Jisc Assent Service Technical Specification

Version: 1.0 - March 2015

1. Introduction

1.1. Overview

This document is the Technical Specification for the Jisc Assent service provided in the UK by Jisc and is subject to periodic revision; changes will be notified to registered contacts at participating organisations.

1.2. Implementation

For detailed guidance on implementing this specification, see the Jisc Assent service documentation and Moonshot technical documentation[1].

Many of these requirements are fulfilled by default and are only applicable when using customised software.

1.3. Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119][2].

1.4. Definitions

1.4.1 Moonshot entity – a RADIUS server connected to the Trust Router fabric that is providing either Moonshot Identity Provider or Moonshot Relying Party services.

1.4.2. RFC – A document outlining a standard published by the Internet Engineering Task Force (IETF)

1.4.3. IdP – Identity Provider

1.4.4. RP – Relying Party

[1] https://wiki.moonshot.ja.net/

[2] http://www.rfc-editor.org/rfc/rfc2119.txt - Key words for use in RFCs to Indicate Requirement Le vels S. Bradner [March 1997]

2.1. Requirements for all entities

2.1.1. Software interacting with the Jisc Assent service MUST comply with RADIUS standards RFC2865[3] (and updates) and GSS-EAP standards RFC7055[4] and RFC7056[5].

2.1.2. Accurate time MUST be maintained, using NTP, PTP or an external time source such as GPS.

2.1.3. Moonshot entities MUST be addressable via IPv4 and SHOULD be addressable via IPv6, unless a specific Jisc Assent community that the entity participates in has policy that specifies otherwise.

2.1.4. Forward and reverse DNS entries MUST be created for both IPv4, and IPv6 (where applicable).

2.1.5. Sufficient information to be able to identify the activities of an individual session MUST be recorded and retained for a reasonable period upon request by a lawful authority.

2.1.6. Statistics SHOULD be submitted to Jisc according to the separate statistics and health-monitoring document[6].

2.2. SAML Usage

2.2.1. Participants' Moonshot entities SHOULD be capable of creating or consuming SAML for increased authorisation flexibility.

2.2.2. Software interacting with the Jisc Assent service that supports SAML MUST comply with RFCXXXX[7] and relevant OASIS standards to ensure interoperability.

2.3. Trust Router Interaction

2.3.1. A valid credential, issued by https://portal.moonshot.ja.net/ MUST be used to authenticate to the Jisc Assent service. This credential MUST be kept secret.

2.3.2. Moonshot Entities MUST use the published host name of the Trust Router network for initiating connections. Participants MUST NOT use an IP address or the host name of an individual Trust Router instance.

2.3.3. RadSec keys MUST be discarded after the lifetime specified by the Jisc Assent community policy or Trust Router has elapsed.

[3] http://www.rfc-editor.org/rfc/rfc2865.txt - Remote Authentication Dial In User Service (RADIUS) C. Rigney, S. Willens, A. Rubens, W. Simpson [June 2000]
[4] http://www.rfc-editor.org/rfc/rfc7055.txt - A GSS-API Mechanism for the Extensible Authentication Protocol S. Hartman, J. Howlett [December 2013]
[5] http://www.rfc-editor.org/rfc/rfc7056.txt - Name Attributes for the GSS-API Extensible Authentication Protocol (EAP) Mechanism S. Hartman, J. Howlett [December 2013]
[6] Reference to monitoring
[7] Pending RFC number

3. Requirements for IdPs

3.1. Host and network firewalls MUST be configured to allow the following services to reach an IdP that is part of a Jisc Assent community:

3.1.1. RadSec (SHOULD listen on TCP/2083) from any source

3.1.2. Trust Router (SHOULD listen on TCP/12309) from any source

3.1.3. ICMP echo from portal.moonshot.ja.net

3.2. Usernames:

3.2.1. Home organisations' Moonshot user names MUST conform to the Network Access Identifier (NAI) specification[8].

3.2.2. The realm component registered with the Jisc Assent service and routed to an IdP MUST be a domain name in the global Domain Name System under the control of the Institution (or one of its contractors) providing the IdP.

3.3. EAP Authentication:

3.3.1. Home organisations MUST configure their RADIUS server to authenticate one or more Extensible Authentication Protocol [14] (EAP) types that are capable of EAP channel bindings[9].

3.3.2. EAP-TTLS is currently recommended.

3.4. Use of Attributes:

3.4.1. The originating server MUST set the following RADIUS attributes:

3.4.1.1. Message-Authenticator

3.4.2. The following RADIUS attributes MUST be forwarded by participants' Moonshot Entities, if present in messages.

3.4.2.1. User-Name

3.4.2.2. State

3.4.2.3. Class

3.4.2.4. Message-Authenticator

3.4.2.5. Proxy-State

3.4.2.6. EAP-Message

3.4.2.7. MS-MPPE-Send-Key

[8] http://www.rfc-editor.org/rfc/rfc2486.txt - The Network Access Identifier B. Aboba, M. Beadles [January 1999]
[9] Reference to channel bindings

3.4.2.8. MS-MPPE-Recv-Key

3.4.2.9. Calling-Station-Id

3.4.2.10. GSS-Acceptor-Service-Name

3.4.2.11. GSS-Acceptor-Host-Name

3.4.2.12. GSS-Acceptor-Realm-Name

3.4.2.13. GSS-Acceptor-Service-Specifics

3.4.3. The three levels of pseudonymous identifiers[10] SHOULD be generated

3.4.4. IdPs SHOULD be configured to release Moonshot-Host-TargetedId to any Moonshot RP.

3.4.5. IdPs SHOULD exercise policy control over which RPs to which they release Moonshot-Realm-TargetedId and Moonshot-TR-COI-TargetedID, along with all other PII.

3.4.6. Where the attribute used as the input to any of the three pseudonymous identifiers is released, IdPs SHOULD NOT release the three pseudonymous identifiers as this allows the salt used in the generation of the pseudonymous identifiers to be deduced.

4. Trust Router Interaction

4.1. IdP's MUST verify the GSS-Acceptor-Host-Name and GSS-Acceptor-Realm-Name assertions present in an Access-Request.

4.2. Temporary Identity Requests MUST only be accepted from the identity *trustrouter@apc.moonshot.ja.net*, as verified by the Jisc Assent APC server.

4.3. Incoming RadSec connections and subsequent Access-Requests MUST be validated against constraints provided by the Trust Router network.

[10] Reference to identifier reference

5. Requirements for RPs and RP-Proxies

5.1. Host names to be used by RPs MUST be registered in the Jisc Assent service portal as domain constraints.

5.2. If a RP receives an Access-Accept RADIUS request with a SAML statement enclosed, the RP SHOULD parse it for any additional information contained within that should be used in an access control decision.

5.3. RP-Proxies MUST:

5.3.1. Communicate with their connected RADIUS clients using RadSec or RADIUS over DTLS

5.3.2. Explicitly reject any unknown realms.

5.3.3. Validate GSS-Acceptor-Realm-Name and GSS-Acceptor-Host-Name of connected RADIUS clients.

5.4. Trust Router Interaction

5.4.1. GSS-Acceptor-Realm-Name SHOULD be included in all Access-Requests.

5.4.2. GSS-Acceptor-Host-Name MUST be included in all Access-Requests.

5.4.3. A community MUST be specified in all Trust Path Queries.

6. Requirements for Clients

6.1. User identities SHOULD be configured to identity the correct IdP.

6.2. Clients SHOULD use an anonymous outer identifier (i.e. “@REALM”)