrations

État

Non commencé

Lancement

Élaboration

En place

Cadre pancanadien de la fiabilité - Composante 4 – Infrastructure

Ensemble de services ou capacités nécessaires pour utiliser le cadre de la fiabilité de façon sûre, favorable à la protection des renseignements personnels et fiable.

PROGRÈS RÉALISÉS À CE JOUR :

Volet Infrastructure	Secteur public fédéral	PARTIE FAISANT AUTORITÉ
Établissement de politiques, de normes, de lignes directrices et de spécifications <ul style="list-style-type: none"> ✓ Orientation relativement aux politiques sur la protection des renseignements personnels ✓ Sécurité ✓ Cadre de sécurité applicable ✓ Prestation de services et niveau organisationnel 	Élaboration	Élaboration
Volet Infrastructure <ul style="list-style-type: none"> ✓ Prestation de services et organisation 	Non commencé	Non commencé
<ul style="list-style-type: none"> ✓ Soutien des projets pilotes ✓ Participation aux consultations sur la gestion du consentement ✓ Établissement de nouvelles normes et lignes directrices au besoin 	Lancement	Lancement
	État Non commencé	Élaboration
	Lancement	En place

Documents pancanadiens et instruments de politique FPT publiés/approuvés (2007-présent)

Année	Origine / Administration	Description
2007	SMGI	Rapport du GTIGIA - Établissement de la vision, de la stratégie et du cadre pancanadiens initiaux.
2009	Organisation	Directive sur la gestion de l'identité – Assure l'efficacité des pratiques de gestion de l'identité des personnes, organismes et appareils.
2009	Organisation	IT Security Guidance (ITSG)-31 – Orientation sur l'authentification des utilisateurs des systèmes de TI.
2010	C.-B.	Norme sur l'assurance de l'identité – Offre un cadre pour l'établissement de la confiance entre les parties qui émettent et reçoivent les demandes
2010	C.-B.	Norme sur les preuves d'identité - Offre un cadre pour l'établissement de la confiance entre les parties qui émettent et reçoivent les demandes de renseignements sur l'identité
2010	C.-B.	Norme sur les justificatifs d'identité et l'authentification électroniques - Précise les exigences liées à l'émission, à la gestion et à l'authentification des justificatifs d'identité électroniques à différents degrés.
2010	SMGI	Modèle d'assurance pancanadien – Modèle détaillé décrivant la façon dont les administrations peuvent officialiser les relations de confiance.
2011	SMGI	Approche pancanadienne de la confiance dans l'identité du SMGI – Décrit l'approche de la fiabilité des identités entre les administrations.
2012	IMSC	Spécification technique d'authentification électronique (STAE) 2.1 – Norme sur l'interface technique de l'assurance des justificatifs d'identité.
2012	Organisation	Ligne directrice sur l'établissement des exigences en matière d'authentification Orientation détaillée visant à aider à la réalisation d'évaluation du niveau d'assurance et à l'établissement des exigences en matière d'authentification.
2013	C.-B.	ORIENTATION SUR LES RENSEIGNEMENTS SUR L'IDENTITÉ PERSONNELLE – Orientation sur la confirmation de l'identité
2013	Organisation	Norme sur l'assurance de l'identité et des justificatifs d'identité - Veille à ce que les risques liés à l'identité pour les personnes, les organismes et les appareils soient gérés de façon cohérente et collaborative au sein du gouvernement du Canada et avec les autres administrations et secteurs de l'industrie.
2014	SMGI	Norme pancanadienne de validation de l'identité – normalise les demandes de validation de renseignements sur l'identité et de renseignements personnels entre les organismes fédéraux, provinciaux, territoriaux et municipaux, et la réponse à celles-ci
2015*	SMGI	Ligne directrice sur l'assurance de l'identité – orientation détaillée à l'appui de la mise en oeuvre de la Norme sur l'assurance de l'identité et des justificatifs d'identité (*en publication)
2015*	C.-B.	Norme sur les renseignements sur l'identité - Établit les règles et méthodes en vertu desquelles les données sur les justificatifs d'identité acceptés au cours d'une procédure de confirmation de l'identité sont enregistrés de façon normalisée et cohérente (*pas encore disponible)

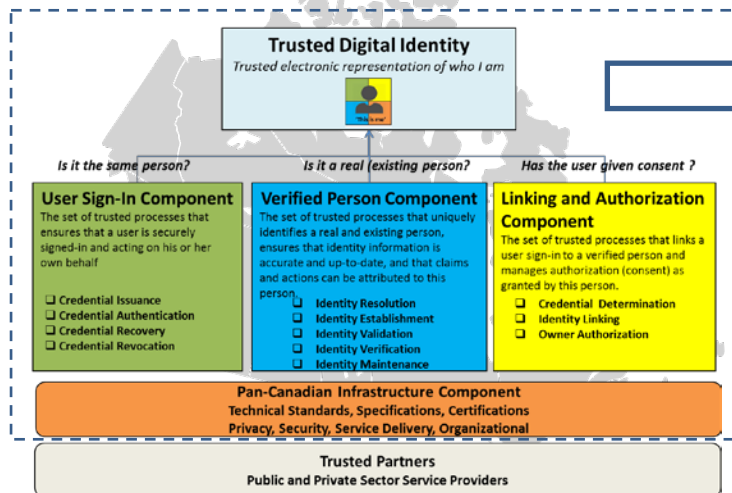
Produits livrables du cadre sur la fiabilité : Description détaillée

Produit livrable	Description	Responsable
Approche du cadre sur la fiabilité	Accord pancanadien sur l'approche globale du cadre de confiance. Comprend une orientation stratégique, la gestion de projet, les communications et documents d'information, au besoin.	<i>Conseils mixtes/Sous-comité sur la gestion de l'identité</i>
PE SCGI-CIAN	Entente décrivant les rôles et responsabilités des groupes de travail sur le CIAN et le SCGI et les processus de gouvernance.	<i>Sous-comité sur la gestion de l'identité</i>
Entente FPT	Entente décrivant l'adoption et la mise en oeuvre du Cadre pancanadien de la fiabilité de l'identité. Pourrait comprendre la gouvernance, le modèle opérationnel et les considérations liées au financement.	<i>Sous-comité sur la gestion de l'identité</i>
Composante sur la fiabilité de la connexion d'utilisateur	Critère de conformité de la connexion d'utilisateur Concept des opérations Méthode d'évaluation de la connexion d'utilisateur	<i>Sous-comité sur la gestion de l'identité</i>
Composante sur la fiabilité de la personne confirmée	Critère de conformité des personnes confirmées Concept des opérations Méthode d'évaluation des personnes confirmées	<i>Sous-comité sur la gestion de l'identité</i>
Composante sur la fiabilité de la liaison et de l'autorisation	Critères de conformité à la liaison et à l'autorisation Concept des opérations Méthode d'évaluation de la liaison et de l'autorisation	<i>Sous-comité sur la gestion de l'identité</i>
Valisation du cadre de la fiabilité Schématisation des processus opérationnels	Comparaison aux processus opérationnels existants (et prévus) Validation des composantes du cadre de la confiance (connexion de l'utilisateur, personne confirmée et liaison et autorisation)	<i>Sous-comité sur la gestion de l'identité</i>
Preuves de concept	Projets pilotes et démonstrations Enseignements tirés et pratiques exemplaires Application des normes techniques	<i>ISED, CIC-PPT EDSC, ARC Telus/BC</i>
Composant Infrastructure fiable	Définitions normalisées des services commerciaux Ententes/contrats modèles Définitions des rôles opérationnels	<i>CIAN</i>

Comparaison à la norme eIDAS

Gouvernance pancanadienne (à déterminer)

Entente FPT

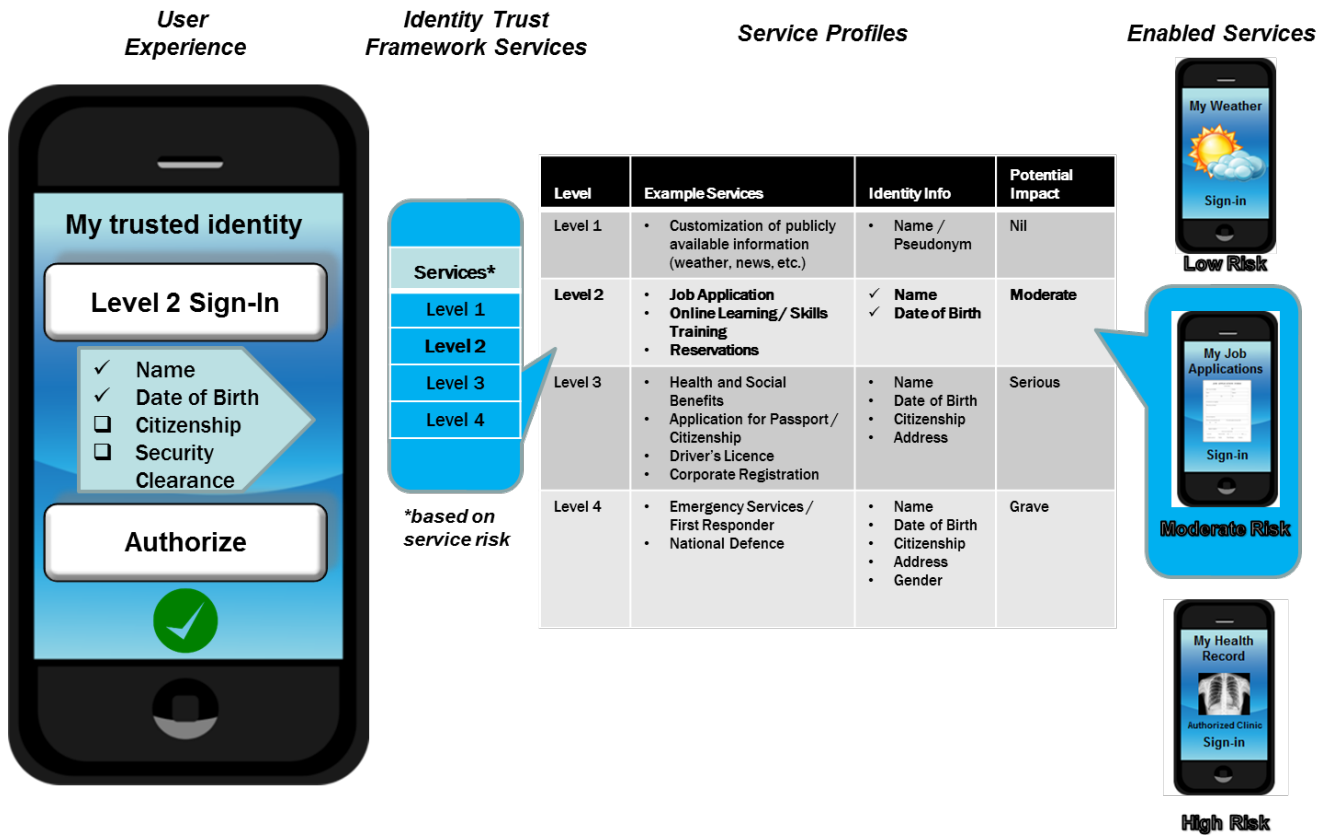


Parlement européen
Conseil de l'Union européenne

Règlement sur eIDAS



Exemples de services



Définitions des composantes de fiabilité

Catégorie de service	Définition du service de confiance	Enjeux à prendre en considération
Connexion d'utilisateur : Ensemble de services qui garantissent que l'utilisateur actuel est la personne dont l'identité a été établie précédemment	Délivrance des justificatifs d'identité – Délivrance, révocation et destruction des justificatifs d'identité.	<ul style="list-style-type: none"> Ensemble, ces services constituent habituellement des services de gestion de l'identité. Ils peuvent être fournis ensemble par un seul fournisseur ou répartis entre plusieurs fournisseurs.
	Stockage des justificatifs d'identité – Stockage des justificatifs d'identité.	
	Authentification des justificatifs d'identité – Processus qui consiste à générer l'assurance des justificatifs d'identité.	
Personne confirmée : Ensemble de services qui permettent de veiller à ce que l'utilisateur actuel soit une personne réelle	Résolution de l'identité – Capacité de distinguer clairement une personne des autres.	<ul style="list-style-type: none"> Ces services, lorsqu'ils sont fournis ensemble, constituent habituellement des services de gestion de l'identité. Ils peuvent être fournis ensemble par un seul fournisseur ou répartis entre plusieurs fournisseurs.
	Validation de l'identité – Confirmation de l'exactitude de l'attribut d'identité.	
	Notification de l'identité – Notification qui indique que les renseignements ont été établis, modifiés ou exposés à des facteurs de risque.	
	Vérification de l'identité – Confirmation que l'attribut d'identité concerne un individu en particulier.	
	Établissement de l'identité – Création du fichier d'identité initial d'une personne.	
Liaison et autorisation : Ensemble de services qui relient la connexion de l'utilisateur à la personne confirmée et qui permettent d'enregistrer les autorisations accordées par la personne, indiquant le consentement ou l'autorisation	Liaison et autorisation – Le fait de relier la connexion de l'utilisateur à la personne confirmée et d'enregistrer les autorisations accordées par la personne, indiquant le consentement ou l'autorisation.	<ul style="list-style-type: none"> Peuvent faire partie d'un service d'inscription, d'un programme d'enregistrement ou d'un processus de gestion de compte. Le consentement peut porter sur un justificatif en particulier; l'utilisateur peut avoir plusieurs justificatifs dont chacun est assorti d'un consentement différent.

Niveaux d'assurance de l'identité normalisés

Source : Norme sur l'assurance de l'identité et des justificatifs du SCT <http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=26776>

Niveau	Description
4	Besoin d'un niveau très élevé d'assurance que la personne est celle qu'elle affirme être. <i>Une compromission pourrait raisonnablement entraîner des préjudices graves, sinon catastrophiques.</i>
3	Besoin d'un niveau élevé d'assurance que la personne est celle qu'elle affirme être. <i>Une compromission pourrait raisonnablement entraîner des préjudices modérés, sinon graves.</i>
2	Besoin d'un certain niveau d'assurance que la personne est celle qu'elle affirme être. <i>Une compromission pourrait raisonnablement entraîner des préjudices minimes, sinon modérés.</i>
1	Besoin d'un faible niveau d'assurance que la personne est celle qu'elle affirme être. <i>Une compromission pourrait raisonnablement entraîner des préjudices inexistantes, sinon minimes.</i>

Niveaux d'assurance de l'identité normalisés

Source : Norme sur l'assurance de l'identité et des justificatifs du SCT <http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=26776>

Niveau	Description
4	Besoin d'un niveau très élevé d'assurance que la personne a gardé le contrôle du justificatif qui lui a été confié et que celui-ci n'a pas été compromis. Une compromission pourrait raisonnablement entraîner des préjudices graves, sinon catastrophiques.
3	Besoin d'un niveau élevé d'assurance que la personne a gardé le contrôle du justificatif qui lui a été confié et que celui-ci n'a pas été compromis. <i>Une compromission pourrait raisonnablement entraîner des préjudices modérés, sinon graves.</i>
2	Besoin d'un certain niveau d'assurance que la personne a gardé le contrôle du justificatif qui lui a été confié et que celui-ci n'a pas été compromis. <i>Une compromission pourrait raisonnablement entraîner des préjudices minimales, sinon modérés</i>
1	Besoin d'un faible niveau d'assurance que la personne a gardé le contrôle du justificatif qui lui a été confié et que celui-ci n'a pas été compromis. <i>Une compromission pourrait raisonnablement entraîner des préjudices inexistantes, sinon minimales.</i>

Établissement du niveau d'assurance de l'identité : Exigences minimales (1/2)

Source : Norme sur l'assurance de l'identité et des justificatifs du SCT <http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=26776>

Exigence	Niveau 1	Niveau 2	Niveau 3	Niveau 4
Caractère unique	Définir les renseignements sur l'identité Définir le contexte			
Preuve d'identité	Aucune restriction relativement à ce qui est fourni à titre de preuve	Un exemple de preuve d'identité	Deux exemples de preuve d'identité (Au moins l'un de ceux-ci doit être une preuve essentielle d'identité.)	Trois exemples de preuves d'identité (Au moins l'un de ceux-ci doit être une preuve essentielle d'identité.)
Exactitude des renseignements sur l'identité	Acceptation de l'autoaffirmation des renseignements sur l'identité par une personne	Les renseignements sur l'identité correspondent de façon acceptable à l'affirmation d'une personne et à la preuve d'identité et Confirmation que la preuve d'identité provient de l'autorité pertinente	Les renseignements sur l'identité correspondent de façon acceptable à l'affirmation d'une personne et à tous les exemples de preuves d'identité et Confirmation des preuves essentielles d'identité au moyen d'une source faisant autorité et Confirmation que les preuves à l'appui de l'identité proviennent de l'autorité pertinente au moyen d'une source faisant autorité ou inspection par un examinateur clé	Les renseignements sur l'identité correspondent de façon acceptable à l'affirmation d'une personne et à tous les exemples de preuves d'identité et Confirmation de la preuve essentielle d'identité au moyen d'une source faisant autorité et Confirmation que les preuves à l'appui de l'identité proviennent de l'autorité pertinente au moyen d'une source faisant autorité ou inspection par un examinateur formé

Établissement du niveau d'assurance de l'identité : Exigences minimales (2/2)

Suite du tableau de la diapo précédente...

Source : Norme sur l'assurance de l'identité et des justificatifs du SCT <http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=26776>

Exigence	Niveau 1	Niveau 2	Niveau 3	Niveau 4
Lien entre les renseignements sur l'identité et la personne	Aucune exigence	Aucune exigence	Au moins l' une des exigences suivantes : i) Confirmation fondée sur les connaissances ii) Confirmation des caractéristiques biologiques ou comportementales iii) Confirmation par un arbitre de confiance* iv) Confirmation de la possession physique	Au moins trois des exigences suivantes : i) Confirmation fondée sur les connaissances ii) Confirmation des caractéristiques biologiques ou comportementales iii) Confirmation par un arbitre de confiance* iv) Confirmation de la possession physique

Cadres et normes pertinents

Administration/Secteur	Norme ou Cadre
Canada	<ul style="list-style-type: none"> • Rapport du GTGIA (2008) • Modèle pancanadien d'assurance (2010) • Norme pancanadienne sur la validation de l'identité (2014) <ul style="list-style-type: none"> • Norme sur l'assurance de l'identité et des justificatifs du SCT (2012) • Ligne directrice sur la définition des exigences en matière d'authentification • Guide sur l'authentification des utilisateurs pour les systèmes TI du CSTC
É.-U.	<ul style="list-style-type: none"> • OMB M04 – 04 (2003) E-Authentication Guidance for Federal Agencies • NIST SP 800 – 63 Electronic Authentication Guideline • FICAM TFPAP • ANSI/NASPO IPDV
R.-U.	<ul style="list-style-type: none"> • GPG-44 Authentication Credentials in Support of HMG Online Services • GPG-45 Identity Proofing and Verification of an Individual (2013) • tScheme
N.-Z.	<ul style="list-style-type: none"> • Evidence of Identity Standard • Authentication Key Strength Standard
UE	<ul style="list-style-type: none"> • Electronic Services and Trust Services Regulation (2014)
AUS	<ul style="list-style-type: none"> • National e-Authentication Framework • National Identity Proofing Guidelines
Industrie	<ul style="list-style-type: none"> • Cadre d'assurance des justificatifs d'identité de Kantara • OIX
Financier/paiement	<ul style="list-style-type: none"> • Norme EMV
ISO	<ul style="list-style-type: none"> • ISO 24760 – Security – A Framework for Terminology and Concepts: Partie 1