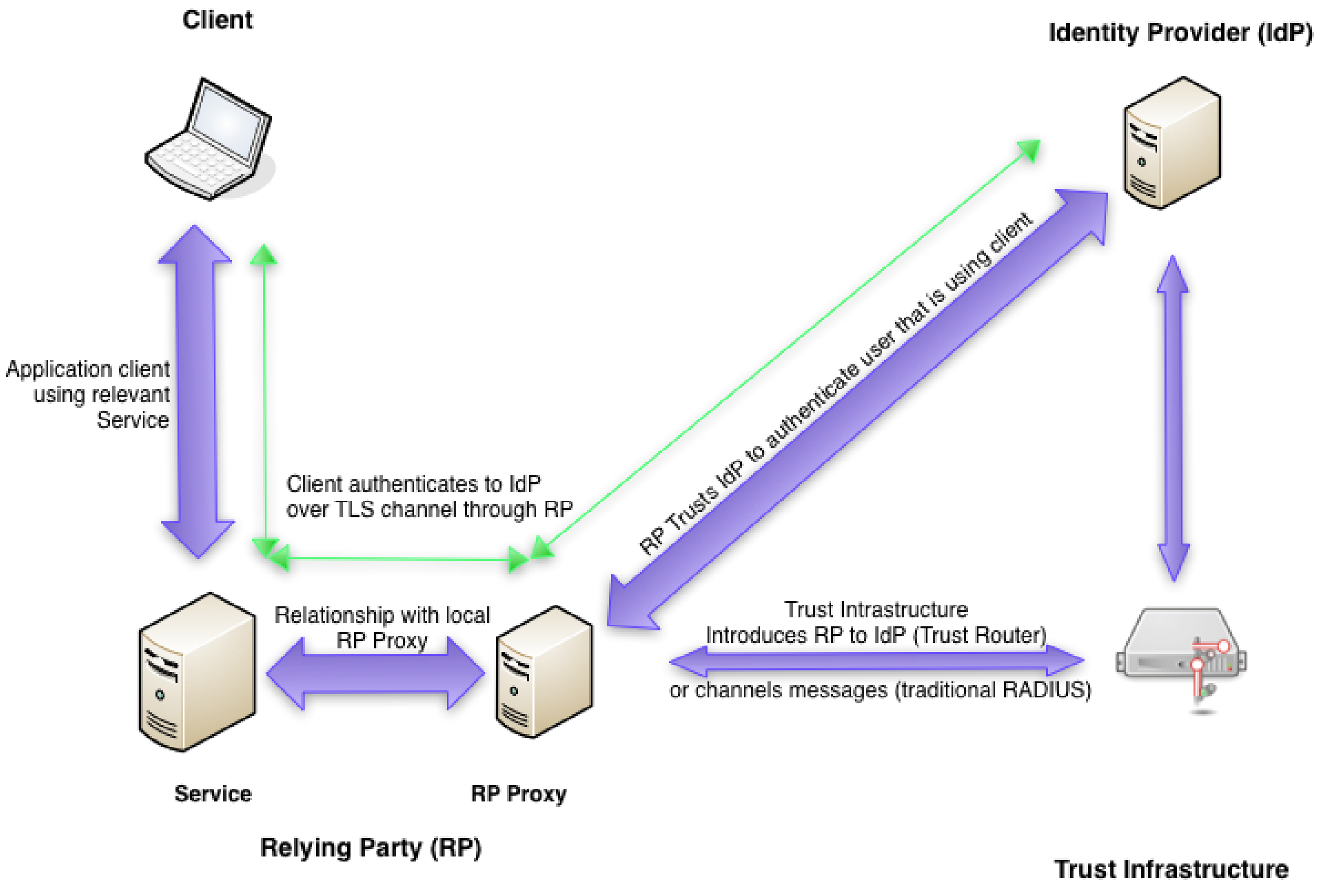
Overview of Moonshot Components

Contents

Components

At the highest level, Moonshot consists of three main components and the interactions between them over specific protocols:

- Client
- Relying Party (RP)
- Identity Provider (IdP)



Client
Identity Provider (IdP)
Application client using relevant Service
Client authenticates to IdP over TLS channel through RP
RP Trusts IdP to authenticate user that is using client
Relationship with local RP Proxy
Trust Intrastructure Introduces RP to IdP (Trust Router)
or channels messages (traditional RADIUS)
Service
RP Proxy
Relying Party (RP)
Trust Infrastructure

Client

The Client consists of parts of the software that exists on the user's device (e.g., laptop) that make up both the start and end point of a Moonshot transaction. A request starts with the Client sending a session request to the Service (Relying Party) and includes an identity selection mechanism that enables the user to choose which identity to use at the Service.

Relying Party (RP)

The RP is essentially the Service that the Client attempts to connect to. Technically, the RP consists of two separate pieces:

- The Service itself
- The Relying Party Proxy (RP Proxy)

The Service is the home of the resource that the user is attempting to connect to; most commonly, some server software or a gateway to computing resources (e.g., an OpenSSH or Microsoft Exchange server).

The RP Proxy is a RADIUS server that connects Services to Identity Providers (IdPs) via a trust infrastructure (either a classic hierarchical RADIUS network or a Moonshot-based Trust Router network).

The Service, upon receiving a session request from the Client, will start the authentication process by speaking to its local RP Proxy. The initial request will typically include a pointer to the home IdP of the user. When using the Trust Router network, the Trust Router enables the RP Proxy to “find” the relevant IdP; the RP Proxy then establishes a secure, direct connection to it.

Identity Provider (IdP)

An IdP is an authoritative source of identity information for users affiliated with the organisation running the IdP. Relying Parties will have a trust relationship of some kind with the IdP that means they trust it to authenticate and authorise users.

The client interacts directly with the IdP through a secure tunnel that passes through the Service and its RP Proxy. The user proves who they are to the IdP through this tunnel via a credential exchange of some kind (e.g., passing a username and password across).

Once the user has successfully authenticated to the IdP, the IdP in turn responds to the Service via its RP proxy; it may provide information solely to acknowledge that a user authenticated correctly, or it may provide further information in the form of attributes such as name or membership information.

Trust Infrastructure

The trust infrastructure is usually managed by an NREN and consists of a classic hierarchical RADIUS network (such as eduroam) or a Moonshot-based Trust Router network (such as the Jisc Assent service).

The trust infrastructure holds information on all RP Proxies and IdPs in the network, and introduces RP Proxies to IdPs on an as-needed basis to establish trust between the two parties.

In a Moonshot-based Trust Router network, once that introduction is made, the RP Proxy can speak to the IdP without any further interaction with the trust infrastructure until the trust expires, after which the next request from a user prompts another introduction cycle.

ⓘ For a much more detailed look at the various components, associated libraries, and protocols, see The Components of Moonshot under Advanced Information.