Full Examples of Background Wording

This table shows the wording currently used by federations in their 'background' descriptions

Back to Federation Policy Mapping

	BACKGROUND and PURPOSE
Austria ACOnet	(2A)The ACOnet Identity Federation is introduced to facilitate and simplify the offering of shared services across the (identity) federation. This is accomplished by using technologies to extend the scope of an (electronic) identity issued by one member of the federation to be valid across the whole federation. (2B)This (federation) policy defines the federation by specifying procedures and practices which allow participating organizations to use available federation technologies for electronic identification and for access to authorization information about individuals, resources and other objects in the federation. This policy does not directly describe practices or procedures specific to any particular choice of federation technology. (2C)Identity Management are the processes by which Identity Providers first issue and then manage identities throughout their life-cycles and by which they also make claims of identity for subjects (e.g. individuals, resources and other objects). A claim of identity is an electronic representation, using a specific identity management technology, of a set of attributes identifying a subject. (2D)The ACOnet Identity Federation policy has three main parts: this document, which describes governance, membership and scope, a set of zero or more (identity) Assurance Profiles and a set of (federation) Technology Profiles. The Assurance Profiles and the Technology Profiles are based on current and evolving standards and best practices and are described in separate documents, available at http://www.aco.net/. An Assurance Profile describes levels of trust in claims and organizations. (2E)An Assurance Profile allows a Service Provider to determine the degree of certainty that the identity of a subject presenting a claim of identity is truly represented by the presented claim. A commonly agreed-upon “Level of Assurance” represents this degree of certainty. Identity assurance is to a large extent independent of the technology used to convey claims of identity. (2F)The Technology Profiles describe concrete realizations of the policy and Assurance Profiles in terms of specific technologies (e.g. SAML, eduroam etc.). By employing specific choices of technologies for identification and authorization this policy MAY be used to support federated identity for a wide range of applications. Technology Profiles govern the use of federation technology. (3A)The purpose of the ACOnet Identity Federation is to make it possible for (Application / Information) Service Providers to provide services to end users in the federation. This is accomplished by making infrastructure for federated identification and authentication available to the ACOnet constituency (see http://www.aco.net/teilnehmer.html).
Australia AAF	1.1 The purpose of the AAF (Òthe FederationÓ) is to provide a mechanism for connecting members of the education and research sectors including academics, researchers, and students (ÒEnd UsersÓ) securely and reliably to online information, infrastructure, services and resources.1.2 Subscription to the Federation is available to organisations and institutions (ÒSubscribersÓ) which undertake or support education, research or research and development in Australia and agree to be bound by the Federation Rules (ÒRulesÓ).1.3 The Federation relies on Subscribers, as Identity Providers, correctly and accurately asserting information about the identity of its End Users to other Subscribers who, as Service Providers, will use that information to grant (or deny) access to the services and resources they offer to End Users.1.4 The scope of the Federation may be extended over time to include a broader range of Subscribers beyond the education and research sectors.1.5 The electronic exchange of authentication information between End Users, Identity Providers and Service Providers and the provision of support services for Subscribers may be managed by one or more Operators on behalf of the Federation.
Canada CAF	0.1 WHEREAS CUCCIO has established an access federation in Canada for use by research and education institutions and suppliers to those institutions to enable users of one domain to securely access the systems of another domain for research and educational purposes (the “Canadian Access Federation”) 0.6 NOW THEREFORE in consideration of the mutual covenants set out in this Agreement and for other good and valuable consideration (the receipt and sufficiency of which is hereby acknowledged by each of the parties), the parties agree as follows:
Czech Republic eduID	1.1 eduiD.cz is a Czech National Academic Identity Federation providing its members with a framework for sharing user identities while controlling access to network services, adhering to personal data protection principles. 1.2 This Document defines the organization Policy to be used in the operation of the eduID.cz Federation.
Denmark WAYF	left out due to length
Spain - SIR	NONE
Finland - HAKA	left out due to length
France - Federation Recherche	no cut and paste version of agreement available.
Ireland - edugate	1.1 The purpose of this document is to set out the rules, terms and conditions that service provider members of the Edugate Federation shall subscribe to. 1.2 These rules, terms and conditions aim to safeguard a user’s personal data and provide a basis of assurance for service providers when receiving identity data issued by a user’s organisation which organisations are generally described as identity providers. The Edugate Federation exists to facilitate the convenient exchange of online services based on these safeguards and assurances.

Japan - Gakunin	Article 1. Purpose These Guidelines are for members to implement the GakuNin Academic Access Management Federation (hereinafter called GakuNin). They have been drawn up by the Certification Working Subcommittee of the Organization for Science Network Operations and Coordination in the National Institute of Informatics (hereinafter called "CWSC"). Article 2. Description of GakuNin GakuNin ensures interoperation among the authentication platforms of various universities and research organizations. It enables single sign-on authentication across organizations by coordinating the technical specifications, system administrative standards, and usage conventions across participating organizations. It facilitates mutual agreement on matters affecting its participants.
Norway - FEIDE	1.1 Background and Purpose of the Agreement UNINETT is a 100 % State-owned limited company under the Ministry of Education and Research, with the objective of: • developing a nationwide electronic computer network with services for research and • education; • accelerating the use of open international standards within data communication; • providing for peering with current national and international network operators; and • stimulating necessary research and development activity in UNINETT's sphere of activity. UNINETT's operations are primarily funded by government grants allocated to UNINETT directly. To a growing extent, parts of the organization are user-funded. UNINETT has implemented standards, programs and Web services which are included in a system for authentication of people who wish to log on to electronic services designed for the research and educational sector. This system is hereinafter referred to as "Feide". The primary target group for the authentication system is public-sector research and educational institutions in Norway that wish to enter into an agreement with UNINETT regarding the use of Feide. Private-sector players within the research and educational sector may be offered the opportunity to connect to Feide where UNINETT finds this practical for Feide's primary target group. On the basis of the same objectives, UNINETT will establish collaborative agreements with owners/administrators of foreign authentication systems for the research and educational sector. UNINETT is responsible for the top-level management and administration of Feide. UNINETT also takes care of the operation of certain Web services which are incorporated in Feide, including the Feide login service used for logging on to electronic services. Organizations and service providers that are linked to Feide must themselves implement, manage and operate services. Linked organizations must themselves implement and manage databases of the organization's own users. The objective of Feide central services is to provide: • a login service in stable operation 24/7. This includes operation, second-line user support to host organizations, further development of the login service and standardization of integration • systems of agreements in Feide and policy for identity management, both internally in Feide and with respect to other federations • information model for personal information with attribute document and standardization of the interface • architecture for Feide A condition for connecting to and using Feide is that an agreement regarding this has been entered into with UNINETT, and this is the background for formation of the current agreement between UNINETT and the Organization. All use of Feide is subject to UNINETT's regulations in effect at any time.
Portugal-RCTSAAI	1 INTRODUCTION The increased sharing of resources between institutions is a reflection of inter-institutional collaboration. Authentication and authorisation infrastructure is designed to simplify access to Web services shared between various institutions in a secure, distributed and confidential manner, using a single login and without dependence on the user's location. This type of infrastructure is based on the principle that, when accessing a Web service, a user is authenticated based on the credentials of their own institution and is authorised based on attributes provided by the user's institution to the respective service. The management of authentication and authorization infrastructure relies on the establishment of a relationship between the institutions involved which is based on trust, so that a common set of policies can be used, together with attributes which must be guaranteed in the exchange of information between users and services. Federations are set up in order to develop this trust and to facilitate the management of the integration of privacy rules and the set of common attributes. A federation is a group of institutions which agree to collaborate among themselves using an authentication and authorisation infrastructure. The RCTSaai federation was set up by FCCN in the context of the "Utilizador RCTS" (RCTS User) service and its objective is the conception of a federation at a national level and the use of federated services by participating institutions. Thereafter, a formal framework will be needed, embodied specifically in the acceptance of and compliance with a set of rules and principles to be followed within the RCTSaai federation.
Sweden SWAMID	(1A)The Swedish Academic Identity Federation is introduced to facilitate and simplify the introduction of shared services across the (Identity) Federation. This is accomplished by using Federation Technologies to extend the scope of an (Electronic) Identity issued by one Member of the Federation to be valid across the whole Federation. (1B)This (Federation) Policy defines the Federation by defining the procedures and practices which allows participating organisations to use available Federation Technologies for electronic identification and for access to authorisation information about individuals, resources and other objects in the Federation. In what follows the Swedish Academic Identity Federation is abbreviated SWAMID. This Policy does not directly describe practices or procedures specific to any particular choice of Federation Technology. (1C)Identity Management are the processes by which Identity Providers first issue and then manage identities throughout their life-cycles and by which they also make Claims of identity for Subjects (e.g. individuals, resources and other objects). A Claim of identity is an electronic representation, using a specific identity management technology, of a set of attributes identifying a Subject. (1D)The SWAMID Policy has three main parts: this document which describes governance, membership and scope. Further, a set of (Identity) Assurance Profiles and a set of (Federation) Technology Profiles. The Assurance Profiles and the Technology Profiles are based on current and evolving standards and are described in separate documents. (1E)An Assurance Profile describes levels of trust in claims and organisations. An Assurance Profile allows a Relying Party (also known as a Service Provider) to determine the degree of certainty that the identity of a Subject presenting a Claim of identity is truly represented by the presented claim. This degree of certainty is represented by a commonly agreed-upon "Level of Assurance". Identity assurance is to a large extent independent of the technology used to convey Claims of identity. (1F)The Technology Profiles describe concrete realisations of the Policy and Assurance Profiles in terms of specific technologies (eg SAML, eduroam etc). By employing specific choices of technologies for identification and authorisation this Policy MAY be used to support federated identity for a wide range of applications. The use of federation technology (e.g. SAML, 802.1x, WS-Federation, OpenID) is governed by a Federation Technology Profile. (3A) The purpose of SWAMID is to make it possible for Service Providers to provide services to End Users in the Federation. This is accomplished by making infrastructure for federated identification and authentication available to the higher education and research community in Sweden, including but not limited to universities, university colleges, research hospitals, government agencies and private sector organisations involved in higher education and research.
UK UK federation	(intro-a)The purpose of the Federation is to create a framework within which Members can exchange access management information in a way that is responsible and respects End User privacy. (intro-b)The framework is created by each Member agreeing to be bound by these Rules which set out an agreed set of rules for exchanging information about End Users and resources, to enable access to and use of resources and services. 13.6. These Rules and all the documents referred to in them supersede all other agreements, arrangements and understandings between the parties in respect of their subject matter, and constitute the entire agreement between them relating to their subject matter. For clarity, the Explanatory Notes contained at the end of these Rules are designed to provide background and explanation to the relevant Rule. They are not themselves incorporated into these Rules.

US - InCommon	Internet2 has created InCommon as a service to higher education and research organizations in the U.S. The InCommon Federation is an activity of InCommon and is generally governed by a Steering Committee representing the interests of Participants. The purpose and role of the Federation is set forth in more detail in the Limited Liability Company Agreement ("LLC Agreement") and Federation Operating Practices and Procedures ("FOPP") of the Federation as amended from time to time by the InCommon Steering Committee. InCommon accepts applications from organizations that are potential Participants in the Federation, as defined in the FOPP, and provides the Federation services to Participants ("InCommon Participants") under the terms and conditions of this Agreement.