Fédération canadienne d'accès :
Confirmation de fiabilité (DCF) pour les fournisseurs de services

But

Les attributs sont les « paramètres » d'une « identité » (nom, département, emplacement, identifiant, nombre d'employés, courriel, etc.).

Une exigence que doivent absolument respecter les organisations qui adhèrent à la Fédération canadienne d'accès (FCA) consiste à transmettre aux autres participants les attributs exacts des identités sans lesquels on ne pourra accéder aux ressources offertes. Parallèlement, les participants qui obtiennent les attributs dont la véracité a été confirmée sont tenus de les protéger et de respecter les contraintes qui s'y appliquent, fixées par l'organisation d'origine.

Dans cette optique, CANARIE demande à l'organisation de transmettre aux autres participants de la FCA les réponses aux questions qui suivent.

Exigence de la Fédération canadienne d'accès

La confiance qui règne au sein de la communauté de la FCA repose sur les « meilleurs efforts possibles » et la transparence des pratiques. Chaque organisation fournit aux autres participants la documentation sur ses pratiques en gestion des identités et des accès qu'elle sait pouvoir respecter. Elle met à leur disposition des renseignements de base sur les systèmes de gestion des identités et d'accès aux ressources qu'elle a inscrits à la FCA. Ces renseignements comprennent la manière dont les attributs identitaires sont définis et la façon dont les services utilisent ces attributs.

Publication

Les réponses aux questions qui suivent seront remises à CANARIE, qui les affichera sur son site Web. Il revient à l'organisation de garder à jour le Document de confirmation de fiabilité (DCF).

1. Renseignements sur le participant

1.1 Nom de l'organisation : Fédération des cégeps

1.2 Les informations qui suivent étaient exactes le 10/29/2023

1.3 Coordonnées

1.3.1. Veuillez indiquer le bureau, le service, le département ou la personne en mesure de répondre aux questions sur le système de gestion des identités ou les politiques/pratiques concernant l'accès aux ressources de l'organisation.

Remarque : Il est préférable que ces renseignements se rapportent à un département ou à un bureau plutôt qu'à une personne pour qu'on puisse obtenir une réponse aux questions si jamais un changement survient au niveau du personnel.

Département (ou nom du contact) : TECHNOLOGIES DE L'INFORMATION

Courriel : jean.benard@fedecegeps.qc.ca

Téléphone : (514) 381-8631

1.4 Gestion des identités / Informations sur la protection des renseignements personnels

1.4.1. Quelles sont les politiques qui régissent l'usage des attributs que l'organisation pourrait transmettre aux autres participants de la FCA? Si ces politiques peuvent être consultées en ligne, veuillez en fournir l'URL.

https://fedecegeps.ca/politique-de-confidentialite/

1.4.2. Veuillez indiquer l'URL de votre politique concernant la protection des renseignements personnels et fournir des renseignements sur les autres politiques éventuelles régissant l'usage des attributs que l'organisation pourrait transmettre aux autres participants de la FCA.

https://fedecegeps.ca/wp-content/uploads/2023/10/daj-pol-protection-renseignements-personnels-adopte-6septembre2023.pdf

2. Renseignements sur le fournisseur d'identités (GFI / eduroam)

Sans objet

3. Renseignements sur le fournisseur de services (Gestion fédérée des identités / eduroam)

Le fournisseur de services qui reçoit la confirmation de la véracité des attributs d'un participant respectera les politiques, les règles et les normes établies par ce dernier pour protéger et utiliser ses données. Les informations fournies ne serviront qu'aux fins pour lesquelles elles ont été remises.

On présume que le fournisseur de services ne demandera que les informations strictement nécessaires pour prendre la bonne décision concernant le contrôle des accès et n'utilisera pas l'information transmise à mauvais escient. Le fournisseur de services décrira ce sur quoi il s'appuie pour donner accès aux ressources qu'il gère et les pratiques qu'il applique aux attributs obtenus des autres participants.

3.1 Attributs

3.1.1. Quels renseignements réclamez-vous sur les attributs d'une personne? Veuillez décrire chaque service offert aux participants de la FCA séparément (un service par rangée).

Service	S'agit-il d'un service R&S?	Attributs requis	Motif	L'information est-elle partagée?
eduroam	N/A	**Jeu standard d'attributs RADIUS (annexe A du document** eduroam Compliance Statement**)** • référence temporelle de la demande d'authentification et de la réponse correspondante • identité EAP externe de la demande d'authentification (attribut User-Name) • identité EAP interne (identifiant réel de l'utilisateur) • adresse MAC du client établissant la connexion (attribut Calling-Station-Id) • réponse d'authentification (acceptée ou refusée)	Authentification	Non

Remarques. *Les attributs normalisés par eduroam ont été inscrits à l'avance afin que le document soit plus facile à remplir. Si vous n'offrez pas eduroam, veuillez supprimer cette rangée.*

Un service GFI de la catégorie d'entité Research & Scholarship (R&S) et les attributs qui s'y associent ont aussi été inscrits à titre d'illustration. Veuillez le supprimer et insérer vos propres données au besoin. Ajoutez des rangées au tableau s'il y a lieu.

3.2 Contrôles techniques

Les contrôles techniques servent à réguler l'accès aux données sensibles et l'exploitation de ces dernières. On s'attend à ce qu'ils s'appliquent à tous les services. S'il y a des exceptions, veuillez les décrire.

3.2.1. Décrivez les mesures humaines et techniques mises en place pour contrôler l'accès aux attributs susceptibles d'identifier une personne et leur utilisation.

Authentification 2FA pour les administrateurs de domaine et pour les utilisateurs réguliers. VLAN de gestion informatique séparé pour avoir accès au serveur de contrôle d'accès et à AD. Les serveurs sont segmentés dans une LAN et une DMZ avec des limites de pare-feu. Tous les placards informatiques et salles de serveurs sont protégés par accès par carte (RFID)

3.2.2. Décrivez les mesures humaines et techniques mises en place pour gérer les comptes des super utilisateurs et les autres comptes avec privilèges pouvant donner accès à des informations susceptibles de permettre l'identification d'une personne.

Mot de passe fort et authentification 2FA . L'audit AD est activé en cas de réussite ou d'échec, les serveurs AD et NPS RADIUS et les contrôleurs Meraki se trouvent sur leurs propres VLAN d'administration et sont protégés par un pare-feu.

3.2.3. Si des informations permettant d'identifier quelqu'un sont compromises, quelles mesures prenez-vous afin d'en aviser ceux que cela pourrait toucher?

Contactez les utilisateurs directement via leur adresse courriel et les informer de la situation avec une copie conforme pour **dti1@fedecegeps.qc.ca**

3.3 Autres considérations

3.3.1. Quelles autres considérations ou informations aimeriez-vous signaler aux participants de la FCA avec lesquels vous pourriez interagir?

N/A