Nom du Participant: Université de Sherbrooke

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 de Sherbrooke

2.1.2. L'information qui suit était exacte à la date indiquée ci-dessous : 2016-12-20

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?

http://www.usherbrooke.ca/registraire/droits-et-responsabilites/protection-des-renseignements-personnels/

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.

Aspects administratifs :

Frédéric Brochu
Secrétaire général adjoint
Frederic.Brochu@USherbrooke.ca
819 821-7714

Aspects techniques :

Francis Bouchard Boulianne
Responsable de la Gestion d'identité, Analyste d'affaire
Francis.Bouchard-Boulianne@USherbrooke.ca
819 821-8000 x 63465

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?

Étudiants incluant les diplômés; employés et retraités; invités (parrainés). Certaines applications autorisent les personnes « auto-enregistrées »

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

Seulement : Étudiants incluant les diplômés; employés et retraités; invités (parrainés).

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.

Étudiants : identités créées par processus d'admission

Employés : identités créées à l'engagement

Invités : parrainés par un membre de la communauté

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.

- Authentification usager et mot de passe transmis à Active Directory par RADIUS selon les exigences EduRoam.

- Authentification par CAS pour le SSO Web par usager et mot de passe à LDAP utilisé pour Shibboleth

Ces authentifications sont distinctes et ne donnent pas d'accès mutuels.

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.

Contraire à nos règles de sécurité (Directive 2600-028). En cas d'infraction, contactez securite-informatique@usherbrooke.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 ».

Un délai d'inactivité de 4h utilisé. L'usager peut être redirigé vers https://cas.usherbrooke.ca/logout pour être déconnecté immédiatement. Chaque site distinct doit être autorisé et doit demander un jeton pour une nouvelle session. L'usager peut demander d'être notifié du changement de site.

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?

Les identificateurs CIP ne sont jamais réattribués.

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?

Étudiants gérés par le Bureau de la registraire; employés gérés par le Service des ressources humaines; invités gérés par le Service des technologies de l'information. Pas de locaux dédiés à cette activité. Coordonnées personnelles modifiables en ligne par les employés et les étudiants.

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?

Nom, unité administrative, lien d'emploi (titre), local, téléphone à l'emploi, télécopieur, adresse de courriel. Utilisation pour fins commerciales interdite.

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.

Tous types d'utilisation académique et administrative ainsi que le courrier électronique.

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.

Les informations sont gérées par le Bureau de la Registraire et le Service des ressources humaines – à l'exception des attributs modifiables en ligne mentionnés plus haut. Il y a un processus de parrainage pour les utilisateurs invités.

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 attributs doivent être utilisés pour les fins auxquelles ils sont destinés, nommément l'identification des participants et le contrôle d'accès. Toute utilisation à des fins commerciales est strictement interdite, à moins d'autorisation spécifique.

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?

Le cadre légal Québécois doit être respecté. Voir aussi : http://www.usherbrooke.ca/registraire/droits-et-responsabilites/protection-des-renseignements-personnels/

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

http://www.usherbrooke.ca/registraire/droits-et-responsabilites/protection-des-renseignements-personnels/

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.

Non applicable

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?

Non applicable

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

Non applicable

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?

Non applicable

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?

Non applicable

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?

Contrôle d'accès aux informations en fonction des rôles. Chiffrement des informations véhiculées sur les réseaux. Chiffrement d'informations jugées très sensibles dans les bases de données.

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.

Limitation stricte du nombre de codes privilégiés.

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?

Contacter la personne concernée, l'informer des impacts. Dans le cas où les éléments d'authentification sont compromis, le mot de passe est réinitialisé et l'usager doit s'en attribuer un nouveau.

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 v3.2.X

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

RHEL 6.8

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

1.1 et 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?

Pour toutes considérations de sécurité, contactez securite-informatique@usherbrooke.ca.