

Fédération canadienne d'accès : Document de confirmation de fiabilité (DCF)

1. But

Une exigence fondamentale à laquelle doivent se plier les Participants de la Fédération canadienne d'accès consiste à assigner des attributs d'identité exacts et faisant autorité aux ressources qui sont consultées. Les Participants qui reçoivent de tels attributs sont tenus de les protéger et de respecter les contraintes de confidentialité que le Participant émetteur y a associées.

À cette fin, CANARIE demande aux Participants de mettre à la disposition des autres Participants les réponses aux questions qui suivent.

1.1 Exigence de la Fédération canadienne d'accès

Pour l'instant, la confiance qui règne au sein de la communauté s'appuie sur les « meilleurs efforts » des Participants et sur des pratiques transparentes. Chaque Participant fournit aux autres Participants de la documentation sur les pratiques d'identification et de gestion des accès qu'il est sûr de pouvoir respecter. Ainsi, chaque Participant devrait mettre à la disposition des autres Participants l'information de base sur le système de gestion des identités et les systèmes de gestion des accès aux ressources qu'il a enregistrés en vue d'un usage dans la Fédération canadienne d'accès. Pareille information comprend habituellement la manière dont les attributs d'identité sont définis et la façon dont les services exploitent ces attributs.

1.2 Publication

Les réponses aux questions qui suivent doivent :

1. être soumises à CANARIE pour qu'il les affiche sur son site Web;
2. être affichées à un endroit aisément accessible sur le site Web du fournisseur.

Le Document de confirmation de fiabilité doit être tenu à jour.

2. Fédération canadienne d'accès - Renseignements sur le Participant

2.1.1. Nom de l'organisation : _Université Laval_____

2.1.2. L'information qui suit était exacte à la date indiquée ci-dessous :
19/09/2018_____

2.2 Gestion des identités ou information sur la protection des renseignements personnels

2.2.1. Où les autres Participants de la Fédération canadienne d'accès peuvent-ils trouver des renseignements supplémentaires sur vos pratiques concernant la gestion des identités ou de l'information sur la protection des renseignements personnels?

Sur le site Web du Bureau de sécurité de l'information de l'Université Laval :
<http://www.fsa.ulaval.ca/politique-de-confidentialite/>

2.3 Personne-ressource

2.3.1. Indiquer la ou les personnes ou le service en mesure de répondre aux questions sur le système de gestion des identités ou sur les politiques ou pratiques de gestion des accès aux ressources du Participant.

Nom : Douglas Doyer
Titre ou rôle : Directeur du Bureau de sécurité de l'information
Courriel : Douglas.Doyer@bsi.ulaval.ca
Téléphone : 418.656.2131 (poste # 14443)

3. Information sur le Fournisseur d'identité

Deux critères déterminent la fiabilité des attributs conférés par les Fournisseurs d'identité : (1) que la responsabilité du système de gestion des identités incombe à la haute direction ou à la direction commerciale de l'organisation et (2) que le système qui délivre les justificatifs d'identité de l'utilisateur (par ex., nom d'utilisateur/mot de passe, jetons d'authentification, etc.) intègre des mesures appropriées pour gérer les risques (à savoir, pratiques de sécurité, contrôles en cas de changement au niveau de la direction, piste de vérification, reddition de comptes, etc.).

3.1 Communauté

3.1.1. En tant que Fournisseur d'identité, de quelle manière définissez-vous les personnes qui peuvent obtenir une identité électronique? S'il y a des exceptions, qui les approuve?

Une personne peut obtenir une identité électronique lorsque celle-ci a un lien d'étude, d'emploi ou d'affaires avec l'institution et pour lequel l'accès à au moins une technologie de l'information est nécessaire. Les exceptions sont approuvées par le Bureau de sécurité de l'information.

3.1.2. Quel sous-ensemble de personnes inscrites dans votre système de gestion des identités considèreriez-vous comme des « Participants » auprès des Fournisseurs de services de la **FCA**, en termes d'authentification de l'identité SAML?

Toutes les personnes ayant un privilège d'accès actif au Réseau de l'Université Laval (RESUL) via la technologie sans-fil.

3.2 Justificatifs de l'identité électronique

3.2.1. Veuillez décrire en termes généraux le processus administratif permettant de créer une identité électronique qui fera en sorte que la personne pour laquelle l'identité a été créée se retrouve inscrite dans votre base de données. Veuillez identifier le ou les services qui conservent ces inscriptions.

Les personnes ayant un lien d'étude ou d'emploi bénéficient d'un processus administratif automatique pour la création de l'identité électronique en fonction des informations données au service d'affaires concerné. Pour les autres personnes, certaines informations obligatoires doivent être fournies à l'unité répondant à ce service (La Direction des technologies de l'information). Toutes autres questions à ce sujet sont traitées sur une base individuelle. Contactez le Bureau de sécurité de l'information via l'adresse courriel suivante : info@bsi.ulaval.ca.

3.2.2. Quelles sont les technologies d'authentification appliquées aux justificatifs de l'identité électronique (par ex., Kerberos, nom d'utilisateur/mot de passe, ICP, ...) pertinents pour les activités de la Fédération canadienne d'accès? Si vous émettez plus d'un justificatif électronique, veuillez indiquer comment on identifie ceux qui obtiendront tel ou tel

justificatif. Si les justificatifs sont reliés, veuillez indiquer comment on les gère (à savoir, une personne possédant un justificatif Kerberos peut-elle aussi obtenir un jeton ICP?) et comment on procède aux vérifications.

Émission de jetons SAML 2.0 basée sur une authentification par IDUL (IDentifiant Université Laval)/NIP (mot de passe) via un « bind » au domaine institutionnel.

- 3.2.3. Si les justificatifs de l'identité électronique nécessitent l'usage d'un mot de passe secret ou d'un NIP et que ceux-ci pourraient, dans certaines circonstances, être transmis sur un réseau sans être protégé par encryptage (à savoir, si on recourt à des « mots de passe en clair » pour accéder aux services du campus), veuillez indiquer qui, dans l'organisation, pourrait discuter avec un Participant que préoccuperait une telle pratique.

Le Bureau de sécurité de l'information via l'adresse courriel suivante : info@bsi.ulaval.ca.

- 3.2.4. Si vous recourez à un système d'authentification unique (*single sign-on* ou SSO) ou à un système similaire permettant à l'utilisateur d'accéder à de multiples applications après avoir été authentifié une seule fois, et que ce système servira à authentifier les personnes qui accéderont aux services des Fournisseurs de services de la **FCA**, veuillez décrire les principales mesures de sécurité implantées, y compris l'application éventuelle de délais d'inactivité, la possibilité pour l'utilisateur de mettre fin à la session et la protection assurée quand on recourt à des « sites à accès public ».

S.O. : Ce système ne servira pas à authentifier les personnes qui accéderont aux services des Fournisseurs de services de la FCA.

- 3.2.5. Les principaux identificateurs électroniques de personnes comme « NetID », eduNomPersonne ou eduIDPersonnel sont-ils considérés uniques pour toujours, une fois qu'ils ont été attribués? Si ce n'est pas le cas, quelle est la politique concernant la réattribution des justificatifs d'identité et quel intervalle doit-il s'écouler avant que les justificatifs puissent être réutilisés?

Le principal identifiant électronique à l'Université Laval est l'IDUL (Identifiant Unique Université Laval) et ils sont uniques pour toujours une fois qu'ils ont été attribués à une personne.

3.3 Base de données des identités électroniques

- 3.3.1. Comment saisit-on et actualise-t-on l'information dans la base de données sur les identités électroniques? L'administration a-t-elle désigné des locaux spécifiques pour cette activité? Les gens sont-ils autorisés à actualiser les informations les concernant en ligne?

Le changement des informations personnelles est fait par le Bureau du registraire (Étudiant), les Ressources humaines (employés et autres) ou par la personne elle-même directement en ligne. L'identifiant numérique est réalisé par le Bureau de sécurité de l'information.

- 3.3.2. Quels renseignements dans la base de données considère-t-on comme du domaine public, donc susceptibles d'être transmis à n'importe quelle partie intéressée?

Toutes questions à ce sujet sont traitées sur une base individuelle. Contactez le Bureau de sécurité de l'information via l'adresse courriel suivante : info@bsi.ulaval.ca.

3.4 Utilisation du système de justificatifs de l'identité électronique

- 3.4.1. Veuillez indiquer les catégories d'applications typiques pour lesquelles votre organisation utilise des justificatifs d'identité électronique.

Les accès aux technologies de l'information : les systèmes d'information développés pour la mission de l'institution, les progiciels, les outils de télécommunication, les logiciels commerciaux, les systèmes d'exploitation, le réseau informatique, etc.

3.5 Attributs d'authentification

Il s'agit des éléments d'information que vous pourriez transmettre à un autre Participant de la Fédération canadienne d'accès pour authentifier l'identité d'une personne inscrite dans votre système de gestion des identités.

- 3.5.1. Veuillez décrire la fiabilité des attributs d'authentification de votre fournisseur d'identité. Toutes questions à ce sujet sont traitées sur une base individuelle. Contactez le Bureau de sécurité de l'information via l'adresse courriel suivante : info@bsi.ulaval.ca.
-

- 3.5.2. Estimez-vous que les attributs d'authentification sont assez fiables pour :

- a) contrôler l'accès aux bases de données en ligne que votre organisation est autorisée à exploiter? _Oui _____
- b) acheter des biens ou des services pour l'organisation? _Oui _____
- c) permettre l'accès à des renseignements de nature personnelle comme des données sur le dossier de l'étudiant? _Oui _____

3.6 Protection des renseignements personnels

Les Participants de la Fédération canadienne d'accès doivent respecter les exigences imposées par la loi et les exigences de l'organisation en matière de protection des renseignements personnels eu égard à l'information sur les attributs que fournissent les

autres Participants. Ces informations ne doivent servir qu'aux fins auxquelles elles sont destinées.

- 3.6.1. Quelles restrictions imposez-vous à l'utilisation des données sur les attributs que vous pourriez transmettre aux autres Participants de la Fédération canadienne d'accès?

Les restrictions sont évaluées au cas par cas pour chacun des participants. Les seuls attributs retournés aux participants correspondent aux attributs qui ont été demandés et autorisés par l'Université Laval.

- 3.6.2. Quelles politiques régissent l'usage des informations sur les attributs que vous pourriez transmettre à d'autres Participants de la Fédération canadienne d'accès?

Vous pouvez consulter la section #5 dans la page Web du Cadre régissant la sécurité de l'information du Bureau de sécurité de l'information via l'adresse Web suivante : <https://www.bsi.ulaval.ca/documents-de-reference>. Pour plus d'information concernant spécifiquement la protection des renseignements personnels à l'Université Laval, contactez le Bureau de sécurité de l'information : info@bsi.ulaval.ca.

- 3.6.3. Veuillez indiquer l'URL de votre politique de protection des renseignements personnels.

<http://www.fsa.ulaval.ca/politique-de-confidentialite/>

4. Information sur le Fournisseur de services

Les Fournisseurs de services qui reçoivent les attributs d'authentification d'un autre Participant respecteront les politiques, les règles et les normes applicables à la protection et à l'utilisation de ces données. De telles informations ne peuvent être utilisées qu'aux fins auxquelles elles sont destinées.

On fait confiance aux Fournisseurs de services pour qu'ils ne réclament que l'information dont ils ont besoin pour parvenir à la décision appropriée en ce qui concerne le contrôle des accès et pour qu'ils ne se servent pas des données que leur procurent les Fournisseurs d'identité à mauvais escient. Les Fournisseurs de services décriront ce sur quoi ils se fondent pour autoriser l'accès aux services qu'ils gèrent et dévoileront leurs pratiques eu égard à l'information sur les attributs qu'ils obtiennent des autres Participants.

4.1 Attributs

4.1.1. De quelles informations sur les attributs d'une personne avez-vous besoin pour gérer l'accès aux ressources que vous mettez à la disposition des autres Participants? Donnez-en une description distincte pour chaque application que vous proposez aux Participants de la FCA.

L'Université Laval expose les fournisseurs de services (Service Providers) suivants à la communauté :

1. Géoindex+ (entityID="https://geoapp.bibl.ulaval.ca/shibboleth")

Les attributs requis sont les suivants :

<u>Nom attribut</u>	<u>Identifiant attribut</u>	<u>Utilisation</u>
eduPersonAffiliation	urn:oid:1.3.6.1.4.1.5923.1.1.1.1	Gestion des droits d'accès
eduPersonOrgDN	urn:oid:1.3.6.1.4.1.5923.1.1.1.3	Gestion des droits d'accès
eduPersonOrgUnitDN	urn:oid:1.3.6.1.4.1.5923.1.1.1.4	Gestion des droits d'accès
eduPersonPrincipalName	urn:oid:1.3.6.1.4.1.5923.1.1.1.6	Identifiant unique de l'utilisateur à l'intérieur de Géoindex+
mail	urn:oid:0.9.2342.19200300.100.1.3	Notifications courriel
sn	urn:oid:2.5.4.4	Identification de l'utilisateur
givenName	urn:oid:2.5.4.42	Identification de l'utilisateur

4.1.2. Que faites-vous de l'information sur les attributs que vous recevez en sus de celle dont vous avez besoin pour prendre une décision sur l'accès à vos ressources?

Elles sont ignorées.

- 4.1.3. Utilisez-vous les attributs pour garantir à l'utilisateur une expérience uniforme lors de sessions multiples?

Tous les attributs retournés sont tirés des bases de données des systèmes institutionnels de l'Université Laval. Tout dépendant des besoins des participants, le même attribut peut être retourné à plus d'un participant si cet attribut correspond à la même donnée institutionnelle.

- 4.1.4. Regroupez-vous les données sur les accès ou enregistrez-vous l'information spécifique qui a été consultée en fonction des données sur les attributs?

Le mécanisme interne d'enregistrement de consentements de Shibboleth IDP 3.0 est utilisé. Les consentements sont enregistrés dans une base de données institutionnelle de l'Université Laval. Les consentements sont enregistrés par participant (Service Provider)+IDUL et identifient tous les attributs retournés au participant.

- 4.1.5. Mettez-vous l'information sur les attributs à la disposition d'autres services que vous procurez ou à d'autres organisations partenaires?

Toutes questions à ce sujet sont traitées sur une base individuelle. Contactez le Bureau de sécurité de l'information via l'adresse courriel suivante : info@bsi.ulaval.ca.

4.2 Contrôles techniques

- 4.2.1. Quelles mesures humaines et techniques ont-elles été instaurées pour contrôler l'accès aux données sur les attributs et l'utilisation de ces dernières quand elles se rapportent à une personne précise (à savoir, renseignements qui permettraient d'identifier une personne)? Par exemple, l'information est-elle encryptée avant d'être stockée dans le système?

Toutes questions à ce sujet sont traitées sur une base individuelle. Contactez le Bureau de sécurité de l'information via l'adresse courriel suivante : info@bsi.ulaval.ca.

- 4.2.2. Décrivez les mesures humaines et techniques instaurées pour contrôler la gestion des comptes de super utilisateurs et d'autres comptes privilégiés susceptibles d'être combinés à l'autorisation de consulter l'information qui permettrait d'identifier des particuliers.

Toutes questions à ce sujet sont traitées sur une base individuelle. Contactez le Bureau de sécurité de l'information via l'adresse courriel suivante : info@bsi.ulaval.ca.

4.2.3. Quelles mesures prenez-vous pour aviser les personnes susceptibles d'être affectées quand l'information permettant l'identification des particuliers est compromise?

Toutes questions à ce sujet sont traitées sur une base individuelle. Contactez le Bureau de sécurité de l'information via l'adresse courriel suivante : info@bsi.ulaval.ca.

5. Autres renseignements

5.1 Normes techniques, versions et interopérabilité

5.1.1. Veuillez identifier les produits SAML que vous utilisez. Si vous recourez aux produits à source ouverte Shibboleth d'Internet2, veuillez préciser la version employée.

Shibboleth Identity Provider installé via l'installateur de la CAF.

SAML V2.0 for ASP.NET Core from ComponentSpace

5.1.2. Sur quelles plateformes d'exploitation se trouvent les implémentations?

Shibboleth : CentOS

ComponentSpace : Windows

5.1.3. Quelles versions du protocole SAML (1.1 ou 2.0) les implémentations acceptent-elles?

2.0

5.2 Autres considérations

5.2.1. Y a-t-il d'autres considérations ou informations que vous aimeriez faire connaître aux Participants de la Fédération canadienne d'accès avec qui vous pourriez transiger? Par exemple, avez-vous des préoccupations concernant l'usage de mots de passe en clair ou les responsabilités advenant un problème de sécurité avec les informations d'identification que vous avez fournies?

Aucune considération ou information supplémentaire à donner.
