Canadian Access Federation:
Trust Assertion Document (TAD) for Service Providers

Purpose

Identity attributes are characteristics of an identity -- such as a name, department, location, login ID, employee number, e-mail address, etc.

A fundamental requirement of Participants in the Canadian Access Federation (CAF) is that by their authority they send accurate identity attributes to other Participants to allow access to resources, and that Participants receiving an attribute assertion protect it and respect privacy constraints placed on it by the asserting Participant.

To accomplish this practice, CANARIE requires Participants to make available to all other Participants answers to the questions in this document.

Canadian Access Federation Requirement

The CAF community of trust is based on “best effort” and transparency of practice. Each Participant documents, for other Participants, their identity and access management practices, which they can confidently meet. Each Participant makes available to other Participants basic information about their identity management system and resource access management systems registered for use within the Canadian Access Federation. The information includes how supported identity attributes are defined and how attributes are consumed by services.

Publication

Your responses to these questions must be submitted to CANARIE to be posted on the CANARIE website. You must maintain an up-to-date Trust Assertion Document.

1. Participant Information

1.1 Organization Name: Modern Campus Inc. (formerly Destiny Solutions)

1.2 Information below is accurate as of this date: 01/26/2026

1.3 Contact Information

1.3.1. Please list the office, role, department, or individual who can answer questions about the Participant's identity management system or resource access management policy or practice.

Note: This information should be for a department or office rather than an individual, in order to avoid responses going unanswered if personnel changes occur.

Department (or Contact Name): Chad Rowe OR Hoan Luong

Email Address: crowe@moderncampus.com OR hluong@moderncampus.com

Telephone: Click or tap here to enter text.

1.4 Identity Management and/or Privacy Information

1.4.1. What policies govern the use of attribute information that you might release to other CAF Participants? If policies are available online, please provide the URL.

Modern Campus does not release identity attributes to other CAF participants. Attributes received from Identity Providers are used solely for authentication and authorization within Modern Campus' application.

1.4.2. Please provide your Privacy Policy URL, as well as information regarding any other policies that govern the use of attribute information that you might release to other CAF Participants.

Modern Campus does not release identity attributes to other CAF participants. Attributes received from Identity Providers are used solely for authentication and authorization within Modern Campus' application.

2. Identity Provider Information (FIM and/or eduroam)

Not applicable

3. Service Provider Information (Federated Identity Management and/or eduroam)

Service Providers, who receive attribute assertions from another Participant, shall respect the other Participant's policies, rules, and standards regarding the protection and use of that data. Such information must be used only for the purposes for which it was provided.

Service Providers are trusted to ask for only the information necessary to make an appropriate access control decision, and to not misuse information provided to them by Identity Providers. Service Providers must describe

the basis on which access to resources is managed and their practices with respect to attribute information they receive from other Participants.

3.1 Attributes

3.1.1. What attribute information about an individual do you require? Describe each service that you offer to CAF Participants separately (one service per row).

Service Name	Is this an R&S service?	Attributes Required	Rationale	Is information shared with others?
eduroam	N/A	**Standard RADIUS attribute set (Appendix A of the eduroam Compliance Statement):** • timestamp of authentication requests and corresponding responses • the outer EAP identity in the authentication request (User-Name attribute) • the inner EAP identity (actual user identifier) • the MAC address of the connecting client (Calling-Station-Id attribute) • type of authentication response (i.e. Accept or Reject).	For authentication purposes	No
Example **{FIM Service 1}**	☐	• **user identifier** (eduPersonPrincipalName + eduPersonTargetedID) • **person name** (givenName + sn) • **email address** • **affiliation** (eduPersonScopedAffiliation)	For authentication (user identifier, person name, email address) and authorization (affiliation) purposes	No
{FIM Service 2}	☐			

Notes: *The standard attributes for eduroam have been pre-filled to assist with completion. If you are not implementing eduroam, please delete this row.*

Additionally, an example of a Research & Scholarship (R&S) Entity Category FIM service and its associated attributes has been included. Please delete this example and enter your own data, as applicable. Add additional rows to the table, as required.

3.2 Technical Controls

Technical controls are a basis for controlling access to and usage of sensitive data and are expected to be applied across all services. If there are exceptions for a particular service(s), please describe these exceptions.

3.2.1. Describe the human and technical controls in place for access to and use of attributes considered personally identifiable information.

Modern Campus does not request, require, or expand attribute release beyond what is explicitly configured and approved by the institution. From a human controls perspective, access to SSO-provided attributes within Modern Campus is restricted to authorized personnel with a legitimate operational need, governed by role-based access control and least-privilege principles. Employees and contractors are subject to background screening where permitted by law, mandatory security and privacy training, and confidentiality obligations. Access to systems handling authentication and identity data is reviewed periodically and revoked promptly upon role change or termination. From a technical controls perspective, SSO integrations use standards-based federation protocols (e.g., SAML) to securely transmit attributes from the institution's IdP to Modern Campus. Attribute data is protected through encryption in transit, logical segregation of customer data, and access logging. Modern Campus processes and stores only the attributes released by the institution and uses them solely for authentication and authorization purposes defined by the service, supporting institutional control over identity data while ensuring confidentiality, integrity, and availability.

3.2.2. Describe the human and technical controls that are in place for the management of super-user and other privileged accounts that may have the authority to grant access to personally identifiable information.

Modern Campus implements strict human and technical controls to manage super-user and other privileged accounts that may have the ability to grant access to personally identifiable information (PII). As a service provider, Modern Campus does not control institutional identity systems or the release of identity attributes; however, it maintains controls over privileged access within the application and supporting infrastructure. From a human controls perspective, privileged access is limited to a small, authorized group of personnel whose roles require elevated permissions for operational support or system administration. Access is provisioned following management approval, governed by role-based access control and least-privilege principles, and supported by background screening where permitted by law, mandatory security and privacy training, and confidentiality obligations. Privileged access is reviewed periodically and promptly revoked upon role change or termination. From a technical controls perspective, privileged accounts are protected through strong authentication mechanisms, including multi-factor authentication where applicable, and are subject to logging and monitoring to record administrative actions. Access to functions that could grant or modify access to PII is restricted to defined roles, and customer data is logically segregated by tenant. Modern Campus does not independently create or release identity attributes; it processes only those attributes provided by the institution's identity provider via standards-based SSO, and privileged actions within the service are constrained to the scope necessary to support authorized operations.

3.2.3. If personally identifiable information is compromised, what actions do you take to notify potentially affected individuals?

In the event of a PII compromise, Modern Campus promptly notifies the affected institution and supports investigation and remediation in accordance with its incident response procedures. As the service provider, Modern Campus does not directly notify individuals; notification decisions and communications are managed by the institution as the data controller, with Modern Campus providing reasonable assistance as required.

3.3 Other Considerations

3.3.1. Are there any other considerations or information that you wish to make known to other CAF Participants with whom you may interoperate?

Modern Campus does not release identity attributes to other CAF participants. Attributes received from Identity Providers are used solely for authentication and authorization within Modern Campus' application.