Appendix 1. Key concepts of the Authentication and Authorization Infrastructure (AAI) service

AAI	Authentication and Authorization Infrastructure. See Authentication, see Authorization.
Advisory Committee	Haka Identity Federation body which represents the Federation Participants and whose task is to promote and coordinate the deployment and use of the Federation.
Assertion	A set of data that follows a specification and contains statements by an Identity Provider concerning the End User's authentication, attributes and authorizations.
Attribute	A piece of information describing the End User, their properties or roles in their Home Organization
Attribute Release Policy (ARP)	A Shibboleth term for the configuration of attributes to be released to a Service Provider, as defined by the End User or their Home Organization.
Authentication	See Identity verification
Authorization	Process of granting or denying access rights to a service for an authenticated End User.
Code of conduct	Sector-specific rules for data controllers or their representative organization that concern the proper processing of personal data in accordance with data protection legislation.
Data Controller	(EU General Data Protection Regulation) "Controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.
Data protection legislation	Agreement references to data protection legislation include the EU General Data Protection Regulation ((EU) 2016/679), Data Protection Act (1050/2018), other data protection legislation valid and applicable in Finland, and binding regulations set forth by data protection authorities.
Data subject	The Home Organization End User, whose attributes are released by the Home Organization in the Federation to the Service Provider. The definition refers to the definition given in the EU General Data Protection Regulation.
Discovery Service	(Where Are You From (WAYF)) A server set up by an Operator or Service Provider and used by an End User to select their Home Organization.
End user	A student, employee or person otherwise affiliated with a Home Organization that uses services provided by Service Providers.
Federation	A group of organizations which decide to cooperate in the area of inter-organizational authentication and authorization.

	It should be noted that the term "Federation", whether used alone or in conjunction with other terms, shall be descriptive only and shall not indicate any association, joint venture, partnership or other legal structure of Federation members. Note! In the Service Agreement, "Federation" refers to the Haka Identity Federation.
Federation Member	University, university of applied sciences, research institute or an organization supporting research and education (specified in greater detail in Appendix 2) that has joined the Federation by signing the Service Agreement for Federation Members. Within the Federation framework, a Federation Member may function both as a Home Organization and a Service Provider.
Federation Participant	Operator, Member or Partner in the Federation.
Federation Partner	An organization that is not a Federation Member but has signed the Service Agreement for Federation Partners concerning the provision of services to End Users in Federation Member organizations.
FunetEduPerson schema	Specification about the syntax and semantics of common attributes released within the Federation.
Haka Identity Federation	The Federation founded by universities and universities of applied sciences under the jurisdiction of the Finnish Ministry of Education and Culture. In this appendix, Federation refers to the Haka Federation
Home Organization	(aka Identity Provider, Credential Provider) A university, university of applied sciences, research institution or organization supporting education and research that maintains the attributes of users in its organization (End Users) and is responsible for the authentication of their identity in the Federation. The Home Organization maintains the attributes of end users in its organization and is responsible for the authentication of their identity in the Federation. The Home Organization sets up an Identity Provider and registers it in the Federation.
Identity	Abstraction of a real person in an information system. Consists of a set of attributes describing them.
Identity Provider	A server set up by a Home Organization to authenticate the identity of an End User when signing on and release the End User's assertion to the Relying Party.
Identity verification	Process of proving the identity of a previously registered End User.
Metadata	Technical and administrative data describing Home Organizations and Service Providers in the Federation and their Identity Providers and Relying Parties.
Name identifier	A reference number given to an End User by the Identity Provider. Used by the Identity and Relying Party to refer to a specific End User.
OpenID Connect	A simple identity layer added to the OAuth 2.0 protocol that allows Relying Parties to direct an End User to an Identity Provider

	for authentication and receive the End User's attributes.
Operations Committee	An advisory body whose task is to serve as a technical discussion forum for Federation Participants.
Operator	Organization that maintains central Federation structures, such as Federation metadata and WAYF or DS servers.
Personal data	(EU General Data Protection Regulation) "Personal data" means any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. Indirect identification can be done not only by means of personal data being processed at a given time, but also using a combination of this data and easily available additional data. An attribute or a set of attributes is considered as personal data if it identifies an individual as defined above.
Privacy Policy	Drafted in order to comply with the notification obligation in data protection legislation, this document is used to fulfil the notification obligation of the Data Controller and serves as the basis for assessing whether network services that collect personal data comply with data protection legislation. The Privacy Policy is also often referred to as a Privacy Statement.
Processing of personal data	(EU General Data Protection Regulation) The processing of personal data ("Processing") means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Processor of personal data	(EU General Data Protection Regulation) A processor of personal data ("Processor") means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
Relying Party/Service Provider	A server set up by a Service Provider to receive the authenticated End User's assertion from the Identity Provider.
SAML	(Security Assertion Markup Language) An XML-based framework defined by OASIS for exchanging identity management related data between organizations.
Service Provider	A Federation Member or Partner that provides electronic services to End Users in Home Organizations. A Service provider may be a Member or Partner that is a university, research institute, a joint organization formed by these or another actor. A Service Provider sets up a Relying Party and registers it in the Federation.
Shibboleth	An open source server program maintained by the Shibboleth

	Consortium that implements the Identity Provider and Relying Party.
User administration, Identity management	Procedures and mechanisms used by an organization for keeping track of its End Users and their user rights.

Appendix 2. Organization of the Federation

1. Introduction

This document defines the criteria for membership in the Federation and its bodies.

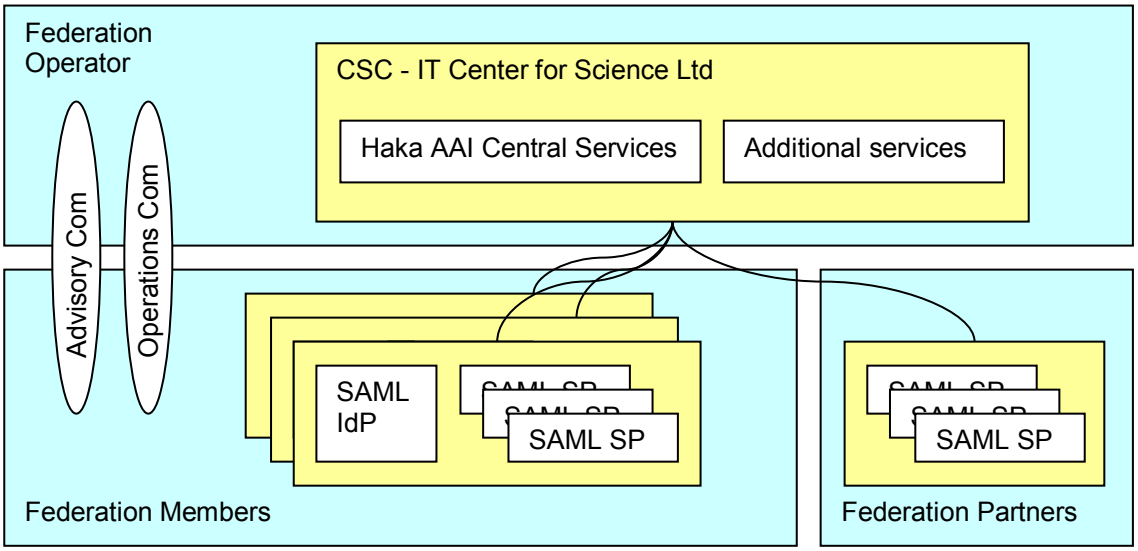
2. Criteria for membership in the Federation.

2.1. Federation Participants

Participants in the Haka Identity Federation are divided into the following groups:

- Members, which may function both as a Home Organization and a Service Provider in the Federation.
- Partners, which are not Home Organizations, but provide electronic services to authenticated users in them.

Universities, universities of applied sciences, state and publicly-owned research institutions, and other organizations supporting research and education may be admitted to the Federation as Members as described below in section 2.2. The Federation may also use external partners (Federation Partner). However, a requirement for functioning as a Member and Partner is that the processing of personal data in the person register of the Service Provider or Home Organization is not in conflict with the purpose of the Federation as well as that the organization meets the other Federation requirements (specified in Appendix 3).



2.2. Members

- Within the Federation framework, a Federation Member may function both as a Home Organization and a Service Provider.
- Category A:
    - Universities as defined by the Universities Act (558/2009)

- Universities of applied sciences as defined by the Universities of Applied Sciences Act (932/2014)

- Category B:
  - Bodies, authorities and research institutes of science and arts which are founded by law for public duty in Finland
  - Other organizations for the public good or publicly-owned organizations supporting research and education in universities, universities of applied sciences and research institutes (e.g. CSC - IT Center for Science Ltd.).
  - The membership of organizations in category B is subject to approval by the Advisory Committee of the Federation upon a proposal made by the Federation Operator. There is a two-week deadline for responding to the Operator proposal. A new Member will be accepted:
    - automatically at the end of the two-week deadline if no member of the Advisory Committee opposes membership or recommends that the membership application be discussed at an Advisory Committee meeting; or
    - immediately after the most recent approval if all members of the Advisory Committee accept admission of the new Member; or
    - at the Advisory Committee meeting in case a member of the Advisory Committee has opposed the acceptance or has suggested a discussion of the membership application

- The membership of a Member admitted to the Federation will enter into effect when both the applicant organization and Operator have signed the Service Agreement on behalf of and authorized by the other Federation Participants.

2.3. Partners

- Partners, which are not Home Organizations, but provide electronic services to users in them, may join the Federation.
  - Admitting Partners to the Federation is subject to approval by the Advisory Committee upon a proposal made by the Federation Operator via email. There is a two-week deadline for responding to the Operator proposal. A new Partner is accepted:
    - automatically at the end of the two-week deadline if no member of the Advisory Committee opposes membership or recommends that the membership application be discussed at an Advisory Committee meeting; or
    - immediately after the most recent approval if all members of the Advisory Committee accept admission of the new Partner; or
    - at the Advisory Committee meeting upon opposition by a member of the Advisory Committee or a recommendation to discuss the membership application

- The membership of a Partner admitted to the Federation will enter into effect when both the applicant organization and Operator have signed the Service Agreement on behalf of and authorized by the other Federation Participants.

2.4 The Operator is also required to inform the Advisory Committee of any applications which it has not submitted for approval.

2.5. Operator

The Federation Operator, CSC - IT Center for Science Ltd. ("Operator") coordinates Federation operations in a manner described in greater detail in this Agreement and its appendices.

The Operator shall provide Participants with up-to-date information on the Federation Participants and Partners, Federation service agreements and appendices, and the applicable code of conduct.

The Federation Operator also functions as a Home Organization and Service Provider.

3. Organizational bodies in the Federation

3.1. Advisory Committee

Haka Identity Federation body which represents the Federation Participants and whose task is to promote and coordinate the deployment and use of the Federation. In addition to other provisions stated in the Agreement and its appendices, matters to be addressed by the Advisory Committee includes

- approval of the Federation Plan of Work
- launching Federation projects
- funding
- the vision and strategy of the Federation
- policies and operating practices
- risk management
- projects for further development

The Advisory Committee is nominated for two years at a time and consists of eight representatives, who are nominated as follows:

- The Network of Finnish Universities' Chief IT Officers (FUCIO) nominates two (2) representatives
- The Universities of Applied Sciences IT Managers AAPA meeting nominates two (2) representatives
- CSC – IT Center for Science Ltd. nominates one (1) representative
- The Advisory Committee meeting nominates the remaining three (3) representatives

The Operator is responsible for convening and preparing the meetings and serves as meeting secretary.

3.2. Operations Committee

An advisory body whose task is to serve as a technical discussion forum for Federation Participants. The Operations Committee tasks include:

- Best Federation practices
- Drafting an attribute schema (funetEduPerson) resolution for the Advisory Committee (e.g. funetEduPerson schema)

The Operations Committee is convened by the Federation Operator or a person nominated by the Advisory Committee. The secretaries of the Advisory Committee are responsible for conveying information between the Operations Committee and Advisory Committee.

Each Federation Member is entitled to nominate one representative to the Operations Committee. The Operator may also nominate additional specialists to the Operations Committee.

Appendix 3. Service description and requirements

1. BASIC SERVICES PROVIDED BY THE OPERATOR

This chapter presents the basic Federation services provided by the Haka Identity Federation Operator. All Federation Participants are entitled to use of these basic services.

1.1. Center of expertise

The Operator has a ***test service***, in which the functionality of the Federation can be tested. The instruments used in testing include an Identity Provider and Relying Party.

The Operator organizes ***events*** that support the implementation and development of the Federation and increase knowledge of the Federation in Finnish higher education institutions.

The Operator, serving as the secretary of the ***Advisory and Operations Committees*** convenes and prepares the Committee meetings.

The Operator maintains ***contacts*** with other national and international Identity Federations and cooperative bodies recognized by the Advisory Committee as well as the developers of technologies used in the Federation.

1.2. Identity Provider Discovery Service and Federation metadata

The Operator maintains a central Identity Provider Discovery Service and a register of metadata describing the Federation, including:

- Contact details for the administrative and technical personnel of the Federation Members and Partners as well as contact details for dealing with data security breaches
- Addresses of the servers registered to the Federation
- A list of the attributes needed for the services provided by the Service Providers belonging to the Federation as well as the address of the service Privacy Policy.

The Operator makes Federation metadata available to Federation Members and Partners.

1.3. Plan of Work and Communications

Under the supervision of the Advisory Committee, the Operator is responsible for planning the operational development of the Federation. The aim of development is to identify the changing needs of Federation Members and respond to them.

The Operator is responsible for maintaining the profile of the Federation in Finnish higher education and research institutions. The aim of communications is to ensure that Home Organizations and Service Providers are aware of the benefits and opportunities afforded by the Federation.

2. OBLIGATIONS OF FEDERATION PARTICIPANTS

The Federation requires the items presented in this chapter of the Federation Participants.

2.1. Operator

In addition to what is presented in chapter 1,

2.1.1. The Operator shall primarily monitor the development of software line products designed to support Shibboleth Consortium authentication and, whenever possible, other *software components* that the Federation Members and Partners may use as Identity Providers, Relying Parties or tools supporting these in the Federation. Whenever possible, the Operator participates in the development of the Shibboleth Consortium and its software.

2.1.2. The Operator shall take the necessary measures to ensure and monitor the seamless function of the Federation servers it maintains. Any planned interruptions in Federation service shall be announced in advance.

2.1.3. The Operator shall provide Federation Member technical contacts with Helpdesk *service* to troubleshoot operational problems.

2.1.4. The Operator shall notify Federation Members and Partners of any serious vulnerabilities, *security updates* and patches, and make every effort to maintain Federation security.

2.1.5. The Operator shall compile modification requests and needs concerning the *funetEduPerson schema* used in the Federation and, based on these, prepare proposals for modifications to the *funetEduPerson schema* for the Federation Operations Committee. Furthermore, the Operator shall provide the Home Organizations and Service Providers with detailed instructions on use of the schema and the syntax and semantics of attributes being transmitted within the Federation.

2.2. Federation Members and Partners

2.2.1. Federation Members and Partners shall be responsible for providing the proper data security, protection and security updates for its servers. Federation Members and Partners shall *install and update* its components connected to the Federation in accordance with good and data secure practices as well as Federation operating practices in such a manner that the reliability, data security and data protection are not compromised. Members and Partners shall also notify the Operator of any vulnerabilities, security updates and patches that they are aware of.

2.2.2. Federation Members and Partners shall ensure that the Federation *metadata* they are using is up to date.

2.2.3. Federation Members and Partners shall notify the Operator of any *changes* to their own metadata immediately.

2.2.4. Federation Members and Partners shall provide the Operator with the details of its technical and administrative *contact* and *its contact details* for dealing with data security breaches as well as notify the Operator of any changes to contacts and their contact details immediately.

2.2.5. Federation Members and Partners shall maintain procedures and practices for dealing with data security breaches and are able to identify such a breach, limit its impact and recover from it.

2.3. Special provisions concerning Home Organizations

Only Federation Members may function as a Home Organization

2.3.1. Home Organizations shall *install* the Identity Provider required for the Federation and other necessary components and integrate them with local user management systems in the organization.

2.3.2. *When issuing a username* to a new End User, the Home Organization shall verify the identity of the user account recipient in accordance with Federation policies and practices and require that the user accepts and pledges to abide by the Home Organization acceptable usage policy.

2.3.3. The Home Organization shall *authenticate* the identity of the End User using a password or more reliable means in accordance with Federation policies and practices whenever an End User attempts to access services connected to the Federation.

2.3.5. The *attributes* collected on the Home Organizations' own users and provided for use in the Federation shall be in conformance with the most current funetEduPerson schema. At least attributes marked as MUST shall be populated. Several services will require a value also for other attributes.

2.3.6. Home Organizations take the necessary precautions to ensure that only adequate, relevant and necessary attributes are released to the Service Provider. When a Service Provider functions as the processor of attributes on behalf of a Member, the Member shall ensure that only data necessary to provision of the service is transferred to the processor.

2.3.7. The Home Organization shall keep up to date *attribute release policies*, which define which user attributes are to be released to each of the Service Providers.

2.3.8. The Home Organization shall inform the End User of any disclosure of data in accordance with data protection legislation. The End User shall be given an opportunity to familiarise themselves with the service Privacy Policy, at least in cases where the Service Provider is not the Home Organization or it does not process attributes on its behalf.

2.3.9. Taking the provisions of data protection legislation into consideration, the Home Organization shall keep a **log**, which contains at least a name identifier and timestamp so that the user can be connected with an assertion released to the Service Provider.

2.3.10. The Home Organization shall *inform* the End User as to what data on service use is being collected by the Home Organization, where the data being collected will be used and possibly released.

2.3.11. The Home Organization shall establish a *helpdesk* for the purpose of addressing problems related to the Federation for the organization's End Users.

2.3.12. The Home Organization shall draft a description of its *identity management procedures* to the extent that they are important to the function of the Home Organization in the Federation. The description shall be made publicly available to other Federation Members and Partners.

2.3.13 Home Organizations shall periodically conduct self-audits of identity management systems, processes and their data security in accordance with a plan approved by the Advisory Committee.

2.4. Special provisions concerning Service Providers

Both Federation Members and Partners may function as Service Provider.

2.4.1. Service Providers shall *install* servers and other necessary Federation components and integrate them with their service.

2.4.2. The Service Provider shall notify the Operator as to which attributes are *necessary* to their service.

2.4.3. If the Service Provider processes attributes which are considered as personal data, the Service Provider shall inform the Operator about the URL in which the End Users are able to read the service *Privacy Policy* in advance. If the purpose of processing of attributes in the service is changed, the Service Provider shall be considered a new service in the Federation.

2.4.4. The Service Provider shall ensure that only *authorized End Users* may access the service. Access control may be based on the attributes released by the Home Organization.

2.4.5. Taking the provisions of data protection legislation into consideration, the Service Provider shall keep a **log**, which includes at least a Name Identifier. The Service Provider shall provide the necessary log entries to the Home Organization in order to investigate cases of misuse.

2.4.6 Other data protection obligations of the Service Provider

In processing attributes released by the Home Organization, the Service Provider shall be obligated as Data Controller to abide by the *GÉANT Data Protection Code of Conduct* established for a Service Provider. A

version of the above Code of Conduct is made publicly available by the Operator to Federation Participants. The Operator shall notify Federation Participants of any changes made to the Code of Conduct.

The *GÉANT Data Protection Code of Conduct* is intended to serve as a code of conduct for meeting the requirements of the EU General Data Protection Regulation in federated identity management. In cases where the code of conduct has been approved by a data protection authority in accordance with Article 40 of the General Data Protection Regulation ((EU) 2016/679), the approved version shall thus be applied.

The Operator shall supervise the code of conduct approval process as well as projects involving the updating or renewal of the code of conduct. The Operator shall also update the version for Federation Participants and the publicly available version of the code of conduct to an up-to-date version approved by the data protection authority in question.

When a Partner is located outside the EU or EEA, said Partner shall approve, at the behest of the Operator, the terms and conditions concerning the processing of personal data based on EU model contract clauses. Approval shall be made in connection with the membership agreement or within three (3) months of a change being made, wherein the location of a Partner is no longer within the EU or EEA during the Agreement period of validity.

3. COLLABORATION WITH OTHER IDENTITY FEDERATIONS

The Operator may sign Federation agreements with other federations that provide AAI services. The purpose of collaboration is to support the international networking and cooperation of Haka Federation Members. The Advisory Committee approves collaboration arrangements for the Haka Federation.

The exposure and involvement of an Identity or Service Provider from the Haka Federation in an international collaboration arrangement are always based on a request by the Federation Member or Partner who has registered the Identity or Service Provider in the Federation.

Through a collaboration arrangement, Federation Members and Partners receive metadata on foreign Identity and Service Providers who are typically not under any obligation to the policies and rules of this Agreement. In such cases, the Operator shall provide the metadata of foreign Providers to Federation Members and Partners in a way that clearly distinguishes it from Haka Federation metadata. Furthermore, the Operator maintains information on the main differences in policies and rules between the collaborating foreign Identity and Service Providers and the Members and Partners under obligation to this Agreement.

Appendix 5. Process for joining the Federation and beginning operations

1. Introduction

This document defines the process for how a Federation Member or Partner

- a) joins the Federation.
- b) registers an Identity Provider to the Federation
- c) registers a Relying Party to the Federation

Item a) always precedes items b) and c). The order of items b) and c) is up to the Federation Member. A Federation Partner may not register an Identity Provider to the Federation.

Each Federation Member is allowed to register one Identity Provider and multiple Relying Parties to the Federation. Each Federation Partner is allowed to register multiple Relying Parties to the Federation.

2. Joining the Federation

Joining the Federation involves the following process:

1. The applicant organization fills in and signs the Application for Federation Membership or Partnership and sends it to the Federation Operator. Two Service Agreements for Federation Members or Partners signed by the applicant must be attached to the application. The Service Agreement may also be signed electronically in a manner approved by the Advisory Committee.
2. If the organization applies for membership, the Operator, depending on the category of the applicant (Appendix 2), shall:
    - a. state that the applicant belongs to Category A; or
    - b. state that the applicant belongs to Category B and bring the application to the Advisory Committee for approval; or
    - c. state that the applicant belongs neither to Category A nor to Category B and cannot therefore be accepted as a Federation Member.

    If the organization applies for a partnership in the Federation, the Operator shall either:

    - a) state that the organization fulfills the criteria for a Federation Partner (Appendix 2) and bring the application to the Advisory Committee for approval; or
    - b. state that the organization does not fulfill the criteria for a Federation Partner.
3. The Operator signs the Service Agreement attached to the application, returns one copy of the Agreement to the applicant and adds the organization to the list of Federation Members or Partners.

3. Registering an Identity Provider to the Federation

A Federation Member that wants to become a Home Organization:

1. Sets up the necessary servers (Identity Provider).
2. The administrative contact person of the Federation Member completes an application for registering the Identity Provider to the Federation and sends it to the Federation Operator in writing or electronically.
3. The Operator confirms that it has received the application.
4. The Federation Member conducts an internal audit of its identity management under the supervision of the Operator.
5. Based on the information provided by the Federation Member, the Operator assesses how the Federation Member fulfills the obligations specified in Appendix 3 and determines whether or not the Federation Member is able to register an Identity Provider to the Federation.
6. The Federation Operator registers the Member's Identity Provider to the Federation metadata.
7. Registration of a Relying Party to the Federation.

4. Registering a new service

A Federation Member or Partner that wants to register a (new) service to the Federation:

1. Sets up the necessary servers (Relying Party).
2. The administrative contact of the Federation Member or Partner ensures that:
    - the service is not in conflict with the purpose of the Federation ("The purpose of the Haka Identity Federation is to support higher education and research institutions by developing and maintaining an infrastructure for user authentication and authorization.")
    - the End User attributes specified on the application that the service considers adequate, relevant and necessary to its provision (Principle of data minimization in personal data legislation)
    - the Member or Partner has made the Privacy Policy, which is applicable to the service it is providing, available to the End Users
3. The administrative contact person of the Federation Member or Partner completes an application for registering the Identity Provider to the Federation and sends it to the Federation Operator in writing or electronically.
4. The Operator confirms that it has received the application.
5. If the applicant is a Federation Partner and the service is a new kind of service for the Federation, the Operator shall forward the registration application to the Advisory Committee for approval.
6. The Federation Operator registers the Relying Party to the Federation metadata.

Appendix 6: General Terms of Contract Concerning the Sale of Services by CSC – IT Center for Science Ltd.

Appendix starts from next page.

GENERAL TERMS OF CONTRACT CONCERNING THE SALE OF SERVICES BY CSC – IT CENTER FOR SCIENCE LTD.

1. CONTRACTING PARTIES AND CONCLUDING A CONTRACT

1.1 These general terms of contract concerning the sale of services apply to contracts where the provider of services, CSC – IT Center for Science Ltd. (hereinafter CSC), and the purchaser of services (hereinafter the Client) agree on the sale of services. The above contract and these general terms of contract are below referred to collectively as "the Contract".

1.2 These terms come into force on 1 January 2007 and shall remain in force until further notice. They replace the previous general terms of contract concerning the sale of services.

1.3 A written offer given by CSC is valid for one month from its date, unless otherwise mentioned in the offer.

1.4 A contract is considered to have been concluded once CSC and the Client have signed the Contract concerning the sale of services.

1.5 In conjunction with a contract concerning the sale of services, the contracting parties may agree in writing that these general terms of contract, or some items in them, do not apply to the Contract in hand, or that some other terms are binding to the parties. These exceptions shall be specified in the contract document.

1.6 If a contracting party waives or relinquishes a right defined in the Contract, this shall not be construed to mean that said right will be relinquished on similar or other occasions later; nor does waiving or relinquishing a right mean that the party henceforth refrains from demanding observance of the right.

2. ORDER OF PRECEDENCE

2.1 Should there be a discrepancy between the Contract and its enclosures, the signed contract document shall take precedence, taking into account the provisions of section 1.5. These general terms of contract concerning the sale of CSC's services are applied next. Thereafter, other enclosures to the Contract are applied in numerical order, unless otherwise determined in the signed contract document.

3. OBJECT OF AGREEMENT

3.1 The object of agreement consists of the service produced and offered by CSC to the Client. The Client agrees to use CSC's service on the terms defined in the Contract.

4. OBLIGATIONS, RESPONSIBILITIES AND WARRANTIES OF CSC

4.1 CSC performs the service within the timetable agreed in the Contract. If the Contract specifies no timetable, the service is performed without undue delay.

4.2 CSC carries out the tasks defined in the Contract with care and with the professional approach required by the tasks. CSC sees to it that the service is performed by persons having appropriate competence.

4.3 In the event of a delay in the performance of the service, CSC has the right to extend the time reserved for the service correspondingly if the delay is caused by a force majeure referred to in section 14.1, by some other circumstances beyond CSC's control, or by the Client or circumstances for which the Client is responsible.

4.4 In the event that CSC's performance is altered or delayed, or the work is interrupted, and this is caused by the Client or by circumstances for which the Client is responsible, CSC is entitled to compensation from the Client for the costs and damage incurred.

4.5 If the Client has supplied documents and other material to CSC, CSC returns this material to the Client only if it has been agreed in writing that the material is returned. CSC has the right to keep copies of the Client's documents and other material to the extent required by law or by regulations issued by the authorities.

4.6 Unless the Contract expressly mentions otherwise, CSC does not give any guarantee or warranty for its products and services beyond what has specifically been mentioned above.

4.7 CSC transmits other manufacturers' products, software and services as they stand, and grants no warranties whatsoever for them. However, the original manufacturers or suppliers of these products and software, or the providers of these services, may give their own warranties for said products or

These Terms dated 23.9.2008 deviate from the Terms dated 1.1.2007 only with regard to CSC's official name that was changed on 28.8.2008

services. Whenever applicable, the Client may appeal to these warranties in dealings with the provider of the product or service.

5. THE CLIENT'S OBLIGATIONS AND RESPONSIBILITIES

5.1 The Client is responsible for the use of the usernames and passwords required by the application of the services described in the Contract and for all direct and indirect activities enabled by these usernames and passwords. The Client agrees to notify CSC promptly if usernames and/or passwords have been used without permission or if they have been lost. The Client is responsible for any damage resulting from the unauthorized use of usernames and/or passwords.

5.2 The Client uses information networks and other hardware and software included in the service at his own responsibility.

5.3 The Client is responsible for taking appropriate backup copies of his data material. CSC is never responsible for the loss or destruction of the Client's data or files.

5.4 The Client is responsible for ensuring that his activities do not infringe the copyright or other immaterial rights of CSC or third parties, and that the Client acts in accordance with the applicable law and regulations issued by the authorities.

5.5 When the results of the service are published, CSC's name must be mentioned in an appropriate manner, as "CSC – IT Center for Science Ltd.".

5.6 CSC's name can be used in advertising or publicity material only if written consent has been obtained in advance from CSC.

5.7 The Client must immediately return any confidential material given by CSC to the Client, including all copies thereof, when requested by CSC or when the Client no longer needs said material for the purpose required by the service. The Client has the right to keep copies of the confidential material obtained from CSC to the extent required by law or by regulations issued by the authorities.

5.8 Once the Contract has expired, the contracting parties agree promptly to return – or if so agreed in writing, to destroy – all copies of the other party's confidential material that they have stored on memory devices or that are otherwise in their possession.

5.9 The Client agrees to comply with all export and import regulations, and the consequent restrictions on use, that Finland or other countries (including the USA) have imposed on products and software included in the service.

6. USER RIGHTS AND PROPRIETARY RIGHTS

6.1 When a contracting party has received background information and other material from the other contracting party for performing tasks laid down in the Contract, this material may only be used for carrying out the tasks defined in the Contract.

6.2 CSC has the right to utilize the professional skill and experience achieved during the service for activities other than those referred to in the Contract.

6.3 When the material resulting from the service belongs to the Client, the proprietary right to the material is transferred to the Client only after the service has been paid in full.

7. IMMATERIAL RIGHTS

7.1 The contracting parties agree in writing how the immaterial rights to the material resulting from the service are divided. Unless otherwise agreed in writing, CSC holds the immaterial rights to the resulting material.

7.2 If the material resulting from the service includes an invention, the inventor is entitled to reasonable remuneration for the invention. The contracting party who has, or will have, the rights to the invention included in the material pays the costs incurred in the patenting of the invention and the remuneration to the inventor.

8. DATA PROTECTION AND CONFIDENTIALITY

8.1 During the contract term and after its expiry, the contracting parties agree to keep confidential the other party's business and professional secrets and other confidential information obtained from the other party. The contracting parties will not use this information for purposes other than those defined in the Contract and will not pass this information on to third parties. Confidential information means all material and information that has been marked as confidential or that should be understood to be confidential owing to its nature. The requirement to keep information confidential as described in this section 8 will cease ten (10) years after the expiry of the Contract, unless otherwise agreed in the Contract. The confidentiality requirement does not apply to information that (a) has subsequently become public knowledge without a contracting party's negligence, (b) a contracting party has obtained legally from a third party without the obligation of confidentiality, or (c) a contracting party can show that he has developed independently without relying on confidential information received from the other contracting party.

8.2 The contracting parties agree to handle confidential and secret information only to the extent required by the performance of the services described in the Contract.

8.3 For their own part, the contracting parties are responsible for ensuring that they comply with the applicable law, especial-

These Terms dated 23.9.2008 deviate from the Terms dated 1.1.2007 only with regard to CSC's official name that was changed on 28.8.2008

ly laws and regulations on data protection, and with good information management practice.

9. RATES AND FEES

9.1 CSC invoices for its services according to its currently valid price lists, unless no other written agreement has been made on prices and invoicing.

9.2 Prices do not include the value-added tax or any other taxes or public fees that may be charged. The value-added tax and other taxes or public fees are added to prices according to the rates valid at the time of invoicing.

9.3 If it is agreed that CSC will complete some task as overtime work or through some other special arrangements, CSC is entitled to invoice the ensuing extra costs separately, in accordance with the currently valid price list.

9.4 CSC has the right to change prices by notifying the Client thereof in writing at least 30 days before the changes come into effect.

9.5 Any comments concerning an invoice shall be made by its due date. The term of payment is 14 days.

9.6 If a payment is not made on the due date at the latest, CSC is entitled to charge interest for late payment in accordance with the Interest Act and to suspend the provision of the service to the Client.

9.7 If the payment is more than 30 days overdue, CSC is entitled to cancel the Contract in full or in part by notifying the Client of the cancellation in writing.

10. ERRORS IN THE SERVICE AND LIMITATION OF LIABILITY

10.1 CSC is not responsible for problems, disturbances, interruptions or other errors in third parties' networks, software or other products. Nor is CSC responsible for problems, disturbances, interruptions or other errors in the service described in the Contract, when they result from a force majeure referred to in section 14 or when they are otherwise the responsibility of the Client or a third party.

10.2 Should there be an error in the service, the Client shall present his claim to CSC in writing without delay, and not later than within seven (7) days of the occurrence of the error.

10.3 In all cases, CSC's liability for direct damage is limited to a maximum of thirty (30) per cent of the fee paid by the Client to CSC for the service described in the Contract. CSC is never liable for any indirect or consequential damage including, but not limited to, loss of profit, cost of procuring substitute service, loss of use or loss of benefits arising from use, or damaged data or files.

11. ASSIGNMENT OF THE CONTRACT

11.1 The contracting parties are entitled to assign the Contract and the consequent rights or responsibilities to a third party only if the other contracting party has consented to this in advance in writing.

11.2 CSC is entitled to assign the Contract, in part or in full, to another unit in state administration without the Client's advance consent by notifying the Client of the assignment in writing.

12. USE OF SUBCONTRACTORS

12.1 At its discretion, CSC may use subcontractors for meeting the obligations specified in the Contract.

12.2 CSC is responsible for the activities of its subcontractors in the same way as it is responsible for its own activities.

13. TERMINATION AND CANCELLATION OF THE CONTRACT

13.1 Each contracting party is entitled to terminate the Contract by giving written notice thereof thirty (30) days before the termination.

13.2 If a contracting party breaches the terms of the Contract in a material way, the other contracting party is entitled to cancel the Contract by notifying the first-mentioned party thereof in writing.

13.3 If the Client breaches the terms of the Contract, CSC is likewise entitled to suspend the provision of the service for the Client. The above does not limit CSC's right to cancel the Contract by virtue of the Client's breach of contract.

13.4 CSC is entitled to cancel the Contract if the Client is apparently insolvent, is placed into liquidation, has agreed on a composition with creditors, is under business reorganization, or is declared bankrupt.

13.5 Each contracting party is entitled to cancel the Contract if the force majeure referred to in section 14 continues so that fulfilling the Contract becomes impossible or is delayed by more than 12 months.

13.6 If the Client cancels the Contract, the Client shall pay compensation to CSC, in accordance with the agreed rates, for any part of the service delivered as per the Contract until the date of cancellation, or if it is agreed that the service will continue after the date of cancellation, until the date of terminating the service.

13.7 If CSC cancels the Contract because of a reason for which the Client is responsible, CSC is entitled to compensation from the Client for costs and damage resulting from the cancellation of the Contract.

These Terms dated 23.9.2008 deviate from the Terms dated 1.1.2007 only with regard to CSC's official name that was changed on 28.8.2008

14. FORCE MAJEURE

14.1 A force majeure is an event that a contracting party cannot reasonably be expected to have taken into consideration at the time of signing the Contract and that makes it impossible or unreasonably difficult to perform the service within the time set or in the manner agreed. Examples of a force majeure include wars, insurrections, natural disasters, interruptions in energy supply or data communications, fires, substantial restrictions on CSC's operations placed by the State Budget or by the Government, strikes, blockades, or other equally significant and uncommon events beyond the control of the contracting parties.

14.2 An error or a delay attributable to subcontractors, suppliers or other similar parties is considered a force majeure affecting CSC if the error or delay is caused by an event mentioned above in section 14.1 and CSC cannot without unreasonable loss of time or extra costs secure the subcontracting or supply of goods from other sources.

14.3 A contracting party shall notify the other party promptly in writing of any force majeure that will prevent or delay the performance of the obligations as per the Contract. Similarly, the contracting parties shall inform each other promptly when a force majeure has passed.

15. DISPUTES

15.1 Any disputes arising from the Contract are primarily settled through negotiation between the contracting parties.

15. If the contracting parties cannot reach agreement in mutual negotiations, disputes are settled through arbitration by one (1) arbitrator appointed by the Central Chamber of Commerce. The arbitrator thus appointed shall be familiar with information technology and law. The arbitration shall take place in Helsinki in accordance with the rules laid down by the Arbitration Institute of the Central Chamber of Commerce. The above notwithstanding, CSC shall always have the option of recovering any undisputed claims based on the Contract by instituting proceedings in a general court of first instance.

16. APPLICABLE LAW

16.1 The Contract is governed by Finnish law.

These Terms dated 23.9.2008 deviate from the Terms dated 1.1.2007 only with regard to CSC's official name that was changed on 28.8.2008

Appendix 7. Prices

The services described in this Agreement are funded by the fees agreed upon in the Funet Service Agreement between higher education institutions. For non-Funet member organizations CSC defines pricing based on the costs of developing the service and costs accrued from the services.

Services ordered separately from CSC - IT Center for Science Ltd that are not included in the service described in Appendix 3 shall be invoiced according to a prescribed pricing schedule.