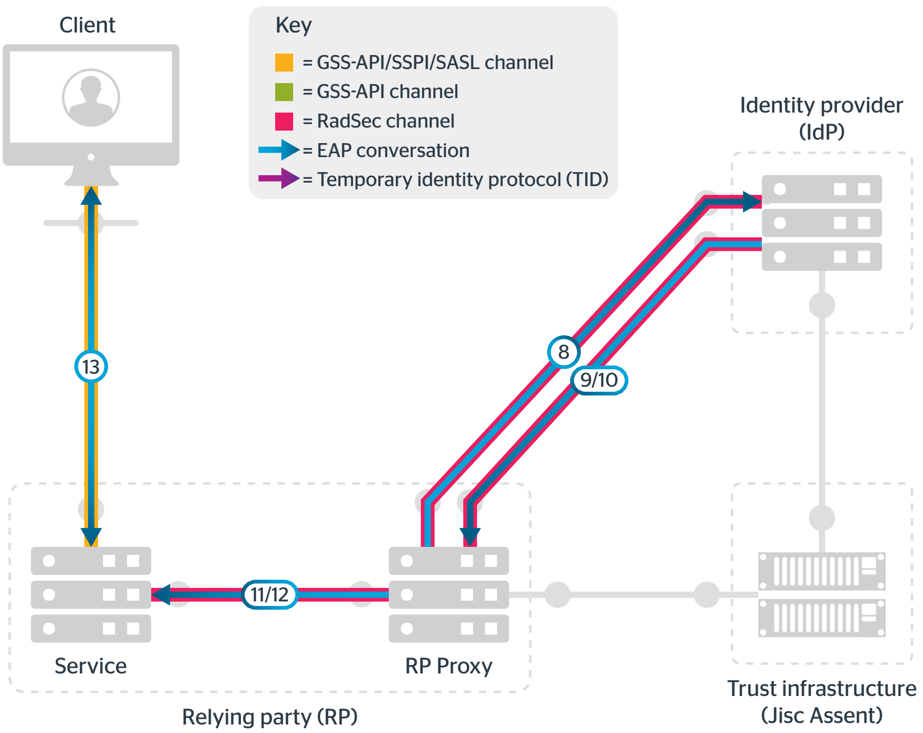


Steps 8-13

8. The RP Proxy passes an EAP authentication request to IdP over the RadSec tunnel.

9. The IdP authenticates the request and builds a response.

10. The IdP sends its response back to the the RP proxy over the RadSec tunnel.

11. The RP proxy processes the response by:
 » doing local authorisation decisions
 » doing local account mapping
 » doing anything else that may be needed to allow access to the service.

12. The RP proxy responds to the service to the client over RadSec.

13. The service logs the client in over GSSAPI. The user can now access resources and work.

The whole process takes about 12 to 15 seconds, the first time a user from an organisation signs in. Subsequent users' requests from the same RP will bypass the trust router and proceed directly to the IdP for authentication via the RadSec tunnel.

NEXT STEPS

To sign up to Assent, visit **jisc.ac.uk/assent** and complete the sign-up form.

To find out more about Assent and how you can get involved, visit **jisc.ac.uk/assent**, call **0300 300 2212** or email **assent@jisc.ac.uk**.

To see the Moonshot wiki, visit **wiki.moonshot.ja.net**.

Network & Technology

FACT SHEET

Assent

Enable federated access to a wide range of services, including HPC and grid computing

Assent is a ground-breaking trust and identity service from Jisc. It enables federated access to a broad range of services, including HPC and grid computing – allowing the option of single sign-on for users across multiple services, both within and between organisations.

It works by acting as a 'trust broker' between a service provider and an identity provider – whose respective organisations subscribe to and are trusted by the Assent service, but may not have shared credentials with each other.

What Assent does

Assent makes it simpler, more efficient and cost-effective to offer access to a wide range of services. Using Assent, you can enable federated access to services such as:

» HPC and grid computing services, including data analysis facilities

» private and public cloud resources such as VLEs

» commonly deployed services such as email, file store and instant messaging.

This helps IT teams to:

» simplify sign-on for users – reducing the IT admin time involved in managing multiple user identities

» deploy and manage access to a broad range of services using a single mechanism – reducing the need to support different authentication technologies, and avoiding duplication of effort

» secure access efficiently. You can revoke permissions quickly when a staff member leaves, because when you disable an account via your standard identity management practices, access to other services also ceases

» authenticate external collaborators via their existing sign-on when they request on-site accounts and resources.

Assent is built on the same technologies that underpin our other trust and identity services – so it also maximises your existing IT investment. If you have already deployed eduroam using the FreeRADIUS software, getting Assent set up is straightforward.

How Assent works: a summary

The Assent service works by acting as a 'trust broker' between a relying party (RP) proxy server and an identity provider (IdP) – who are both known to the Assent 'trust router' (TR) because the organisations who run them subscribe to Assent.

Once the TR has confirmed the identities of both the RP and IdP and checked the trust path, it gives the RP and IdP two halves of a secure key – allowing them to complete authentication via a secure (RadSec) tunnel directly with each other.

Assent uses Moonshot technology – which bridges the gap between network-level and web-specific authentication, theoretically enabling federated access to virtually any service. Moonshot builds on proven technologies including:

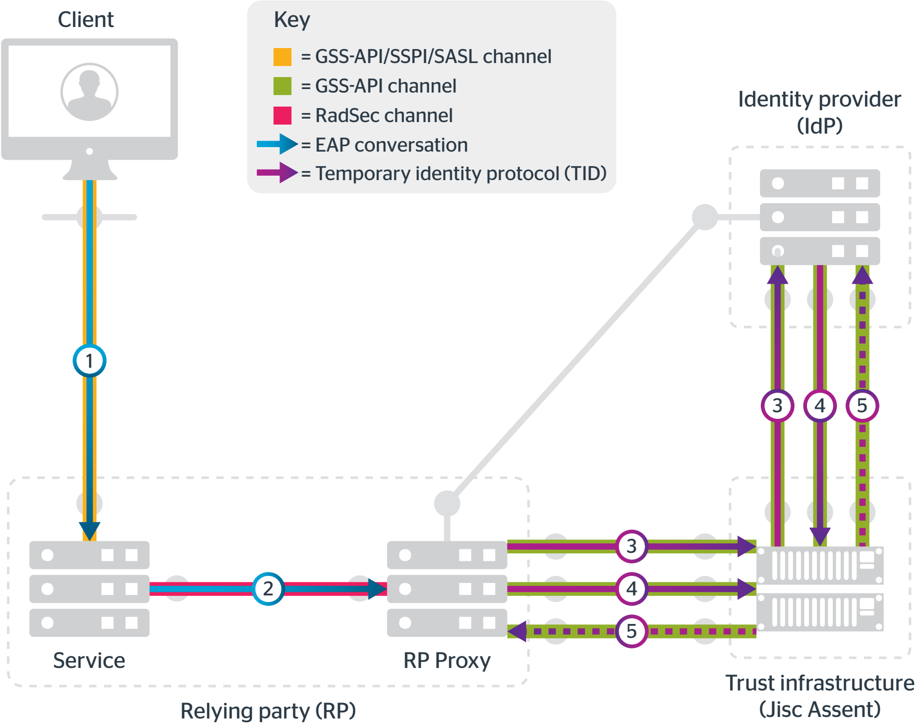
» EAP/RADIUS authentication, as already used by our network sign-in service, eduroam

» SAML authorisation, as used by many national federations

» service/application integration as used by many major applications (operating system security APIs).

How Assent works: a step-by-step process

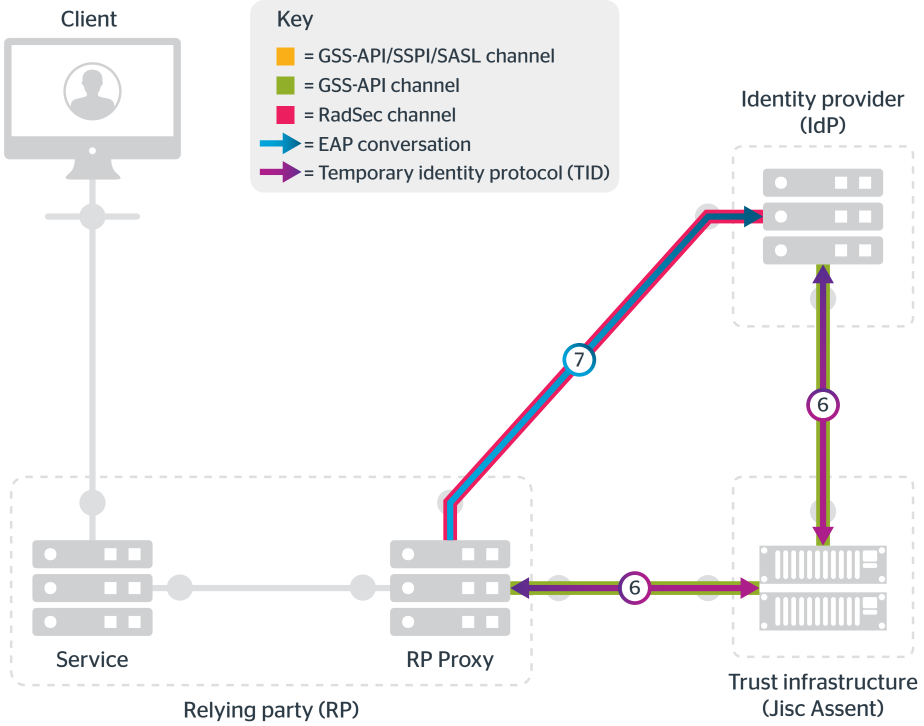
Steps 1-5



When a user logs in to a service using Assent, the following happens:

1. The client initiates an EAP conversation with the service over the Generic Security Services API (GSSAPI) – that is, a generic security API as used by many operating systems.
2. The service forwards the authentication request to its relying party (RP) proxy, over TLS-secured RADIUS traffic (RadSec).
3. The RP proxy contacts the Assent trust router (TR) to find the identity provider (IdP) for the request, using the temporary identity (TID) protocol.
4. Both the RP proxy and the IdP identify themselves to the TR using the same steps above.
5. The TR checks the trust path to confirm whether the IdP and the RP proxy may talk.

Steps 6-7



6. If step 5 is successful, the TR issues both the RP proxy and the IdP with details of the other party – and mediates a Diffie-Hellman (DH) key exchange between the two parties.
7. When the successful negotiation is complete, the RP proxy contacts the IdP and negotiates a TLS-secured RadSec tunnel with its half of the DH key.

Technology requirements

Here's what you need to run Assent:

On client device (Linux or Windows workstation/laptop)
Moonshot client (Moonshot GSS mechanism for Linux; Moonshot SSP for Windows)

On service accessible with Moonshot
Moonshot client
Moonshot-compatible service software (see Moonshot wiki at wiki.moonshot.ja.net for the latest tested software)

On RADIUS proxy (gateway and connected to Assent service)
Moonshot client
FreeRADIUS 3.x with Trust Router support

On IdP (connected to Assent service)
Moonshot client
FreeRADIUS 3.x with Trust Router support