Govroam service definition

Version 4

1 Executive Summary

Govroam is a secure national roaming service for members of the UK public sector. Govroam is based on a set of defined organisational and technical requirements that each participant member must agree to (by signing and following the govroam policy declaration).

The govroam service is managed by the Jisc Operations Team (JOT). The JOT carries out the day-to-day operations of govroam.

This document describes the govroam service. It contains:

- A general overview of the service, including its aims, its elements, and security model;
- A descriptive breakdown of the service into service elements, users, and operations;
- A breakdown of the govroam service organisation;
- A description of the operational requirements required of govroam members.

Date of Issue: 12 December 2017

Document Code: gov/001.4

Author: Mark O'Leary

Based on the eduroam Service Definition OD/MO/JRS/DOC/001

Description: Govroam Policy Service Definition

1 Executive Summary 1

2 Introduction 5

3 Service Elements 6
3.1 Technology Infrastructure 6
3.1.1 Hierarchical Routing Model 6
3.1.2 National RADIUS Proxy Servers (NRPS) 7
3.1.3 Regional-level RADIUS Proxy Server (RRPS) 7
3.1.4 Govroam Identity Providers (IdPs) 7
3.1.5 Govroam Service Providers (SPs) 8
3.1.6 Network Access Elements 8
3.2 Supporting Infrastructure 9
3.2.1 The govroam CAT 9
3.2.2 Monitoring, Diagnostics and Metering 9
3.2.3 Govroam Website 9
3.2.4 Govroam Wiki 9
3.2.5 Trouble Ticketing System (TTS) 10
3.2.6 The govroam companion app 10
3.2.7 Mailing Lists 10

4 Users 10
4.1 End Users 10
4.2 Administrative Personnel 11
4.2.1 Regional-level Personnel 11
4.2.2 Organisation-level Personnel 11
4.3 Govroam User Summary 12

5 Service Organisation 13
5.1 Roles and Responsibilities 13
5.1.1 Regional federation operators (RFOs) 13
5.1.2 Technical Working Group (TWG) 14
5.1.3 Jisc Operations Team (JOT) 14
5.1.4 Service Level Definition 14

5.1.5 SLAs 14

6 Service Operation 15
6.1 User Support Processes 15
6.1.1 Support for End Users 15
6.1.2 Administrative Personnel 16
6.1.3 Problem Escalation Scenarios 16
6.2 Maintenance Procedures 18
6.2.1 Scheduled Maintenance 18
6.2.2 Unscheduled Maintenance 18
6.3 Security Incidents 18
6.4 Policy Violation 18
6.5 Malfunction 19
6.5.1 RADIUS Attribute Monitoring 19
6.6 Handling Membership 19
6.7 Service Reports 20

7 Govroam Member Requirements 20
7.1 Policy Declaration 20
7.2 Operational Requirements for Govroam Federation Members 21
7.2.1 General Requirements for Federation Members 21
7.2.2 Govroam Security Requirements 21
7.3 Technical Requirements for Govroam Members 21
7.3.1 Specifications and Operational Requirements: Regional Federation Level 22
7.3.2 Specifications and Operational Requirements: Identity Providers 23
7.3.3 Specifications and Operational Requirements: Service Providers 24
7.3.4 Specifications and Operational Requirements: End-user Devices 26

8 Liability and Branding 26
8.1 Liability 26
8.2 Branding 27

9 References 28

10 Appendix A: End-to-end Encryption of User Credentials 31

11 Appendix B: Logging of Authentication and Accounting Packets 32

12 Appendix C: Web-redirect Systems.....33

2 Introduction

Govroam allows users from participating public sector organisations to gain secure Internet access at any govroam-enabled organisation. The architecture that enables this is based on a number of technologies and agreements, which together provide the govroam user experience: "open your laptop and be online".

The basic principle underpinning the security of govroam is that the authentication of a user is carried out at either his/her home organisation or an identity provider under contract to that organisation, using the organisation's specific authentication method via a robustly encrypted network tunnel. The authorisation required to allow access to local network resources is carried out by the visited network.

The govroam service provides this facility as a federated service, built hierarchically. At the top level sits the national RADIUS proxy service (NRPS), which primarily provides the central infrastructure required to grant network access to all participating members of the govroam service at any time. This national federated service is built upon a combination of both regional[1] roaming federations, operated by regional roaming federation operators (RFOs: in most cases, PSNs for example) that aggregate a local hierarchical RADIUS infrastructure under a single regional RADIUS proxy server (RRPS). Where there is no regional arrangement in place, individual organisations wishing to participate may directly peer with the national proxies from their local organisation-level RADIUS proxy servers (ORPS).

A hierarchical system of Remote Authentication Dial-In User Service (RADIUS) servers is used to transport the authentication request of a user from the visited organisation to his/her home organisation or its nominated IdP, and return the authentication response. Typically, every organisation deploys a RADIUS server (ORPS), which, in turn, is connected to a local user database. This RADIUS server is connected (either directly, or indirectly via a RRPS) to the central, national RADIUS server (NRPS).

Where an organisation wishing to participate does not wish to manage an ORPS themselves or through commercial agreement, a central "home for the homeless" IdP and RADIUS server may in future be deployed through which users can self-register to obtain govroam credentials.

Govroam users have usernames in the format "*user@realm*" (where *realm* is the organisation's DNS domain name, often in the form of *organisation.TLD*, where TLD is the sector code, e.g. *gov.uk* or *nhs.net*). The various RADIUS servers of the govroam infrastructure can use this information to route the request through the hierarchy until the home organisation is reached.

Access points or switches use the IEEE 802.1X standard that encompasses the use of the Extensible Authentication Protocol (EAP). Using the appropriate EAP method either a secure tunnel from the user's device to his/her home organisation is established, through which the actual authentication information (username/password, certificate etc.) is carried (e.g. via EAP-TTLS or PEAP), or mutual authentication by public X.509 certificates is used (EAP-TLS). These three authentication

1 'Region' in this context may either be a geographical or an organisational demarcation: KentPSN is an RFO, as would be a single operator coordinating participation for all of the National Park authorities distributed around the UK.

methods[2] are able to establish a secure TLS session from the end-user device to its home authentication server so users' private credentials are not subject to eavesdropping by intermediate parties.

The federated govroam service encompasses all the necessary elements to provide a service to the users. Aside from the federation infrastructure itself, these elements include:

- Establishing trust between the member federations;
- Monitoring, diagnostic and metering facilities;
- Central data repository providing information about the govroam service (govroam database);
- Federation-level user support (i.e. support for member regions or directly-connected organisations).

These elements are described in more detail in the following sections.

3 Service Elements

This 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).

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, and as of April 2016, the following protocols exist: RADIUS/UDP, RADIUS/TCP, RADIUS/DTLS and RADIUS/TLS.

Govroam supports transport over RADIUS/UDP and RADIUS/TLS, and recommends the use of RADIUS/TLS. Routing of RADIUS messages is accomplished by a hierarchy of RADIUS servers.

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

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). See Figure 3.1.

2 Other EAP methods may be designed in the future which may depend on security mechanisms other than TLS exchange. Those methods may be used as long as they provide effective protection against eavesdropping for critical user data (such as passwords).

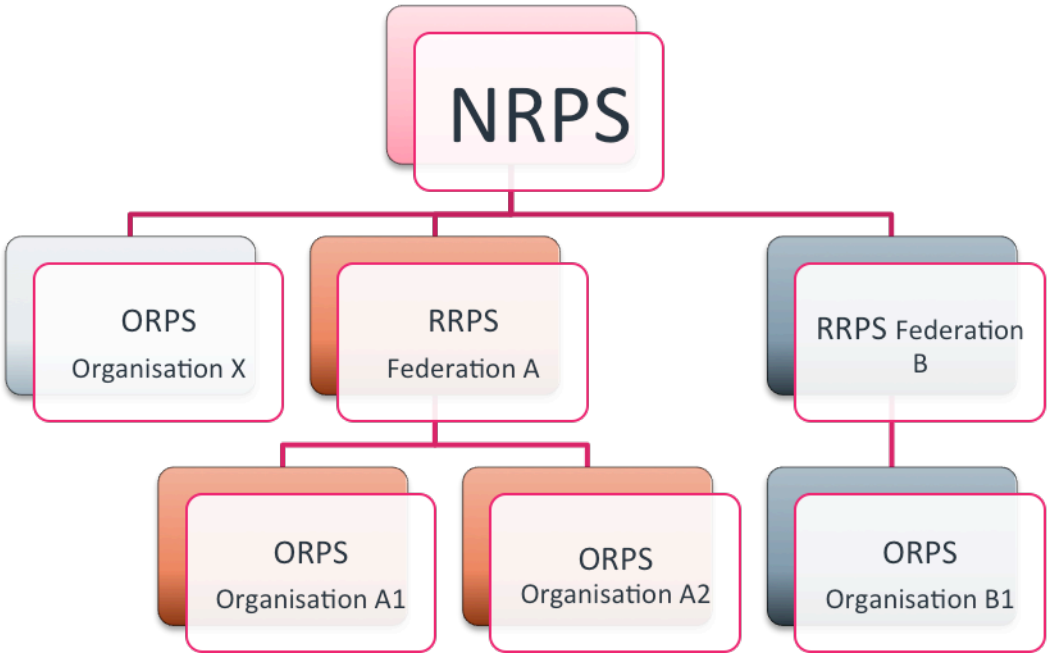

Figure 3.1: Current govroam federation structure

The govroam top-level RADIUS servers (NRPS) interconnect the participating govroam regional federations (RRPS) and individual directly connected 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.

3.1.2 National RADIUS Proxy Servers (NRPS)

The national RADIUS Proxy Servers (NRPS) for govroam in the UK are operated out of Jisc's Manchester office. Each server has a list of connected, regional- and organisational-level domains (.cambridge.cc, etc.) 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 domains that the servers are not responsible for will be dropped. At a later point, if govroam UK joins an international confederation of compatible govroam services, such requests will be passed up the hierarchy to the international top-level infrastructure.

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.

3.1.4 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.

3.1.5 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.

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

3.1.6 Network Access Elements

Govroam is not dependent on specific access technologies. Users of govroam can access the service either by wireless (the main focus of govroam at launch), or wired 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 device.

The elements mentioned above are described below.

3.1.6.1 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.

3.1.6.2 Access Points

Access points are only required for wireless access to the network.

Access points need to be IEEE 802.1X capable. They must also 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.

3.1.6.3 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.

3.2 Supporting Infrastructure

3.2.1 The govroam CAT

Govroam Configuration Assistance Tool (CAT) allows local govroam administrators to enter their govroam configuration details and, based on them, the govroam CAT builds customised installers for a number of popular platforms. End users can access these installers either from the CAT webpage or via a dedicated app.

An installer prepared for one organisation will not work for users of another one, therefore if your organisation is not on the list, you cannot use this system. Please contact your local administrators to discuss adding your organisation configuration to the govroam CAT.

The govroam CAT is run maintained by the JOT team and can be found at **https://cat.govroam.uk**

3.2.2 Monitoring, Diagnostics and Metering

The basic purposes of the govroam monitoring, diagnostics and metering service are:

- to test the functionality of the ORPS, RRPS, NRPS and the whole confederation infrastructure;
- to collect information about the authentication traffic from the NRPS.

The design of the monitoring and diagnostics element will allow implementation of different monitoring scenarios in order to test various operational aspects of the govroam service. It can also complement other (e.g. regional-level) monitoring services.

The planned govroam monitoring and diagnostics element will report the results of the tests, both as a colour-coded map and as graphs showing the response-time behaviour. An alert system is also implemented in order to inform responsible staff about any malfunctions in the core service as soon as they occur.

The Web Portal (available end of Q4 2017) will provide various information including govroam monitoring, diagnostics and reporting. Some of those details are public, while others are restricted to predefined user groups. The decision on the availability of the information lies with the Jisc Operations Team (JOT).

3.2.3 Govroam Website

The govroam website **www.jisc.ac.uk/govroam** is run and maintained by the JOT.

It is the central information point for govroam users, providing information and links for all user groups (see Section 4, Users).

3.2.4 Govroam Wiki

A wiki for the govroam service is available at **https://wiki.govroam.uk**. The information stored in the govroam wiki 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);
- Monitoring information;
- Information about the usage of the service.

Some wiki pages are public, while others are restricted to predefined user groups. The decision on the availability of the information lies with the JOT.

The govroam wiki is run and maintained by the JOT.

3.2.5 Trouble Ticketing System (TTS)

The JOT 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 **govroam@jisc.ac.uk** will create a new ticket; when replying to an existing ticket, please retain ticket reference text (e.g. (Ref:IN:12345678)) in the subject line. The TTS operates within an SLA of acknowledgement of receipt within 4 hours, resolution or substantial further action within 5 working days.

3.2.6 The govroam companion app

Jisc provides an app, available for iOS and Android, which documents the physical location of all govroam venues, and helps the user navigate to a specific venue if required.

The data that this app relies upon is entered via a geolocation tool by the admins of each regional federation, or their nominees (i.e. RFO staff can delegate this role to each member organisation). Credentials to access the geolocation tool are provided when an RFO completes registration.

3.2.7 Mailing Lists

The mailing list provided:

- Govroam general discussion list (***roaming@jiscmail.ac.uk***)
- Admin-only technical list (***govroam-technical@jiscmail.ac.uk***)

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

4 Users

This section describes the identified user categories and the way the govroam service elements are mapped to these categories. A summary of this mapping is provided in Section 3.4.

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. Broadly speaking, there are two types of end-users: the 'technology aware' and the 'technology unaware'. The former ("power users") will understand documentation on govroam and will understand how to configure their device(s) to use govroam. The latter ("consumers") require more assistance. In terms of the current service portfolio, no distinction is made between these two categories and, for now, they are addressed in the same way. It is recognised that

over time, a more refined distinction between end-user categories should be made, with corresponding refinement of the service portfolio mapping.

That said, the best practice recommendation is for all organisations to create a profile on the govroam CAT service, and to direct all of their users to configure their devices by downloading an automatically generated device-specific profile from the CAT, thus guaranteeing that their device profile is accurately configured.

The end user device profile is part of the overall security provision for the service, and participating organisations are responsible for ensuring it is set up correctly.

4.2 Administrative Personnel

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

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. Since a number of 'govroam prototypes' have already been running for some time (e.g. KentPSN et al.), it is expected that this group already have a high level of skill regarding operating a RADIUS server infrastructure.
- **Staff for trouble ticketing and handling user support:** The govroam trouble-ticketing system will have a federated structure. This means that at the regional federation level, there will be staff handling trouble tickets themselves, escalating tickets to the Jisc Operations Team, or delegating them to the affected organisations in their constituency. Since the various govroam prototypes in service do not include trouble ticket management, it will be useful to provide supporting material on how to work with the TTS.
- **Miscellaneous tasks:** These duties would include maintaining the regional federation entries via the geolocation tool so that they are available and up to date for the govroam companion app; creating and maintain a profile on the govroam CAT; maintaining a federation-level govroam web page; collating federation membership support contact detils and submitting them to the JOT; contributing to the govroam wiki; reporting; contracts; financials etc.

4.2.2 Organisation-level Personnel

- **Staff for ORPS and service operation:** Service operation on an organisation 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 JOT 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. Govroam JOT will provide basic materials in order to help them provide consistent and uniform service to the end users.
- **Miscellaneous tasks:** These duties might include maintaining the regional federation entries via the geolocation tool if delegated by the RFO; creating and maintain a profile on the govroam CAT; maintaining a federation-level govroam web page; collating federation membership support contact detils and submitting them to the JOT; contributing to the govroam wiki; reporting; contracts; financials etc.

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 elements	User Group		
	End user	**Organisation-level personnel**	**Federation-level personnel**
Basic monitoring facilities	Yes	Yes	Yes
Full monitoring and diagnostics facilities	No	Yes (limited to their respective inst.)	Yes
Public access to the govroam website	Yes	Yes	Yes
Access to the internal govroam website	No	Yes (limited to their respective inst.)	Yes
Public access to the govroam wiki	Yes	Yes	Yes
Access to the all information in the govroam wiki	No	Yes (limited to their respective inst.)	Yes
TTS	No	Yes	Yes
Govroam CAT	Yes (device config)	Yes (organisation profile creation)	Yes (organisation profile creation)
Geolocation tool	No	No (unless delegated by RFO)	Yes
JOT Mailing lists	No	No (Yes if no regional structure)	Yes
Support from JOT	No	No (Yes if no regional	Yes

	structure)

Table 4.1: Service elements

5 Service Organisation

The public sector roaming solution, govroam, is run by the JOT on behalf of its members. 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 Operations Team (JOT). The govroam service model is illustrated in Figure 5.1:

Figure 5.1: Govroam service model

5.1 Roles and Responsibilities

This section describes the specific roles and responsibilities, including those of the:

- Regional federation operators (RFOs);
- Technical working group (TWG);
- Jisc Operations Team (JOT).

5.1.1 Regional federation operators (RFOs)

The tasks of the RFO members include:

- Operating the RRPS for the region;
- Monitoring performance and availability of RADIUS infrastructure within the region;
- Assuring adherence to the govroam policy and contractual terms in their region;
- Provisioning of necessary support and information to the JOT;
- Provisioning of the second line support to roaming users within their constituency;
- Managing financial aspects of participation in the service;
- Monitoring and reporting on SLAs.

5.1.2 Technical Working Group (TWG)

The TWG manages the technical development of the govroam service. It works closely with the JOT and provides it with necessary input. The tasks of the TWG include:

- Developing technical policy;
- Formulating recommendations on monitoring and diagnostic tools, and supporting scripts that should be used in providing service;
- Providing input to the JOT to inform further policy development including recommendations related to establishing trust between members;
- Improving of govroam service definition and procedures;
- In the medium term, developing proposals for a 'phase II' govroam service with expanded scope.

5.1.3 Jisc Operations Team (JOT)

The JOT handles day-to-day operations. It is responsible for the smooth operation of the federated service. The tasks of JOT 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.
- The JOT also coordinates the operation of govroam in the UK, approves and develops its policies and budget plans, and handles membership matters.
- The JOT may, from time to time create a technical working groups. The tasks of the TWG are outlined in 5.1.2

5.1.4 Service Level Definition

The JOT is responsible for running the federation service. Therefore, the JOT maintains:

- Federation infrastructure (explained in Section 3.1);
- Monitoring and diagnostic facilities;
- Govroam wiki;
- Govroam website;
- Govroam CAT;
- Govroam companion app and associated geolocation tool;
- Govroam trouble ticketing system.

The goal for the availability of these services is 99.5%. The availability of each of the services listed above will be measured as the ratio between the accomplished and theoretically possible uptime of the respective servers, excluding scheduled maintenance. Proper monitoring tools will be used for that purpose and the results will be kept by the JOT.

5.1.5 SLAs

RFOs shall comply, and shall ensure that their members organisations comply, with the following incident reporting, escalation and resolution service levels:

Severity 1 Incident	Severity 2 Incident	Severity 3 Incident

	(Multiple RFO member organisations suffer complete loss of service)	(Individual RFO member organisation suffers complete loss of service)	(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

6 Service Operation

This section defines basic operational procedures for the govroam service.

The JOT will use the following communication tools:

- Mailing lists (see Section 3.2.5);
- Trouble Ticketing System (TTS);
- Govroam website;
- Govroam wiki;
- Face to face meetings and videoconferences (via the Jisc Vscene service).

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 prepare the user with the information and knowledge to use the govroam service before they roam. When they subsequently visit other organisations, it is up to the home organisation to provide the necessary user support to the roaming user.

RFOs and their member organisation are encouraged to provide some categories of user support to visiting users regarding the use of govroam service by providing information through signage and web.

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

6.1.1 Support for End Users

In normal circumstances an end user 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 JOT by the organisation-level personnel. **End users should never contact these functions directly.**

However, if established local arrangements are in place for the region, these may be used instead. Note, when users roam outside of the region, they will use the default govroam support model.

RFOs and their member organisation are encouraged to provide user support (via web documentation, signage etc) to visiting users.

6.1.2 Administrative Personnel

Regional Federation Operator-level Personnel:

- Work with regional member organisations to resolve support issues as required;
- Escalate problems to the JOT whenever the problem includes the federation service or deals with the basic govroam technology in accordance with the SLA's as described in section 5.1.5;

Organisation-level personnel:

- Resolve issues directly involving your staff when roaming off site;
- Work with the support function of visitor's home sites to resolve issues involving visitors;
- Escalate problems to the federation-level personnel when required in accordance with the SLA's as described in section 5.1.5;
- Contact the JOT whenever the problem includes the central federation service, but must also inform regional federation-level personnel.

6.1.3 Problem Escalation Scenarios

6.1.3.1 Problem Escalation Involving User and Organisation-level Personnel

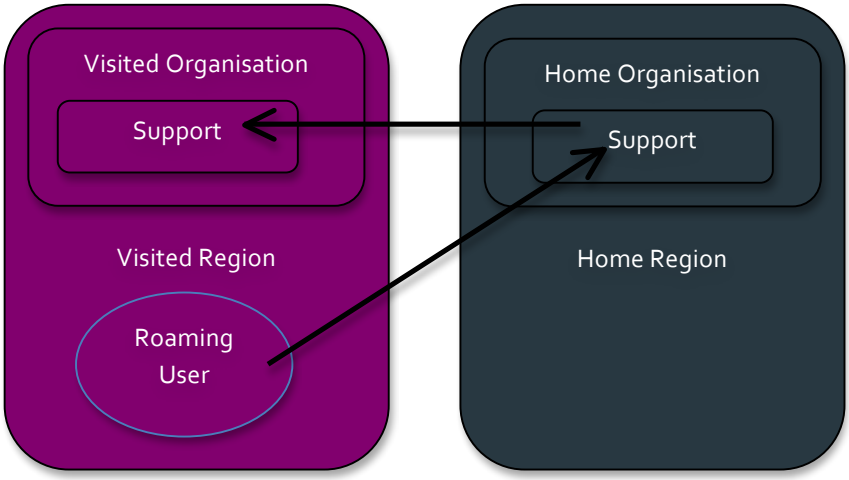

Figure 6.1: Problem escalation scenario, user and organisation personnel

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. 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 home organisation should inform the visiting user how to fix the problem.

6.1.3.2 Problem escalation involving user, organisation and regional federation-level personnel

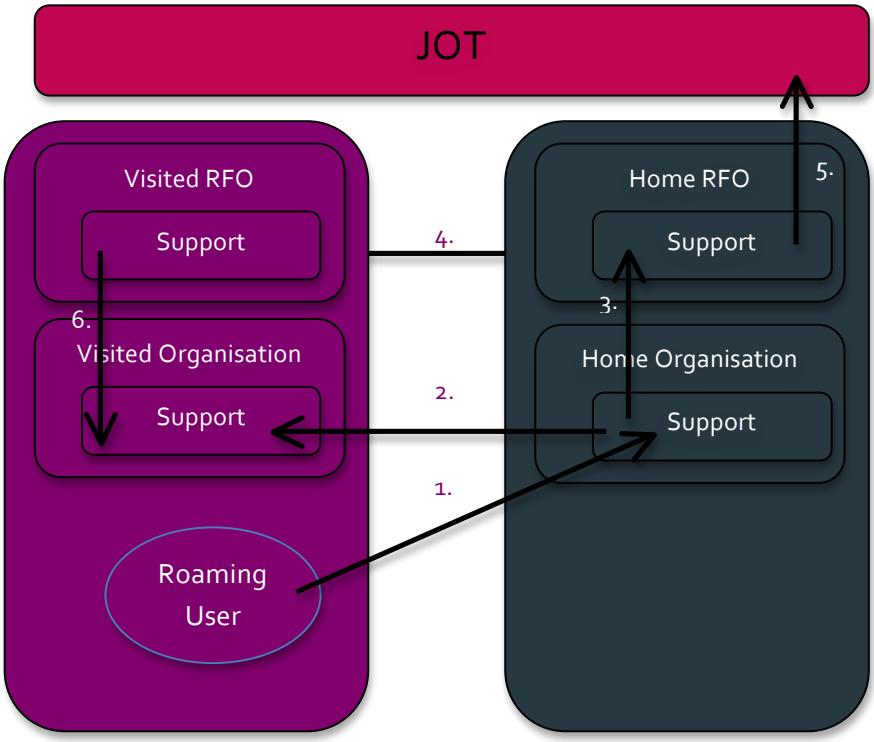

Figure 6.2: Problem escalation scenario, user, organisation and regional federation-level personnel

In this scenario, the user has a problem accessing the network while using the govroam service outside of his/her home regional federation, but 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 via the respective part of the govroam infrastructure. 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 JOT 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.

6.2 Maintenance Procedures

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

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 JOT, and must be announced at least seven (7) days in advance through the **govroam-technical@jiscmail.ac.uk** mailing list. Scheduled maintenance may be scheduled from Tuesday to Thursday, 06:00 – 08:00. A ticket on the TTS should be opened by the respective JOT member and closed with a short comment on the performed action.

Scheduled maintenance of infrastructure must be planned to avoid any break in the service.

Scheduled maintenance work performed by RFOs within their respective regions should be announced at least two (2) days in advance through the **govroam-technical@jiscmail.ac.uk** mailing list. A ticket on TTS should be opened by the respective RFO representative (i.e. by emailing **govroam@jisc.ac.uk**), and closed with a short comment on the performed action.

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 service malfunction.

Unscheduled maintenance of the govroam central infrastructure, as well as the other servers and services under control of the JOT, 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) through the **govroam-technical@jiscmail.ac.uk** mailing list. A ticket on TTS will be opened by the respective JOT 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) through the **govroam-technical@jiscmail.ac.uk** mailing list. A ticket on the TTS should be opened by the respective RFO representative (i.e. by emailing **govroam@jisc.ac.uk**), and closed with a short comment on the performed action.

6.3 Security Incidents

In the case of any security incidents, the JOT 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 wiki.

RFOs should regularly report to the JOT about the number and type of these incidents.

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

6.4 Policy Violation

In the case of a severe policy violation by a regional federation or individual organisation, the JOT will react in the following way:

- Record 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.

- If required, propose a temporary quarantine period during which the user or organisation involved would be blocked from further access to govroam (the length of the period, as well as the exact measures required are handled on a case-by-case basis). RFO's and home organisations affected by such a block will be informed.
- Should the issue not be resolved satisfactorily:
    - Propose a disqualification of the region/organisation from the federation.
    - Act upon the decision and announce membership termination.

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

6.5 Malfunction

Malfunction of the NRPS, as well as the other servers and services under control of the JOT, must be reported to the govroam mailing list. The JOT should start resolving the problem not later than two (2) working hours after the malfunction has been discovered or reported by a govroam user or a member. A ticket on the TTS should be opened by the respective JOT member and closed with a short comment on the performed action.

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

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 JOT will monitor packets en route for the presence of VLAN tagging attributes, namely:

- *Tunnel–Type*
- *Tunnel-Medium-Type*
- *Tunnel-Private-Group-ID*

The JOT 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.

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 the JOT, on request of the prospective member, confirms that the federation adheres to the Policy, the membership of the new regional federation will be approved.

If an organisation belonging to the RFO's constituency cannot be routed through the RFO's servers for any technical reason, the RFO may make a request to JOT to add the respective organisation directly to the NRPS instead. Upon such a request by the respective federation, the JOT checks the technical reasons and, if justified, modifies configuration on the central infrastructure and reports back on the execution of the configuration change.

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 three months' 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, the JOT may exclude a member from any further participation in the govroam federation.

An excluded member or an RFO whose application has been turned down by the JOT has right to present an appeal document. Decisions on membership following consideration of such appeals are final.

The list of members is publicly available on the govroam website. Changes in membership are announced using the govroam website.

6.7 Service Reports

The JOT prepares a govroam service report every six (6) months. The report should provide information on:

- Number of member organisations;
- Number of successful roaming sessions;
- Number of successful roaming sessions inside the regional federations;
- Number of security incidents and malfunctions;
- Report on maintenance activities;
- Central infrastructure up-time;
- Data collected by the monitoring system;
- Service improvements.

RFOs must provide the respective data to the JOT.

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.

7.1 Policy Declaration

The govroam policy declaration enables the establishment of the govroam federation by formalising the organisational and technical requirements.

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

Violation of the Policy declaration MUST be reported to the JOT.

7.2 Operational Requirements for Govroam Federation Members

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 service requirements and best practices, both at the regional and respective organisational levels;
- Establish a user support service for its end users, as explained in Section 6.1, "User Support Processes";
- Provide any information required for the govroam database (see Section
- 3.2.3);
- 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.

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 (JOT, 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, 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 JOT guarantees that the necessary infrastructure to run the federation services is operational and maintained according to server build, configuration and security best practices. The JOT also ensures that it will start resolving reported incidents concerning the govroam federation no later than two (2) working hours after the incident has been discovered. All such incidents will be logged.

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.

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.
- F-Ticks. The server MUST generate F-Ticks and send them to the monitoring infrastructure. If dynamic RADIUS routing (see Section 3.1.1.2) is used by the individual SPs, then it is the responsibility of the respective RFO to ensure that appropriate F-Ticks are sent to the monitoring infrastructure, either by enforcing that the SPs send them to the monitoring infrastructure themselves, or by collecting information of the authentication events and sending these on to the monitoring infrastructure on the SP's behalf.
- 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 MUST set up a web server in order to publish information about the govroam service. The address of that server SHOULD be www.govroam.<tld>.
- An RFO's web server MUST provide data in XML format, based on the specification defined by the JOT.

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 three 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).

7.3.2 Specifications 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 three 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 7.3.2, and the list of supported EAP types in the supplicant software in Section 7.3.4 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, eduroam 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.

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;
- If dynamic RADIUS routing (see Section 3.1.1.2) is used, appropriate F-Ticks MUST be sent to the monitoring infrastructure, either directly or through the RFO services (see Section 7.3.1).

Network:

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

Standard IPSec VPN	IP protocol 50 (ESP)	incoming and outgoing
	IP protocol 51 (AH)	incoming and outgoing
	UDP port 500 (IKE)	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)	incoming and outgoing
	TCP port 1723	outgoing
SSH	TCP port 22	outgoing
HTTP	TCP port 80	outgoing
	TCP port 443	outgoing
	TCP port 3128	outgoing
	TCP port 8080	outgoing
Mail sending	TCP port 465	outgoing
	TCP port 587	outgoing
Mail reception	TCP port 143	outgoing
	TCP port 993	outgoing
	TCP port 110	outgoing
	TCP port 995	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 three 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.

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.

8 Liability and Branding

8.1 Liability

The govroam Terms and Conditions regulates the liability issues arising between the Parties participating in the govroam service.

8.2 Branding

Govroam and the govroam logo are registered trademarks[3] of BELNET, the Belgian national research and education network operator, on behalf of all NRENs supporting public sector roaming through the European confederation of govroam operators.

For further information, see the govroam web pages of BELNET (**http://govroam.be/**).

All locations providing govroam should clearly indicate the availability of the service through branded collateral, in order to promote user awareness and ensure a high level of trust in the brand and service.

3 **https://tmdb.eu/trademark_registration/trademark_014246565_ohim_govroam**

9 References

[eduroam] **http://www.eduroam.org**

[govroam] **https://www.jisc.ac.uk/govroam**

[IEEE 802.1X] **http://www.ieee802.org**

Glossary

AAA	Authentication, Authorisation and Accounting
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)
JOT	Jisc Operations Team
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
RO	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
VLAN	Virtual Local Area Network
WPA2	Wi-Fi Protected Access, version 2

10 Appendix A: 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.

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.

11 Appendix B: 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.

12 Appendix C: 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 organisations (potentially including abroad).

Govroam provides, in a secure manner, Internet network access for a closed, national user group: the public sector. The network must be restricted to the community in order to keep the level of trust sufficiently high for organisations to give users from the "outside" access to their networks.

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").