Report: Code of Conduct for Relying Parties for services to Government

Introduction

This document (Report: Code of Conduct for Relying Parties) provides supporting guidance to the controlling documents of the Kantara Initiative Identity Assurance Framework (IAF) so that, in the fullness of time, the IAF and its controlling document suite could be extended to include the role of Relying Parties (RPs).

The intended audience for this document are Trust Framework operators that may require requirements for RPs be specified.

A complete Code of Conduct for Relying Parties, that spans the full extent of a RP's policies, processes and procedures, might include Sections such as the following:

1. Data Protection,
2. Admin, Record Keeping and Process,
3. Audit and Compliance,
4. Exit and Off Boarding and
5. Marketing.

It should be noted that other aspects, applicable to a given context or domain, might be required to make it comprehensive.

At this time the document is not intended to be a complete set of requirements for good behaviour of a RP. Rather, it is intended to give pointers to the rang e of topics that should typically be addressed in describing this set of requirements. A few exemplars have been provided for some of the topics.

On conceptualizing a typical Table of Contents for a code of Conduct for Relying Parties

This document offers an insight into what a typical Code of Conduct for Replying Parties might contain by presenting a draft Table of Contents. Further, it assumes that the Code of Conduct for Relying Parties would form just one component of a larger document suite (e.g., the IAF) covering other aspects of federated identity activities.

It assumes that the following artefacts and conditions exist in that broader framework document set for the federation:

1. a set of agreed definitions/terminology,
2. Scope and specification of the Replying Party activities,
3. a legal contract in force to make all obligations clear for interpretation,
4. that a federated trust framework is operating, and
5. that a quality ISMS is operating in the RP/AP environments..

With the above conditions met, a Table of Contents for the Code of Conduct for Relying Parties aspect of the document set might include:

- Introduction and Purpose
- Executive Summary
- Assumptions
- Definitions/Terminology
- References and bibliography
- Activities in scope for the Relying Party
- Data Protection*
- Administration, Record Keeping and processes/procedures*
- Audit and Compliance
- Exit and Off boarding*
- Marketing

* (note: example text for this topic has been drafted below)

.....

Exemplar draft text for the Table of Contents headings above selected and marked as *

Note: the test in square brackets [..] indicate a principle or objective that the statement seeks to address.

Data Protection

The RP/Service Provider agrees and warrants:

1. [Legal compliance] to only process the Attributes in accordance with the relevant provisions of the law applicable to the RP/Service Provider /Federation;
2. [Purpose limitation] to only process Attributes of the End User that are necessary for enabling access to the service provided by the Service Provider;
3. [Data minimisation] to minimise the Attributes requested from a party to the Federation to those that are adequate, relevant and not excessive for enabling access to the service and, where a number of Attributes could be used to provide access to the service, to use the least intrusive Attributes possible;

4. [Deviating purposes] not to process the Attributes for any other purpose (e.g. selling the Attributes or selling the personalisation such as search history, commercial communications, profiling) than enabling access, unless prior consent has been given to the Service Provider by the End User;
5. [Data retention] to delete or anonymise all Attributes as soon as they are no longer necessary for the purposes of providing the service;
6. [Third parties] not to transfer Attributes to any third party (such as a collaboration partner) except 1. if mandated by the Service Provider for enabling access to its service on its behalf, or 2. if the third party is committed to the Code of Conduct or has undertaken similar duties considered sufficient under the data protection law applicable to the Service Provider or 3. if prior consent has been given by the End User;
7. [Security measures] to take appropriate technical and organisational measures to safeguard Attributes against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access. These measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected, having regard to the state of the art and the cost of their implementation.
8. [Information duty towards End User] to provide to the End User, at least at first contact, in an easily, directly and permanently accessible way a Privacy Policy, containing at least the following information:
    a. the name, address and jurisdiction of the Service Provider;
    b. the purpose or purposes of the processing of the Attributes;
    c. a description of the Attributes being processed
    d. the third party recipients or categories of third party recipient to whom the Attributes might be disclosed, and proposed transfers of Attributes to countries outside of the jurisdiction/federation
    e. the existence of the rights to access, rectify and delete the Attributes held about the End User;
    f. the retention period of the Attributes;
    g. a reference to this Code of Conduct;
9. [Information duty towards the Federation party/IDP] to provide to it or its Agent at least the following information:
    a. machine-readable link to the Privacy Policy;
    b. indication of commitment to this Code of Conduct;c. any updates or changes in the local data protection legislation, which are less strict than the principles set out in this Code of Conduct;
10. [Security Breaches] to, without undue delay, report all suspected privacy or security breaches(including unauthorized disclosure or compromise, actual or possible loss of data, documents or any device, etc.) concerning the Attributes, to the Federation Party/IdP or its Agent;
11. [Transfer to third countries] when Attributes are being transferred outside the jurisdiction and to countries with adequate data protection pursuant to adequacy law/rules etc.. to ensure an adequate level of protection of the Personal Data by taking appropriate measures pursuant to the law of the country in which the RP/Service Provider is established, such as requesting End User consent or entering into agreements with the RP /Service Provider.

Admin, Record Keeping and Processes/procedures

1. [Payment] pay the Charges in accordance with XXXX clause in the Federation Agreement;
2. [Co-operation] co-operate with Federation/IdP personnel in connection with its background checking/identity proofing of RP/SP responsible officers, registering authorisation policy for and provide access to records and resources, operation and safe-guarding of the Service/s; and advise IdP promptly of any Service anomalies, suspicious or unusual usage, or complaints relating to the Services and provide reasonable assistance to Federation/IdP in the investigation of such anomalies, usage or complaints;
3. [Standards Compliance] comply with any standards or specifications issued by the Federation/IdP and any reporting obligations required by the IdP/AP from time to time in accordance with any relevant legislation (including those of a contracted third party to the RP/SP)
4. [Audit] provide appropriate assistance, where reasonably requested by IdP/AP, in carrying out any audit of the Client's use of the Services or related systems or suppliers; comply with all certification and accreditation requirements
5. [Federation Reporting] participate in progress reporting as specified in the Service Schedule;
6. [transparent relationship] ensure that the agency Service Provider/RP's website terms and conditions explain the inter-relationship of the Services and the Client's systems in terms agreed with Federation/IdP; that the RP/Service Provider maintains an accurate and up to date register of its roles and activities
7. [Promotion] use its best endeavours to promote the Services and instructions for use, to its customer base to encourage service uptake and use;
8. [Maintenance and notification] use and maintain the Service Interface including the security between the Client's systems and the Service System; register/modify/remove/retrieve meta-data, maintain PKI certificates as defined in the XX Federation Documentation XX; notify IdP of any network changes or certification renewals that may impact on any part of the Service, use the Admin interface to register and update details relating to the Service and the officers charged with administering the service
9. [Technical Consistency] Requirements for mandatory conformance testing before being connected to the production environment; Requirements for session management and logout (e.g. requirements for session timeout periods and single logout behaviour across the federation); Requirements for logging certain events (e.g. SAML Request/Responses) and to establish correlation identifiers in logs; Requirements for UI (to ensure a consistent user experience across the federation - e.g. layout and placement of 'logout' buttons etc.); Requirements for certificates used to secure communication between SP and IdP.

Exit and Off boarding

1. [Exit and off boarding]: RP must have an explicit written policy to address and mitigate impacts to existing users (e.g portability of accounts if feasible, re-enrollment, credential switching) in the event that the RP terminates or is terminated from its role.
2. [Exit and off boarding]: RP must have predetermined processes to put into action to update Helpdesk on status, call handling procedures and documentation, website information, test scripts and system flows to reflect the terminated state of the RP

References

GEANT**:** http://www.geant.net/uri/dataprotection-code-of-conduct/V1/Pages/default.aspx **(**accessed from https://www.clarin.eu/content/how-can-i-comply-data-protection-code-conduct**)**

Federal Government of Canada: 'Adding and removing Credential Service Providers under the Credential Broker Service' TBS Canada, CIO Branch, Feb 2015, Version 4.0

Kantara Initiative: Identity Assurance Framework

InCommon: https://www.incommon.org/docs/policies/InCommonFOPP.pdf

IETF: Vectors of Trust: https://datatracker.ietf.org/doc/draft-richer-vectors-of-trust/?include_text=1 for the latest version, taken from https://www.ietf.org/mailman/listinfo/vot

NZ RealMe: https://www.realme.govt.nz/ though the MOU from which some text for the Admin, Record-Keeping and Processes/Procedures section is not published

TERENA: https://refeds.terena.org/index.php/Federations

NemLog-in Denmark: http://www.digst.dk/~/media/Files/NemLogin/Tilslutnings-doks/Guide-til-foederationstilslutning-V1-1.pdf

.....