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

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.

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.

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.

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

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

1.1.1. Nom de l'organisation : Université de Montréal

1.1.2. L'information qui suit était exacte à la date indiquée ci-dessous :

24 janvier 2017

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

1.2.1. 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://secretariatgeneral.umontreal.ca/documents-officiels/

1.3 Personne-ressource

1.3.1. 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 : Benoit Faucher
Titre ou rôle : Officier de sécurité
Courriel : benoit.faucher@umontreal.ca
Téléphone : 514 343-6111 poste 5216

2. 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.).

2.1 Communauté

2.1.1. 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?

Les identités électroniques sont attribuées aux employés, étudiants et invités. Les exceptions doivent être approuvées par la Sécurité informatique.

2.1.2. 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?

Essentiellement les employés et les étudiants.

2.2 Justificatifs de l'identité électronique

2.2.1. 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 identités d'employés sont créées suite à l'embauche d'une personne par les Ressources humaines. Celles des étudiants sont créées suite à l'admission d'un étudiant dans un programme/cours. Les identités sont conservées dans notre progiciel de gestion intégré (ERP).

2.2.2. 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.

Les systèmes d'authentifications utilisent la combinaison de nom utilisateur/mot de passe pour les services de la FCA auquel l'Université de Montréal souscrit.

2.2.3. 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.

Les authentifications sont chiffrées.
Les questions peuvent être adressées à l'Officier de sécurité de l'Université de Montréal.

2.2.4. 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 ».

En date de parution de ce document, relativement aux services de la FCA auxquels l'Université de Montréal souscrits, il n'y a pas d'intégration avec nos services SSO.

2.2.5. 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?

Oui, les principaux identificateurs électroniques sont considérés uniques pour toujours.

2.3 Base de données des identités électroniques

2.3.1. 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?

Les identités électroniques origines de notre progiciel de gestion intégré (ERP) institutionnel. Le Centre d'Expertise Synchro (CDE) possède la responsabilité d'administrer ces informations. Les utilisateurs sont autorisés à actualiser une partie restreinte de leurs informations ; par exemple, ils peuvent modifier leur mot de passe en respect des meilleures pratiques de l'industrie en la matière.

2.3.2. 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?

Les informations de contact des employés sont publiques.

2.4 Utilisation du système de justificatifs de l'identité électronique

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

Les justificatifs d'identité électronique sont utilisés pour l'accès aux systèmes académiques, l'accès aux systèmes administratifs et l'accès au réseau institutionnel,

2.5 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.

2.5.1. Veuillez décrire la fiabilité des attributs d'authentification de votre fournisseur d'identité.

Les attributs d'authentification sont très fiables.

2.5.2. 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? **N/A**

c) permettre l'accès à des renseignements de nature personnelle comme des données sur le dossier de l'étudiant? **OUI**

2.6 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.

2.6.1. 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?

L'utilisation des données institutionnelles de l'Université de Montréal est régie par les politiques décrites aux points 2.6.2 et 2.6.3.

Les informations transmises aux autres Participants doivent préalablement faire l'objet d'une autorisation de la part des autorités institutionnelles compétentes en la matière.

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

A-2.1 - Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels

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

http://secretariatgeneral.umontreal.ca/documents-officiels/reglements-et-politiques/telechargement/reglement/politique_sur_la_protection_des_renseignements_personnels/

3. 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.

L'université de Montréal 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.

3.1 Attributs

3.1.1. 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.

Les autres Participants peuvent accéder le réseau sans-fil Eduroam offert à l'Université de Montréal. L'authentification est redirigée vers les services correspondants de leur institution d'appartenance. Cette redirection est basée sur le domaine fourni par le Participant lors de son identification ; ex.: usager@umontreal.ca.

L'Université adhère au Service fédéré d'authentification unique (FSSON) mais n'offre présentement aucun service aux autres Participants.

3.1.2. 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?

N/A

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

N/A

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

N/A

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

N/A

3.2 Contrôles techniques

3.2.1. 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?

N/A

3.2.2. 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.

N/A

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

N/A

4. Autres renseignements

4.1 Normes techniques, versions et interopérabilité

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

CAF Shibboleth Package 3.x (Dec 2016)

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

OLS (Oracle Linux) 7.2

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

Les deux, SAML 2.0 par défaut.

4.2 Autres considérations

4.2.1. 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?

Tout incident de sécurité relatif aux informations institutionnelles d'identifications et aux attributs transmis aux autres Partenaires doit être immédiatement rapporté à l'Officier de sécurité de l'Université de Montréal en utilisant l'adresse securite@umontreal.ca