Govroam

G-Cloud 15 Service Definition

1. Introduction

This is a service definition for Jisc's govroam.

1.1 Document Sections

This document has the following sections:

Section 1 – Introduction
Section 2 - Service Information. Contains essential information about our service, it's functionality, security, and brief aspects of pricing.
Section 3 - G-Cloud Alignment Information. Details how our service and company aligns with the G-Cloud buying process and provides typical information to help you understand how to buy, configure and consume our services, and how to leave our services should the need arise.
Section 4 - About Our Company and Our Services. Provides information specific to Jisc and how we can solve the problems faced by customers in the public sector.
Section 5 – References from throughout this document
Section 6 – Glossary of the terms and definitions used throughout this document.
Section 7 – Appendices. Supplementary service information explaining the functionality and benefits in more detail.

1.2 How to Use This Document

This service definition is an active document; you can click on the links provided to move around the document, viewing only those sections you are interested in during the different phases of your buying process. There are also links to enable you to return to this section, or the table to contents, to speed up the reviewing process.

2. Service Information

2.1 Section Introduction

In this section we describe our govroam service functionality.

2.2 Govroam overview

Drivers

The public sector is increasingly encouraged to *collaborate* effectively. Interworking and sharing information enables the convergence of health and social care provision, multidisciplinary approaches to local government challenges, the cooperative approaches to intelligence and situation management between emergency services. Easy, cheap mobile connectivity is essential enabler in unlocking this kind of collaboration.

Estate rationalisation is an increasing requirement, both in reducing the overall size of estate and its associated overheads, and increasing the flexibility of existing facilities to accommodate temporary hosting and shared facilities. Again, connectivity provision is an essential to this; multi-tenanted buildings where each floor has a different wireless network design and separately provisioned backhaul are no longer tenable.

With ICT tailored to their needs, a *mobile workforce* operating effectively across the UK can work smarter and deliver savings. This flexibility also supports a good work/life balance for staff.

Govroam - addressing these challenges

The govroam service, designed to eliminate the overheads of offering and making use of seamless guest connectivity provided by other public organisations, is a rational response to these drivers, making offsite connectivity simple without requiring extensive investment in new infrastructure. Employers have the added benefit of being able to monitor the roaming behaviour of staff.

Govroam is, at its heart, a trust fabric that deploys appropriate, proven technologies to ensure that your existing staff authentication protocols can safely and securely be used off-site. Your staff can gain access to appropriate network facilities when working at other organisations without having to locate a support service onsite, provide identity proof, or modify the configuration of their mobile devices. This leads to significant savings on mobile charges, as well as in the costs of administration and support. Conversely, it also allows you to offer connectivity at your own venues to public-sector staff and authorised contractors without having to build underpinning support and identity provision.

In the vast majority of cases, existing wireless deployments can be reconfigured to support govroam in less than a day. It's based on proven technologies developed within the education sector (eduroam), benefiting from many years of successful operational experience supporting millions of individual users world-wide.

Key benefits

- Derive additional benefit from/extend life of existing WLAN infrastructure;
- Meet the connectivity needs of an increasingly mobile workforce through a 'zerotouch' user-friendly approach;
- Standardise wireless network provision across multi-tenanted spaces and in hotdesking hubs to an industry best practice standard;
- The reassurance of a real-time "member in good standing" check whenever you grant someone guest access to your visited network (backed by the understanding that a guest's home organisation will assist in the resolution of any incident arising from that use);
- Reduce/remove the need for customer-facing visitor support, cutting costs and freeing staff resources;
- Reduce/remove the need for 'temporary account' processes, reducing the attack surface of the network;
- Reduce/remove costs associated with SIM-based telephony data provision for roaming staff;

- Increased off-site connectivity and hot-desking opportunities for your staff, increasing productivity;
- Reduce the overheads of connectivity provision for meetings, conferences and events;
- Exert real-time control over staff use of off-site connectivity as the authentication decision rests with your organisation;
- Ensure your staff use connectivity implemented to industry best practices and whose users are traceable in the event of an issue;

Govroam gives you control

Your organisation determines who can access roaming provision, and controls credential issue and revocation to your own policies. Every remote login attempt is referred back to your infrastructure for decision.

In offering guest network provision, you also know that visitors using it are working within the same or equivalent public sector policies, and that their employers are committed to taking an active role in helping resolve any issue that might arise from their mobile staff using your guest service.

Govroam is security

The initial authentication step within govroam is secured by best-of-breed encrypted protocols, but it is important to note that the chosen authentication strength is purely in the hands of the home organisation. For example, some may choose to use staff credentials derived from the home organisation's Active Directory; others may choose to use certificates installed on the device issued to the member off staff. Govroam is the consistent secure transit of authentication data between a visited site and the home organisation, irrespective of mechanism chosen.

Find more in-depth information on the govroam security model in section 2.3.2.

Govroam supports all EAP authentication methods. This includes, but is not limited to, personal certification, device certification, SIM authentication, username/password, and two-factor authentication. See Appendix C for further information.

2.2.1 Service Functional Capabilities

Govroam facilitates visitor access to guest networks at participating sites by replacing temporary local visitor account mechanisms with a lightweight and secure way to reuse credentials issued to the roaming user by their home organisation. This improves visitor productivity, as they no longer need to locate the local IT support desk, run through identity checks, be issued with a visitor account, or reconfigure their device to meet local requirements. As a result, govroam also greatly reduces or removes the need for the visited site to offer visitor support mechanisms and staffing. Instead, a single govroam profile, set up with the help of their home support team, is sufficient to get the user online at all govroam participating organisations without further intervention.

Core service functionality

The primary functional capability of the service is to receive a request for connectivity from a visiting user's device and convey that request securely back to the user's home organisation, where their identity is confirmed and the home organisation decides, based on its policies, whether or not to recommend that the user be allowed to connect. The govroam service conveys that answer back to visited organisation which then grants or blocks access accordingly,

confident that the visitor's home organisation is aware of the transaction and has just made a real-time check that the visitor in question is a member in good standing.

In technical terms, this transaction is mediated by the 802.1X protocol. Supplicant software on the user's device constructs a RADIUS Access-Request packet, which is then strongly encrypted via the AES standard. An anonymous outer identity containing the home realm of the user is applied to this encrypted payload. The packet is then injected into the visited site infrastructure, which is operating in 802.1X pass-through mode, and the visited site RADIUS server recognises that the realm element of the anonymous outer identity is not managed locally, so passes it up a hierarchy of trusted servers via standards-based RADIUS proxy links, ultimately back to the visiting user's home organisation, where the authentication challenge (credentials or certificate) is processed and the appropriate Access-Accept or Access-Reject is returned, allowing the visited site to make a decision around providing connectivity.

Companion app functionality

The 'govroam companion' app (iOS and Android compatible) is available free of charge to all users of the govroam service. It's role is to help users find the nearest available instances of govroam provision, making it easier to remain connected when travelling. By documenting the locations of govroam-enabled guest networks, the app is also a valuable tool in demonstrating the scope of the service.

The companion app features an interactive map of all active registered govroam locations. Users can explore the map, interact with the markers to gain further information on the organisation managing the venue, or request routing information to navigate them to their chosen govroam location.

On joining govroam, participating organisations provide location data for the venues where they will deploy govroam. An opt-out for sensitive locations is available.

2.3 Service Infrastructure

This sub section describes the infrastructure elements of the govroam service. This includes the technology infrastructure and supporting elements (for example, monitoring and diagnostic facilities, central data repository, govroam website and the trouble ticketing system).

2.3.1 Technology Infrastructure

The federation infrastructure relies on a distributed set of AAA servers. The current configuration uses RADIUS as the AAA protocol. There are various transport protocols to carry RADIUS payloads; the following protocols exist: RADIUS/UDP, RADIUS/TCP, RADIUS/DTLS and RADIUS/TLS.

Govroam recommends the use of RADIUS/UDP, though may be able to support other RADIUS transport protocols. The govroam team can advise further [govroam@jisc.ac.uk].
Routing of RADIUS messages is accomplished by a hierarchy of RADIUS servers. See Appendix C: Best Practice Codes of Conduct for more information.

The routing models and infrastructure elements are described in more detail in the following sections.

2.3.1.1 Hierarchical Routing Model

The RADIUS hierarchy for a national govroam federation consists of several RADIUS servers located at the various organisations, which are directly or indirectly connected to the national-level RADIUS proxy server (NRPS).

Figure 2.1: Current govroam federation structure

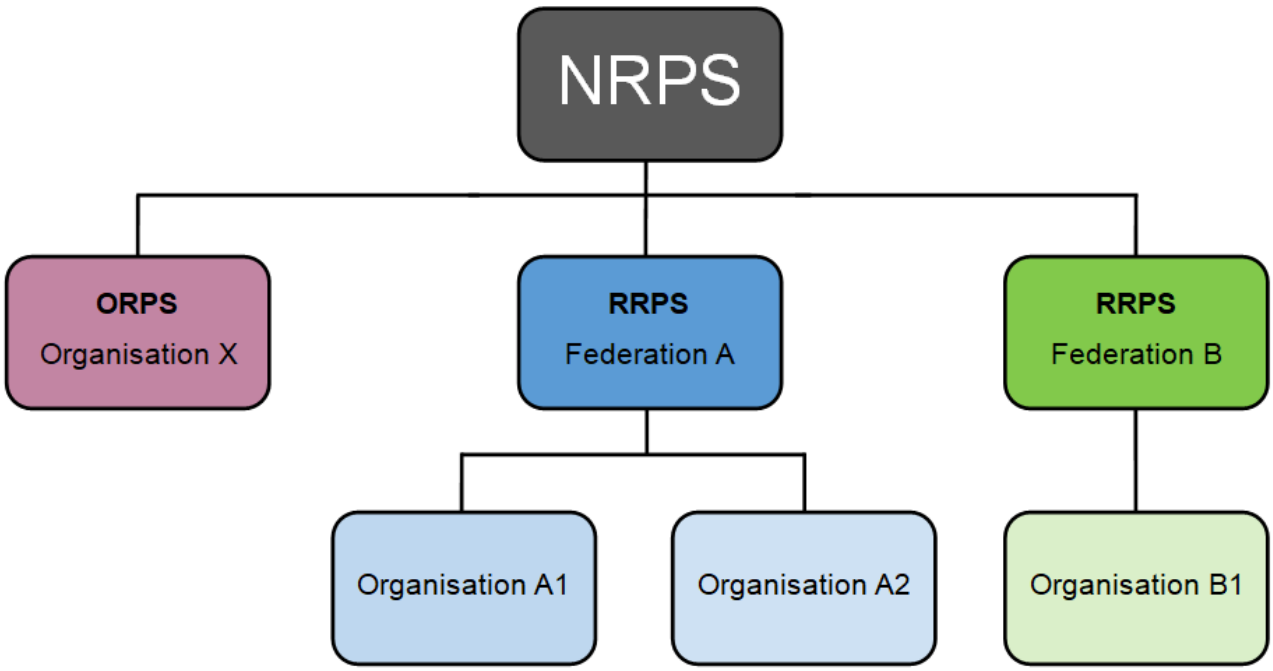


Figure 2.1: Current govroam federation structure

The govroam national RADIUS proxy servers (NRPS) interconnect the participating govroam regional federations (RRPS) and individual organisations (ORPS). They provide the means to find the correct RADIUS server to authenticate a given user, and to transport all information in a secure way. Jisc maintains the govroam NRPS.

2.3.1.2 National RADIUS Proxy Servers (NPRS)

The national RADIUS Proxy Servers (NRPS) for govroam in the UK are operated from Jisc's offices and hosted on JANET at one of our highly secure facilities. Each server has a list of connected, regional- and organisational- level domains (e.g. .cambridge.cc) serving the appropriate groupings or individual public sector bodies. The servers also maintain exception rules for domains whose federation membership is not immediately identifiable in the realm (typically gTLD realms such as 'gov.uk', 'nhs.net', etc.). The servers accept requests for the domains they are responsible for, and subsequently forward them to the associated RADIUS server for that region or organisation, and transport the response (i.e. result of the authentication request) back.

Requests for the domains that the servers are not responsible for will be dropped.
If govroam UK joins an international confederation of compatible govroam services, such requests would be passed up the hierarchy to the international top-level infrastructure.

2.3.1.3 Regional-level RADIUS Proxy Server (RRPS)

A regional aggregating RADIUS server has a list of connected govroam IdP servers (ORPS) and their associated realms, as well as the connected govroam Service Providers within a region. It is connected to the NRPS. The purpose of the RRPS is to receive requests from the NRPS and govroam SPs, and forward these requests to the responsible govroam Identity Provider using static routing.

2.3.1.4 ORPS and IdPs

In most cases, a public sector organisation participating in govroam acts as both an IdP and SP at the same time, using one or more common RADIUS servers.

Govroam Identity Providers (IdPs)

A govroam IdP's RADIUS server (ORPS) is responsible for authenticating its own users (at home or remotely when visiting another organisation) by checking the credentials against a local Identity Management System. The Identity Management System contains information on end users (for example, usernames and passwords). They must be kept up-to-date by the govroam Identity Provider.

Note that the govroam Identity Provider's RADIUS server has the most complex task of all. Whereas the other RADIUS servers merely proxy requests, the Identity Provider's server also needs to actually authenticate users, and therefore, needs to be able to terminate EAP requests and perform identity management system lookups.

Govroam Service Providers (SPs)

A govroam Service Provider's (SP) RADIUS server (ORPS) is responsible for forwarding requests from users visiting this SP to the responsible govroam IdP, by forwarding the request along the hierarchy. Upon proper authentication of a user, the govroam SP's RADIUS server may assign an appropriate VLAN to the user.

Small SPs that do not require VLAN assignment do not necessarily need their own RADIUS server, and can instead connect their network access elements (see below) to the respective RRPS.

2.3.1.5 Network Access for Wired and Wireless Infrastructure

Govroam is not dependent on access technologies. Users of govroam can access the service either by wired or wireless connection.

However, the active network equipment required for each method is different. For a wireless infrastructure, access points are needed, while for a wired infrastructure, switches are required. In both cases, specific supplicant software is required on the user's machine.

2.3.1.5.1 Supplicants

A supplicant is software on an end-user's computing device that uses the IEEE 802.1X protocol to send authentication information, using the EAP protocol. Supplicants are often built into the operating system, but can also be a separate program.
In order to use the govroam service and access the network, the supplicant software on users' devices must be appropriately configured. This single configuration profile is valid throughout the govroam federation.

The govroam Configuration Assistant Tool (CAT) can help support this process. The CAT tool eliminates the risk of accidental misconfiguration and ensures consistent set up across your userbase. See https://cat.govroam.uk/.

2.3.1.5.2 Access Points

Access points are only required for wireless access to the network.
Access points need to be IEEE 802.1X pass-through capable. They must be able to forward access requests coming from a supplicant to the SP's RADIUS server, to allow network access upon proper authentication. Access points may also possibly assign users on to specific VLANs based on information received from the RADIUS server. Furthermore, access points exchange keying material (initialisation vectors, public and session keys, and so on) with client systems to prevent session hijacking and to ensure encryption of user payload data on the wireless medium.

2.3.1.5.3 Switches

Switches are used for wired access to the network.
Wired infrastructure can be configured to provision IEEE 802.1X (and therefore govroam). This means that govroam users can access the network through wired technology, but in order to do this, the switches that are used to connect end users' computers need to be IEEE 802.1X-capable and enabled on the ports used for govroam access.
These switches need to be able to forward access requests coming from a connected supplicant to the SP's RADIUS server, to grant network access upon proper authentication and to possibly assign users to specific VLANs based on information received from the RADIUS server.

2.3.2 Security

Govroam takes a federated approach, and the trust model is therefore split into domains of responsibility for secure provision that take in not only the core Jisc-provided services, but also aspects of provision by the end-users home organisation, and the organisation providing the visitor network to which they roam.

Table 2.1: Security responsibilities

Organisation:	Home organisation	Jisc	Visited organisation
Security-related responsibilities:	Credential issue & revocation; RADIUS IdP; Client device profiles	Core availability; Secure transit of authentication flows.	Credential issue & revocation; RADIUS IdP; Client device profiles

In the public sector, standardised secure approaches to the processes required for govroam participation noted above are already well established. Jisc is responsible for the processes and services that together provide the authentication step in gaining access to the visited organisation's connectivity offer. *Note that under this model, Jisc never has access to plaintext end user data; the govroam service itself only routes encrypted payloads*.

In summary, an 802.1X supplicant on the client device is configured with a govroam profile e.g. by the govroam CAT. In the presence of the govroam SSID, this supplicant initiates an end-to-end encrypted exchange with the users' home site RADIUS server. This transaction occurs over the visited site infrastructure running in 'pass through' mode, and may involve one or more intermediate RADIUS proxying steps, but crucially all of this intermediate processing only has access to an anonymous outer identity on the encrypted tunnel: the encrypted payload of credentials is inaccessible to any third party. The home RADIUS server ultimately returns an

Access- Accept or –Reject message to the visited site infrastructure, based on credential checks and any local policies in place. The visited site can then provide connectivity accordingly.

2.3.2.1 End-to-end Encryption of User Credentials

End-to-end encryption ensures that no intermediate party, be it a govroam central infrastructure operator, the visited organisation, any regional operator, or external third parties, can steal the digital identity of a govroam user. This enables the govroam service to make an important assertion: using govroam never exposes credentials to anyone in the infrastructure except the home organisation. This ensures that the federation infrastructure operators are neither responsible nor liable for password theft.

Since no AAA infrastructure available today provides end-to-end encryption in itself, end-to- end security has to be established by the two ends of the authentication chain: the end-user device (notebook, PDA, smartphone, tablet, etc.) and the home authentication server. This is achieved by using mutual-authentication protocols such as EAP-TTLS, PEAP or EAP-TLS. Most notably, authentication methods in use by web redirect portals such as PAP do NOT provide end-to-end security.

As credentials are encrypted between the user device and home RADIUS server, personal data is never exposed to anyone except the user's home organisation, which will already hold this data. Man-in-the-middle (MitM) attacks that attempt to persuade the user to give up their credentials to rogue infrastructure rely on the user overriding the security warnings around certificate mismatch that are generated, so it is essential that service users are educated around the appropriate response to such warnings.

2.3.3 Supporting Infrastructure

2.3.3.1 Monitoring, Diagnostics and Metering

The govroam team is able to offer limited usage monitoring data on request [govroam@jisc.ac.uk]. Requests will be considered on a case-by-case basis.
We are currently working with RFOs to collect additional usage data, with the aim of offering a more developed monitoring service in the future.

2.3.3.2 Govroam Website

The govroam web page [https://www.jisc.ac.uk/govroam] is run and maintained by the govroam team. This provides useful information about implementing and using the service.
A govroam wiki site provides technical information for sys-admins [https://wiki.govroam.uk/doku.php].

2.3.3.3 Govroam Database

The information stored in the govroam database is collected with help from RFOs and includes:

- Regional representatives and respective contacts;
- Organisational-level govroam SP and IdP official contacts;
- Information about govroam Service Providers (SP location, technical info);

A web interface to the database is implemented, which allows various views of the database content. Some of these are public, while others are restricted to predefined user groups. The decision on the availability of the information lies with the govroam team.

Data exchange with other applications related to the govroam service is subject to prior approval by the govroam team.

The govroam database and its web interface is run and maintained by the govroam team. Information about the eduroam database design and data collection practice is available via the website [https://www.jisc.ac.uk/eduroam].

2.3.3.4 Trouble Ticketing System (TTS)

The govroam team runs and maintains a Trouble Ticketing System (TTS) in order to document its work, and to allow authorised users from the predefined user groups to report any irregularities in the govroam service.

All emails directed to govroam@jisc.ac.uk will create a new ticket in Remedyforce.
The TTS will acknowledge receipt of all emails within four (4) hours, and operates within an SLA of five (5) working days for resolution or substantial action.

2.3.3.5 Mailing Lists

Two mailing lists are provided:

- Govroam general discussion list (roaming@jiscmail.ac.uk)
- Technical information announcements (govroam-technical@jiscmail.ac.uk)

These lists are used for day-to-day communication, as well as official broadcasts.

2.4 Users

This section describes the identified user categories and the way the govroam service elements are mapped to these categories.

2.4.1 End Users

End users are the individuals who use govroam technology to access network services, either at their home organisation or while visiting other sites.

End users have access to the govroam website and database, which provide general information and basic monitoring tools.

2.4.2 Administrative Personnel

Administrative personnel are those users who are running parts of the govroam infrastructure that are not handled directly by the govroam team: the regional layer and the organisation layer. This subdivides this user group into regional-level personnel and organisational-level personnel.

2.4.2.1 Regional-level Personnel

Staff for RRPS operation: This user group would probably contain a small number of staff per participating regional federation. Part or all of this work may be subcontracted to a third-party.

2.4.2.2 Organisation-level Personnel

Staff for ORPS and service operation: Service operation on an organisational level differs significantly from operation of a regional federation server. The staff within organisations need to

configure, monitor and troubleshoot equipment that performs authentication for an identity management system. Given that identity management systems are quite diverse, it is impossible for govroam team to provide exhaustive documentation on how to configure each and every backend system.

Staff for trouble ticketing and handling user support: This group represents local staff that handle day-to-day user support. They should be supported by the respective regional or national operating teams. The govroam team will provide basic materials in order to help them provide consistent and uniform service to the end users.

2.4.3 Govroam User Summary

The table below cross-references user groups with the govroam service elements that they would be expected to use:

Service element	End user	Organisation-level personnel	Federation-level personnel
Basic monitoring facilities	Yes	Yes	Yes
Full monitoring and diagnostics facilities	No	Yes (limited to their organisation)	Yes
Public access to the govroam website	Yes	Yes	Yes
Access to the internal govroam website	No	Yes (limited to their organisation)	Yes
Public access to the govroam database	Yes	Yes	Yes
Access to all information on the govroam database	No	Yes (limited to their organisation)	Yes
TTS	No	Yes	Yes
Govroam team mailing lists	No	Yes (if no regional structure)	Yes
Support from govroam team	No	Yes (if no regional structure)	Yes

Table 2.2: Service elements

2.5 Service Organisation

The public sector roaming solution, govroam, is operated by a dedicated team within Jisc. The organisation of govroam is aligned with the overall needs of the public sector in the UK, and will be adjusted in case of future changes to those needs. Day-to-day operations are carried out by Jisc's govroam team.

2.5.1 Roles and Responsibilities

This section describes the specific roles and responsibilities of the:

- Jisc govroam team;
- Regional federation operators (RFOs);
- Technical working group (TWG).

The interaction of these groups is illustrated in Figure 2.2 (below).

2.5.1.1 Jisc govoram team

Jisc coordinates the operation of govroam in the UK, approves and develops its policies and budget plans, and handles membership matters. Jisc regularly engages with it's members through stakeholder meetings, and considers this feedback in the running of the service.
The govroam team handles day-to-day operations. It is responsible for the smooth operation of the federated service. It's tasks include:

- Operating the govroam federation infrastructure;
- Monitoring the govroam federation;
- Evaluating usage-related data and publishing of corresponding graphs and statistics;
- Handling fault resolution procedures;
- Providing support for new members (organisations or regions);
- Participating in the dissemination work (providing material for web pages, enhancement of the visibility of the federation, including the provision of promotional material);
- Gathering of statistics on usage and error reports;
- Developing diagnostic tools and support for scripts;
- Incident handling, according to the defined and agreed procedures;
- Maintaining the central repository (database) providing information about the govroam service;
- Maintaining the govroam service web pages and trouble ticketing system;
- Participating in organisation of training events;
- Liaising with other public sector roaming (con-) federations internationally.

2.5.1.2 Regional federation operators (RFOs)

RFOs should appoint at least one representative, and may where appropriate expertise exists be asked to contribute to the TWG. The tasks of the RFO members include:

- Assuring adherence to the govroam policy in their region;
- Provisioning of necessary support and information to the govroam team;
- Provisioning of the support to roaming users within their constituency;

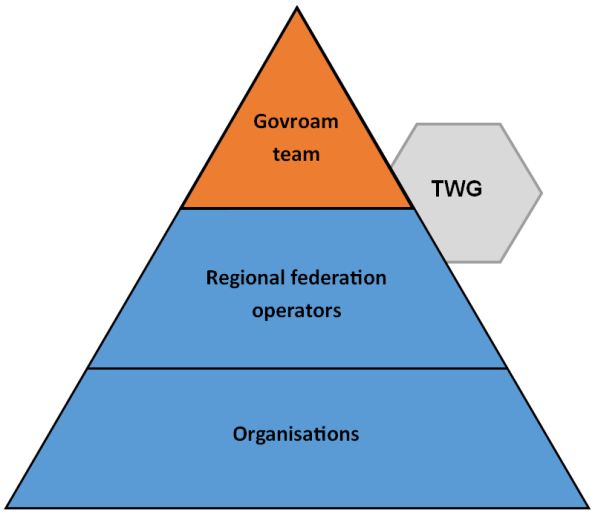
2.5.1.3 Technical Working Group

The TWG supports the technical development of the govroam service, and is assembled as needed from RFO representatives. It works closely with the govroam team and provides it with necessary input.
The tasks of the TWG include:

- Developing technical policy;
- Providing input to the govroam team to inform further policy development including recommendations related to establishing trust between members;
- Improving of govroam service definition and procedures;
- Developing proposals for the next phase on the development roadmap.

The govroam service model is illustrated in Figure 2.2:

Figure 2.2: Govroam service model



2.5.1.4 Service Level Definition

The govroam team is responsible for running the federation service. Therefore, it maintains:

- Federation infrastructure (explained in Section 2.3);
- Monitoring and diagnostic facilities;
- Govroam database;
- Govroam website;
- Federation trouble ticketing system.

The goal for the availability of these services is 99.9%, excluding scheduled maintenance (see section 2.6.2.1).

2.6 Service Operation

This section defines basic operational procedures for the govroam service. The govroam team will use the following communication tools:

- Mailing lists (see Section 2.3.3.5);
- Trouble Ticketing System (TTS);
- Govroam website;
- Face to face meetings and videoconferences.

2.6.1 User Support Processes

The processes for delivering user support are described in this section. However, please note that end-user support is delivered primarily by their home organisation's personnel.

The govroam service organisation model assumes that the home organisation (and respective regional operator, where present) will provide the user with the information and knowledge to use the govroam service. It is up to the home organisation to provide the necessary user support to the roaming user.

Furthermore, RFOs and their member organisations are encouraged to provide some categories of user support to visiting users regarding the use of govroam service.

The govroam team primarily provides support to RFOs, but also disseminates information and tools that can be used by the local organisations' administrators and end users.

2.6.1.1 Support for End Users

End users may roam inside their home regional federation or across its boundaries.

- If an end user roams within their region, the regional federation's user support rules are applied.
- If a user roams across the boundaries of their home regional federation, s/he should contact their home organisation's personnel in order to obtain assistance or report an incident.

If needed, respective federation-level personnel will be contacted along with the govroam team by the organisation-level personnel. End users should never contact these functions directly. RFOs and their member organisations are encouraged to provide user support to the visiting users.

2.6.1.2 Administrative Personnel

Regional Federation-level personnel:

- Escalate problems to the govroam team whenever the problem includes the federation service or deals with the basic govroam technology;
- Contact other involved regions directly, but must also inform the govroam team.

Organisation-level personnel:

- Escalate problems to the federation-level personnel whenever they need assistance;
- Contact the govroam team whenever the problem includes the central federation service, but must also inform regional federation-level personnel.

2.6.1.3 Problem Escalation Scenarios

The following scenarios for user support are informed by our experience with the govroam and eduroam environments.

2.6.1.3.1 Problem Escalation Involving User and Organisation-level Personnel

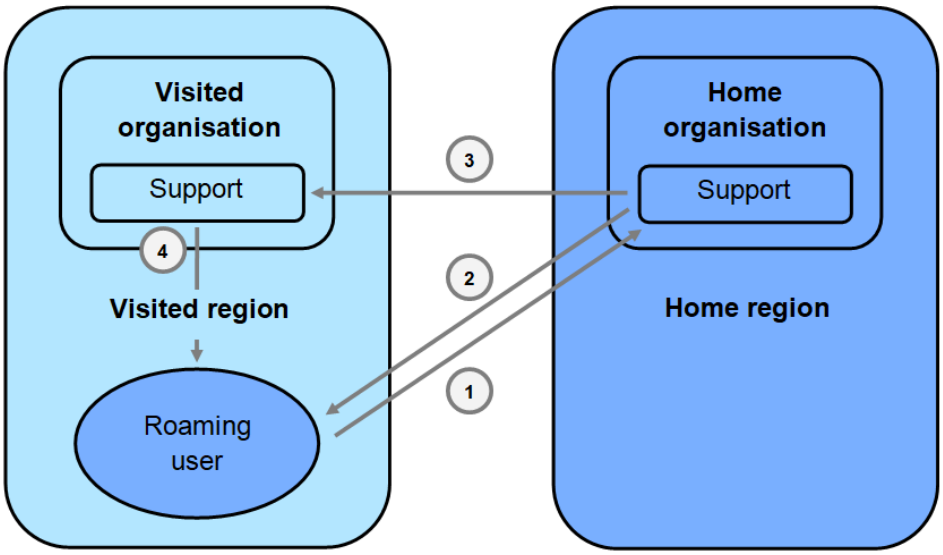
In this scenario, a user has difficulty accessing the network while using the govroam service outside his/her home regional federation.

The steps the user might follow are:

1. The user calls his/her home organisation, and asks for help from administrative personnel.
2. Administrative personnel at the user's home organisation will check the validity of the user's credentials and help in setting up the end-user's machine (e.g. a laptop or smartphone). Personnel should also check if their system receives proper authentication requests from the visited site via the respective part of the govroam infrastructure. If they discover problems with the user's credentials or with the setup of his machine, they should provide necessary help to the end user.

3. If administrative personnel at the user's home organisation discover problems receiving a proper authentication request from the visited site, they should contact administrative personnel at the visited organisation to fix the problem. Local administrative personnel at the visited organisation should provide all necessary information.
4. If needed, administrative personnel at the visited organisation should inform the visiting user how to fix the problem.

Figure 2.3: Problem escalation scenario, user and organisation personnel

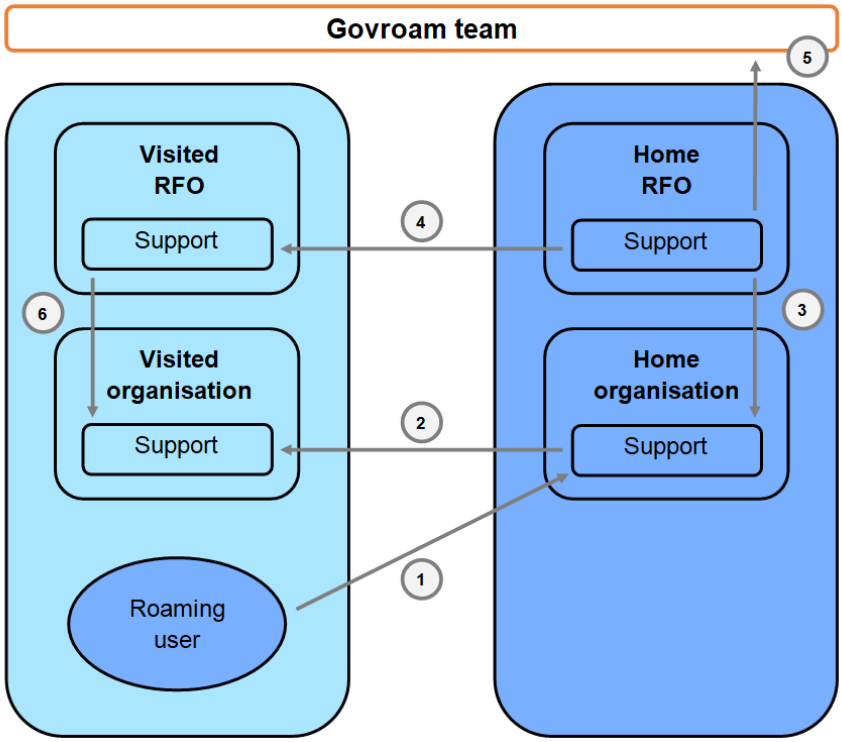


2.6.1.3.2 Problem escalation involving user, organisation and regional federation-level personnel
In this scenario, the user has a problem accessing the network while using the govroam service outside of his/her home regional federation. Following an unsuccessful investigation by the local support team, the problem needs to be escalated to regional federation level:

1. The user must call his/her home organisation and ask for help from administrative personnel. Administrative personnel at the user's home organisation will check the validity of the user's credentials and help to set up the end-user's machine. They should also check if their system receives a proper authentication request from the visited site. If they discover problems with the user's credentials or with the setup of the user's machine, they should provide necessary help to the end user.
2. The end user's home federation administrative personnel should carry out further checks, and if needed, contact the visited federation's administrative personnel. In response, the federation 's administrative personnel should provide necessary information in order to resolve the problem.
3. If administrative personnel at the user's home organisation discover the problem is in receiving authentication requests from the visited site, and they cannot resolve the problem by contacting administrative personnel at the visited organisation, they should contact administrative personnel of their regional federation operator
4. If the problem does not lie with the home RFO, administrative personnel at the regional level should contact the visited region's RFO to investigate further.
5. It may be appropriate to involve the govroam team to ensure that the proper authentication requests can be sent from one federation to the other using the central infrastructure.

6. Visited regional federation administrative personnel should contact the visited organisation's administrative personnel in order to resolve the problem and check if the proper authentication requests are sent, as required.

Figure 2.4: Problem escalation scenario, user, organisation and regional federation-level personnel



2.6.2 Maintenance Procedures

This section outlines main maintenance procedures. Detailed procedures including the working hours are defined by the govroam team.

2.6.2.1 Scheduled Maintenance

Scheduled maintenance of central govroam infrastructure, as well as the other associated servers and services, is under the control of the govroam team and will be announced at least seven (7) days in advance. Scheduled maintenance will be scheduled from Tuesday, 08:00 – 10:00.

Given the highly resilient nature of the central govroam infrastructure, it is usually possible to carry out scheduled maintenance without overall service interruption.

Scheduled maintenance work performed by RFOs within their respective regions should be announced at least two (2) days in advance, and should ideally be scheduled within the maintenance window on Tuesday, 08:00 – 10:00. Scheduled maintenance of infrastructure must be planned to avoid any break in the service. A ticket on TTS should be opened by the respective RFO representative, and closed with a short comment on the performed action.

2.6.2.2 Unscheduled maintenance

Unscheduled maintenance consists of maintenance work that cannot be planned in advance, usually performed to avoid a security incident or following a service malfunction.

Unscheduled maintenance of the govroam central infrastructure, as well as the other servers and services under control of the govroam team, must be announced as early as possible (the preferred period is 24 working hours in advance, but in emergency conditions, such announcement may be made concurrently with addressing the issue). A ticket on TTS should be opened by the respective govroam team member and closed with a short comment on the performed action.

Unscheduled maintenance work performed by the RFO inside the respective region should be announced as early as possible (the preferred period is 24 working hours in advance, but in emergency conditions, such announcement may be made concurrently with addressing the issue). A ticket on the TTS should be opened by the respective RFO representative and closed with a short comment on the performed action.

Emergency outages are reported to the wider govroam community on the Jisc website, and via a dedicated Twitter feed (https://twitter.com/jiscmi).

2.6.3 Security Incidents

In the case of any security incidents, the govroam team assisted by Jisc's CSIRT will apply an agreed security incident handling procedure (https://www.jisc.ac.uk/csirt). In addition there are some further actions (explained below) that must be taken.
In case of a security incident caused by an end user, the affected organisation must inform its RFO. The RFO will then inform the end-user's home region federation through the RFO's respective official contacts in the govroam database.
RFOs should regularly report to the govroam team about the number and type of these incidents.

In case of international confederation incidents, should govroam UK enter a wider global scheme, the govroam team will lead the resolution process.

2.6.4 Policy Violation

Jisc can offer advice and assistance to help members comply with service policy.
In the case of a severe policy violation by a regional federation or individual organisation, as determined by Jisc, the govroam team will react in the following way:

- Issue a notice on the policy breach and initiate an evaluation process not later than four (4) working hours after the violation has been discovered or reported by a govroam user or a member.
- Propose and implement a temporary quarantine period (the length of the period, as well as the exact measures required are handled on a case-by-case basis)
- Should the issue not be resolved satisfactorily, Jisc may disqualify the region/organisation from the federation and announce membership termination.

All incidents that affect the govroam federation service, as well as all severe cases of policy violation, shall be presented as a part of regular govroam team service reports.

2.6.5 Malfunction

Suspected malfunction of the NRPS, or other servers and services under control of the govroam team, must be reported to govroam@jisc.ac.uk by the technical contact at the reporting organisation. The govroam team will start resolving the problem not later than four (4) working hours after the malfunction has been discovered

Malfunction in a member regional federation should be announced. A ticket on the TTS should be opened by the respective RFO representative and closed with a short comment on the performed action.

Table 2.3 Incident Reporting	Severity 2 Incident (Multiple RFO member organisations suffer complete loss of service)	Severity 2 Incident (Individual RFO member organisation suffers complete loss of service)	Severity 3 Incident (RFO member organisation(s) suffer degraded or intermittent service)
RFO member organisation to RFO	RFO member organisation to: > Respond to End User and inform Jisc direct within 1 hour > Use best efforts to fix within 4 hours > Escalate to RFO after 4 hours if still unfixed	RFO member organisation to: > Respond to End User and inform RFO within 1 hour >Use best efforts to fix within 2 days > Escalate to RFO after 2 days if still unfixed	RFO member organisation to: > Respond to End User within 8 hours > Use best efforts to fix within 5 days > Escalate to RFO after 5 days if still unfixed
RFO to Jisc	RFO to: > Respond to RFO member organisation and inform Jisc within 1 hour > Use best efforts to fix within 4 hours > Escalate to Jisc after 4 hours if still unfixed	RFO to: > Respond to RFO member organisation and inform Jisc within 4 hours > Use best efforts to fix within 2 days > Escalate to Jisc after 2 days if still unfixed	RFO to: > Respond to RFO member organisation within 8 hours > Use best efforts to fix within 5 days > Escalate to Jisc after 5 days if still unfixed

2.6.5.1 RADIUS Attribute Monitoring

The existence of VLAN assignment attributes in authentication responses is almost always a sign of a misconfiguration on the sending (identity provider) side. It can be the source of hard-to-trace problems at the service provider side, and ultimately lead to a complete denial of service (a service malfunction) to the affected end user.

However, it cannot be completely ruled out that a given pair of identity and service providers have an agreement about common VLAN tags (e.g. within a regional federation). This makes it imperative that VLAN attributes are not filtered automatically on any level of the infrastructure. To minimise possible malfunctions due to VLAN attributes, the govroam team may monitor packets en route for the presence of VLAN tagging attributes.

The govroam team will notify the regional federation or directly connected organisation generating these packets. Participating regional federations are encouraged to do the same for the organisations in their constituency, and to investigate whether the sender is sending these attributes inadvertently or not, and then take appropriate action.

2.6.6 Handling Membership

Regional roaming federations can join the govroam federation only if the RFO on behalf of their region accepts and signs the govroam policy, thus committing to provide a compliant govroam service within its federation and contribute to the UK govroam service.

If an organisation seeking to belong to a federation cannot be routed through the RFO's servers for any technical reason, it may join as an individual member.

The govroam federation may in future peer with an international roaming confederation, and may be required to sign a global govroam compliance statement.

Any member of the UK govroam federation can, at any time, leave the federation by giving thirty (30) days' notice of their intention to leave. This notice period is required to ensure that all the resultant practicalities of the member leaving (updating websites, top level servers, user notification, and so on) can be taken care of in a timely manner.

In the case of severe violation of the govroam policies, Jisc may exclude a member from any further participation in the govroam federation.

An excluded member or an RFO whose application has been turned down has right to present an appeal document to Jisc by submitting a document of no more than two (2) pages to govroam@jisc.ac.uk. Decisions on membership following consideration of such appeals are final.

2.6.7 Service Reports

The govroam team provides an update on the service at stakeholder meetings approximately every six (6) months. These updates typically include information on:

- Number of member organisations;
- Number of successful roaming sessions between regions;
- Number of security incidents and malfunctions;
- Report on maintenance activities;
- Central infrastructure availability;
- Service improvements.

RFOs will be required to provide the above data to the govroam team. The technical mechanism to do so is currently under development.

2.7 Govroam Member Requirements

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" used in this chapter are to be interpreted as described in RFC 2119.

2.7.1 Policy Declaration

The govroam terms and conditions enables the establishment of the govroam federation by formalising the organisational and technical requirements.

The terms and conditions MUST be signed by each RFO or directly connected organisation. By signing the terms and conditions, the RFO commits to offer the govroam service inside their federation, in line with the govroam policy.

Violation of the terms and conditions MUST be reported to the govroam team.
RFOs must sign an agreement with each member of its federation which includes terms that are materially similar to its agreement with Jisc.

2.7.2 Operational Requirements for Govroam Federation Members

2.7.2.1 General Requirements for Federation Members

Each regional federation joining govroam MUST:

- Establish the necessary infrastructure for govroam, and ensure that it is maintained according to the govroam technical specification and code of practice (see Appendix C)., both at the regional and respective organisational levels;
- Establish a user support service for its end users, as explained in Section 2.6.1, "User Support Processes";
- Provide any information required for the govroam database (see Section 3.1.1);
- Establish and maintain a website, including information with respect to the participating organisations in the region, as well as practical information on how to use govroam. The webpage SHOULD be available in English.

2.7.2.2 Govroam Security Requirements

The basic security principle that governs the govroam infrastructure is:

The security of the user credentials MUST be preserved when travelling through the infrastructure, and all partners providing the service MUST observe privacy regulations.
The relevant technical details are listed in the next section. All govroam participants (govroam team, RFOs, organisations) MUST:

- Always provide trustworthy and secure transport of all private authentication credentials (i.e. passwords) that are traversing the govroam infrastructure;
- Ensure that user credentials stay securely encrypted end-to-end between the user's personal device and the identity provider when traversing the govroam infrastructure. A rationale for this requirement can be found in Appendix A;
- Ensure that govroam servers and services are maintained according to the specified best practices for server build (see section 2.7.3.1), configuration and security, with the purpose of maintaining a generally high level of security, and thereby trust in the govroam federation.

An additional task for RFOs is to ensure that the participating organisations within their region are fully aware of their responsibility to establish an appropriate level of security.

The govroam team guarantees that the necessary infrastructure to run the federation services is operational and maintained according to server build, configuration and security best practices.

The govroam team also ensures that it will start resolving reported incidents concerning the govroam federation no later than four (4) working hours after the incident has been discovered.

2.7.3 Technical Requirements for Govroam Members

All the components in govroam need to have, or provision, access to the Internet. Therefore, in general, the equipment needs to provide all the functionalities for standard Internet access (for example, an IP stack, optional VLANs, etc.). In addition to the general networking requirements, govroam makes use of a number of protocols for user authentication and service provisioning. These authentication-specific and service-specific requirements are listed below. Details regarding the extent of usage of these specifications are also given.

2.7.3.1 Specifications and Operational Requirements: Regional Federation Level

Adherence to the following specifications is REQUIRED:

AAA Servers:

- RADIUS datagram processing to and from the TLRS, as per RFC 2865 or any other of the recommended transports (e.g. RADIUS/TLS). The server MUST be able to proxy RADIUS datagrams to other servers based on contents of the User-Name attribute.
- RFC 3580 (EAP over RADIUS). The server MUST proxy EAP-Message attributes unmodified, in the same order as it received them, towards the appropriate destination.
- The server MUST be set up to allow monitoring requests from the monitoring service.
- All relevant logs MUST be created with synchronisation to a reliable time source (GPS or in its absence NTP/SNTP).
- The server(s) MUST respond to ICMP/ICMPv6 Echo Requests sent by the confederation infrastructure and confederation monitoring service.

Web server:

- RFO SHOULD set up a web server in order to publish information about the govroam service. The address of that server SHOULD be <tld>/govroam. For example, www.rothgen.nhs.uk/govroam.
- An RFO's web server MUST provide data in XML format, based on the specification defined by the govroam team.

Adherence to the following specifications is RECOMMENDED:

AAA Servers:

- RFC 2866 (RADIUS Accounting). The server SHOULD be able to receive RADIUS Accounting packets if a service provider opts to send that data. If RADIUS Accounting is supported, RADIUS Accounting packets with a destination outside the regional federation MUST NOT be forwarded outside the regional federation, and MUST be acknowledged by the RFO's server.
- A RADIUS/TLS endpoint open for connections from all other govroam participants to enable the receiving end of RADIUS/TLS dynamic discovery.
- A DNS-based discovery module for outgoing RADIUS/TLS dynamic discovery.
- Servers SHOULD be highly available, for example by deploying multiple separate servers in a failover configuration in different IP subnets on different physical locations.
- Logs of all authentication requests and responses SHOULD be kept. The minimum log retention time is six months, unless national regulations require otherwise. The information in the requests and responses SHOULD as a minimum include:
  - The time the authentication request was exchanged;

- The value of the User-Name attribute in the request ('outer EAP-identity');
- The value of the Calling-Station-Id attribute in authentication requests;
- The result of the authentication;
- The value of Chargeable-User-Identity (if present in Access-Accept message).

2.7.3.2 Specification and Operational Requirements: Identity Providers

Adherence to the following specifications is REQUIRED:

AAA Servers:

- RADIUS datagram processing as per RFC 2865 or any other of the recommended transports (e.g. RADIUS/TLS). The server MUST be configured to receive authentication traffic from its FLRS and send appropriate replies.
- EAP server endpoint as per RFC 3580.
- A well-managed identity management backend system.
- All relevant logs MUST be created with synchronisation to a reliable time source (GPS or in its absence NTP/SNTP).
- At least one EAP type, which is capable of mutual authentication and capable of generation of keying material for use with IEEE 802.1X in accordance with Section 3.16 of RFC 3580 (IEEE 802.1X RADIUS Usage Guidelines).
- The outer EAP identities (and with it, RADIUS User-Name attributes) for the IdP MUST be in the format of arbitrary@realm. The realm component MUST be a domain name in the global DNS (without the trailing '.' symbol) that the identity provider administers, either directly or by delegation. The part to the left of the '@' symbol is arbitrary; in particular, anonymity support is possible and encouraged.
- The server-side EAP credentials MUST be communicated to the user base, and end- user documentation needs to be precise enough to allow users the unique identification of their EAP server.
- The appearance of the Operator-Name attribute (RFC 5580) in Access-Requests MUST NOT cause these requests to be treated as invalid.
- Logs of all authentication requests and responses MUST be kept. The minimum log retention time is six months, unless national regulations require otherwise. The information in the requests and responses MUST, as a minimum , include:
  - The time the authentication request was exchanged;
  - The value of the User-Name attribute in the request ('outer EAP-identity');
  - The value of the Calling-Station-Id attribute in authentication requests.
  - If tunnelled EAP types are used, the actual user name in the request ('inner EAP identity');
  - If the IdP opts to generate a Chargeable-User-Identity, the value of this attribute;
  - The result of the authentication.

An IdP MUST provide sufficient configuration instructions for their end users so that a unique identification of the IdP is possible for the end user at all times.

Note: the list of supported EAP types as configured by the IdP in Section 6.3.2, and the list of supported EAP types in the supplicant software in Section 6.3.4 MAY have an empty intersection. In such cases, the combination of end-user device and IdP configuration will leave the user without service. To minimise the probability of this, govroam IdPs are encouraged to configure as many EAP types as they can possibly support, and to announce the full list of supported EAP types to their end users.

Adherence to the following specifications is RECOMMENDED:

AAA Servers:

- Generation of a pseudonymous Chargeable-User-Identity (RFC 4372) response if solicited by a Service Provider and on the condition that the Service Provider's Access-Request contains a non-empty Operator-Name attribute. The value of Chargeable-User-Identity attribute returned in the response MUST have a constant value for one user and one Operator-Name attribute value. The value of Chargeable-User-Identity attribute MUST be generated in a way that ensures that the matching of this value to the actual user identity is possible only at the Identity Provider.

2.7.3.3 Specifications and Operational Requirements: Service Providers

Adherence to the following specifications is REQUIRED:

Network Access Servers (NAS):

- Construction and processing of RADIUS datagrams as per RFC 2865 or any other of the recommended transports. The NAS MUST send its RADIUS datagrams either to the SPs local RADIUS server or, in its absence, to the RFO's RADIUS server(s). The generated RADIUS datagrams MUST include the attribute Calling-Station-Id, and the attribute value MUST contain at least the MAC address of the connecting end-user device;
- RFC 3580 (EAP over RADIUS);
- IEEE 802.1X;
- All relevant logs MUST be created with synchronisation to a reliable time source (GPS or in its absence NTP/SNTP);
- Wireless NASs MUST support WPA2/AES, and MAY additionally support WPA/TKIP as a courtesy to users of legacy hardware;
- Wireless NASs MUST deploy the SSID "govroam" and MUST broadcast the SSID "govroam", unless there is more than one govroam SP at the same physical location and the signal overlap would create operational problems, in which case an SSID starting with "govroam-" MAY be used.

Local AAA Servers (in their absence, NAS or RFO RADIUS server(s)):

- Authentication requests MUST be forwarded towards the responsible govroam Identity Provider via the govroam infrastructure;
- The server MUST proxy EAP-Message attributes unmodified in the same order as it received them towards the appropriate destination;
- Sufficient logging information MUST be kept to be able to correlate between a client's layer 2 (MAC) address and the layer 3 (IP) address that was issued after login if public addresses are used. This requirement is void if NAT is used.

Network:

The following set of ports MUST be made available to roaming visitors:

Service	Protocol/Port	Direction
Standard IPSec VPN	IP protocol 50 (ESP) IP protocol 51 (AH) UDP port 500 (IKE)	Incoming and outgoing Incoming and outgoing Outgoing
OpenVPN 2.0	UDP port 1194	Incoming and outgoing
IPv6 tunnel broker service	IP protocol 41	Incoming and outgoing

IPSec NAT – Traversal	UDP/4500	Incoming and outgoing
Cisco IPSec VPN over TCP	TCP/10000	Outgoing
PPTP VPN	IP protocol 47 (GRE) TCP port 1723	Incoming and outgoing Outgoing
SSH	TCP port 22	Outgoing
HTTP	TCP port 80 TCP port 443 TCP port 3128 TCP port 8080	Outgoing Outgoing Outgoing Outgoing
Mail sending	TCP port 465 TCP port 587	Outgoing Outgoing
Mail reception	TCP port 143 TCP port 993 TCP port 110 TCP port 995	Outgoing Outgoing Outgoing Outgoing
FTP (passive)	TCP port 21	Outgoing

Adherence to the following specifications is RECOMMENDED:

NAS or local AAA Servers:

- Inclusion of hotspot location information with the Operator-Name attribute in authentication requests as per RFC 5580.
- Requesting a Chargeable-User-Identity value from the IdP, as per RFC 4372.

Local AAA Servers (in their absence, RFO RADIUS server(s)):

- Logs of all authentication requests and responses SHOULD be kept. The minimum log retention time is six months, unless national regulations require otherwise. The information in the requests and responses SHOULD, as a minimum, include:
  - The time the authentication request was exchanged;
  - The value of the User-Name attribute in the request ('outer EAP-identity');
  - The value of the Calling-Station-Id attribute in authentication requests;
  - If present, the value of the Chargeable-User-Identity attribute;
  - The result of the authentication.

Network:

- Network access to roaming visitors SHOULD not be port-restricted at all (i.e. in addition to the minimum list of open ports from above, allow all outgoing communication). Where this is not possible, the number of filtered protocols SHOULD be kept as low as possible;
- The use of NAT SHOULD be avoided;
- IPv6 connectivity SHOULD be supplied;
- Service providers SHOULD NOT deploy application or interception proxies. Service providers deploying application or interception proxies MUST NOT use the proxy to require users to submit personal information before gaining access to the Internet, and MUST publish information about these proxies on their govroam website. If an application proxy is not transparent, the service provider MUST also provide documentation on the configuration of applications to use the proxy.

Authentication request filtering:
In order to help maximise the efficiency of the National RADIUS Proxy Servers (NRPSs) all organisations providing Visited services SHOULD filter malformed outgoing RADIUS authentication requests on their border Organisation RADIUS Proxy Servers (ORPSs) and not pass bad requests to the NRPSs. This minimises the unsuccessful authentication attempts (ones which will never succeed) and means that genuine authentication requests are dealt with as quickly as possible.

Full details of this requirement are available in the govroam technical specification.

2.7.3.4 Specifications and Operational Requirements: End User Devices

Requirements for user devices:

- IEEE 802.1X support;
- Supplicant software with support for at least one EAP type capable of mutual authentication.

Return to introduction.

3. G Gloud 15 Alignment Information

3.1 On-boarding and Off-boarding Processes

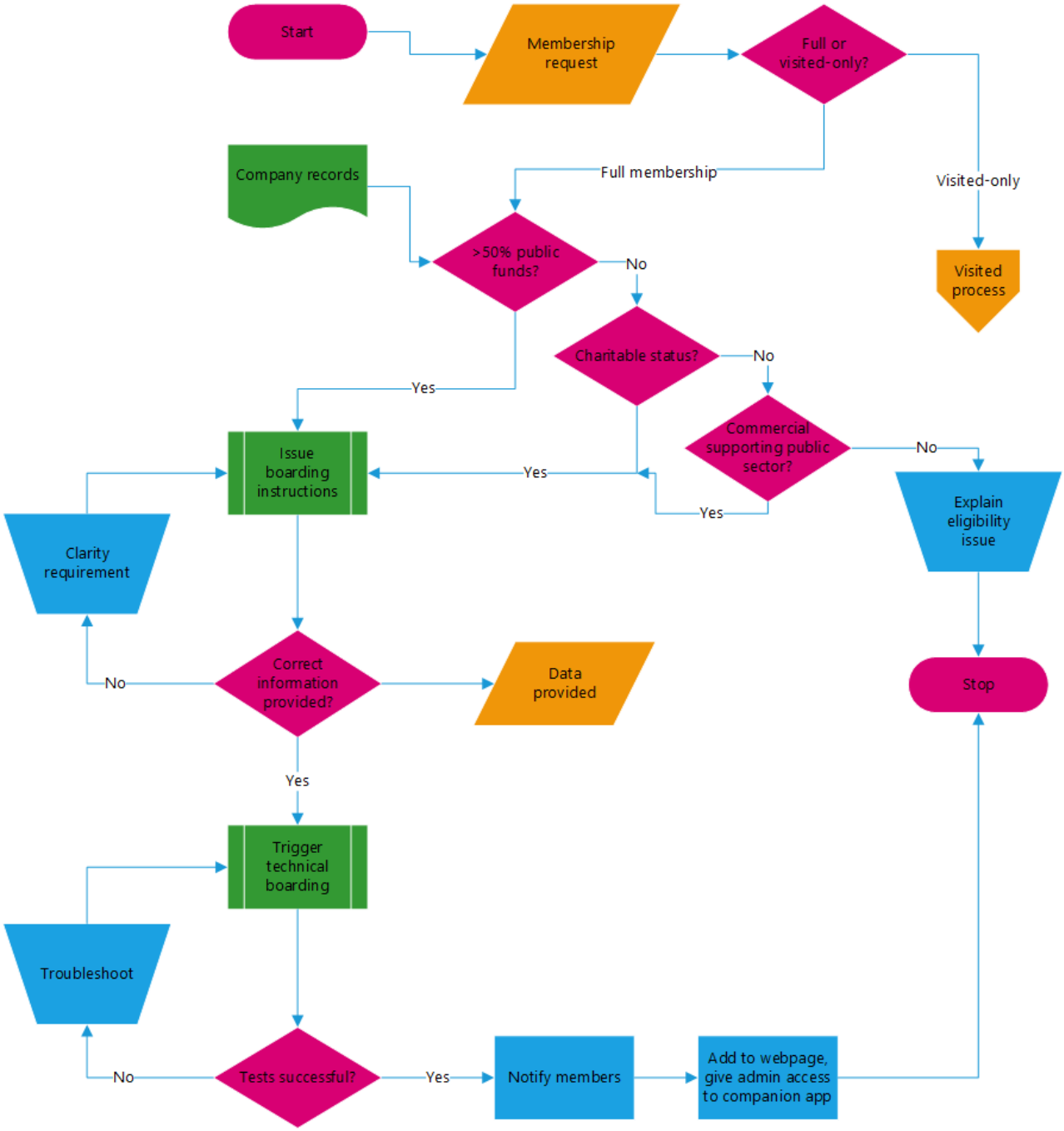
3.1.1 On-boarding

The on-boarding processes for the govroam service have a dual focus: confirming eligibility and authority to request the service on behalf of the organisation or federation; and exchanging shared secrets, test credentials and configuration cues via a secure channel to enable setup and testing. The process is sketched on the next page (Figure 3.1).

Any eligible entity joining is required to supply:

- Letter of authority to join on behalf of the organisation;
- Details of the realm(s) that will be administered;
- A nominated technical contact address within each of the realms listed;
- Details of the top level RADIUS server(s) involved (hostname, IP address and ports used);
- Invoicing details for subscription;
- Signed copy of the govroam terms and conditions;
- A secure email account (S-MIME, GPG etc.) for exchange of shared secrets etc.

The only personal data that JSL processes in association with the delivery of govroam are the contact details for technical and finance issues for each participating entity. These are only exchanged over secure email or an out of band channel following verification of identities of the corresponding parties.



3.1.1.1 Free Trial

An organisation or federation can trial the technical boarding process. They are required to provide the same technical information as for the full on-boarding process outlined above. The participant is then configured to the roaming-beta server and provided with shared secrets and test credentials.

The trial process allows participants to test both outgoing and incoming authentications.
If the participant decides to process with govroam, the configuration is moved to the live servers and the setup process begins again.
The trial does not support roaming: end-users will not be able to use the service from other sites, nor can the participating organisation support visitors.

3.1.2 Off-boarding

JSL requires thirty (30) working days prior written notice to off-board an individual organisation participant. However, if that organisation is a regional federation operator (RFO), we request that sufficient notice is provided for the other members of that regional federation to appoint a new RFO or make alternative arrangements to continue their membership of govroam. During this notice period, the departing entity is encouraged to use the self-service portal tools to recover any roaming data they may require relating to the realm(s) they administer.

The mechanism of off-boarding itself is simply for the Jisc-operated national RADIUS proxies to be configured to no longer process the realm(s) in question, and to remove the shared secret(s) relating to the off-boarding server(s). At this point, all end users of the departing entity will no longer be able to authenticate at govroam participating venues, and visitors to the guest network(s) of the departing entity will no longer be able to gain access using their govroam credentials.

On completion of off-boarding, JSL will inform the remaining members of govroam that the organisation concerned is no longer a member, and remove references to the organisation from online materials. The departing entity is required to cease to hold itself out as being a member of govroam, inform its end users that its membership has ceased, and to remove all instances of the govroam logo from its materials.

3.2 Service Management Details

3.2.1 Technical Boundary

As a solution aimed at promoting free roaming across the public sector, there is a sense in which it is a boundary-less solution.

However, the end-to-end service is delivered in collaboration between Jisc, the home organisation, and the visited organisation.

3.2.2 Personal Data and GDPR

Jisc holds personal data for nominated contacts, for the purposes of technical and invoicing information. Outside of this, Jisc has access to no personal data in association with the delivery of the govroam service.

However, taking an end-to-end view of govroam participant sites do act as data controllers for personal data, though this is for user data that they already normally control. End-to-end encryption ensures that user credentials are only accessible to their home organisation.
The following table sets out the boundaries relevant to data protection.

Table 3.1: Personal data by organisation

Organisation:	Home organisation	Jisc	Visited organisation
Data Protection Issues:	Can map credentials/ certificates to personal identities as operate the IdP (and holds all the usual HR data on their staff); Holds RADIUS logs that identify location of roaming (to the realm level), plus time(s) of access.	Holds technical and invoicing contact details.	Can map IP address issued to a pseudonymous ID – this ID can be reconciled to a personal identity by cooperation with the home site; Pseudonymous ID is persistent, so can track visitor sessions as arising from the same individual.

3.2.3 RADIUS proxying

The trust fabric of govroam is built upon a network of RADIUS servers that use their standards-based proxying capability to route authentication requests with encrypted payloads between the visited site and the home site. Each of these servers is potentially operated by a different managing organisation. The following authentication 'journey' illustrates the various RADIUS management domains crossed in a typical authentication process:

1. Visited site RADIUS: examines anonymous outer identity on the Access-Request to extract home realm information; recognising that the realm does not correspond to a local user, the request is proxied up the hierarchy to the regional federation operator RADIUS server.
2. RFO RADIUS: the regional aggregating server again reads realm data from the anonymous outer identity. If the realm corresponds to another member of its regional federation, it proxies the request direct to the home organisation; if it doesn't recognise the realm data, it proxies the request further up the hierarchy to the Jisc national servers.
3. The National RADIUS Proxy: Jisc's core systems have trust relationships with all the top level RFO RADIUS servers and know which realms they manage. It also examines the outer identity for realm data; if this is not recognised at this national level, the request is dropped because the realm is not a member of govroam; if it is recognised, the request is proxied to the RFO server responsible, and it in turn proxies it on the specified home organisation.
4. Following un-encryption and processing at the home site RADIUS server, the response is encrypted and returns over the same RADIUS tunnel path through the various servers.

3.3 Service Constraints

3.3.1 Planned Maintenance

Scheduled maintenance is under the control of Jisc, and will be announced at least 7 days in advance and will be scheduled into the next available maintenance window.

Updates are, wherever possible, scheduled on Tuesday mornings between 8:00-10:00 am.
The Janet Cloud Connect service will follow ITIL request fulfilment process to manage service requests.

3.3.2 Emergency Maintenance

Unscheduled maintenance, which is only undertaken in an emergency, of the govroam central service, as well as the other servers and services under control of Jisc, will be announced as early as possible.

Major incidents are reported on the Jisc website, and via a dedicated Twitter feed (https://twitter.com/jiscmi).

3.4 Training

Govroam service subscribers have access to business-to-business level telephone and email support. This is primarily aimed at resolving service issues, but we will endeavour to assist in all roaming related enquiries. Where it is anticipated that the scope of the assistance required exceeds that available under the remit of the support line function, JSL will quote for consultancy to address the task against our rate card.

Jisc is also an accredited training organisation, and a variety of training options are available to govroam participants.

3.5 Invoicing Process

See govroam terms and conditions document.

3.6 Termination Terms

See govroam terms and conditions document.

3.7 Government Policy Alignment/Compliance

3.7.1 ICT Greening Policy Compliance

A number of features of the service are well aligned with the government's green policy goals:

- By bringing powerful new functionality to existing investments in wireless and wired LAN infrastructure, govroam extends the working life of this hardware;
- The govroam core services are lightweight without compromising resilience, and virtualised, thus minimising their power and cooling requirements;
- By fostering collaboration, govroam promotes re-use and sharing of resources between public sector organisations;
- Govroam functionality adds additional value to ICT re-use and sharing initiatives already in place such as PSN and Cloud;
- A single national standard for roaming removes duplication and incompatibility between local solutions;
- Ubiquitous connectivity through govroam allows easy access to centrally-held resources, thus reducing the need to print hard copies of documents;

3.7.2 ICT Strategy Policy Compliance

The govroam initiative is explicitly aligned with many of the goals of the government's ICT policy:

- Govroam seeks to increase the efficiency of public service delivery by encouraging collaboration and supporting a mobile workforce;

- Govroam provides a single national standard for federated roaming implementation, and the Jisc service is a single common infrastructure to support this activity;
- The service is built upon proven open standards, re-uses existing network infrastructure of participant organisations, and its software components at the customer end can all be deployed using best-of-breed free open-source offerings;
- Through its impact on the processes of estate rationalisation and facilitating appropriate mobile working, govroam contributes to the attainment of sustainability and greening targets;
- The govroam authentication process attains a high level of information security, and the appropriate level of subsequent transaction security is in the control of the end user, making use of appropriate application-level options such as SSL and IPSEC- VPN;
- The govroam initiative in the UK is compatible with parallel developments across Europe, and ready to join a pan-European interfederation should the stakeholders elect to do so in future;
- The govroam model represents technology transfer of techniques developed using public funds in the education sector and proven over many years.

3.7.3 Website Accessibility and the Equality Act (W3C Compliance)

The govroam service does not provide any customer interfaces, and end users interact only with the supplicant functions of their device's operating system, which typically provides a suite of accessibility tools to support such use.

The govroam companion app inherits the accessibility tools built in to its host operating system (iOS and Android).

3.7.4 EU Cookie Directive

The govroam service itself does not have a web interface. The service roadmap includes future provision of a customer portal for administration and reporting; cookies associated with this new feature will follow Jisc existing policy, compliant with the EU Cookie directive, which is viewable at: https://community.jisc.ac.uk/library/janet-policies/janet-cookies.

Return to introduction.

4. About Our Company and Our Services

In this section you will find details about our company and what we do.

4.1 About Jisc

Jisc is a registered charity working on behalf of UK higher education, further education and skills to champion the use of digital technologies.

Our vision is for the UK to be the most digitally-advanced higher education, further education and research nation in the world. We provide UK universities and colleges with shared digital infrastructure and services, such as the superfast Janet network. We also offer expert and trusted advice on digital technology for education and research, built from over 30 years' experience.

Many of our innovative services developed for education and research have potential benefits in the wider public sector.

4.2 Why Choose Us?

Through the value, savings and efficiencies we offer the education sector, Jisc saves each university on the order of £1M-£5M each year. As a trusted, neutral third party, we can take a standardising approach on a national scale rather than focusing on short-term local solutions. JSL now aims to bring those values to the wider public sector.

4.3 Why Choose Our Services?

Jisc's delivery of govroam builds on our extensive experience managing eduroam, the federated roaming service for UK education which forms part of the eduroam global federation. Eduroam has been deployed by 95% of higher education and 45% of further education organisations in the UK, facilitating roaming connectivity across these sectors. Jisc provides eduroam within the scope of our ISO9001 and ISO27001 certificates, supported by nationally respected Operations and Network Security teams. We aim to translate eduroam's success to the wider public sector.

Govroam allows you to get more from your existing investment in wireless LAN, reducing the overheads of offering and supporting visitor connectivity whilst increasing the reassurance that those visitors are actively sponsored by the organisations they claim affiliation to. It also facilitates your mobile workforce in obtaining connectivity when roaming, increasing their productivity and allowing the business to exert real time control on usage of such facilities.

Govroam offers the highest quality of service, as evidenced by the sustained success of its eduroam predecessor. The cost to participate is low, particularly in light of the significant cashable benefits it unlocks. The technological building blocks of the service are individually proven, established foundations of the modern internet, combined in an innovative way to deliver a unique service. The service itself drives positive cultural change, enabling approaches that favour collaboration and resource sharing. The end user experience is simple and accessible, and once a profile is created on user devices, access to roaming connectivity is a zero-touch automated process. The service delivery is backed by teams that benefit from the eduroam heritage, able to get new customers set up within hours, and provide an excellent level of after-sales and technical assistance.

Return to introduction.

5. References

Eduroam	http://www.eduroam.org
eduroam Database	http://monitor.eduroam.org/database
IEEE 802.1X	http://www.ieee802.org
eduroam Monitoring	http://monitor.eduroam.org/
eduroam TTS	http://tts.eduroam.org

Return to introduction.

6. Glossary

AAA	Authentication, Authorisation and Accounting
AES	Advanced Encryption Standard
AH	Authentication Headers
CERT	Computer Emergency Response Team
DNS	Domain Name Server
EAP	Extensible Authentication Protocol
EAP-TLS	Extensible Authentication Protocol Transport Layer Security (StB IETF)
eduroam	EDUcation ROAMing
ESP	Encapsulating Security Payloads
FTP	File Transfer Protocol
GPS	Global Positioning System
gTLD	generic Top Level Domain
HI	Home Organisation
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
IdP	Identity Provider
IKE	Internet Key Exchange
IPSec	IP Security (StB IETF)
MAC	Media Access Control
NAS	Network Access Servers
NAT	Network Address Translation
NRPS	National RADIUS Proxy Servers
NTP	Network Time Protocol
PPTP	Point-to-Point Tunneling Protocol
RADIUS	Remote Authentication Dial-In User Service (StB IETF)
RFO	Regional Federation Operator
RI	Remote Organisation
RRPS	Regional RADIUS Proxy Servers
SNTP	Simple NTP
SSH	Secure Shell
TCP	Transmission Control Protocol
TLD	Top-Level Domain
TLS	Transport Layer Security
TTS	Trouble Ticketing System
UDP	User Datagram Protocol
Venue	A site or building at which the govroam SSID is available
VLAN	Virtual Local Area Network
WPA2	Wi-Fi Protected Access, version 2

Return to introduction.

7. Appendices

7.1 Appendix A: Logging of Authentication and Accounting Packets

Authenticating a user and the subsequent establishing of the user session is a transaction between the identity provider and the resource provider. The intermediate infrastructure acts only as conveyor of their data. As such, no liabilities for the confederation members or the Jisc Operations Team are involved. Still, logging this data provides an audit trail that may help connected organisations resolve conflicts. Furthermore, the data is useful if debugging a problem is required. Because of that, it is recommended that govroam members, and the federation infrastructure itself, keep logs of the data flowing through the infrastructure. National regulations will inform time frames for data retention.

7.2 Appendix B: Web-redirect Systems

Govroam implements the IEEE 802.1X protocol, creating secure channels for authentication to the users' home organisation, and when the user is visiting other organisation (potentially including abroad).

Govroam securely provides roaming connectivity to the public sector. The network must be restricted to this community in order to keep the level of trust between participating organisations sufficiently high.

The advantage of the IEEE 802.1X protocol is that the user is authenticated before they are handed an IP address and then, in turn, can connect to the Internet. This method ensures that no users can harm the local network installations before being authenticated.

This is unlike web-redirect systems, where the (unknown) user is initially given an IP address in order to authenticate using a web browser. Not only will the user be able to interfere with the network before getting authenticated, but also the authentication session is not secure, since the username and password are traversing the underlying (RADIUS) infrastructure unencrypted. Furthermore, there is no easy way of telling if a web login page is genuine or a ‘rogue’. Fake web login pages can easily be set up by copying the original HTML code and assets to a web server, which then grants the user Internet access and collects user credentials.

Finally, even after being authenticated with web-redirects, there is no security context established for the wireless connection that prevents malicious users from taking over the session of a valid user (“session hijacking”).

7.3 Appendix C: Best Practice Codes of Conduct

This Code of Practice is a MoSCoW prioritised list of considerations that together constitute a best practice guide for deploying govroam infrastructure. Jisc has developed this code in partnership with an independent third party security specialist to ensure that it offers the very best objective advice to the govroam membership.

Regional Federation Operators (RFOs) are required to complete and return this checklist as part of their boarding process, and are expected to comply with (or at least be working towards) all of the mandatory requirements (MUST/MUST NOT) listed below, and hopefully many of the SHOULD/SHOULD NOT’s too.

The quality and consistency of the RADIUS deployment at all participating organisations is a vital part of the overall security model of the govroam service, as a misconfigured server may generate service-disrupting traffic or serve as an attack route against the service or your users. RFOs are strongly recommended to use this document as part of their own process in bringing member organisations into the RADIUS trust fabric of their own regional federations.

Customers must indicate their status at each point, specifying if it's in place, planned, an alternative solution has been implemented or if it is not planned at all. If it is planned, please give an indication of timescales. If an alternative solution is in place, please give details on the alternative solution.

No.	Subject	Control	Detail
1 Network Security			
1.1	Firewall Placement	A layer 4 firewall which separates the Internet facing Radius server from the Internet and internal network MUST be in place.	Network access between external, internal and DMZ assets must all be controlled and monitored to ensure only necessary traffic is permitted.
1.2	Server and network device administration	Administration MUST be performed over a private, internal network.	This prevents external attacks against the administration interfaces.
1.3	DMZ Connectivity	Connectivity to servers using known risky protocols MUST be risk assessed.	Protocols such as SMB and RDP may present security risks and must be heavily locked down or blocked.
1.4	Radius Network Port Access	The open ports on public interfaces MUST be restricted to only those ports required for authentication.	For most instances these will be UDP port 1812, status-server port 18121, and/or TCP port 2083 if RadSec is in use. Radius servers MUST NOT be configured to listen on UDP/1645.
1.5	Radius Network Port Access	The open ports on internal interfaces MUST be restricted to only ports required for administration functions.	Ideally this will be locked down to RDP (TCP port 3389) or SSH (TCP port 22). Only permit administration services that are essential.
1.6	RadSec (RADIUS over TCP/TLS)	If Radsec is used, X.509 certificates MUST be used to identify RADIUS servers.	More information in "Govroam Technical Specification" Section 2.1.1
1.7	ICMP from govroam	Firewalls MUST permit ICMP requests inbound from NRPS and govroam Portal to ORPS, and subsequent replies.	Govroam must be able to ping the organisation's RADIUS servers.
1.8	User Segmentation	Network segmentation SHOULD be considered, so that roaming users, once	Visiting users should not be automatically attached to the same network as local organisation users;

		connected, are placed into the correct segment with appropriate access to internal and external resources.	instead they should be connected to a special segment. Connections back to the guest's home network should be handled by their own systems (most likely through a VPN).
1.9	VLAN spoofing	The visitor network fabric SHOULD prevent devices from maliciously placing themselves onto unauthorised VLANs	Devices should be prevented from manipulating DHCP or VLAN assignments such that they could move onto unauthorised networks.
1.10	Internet Facing Vulnerability Assessment	Customers SHOULD perform a technical vulnerability assessment of Internet-facing estate.	It is important to test what vulnerabilities may be present when exposing the RADIUS server to the Internet.
1.11	Internal DMZ Vulnerability Assessment	Customers SHOULD perform a technical vulnerability assessment from inside the DMZ to the internal network if a DMZ is used.	It is important to test what vulnerabilities may be present when exposing the Radius and CA server to the internal network.
1.12	Visitor Traffic Interception	Participants MUST NOT deploy interception technology that would provide monitoring of visitor traffic.	Transport Layer Security (TLS) / Secure Sockets Layer (SSL) interception proxies MUST NOT be used against govroam visitors.
1.13	Guest Wi-Fi	In addition to offering a govroam service for roaming visitors, an organisation may also offer a facility for non-govroam 'guest' users. Customers SHOULD separate govroam/internal users from such guest users.	Guest Wi-Fi users should be provisioned onto a separate network with appropriate monitoring, control and authentication. Consideration should be given for preventing users operating on the guest network from circumventing organisational security controls.
1.14	Audit trail	Customers MUST ensure that they retain the records required in the govroam service definition to ensure that there is a complete audit trail for authentications and associated devices.	Ensuring an audit trail will help to identify any users misusing the network. Such identification may require reconciling logs between Jisc, the home organisation and the visited organisation.
1.15	Credentials	Credentials SHOULD NOT be shared between users (or between devices where device authentication is used).	Credentials limited to a per user or device prevents access using stolen credentials. A single user credential may be used across

			multiple devices that the user controls, or in BYOD scenarios.
2. Physical Security			
2.1	Wi-Fi Access Points and Cabling	Wi-Fi Access points and network cabling SHOULD be secured as much as possible.	Securing hardware will prevent physical attacks such as the introduction of network taps.
2.2	Servers	All hosts and network equipment MUST be located in a secure environment. Physical access to servers is almost guaranteed to result in compromise and so they must be secured at all times.	A locked server cabinet in a locked room, with administrator-only access is ideal.
3. Server Deployment			
3.1	Redundant RADIUS Servers	Govroam RADIUS servers SHOULD be deployed in a redundant, diverse configuration to minimize the risk of loss of availability.	If a user is not able to connect to their home RADIUS server due to it being offline they will not be able to authenticate and so not be allowed network access. RFOs are required to meet SLAs with Jisc for server availability.
3.2	Dedicated Server	The physical or virtual server used to host the govroam RADIUS function SHOULD be dedicated to the task.	Limited functionality on the server reduces the attack surface.
3.3	Server Hardening	All servers used within the govroam architecture MUST be hardened to appropriate standards before being deployed.	Either NIST or CIS standards are recommended: https://nvd.nist.gov/ncp/repository https://www.cisecurity.org/. This requirement includes any secondary or backup servers whether they are active online or kept offline until required.
3.4	Patch Management	All server operating systems and applications MUST be kept fully patched and up-to-date.	This includes any secondary or backup servers whether they are active online or kept offline until required.
4 Server Monitoring and Logging			
4.1	Monitoring	Monitoring and alerting MUST be enabled to detect attacks such as password brute forcing.	Servers must be configured to detect and log rogue behaviour in both the operating system and the applications. Some automated defence may also be possible (e.g.

			increasing back-off times between multiple failed password attempts)
4.2	Alerting	Alerts MUST be sent to appropriate staff to be acted on. Regular tests should be carried out to ensure alerts are being delivered as expected.	Servers must be configured to send logs and alerts to system administrators in order to detect incidents and attacks in real time.
4.3	Authentication Logging	Logging of all authentication attempts MUST be enabled	More information is available in the "Govroam Technical Specification", section 18. Note that authentication logs may contain personally identifiable data, and that storage and processing of this must be handled in a GDPR-compliant fashion.
4.4	Authentication Log Times	All authentication logs MUST be time-stamped in UTC (see 3.5).	Govroam requires consistent log formats within the UK time zone.
4.5	Authentication Log Retention	All authentication logs MUST be kept for a minimum of 3 months Govroam requires logs be kept for a minimum of 3 months for auditing purposes.	Wider regulatory compliance such as GDPR must be adhered to.
5 User Education			
5.1	User education	Users SHOULD be trained how a legitimate govroam access point behaves. If they see deviation from that they should know not to connect and who to contact.	If users can be tricked into connecting to fake services then they may reveal sensitive information. Any training which will help prevent this is encouraged. Instructional posters are a useful aid.
5.2	Govroam User Expectations	Organisations MUST educate their users to know how the govroam service should behave.	A govroam user should be prepared e.g. not to click ignore when warned of certificate mismatches, not to enter their govroam credentials into web forms etc.
5.3	Govroam Visitor Expectations	Organisations MUST minimize any possibility of confusion between the govroam service and any other guest facility they offer.	Visited organisations must ensure that is not possible for a non-govroam service to be mistaken by visitors for the participant's govroam service.

5.4	Govroam Service Information	Participants MUST publish a govroam service information website.	Such websites must be generally accessible from the Internet and, if applicable, within the organisation to allow visitors to access it easily on site. More information available in "Govroam Tech Spec" document.
5.5	Security contact	Users MUST have an obvious point of contact at their home organization in case of account compromise or loss/theft of devices.	The point of contact must be able to disable accounts and/or to revoke client-side certificates if applicable.
5.6	Support contact	Organisations MUST ensure there's an advertised support infrastructure both for their own users when roaming, and for second line support requests originating from visited organisations or Jisc.	The point of contact must be able reset/disable accounts and assist Jisc/other organisations to identify and fix issues arising.
6 Certificate Authority (CA)			
6.1	Public vs Private Certificates	Organisations MUST undertake a risk based selection of Private vs Public Certificate Authorities. Private is usually preferable and most commonly used.	Pros and cons exist with the use of both private and public certificate authorities. Private CAs carry less chance of security issues. Only consider public CAs if every client will always be auto-configured by the CAT. Make a risk based decision to choose which is best for your organisation.
6.2	CA Server Location	CA server MUST be on a dedicated, locked down server with minimal user access	Compromise of a certificate authority would give an attacker the ability to set up a fake server to trap users. Revocation of the CA and issuing of new certificates is also likely to be a hard and expensive operation.
6.3	Certificate Server Name	The server name SHOULD be a fully qualified domain name (FQDN).	Some end-user device operating systems might (incorrectly) require the name to be parseable as a hostname; so it is a good idea to use a server name which parses as a fully-qualified domain name - the corresponding record does not have to exist in DNS though. The server name should then be both in certificate's Subject field (Common

			Name component) and be a subjectAltName:DNS as well.
7 RADIUS Server Configuration			
7.1	Shared Secret	The shared secret between clients and the RADIUS server MUST have sufficient entropy.	A password of at least 16 characters is required, including upper and lower alpha characters and numbers.
7.2	Do Not Reuse Secrets	Each Access Point <-> RADIUS server relationship MUST have a unique secret.	This limits the scope in case of compromise.
7.3	Disable PAP	Password Authentication Protocol (PAP) between Access Points and the RADIUS server MUST NOT be used.	If there are any proxies between the Access Point and the end server, each proxy must decrypt the PAP password and then reencrypt it with the key for the next hop. This leaves the system vulnerable to password sniffing if a proxy is compromised.
7.4	Disable SPAP	Customers MUST disable the Shiva Password Authentication Protocol.	SPAP passwords are sent in a reversibly encrypted format making the protocol weak and open to interception. Link.
7.5	Disable MS-CHAP	Customers MUST disable Challenge Handshake Authentication Protocol (CHAP).	MS-CHAP (version 1) is considered a weak protocol and must not be used.
7.6	Enable the Message-Authentic-ator attribute	The Message-Authenticator attribute MUST be enabled (where supported).	The Message Authenticator helps to prevent fake message injection through IP spoofing. http://www.networksorcery.com/enp/rfc/rfc3579.txt https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc753271(v=ws.10)
7.7	Encrypt Communicat-ions	Customers SHOULD use a VPN to protect communications between Access Points and the RADIUS server.	For more information see: Link.
7.8	EAP Types	Customers SHOULD use at least one of the following EAP types: TLS, TTLS, EAP-FAST, PEAP	Information about EAP types: https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol.
7.9	Anonymous Outer Identities	Where supported by the EAP type and supplicants,	As not all supplicants support this it cannot be mandated however to add anonymity to the connection

		anonymous outer identities SHOULD be enabled.	this is highly recommended. https://wiki.geant.org/display/H2eduroam/eap-types.
7.10	Enable Chargeable User Identity	Chargeable User Identity (CUI) SHOULD be implemented to ensure users can be traced through the system for accountability purposes.	Enabling this from the outset will greatly enhance accountability which may help with adoption and troubleshooting, especially during early stages of the roll out. CUI use is highly recommended.
7.11	RADIUS Accounting	Radius accounting messages MUST NOT be forwarded to the govroam National RADIUS Proxy Servers (NRPS).	The govroam National RADIUS Proxy Servers (NRPS) do not require visibility of the potentially sensitive information stored within RADIUS accounting messages.
7.12	VLAN Attributes	Dynamic VLAN attributes SHOULD NOT be sent in Access-Accept replies to NRPS	Where an authentication request is received from the NRPS, as opposed to being received from an internal RADIUS client or NAS, a Home organisation's AccessAccept reply should not contain dynamic VLAN assignment attributes, unless a mutual agreement is in place with the Visited organization concerned. This may be achieved by the Home organisation filtering out dynamic VLAN assignment attributes if present in Access-Accept packets sent to the NRPS.
7.13	Specify the Operator-Name	Organisations SHOULD configure their ORPS to insert the OperatorName attribute, accurately composed for their realm, into all Access-Request packets forwarded to a RRPS or NRPS.	Configuring an ORPS to add Operator-Name, with a value set to the domain of the local site, means that all proxies in the chain can easily identify the source of the request. This could be invaluable for audit and security.
8 Device Compliance			
8.1	Automated Configuration	Wherever possible, the govroam "Configuration Assistant Tool" (CAT) SHOULD be used to assist with client deployments.	See https://cat.govroam.uk/. The CAT tool eliminates the risk of accidental misconfiguration and ensures consistent set up across your userbase.
8.2	Manual (non-CAT) configuration	When CAT is not used, the deployment of configuration details to the users SHOULD be done in a prescribed and secure way.	Deployment should be performed by an administrator (not the end user) using a trusted management network. Non-CAT deployments are not recommended.

8.3	Certificate revocation	If an EAP type which uses client side certificates is used (e.g. EAPTLS), a revocation process SHOULD be put in place.	This will cover devices which are lost, stolen or compromised.
8.4	Deployment Speed	Govroam clients SHOULD be deployed within a short window of time.	When deploying govroam to a user base, e.g. with govroam CAT, any unenrolled users may attempt to self-enroll through manual configuration. Self-enrolment is not advisable. A quick roll out of govroam to all users should prevent users trying to self enroll.
9 WI-FI Access Points			
9.1	WPA2-CCMP (AES)	Govroam Visited Wi-Fi services MUST implement WPA2 Enterprise with the use of the CCMP (AES) algorithm.	More information in "Govroam Technical Specification" Section 4.10
9.2	WPA-TKIP	The WPA specification MUST NOT be supported and the TKIP algorithm MUST NOT be employed in govroam services.	More information in "Govroam Technical Specification" Section 4.10
9.3	Rogue AP detection	Customers SHOULD monitor for rogue access points.	A rogue wireless access point is an unauthorised access point that has been installed on the network. Attackers will use rogue access points to trick users into exposing their data and credentials. Tools and processes should be implemented to actively monitor the Wi-Fi network for rogue devices to ensure these are removed.
9.4	Wireless IPS	Customers SHOULD implement Wi-Fi Intrusion Prevention Systems	Wi-Fi Intrusion Prevention Systems can detect more advanced attack techniques such as AP spoofing, malicious broadcasts, and packet floods.
9.5	Use of "govroam" SSID	Customer MUST only use the "govroam" SSID for compliant networks	Other Wi-Fi networks that do not utilise govroam or comply with its standards must not be named "govroam" or by a name that could potentially be confused or associated with govroam.

9.6	Dedicated use of "govroam" SSID	The "govroam" SSID network MUST NOT be shared with any other network	The "govroam" SSID network must be exclusive to providing govroam services.
9.7	Wi-Fi services on non-IEEE 802.11 protocols.	Wi-Fi services MUST only be provided on IEEE 802.11	Other wireless technologies such as Bluetooth are not permitted.
10 Ports and Protocols			
10.1	Default deny policy	Providers SHOULD operate all firewalls and access control lists against a default deny policy, only allowing specific traffic types that are required to pass.	It is better to consciously grant access to useful traffic than to reactively attempt to block traffic that you find is causing a problem.
10.2	Govroam network access control	Providers MUST allow roaming govroam users access to the minimum standard ports and protocols specified in the govroam tech spec.	User need to be able to predict what services (email, web, VPN) will work over govroam when they arrive at a new venue.

Return to introduction.