Govroam technical specification

Version 3

Contents

1. Introduction

1.1 Overview

This is the Technical Specification for govroam, Jisc's federated roaming service for the public sector. Any questions about this document, or the service, should be directed to the govroam team (govroam@jisc.ac.uk).

This document is subject to periodic revision. Changes will be announced via the Govroam-Technical mailing list for registered technical contacts, and via the govroam wiki (http://wiki.govroam.uk), where the most recent version will be found.

This document was last reviewed on 01/06/2021.

1.1.1 Using this document

This document uses the conventions specified in RFC 2119[1] for indicating requirement levels.

This document consists of five sections:

- Section 1 ('Introduction'). Introduction to this document.
- Section 2 ('Common Requirements and Recommendations'). This section is concerned with general requirements that are common for all participating organisations.
- Section 3 ('Home Organisation Requirements and Recommendations'). This section is concerned with the requirements for Home organisations, and primarily the authentication of users.
- Section 4 ('Visited Organisation Requirements and Recommendations'). This section is concerned with the requirements for Visited organisations, and primarily those relating to the visitor network.
- Section 5 (Appendices). Two summaries of the requirements and recommendations laid out in this document; and a glossary defining various technical and non-technical terms.

1.1.2 Technical note

Govroam uses the same federated roaming model and technology as eduroam, the equivalent roaming service for education.

Govroam supports all EAP authentication methods. However, the majority of eduroam participants use username/password-based authentication, and as a result this document focuses on this authentication route. We will continue to build this document to reflect alternative approaches as we gain operational experience.

If you are considering a different route to authentication, such as EAP-TLS, please contact the govroam team to discuss further (**govroam@jisc.ac.uk**).

[1]S. Bradner, RFC2119 - Key words for use in RFCs to Indicate Requirement Levels, 1997.

1.2 Change Log

Version	Date published	Summary of changes
1.0	27/07/2017	n/a
2.0	12/12/2017	Minor adjustments to match requirements of G-cloud framework.
3.0	01/06/2021	Updated to reflect current govroam best practice and shifts in technology use (e.g. new sections on WPA3 and IPv6). Some rephrasing for clarity throughout.

2. Common Requirements and Recommendations

This section specifies the requirements for all govroam participants.

2.1 Participation

2.1.1 Requirements

1. All participating organisations MUST observe the requirements set out in section 2 of this document.

2. Participants that choose to participate as a Home organisation MUST observe the requirements set out in section 3 of this document.

3. Participants that choose to participate as a Visited organisation MUST observe the requirements set out in section 4 of this document.

2.1.2 Recommendations

1. Participants SHOULD observe the recommendations set out in this document.

2.1.3 Discussion

Only members of the govroam federation may participate and provide govroam services in the UK, and all members must abide by this Technical Specification.

A Visited service provider is one that makes available a network connectivity service for govroam users. A Home organisation is one that provides an authentication service for its users to access govroam connectivity services. The two service types can be provided independently of each other.

It is anticipated that most organisations will participate as both a Visited and a Home service type provider; however participation as either Visited-only or Home-only is acceptable where justified.

Although it is recommended that organisations participate as Visited organisations, it is not mandatory. This allows an organisation that may be unable or unwilling to act as a network access service provider (SP) to participate as a Home organisation and enable its own users to benefit from Visited services provided by other participants.

Participation as a Home organisation is not mandatory, although it is recommended. This permits an organisation that may be unable, unwilling or ineligible to act as an identity provider (IdP) and provide an authentication service, to participate as a Visited organisation and offer visitors network access through govroam.

Organisations may partially or wholly out-source provision of their Home or Visited services. In such situations the obligations of the participant to comply with this technical specification do not alter; therefore the terms of the agreement with the out-sourced provider should reflect this.

Alternatively, organisation-level infrastructure may be provided (possibly on a commercial basis) in partnership with other organisations in the context of a govroam regional federation, as would be the case where the partner operates its own RADIUS infrastructure and possibly authentication system, for instance on behalf of a group of federation+ Members. This can be described as the provision of a managed Visited or managed Home service.

2.2 Technical Contact

2.2.1 Requirements

4. Participants MUST designate a technical contact that can be contacted using e-mail and telephone during normal business hours. The contact may be either a named individual or an organisational unit. Arrangements must be made to cover for absence of a named technical contact owing to eventualities such as illness and holidays.

2.2.2 Discussion

A technical contact is required to facilitate the resolution of matters such as technical problems and abuse. Participants should ensure that changes in staff are promptly advised to the govroam team.

2.3 Logging

2.3.1 Requirements

5. Every log entry MUST state the date and time it was logged, derived from a reliable time source. The timestamp MUST be in UTC.

6. Logs MUST be kept for a minimum period of three months.

7. Regional Federation Organisations MUST forward logs to a syslog server specified by Jisc.

    7.1. The syslog log MUST be in RFC 5424 format.

    7.2. The syslog log MUST contain a message body in FTICKS format.

    7.3. There MUST only be one syslog log per roaming event.

    7.4. There MUST NOT be syslog logs sent for unsuccessful authentications, only successful ones.

    7.5. There MUST NOT be syslog logs sent for authentication requests originating from, or being proxied to, the NRPS.

    7.6. There MUST NOT be syslog logs sent for authentication requests originating and terminating within the same realm.

2.3.2 Recommendations

2. Syslog MAY use TLS encryption (RFC5425) to communicate with the syslog server.

2.3.3 Discussion

Accurate logging is necessary for resolving technical problems and tracking abuse. The ability of a host to refer to a standard time is necessary for the production of logs that can be compared with logs maintained at other organisations. The use of a Network Time Protocol[2] (NTP) service that can be used for synchronising the clocks of hosts is recommended.

Whilst the minimum period for retention of logs is specified above, the maximum period is a matter for the organisation's general data protection compliance. It is recommended that raw logs should not be kept indefinitely and that three months is a commonly used threshold for deletion or anonymization.

Jisc is able to see roaming event happening between Individual sites and Federations but roughly 90% of roaming event happen within Federations. To provide a full picture of roamings RFOs need to send roaming logs to the Jisc syslog server.

FTICKS is a log message format specifically created for this task. The message format is a single machine readable line which contains a few key values (realm, source and CSI) which uniquely identifies a roaming event, allows for duplicate detection and doesn't contain any personally identifiable information. Please see http://wiki.govroam.uk/doku.php?id=public:fticks for details on the FTICKS format and how to integrate into common RADIUS servers.

Although the data isn't personal it's best to use TLS encryption, where possible.

Only roams between realms within the Federation are of interest. Roams between realms with the Federation and outside the Federation will be logged by the NRPS. Authentications within a realm (local user at their local site) aren't roams so don't count.

Equally, only successful authentications are relevant to the information generated.

Many RADIUS servers can be configured to send such logs immediately after a successful authentication. One FTICK message per syslog.

2.4 RADIUS Hosts

2.4.1 Requirements

8. Participants' RADIUS (Remote Authentication Dial In Service) clients and servers MUST comply with RFC 2865[3] and RFC 2866[4].

9. Participants' RADIUS clients' and servers' clocks MUST be configured to synchronise regularly with a reliable time source

10. Participants MUST deploy at least one ORPS (organisational RADIUS proxy server).

11. The ORPS operated by a Federation MUST be reachable from the govroam National RADIUS Proxy Servers (NRPS) and MUST be configured to listen on port UDP/1812 (or 2083 if using RADSEC).

2 David L. Mills, RFC 1305 - Network Time Protocol (Version 3), 1992
3 C. Rigney, S. Willens, A. Rubens, W. Simpson, RFC2865 - Remote Authentication Dial In User Service (RADIUS), 2000
4 C. Rigney, RFC2866 - RADIUS Accounting, 2000

12. The ORPS operated by Individual Organisations MUST be reachable from the govroam National RADIUS Proxy Servers (NRPS) and MUST be configured to listen on port UDP/1812 (or 2083 if using RADSEC).

13. Participants using RADSEC MUST use X.509 certificates to identify their ORPS.

14. The ORPS operated by a Federation and the ORPS operated by Individual Organisations MUST respond to Internet Message Control Protocol (ICMP) Echo requests received from NRPS.

15. The following RADIUS attributes MUST be forwarded unaltered by all participant's ORPS (Sites, Federation or Individual Organisation) if present in the RADIUS Access-Request, Access-Challenge, Access-Accept or Access-Reject messages:

    15.1. User-Name

    15.2. Reply-Message

    15.3. State

    15.4. Class

    15.5. Message-Authenticator

    15.6. Proxy-State

    15.7. EAP-Message

    15.8. MS-MPPE-Send-Key

    15.9. MS-MPPE-Recv-Key

    15.10. Calling-Station-Id

    15.11. Operator-Name

    15.12. Chargeable-User-Identity

16. The following RADIUS attributes MUST NOT be forwarded by participants' ORPS:

    16.1. Tunnel-Type

    16.2. Tunnel-Medium-Type

    16.3. Tunnel-Private-Group-ID

    16.4. Airespace-Interface-Name

    16.5. Aruba-User-Role

    16.6. Aruba-User-VLAN

17. Participants MUST NOT forward accounting messages to the NRPS.

18. Participants' ORPSs MUST log all RADIUS authentication requests exchanged with the NRPS; the following information must be recorded.

18.1. The value of the user name attribute in the request (i.e. the anonymous outer identity).

18.2. The value of the Calling-Station-Id attribute in the request.

2.4.2 Recommendations

3. Participants SHOULD deploy a secondary ORPS.

2.4.3 Discussion

The ORPS is the interface between a participating organisation's network and the govroam RADIUS proxy infrastructure. A secondary ORPS should be implemented to improve the resilience of the participant's service and, by ensuring that a receptive ORPS is always online, to minimise RADIUS packet queuing on the NRPS.

The key attributes specified in Requirement 13 MUST be retained in forwarded packets. Where technically feasible, all other RADIUS attributes SHOULD be filtered. The inclusion of spurious RADIUS attributes in packets exchanged between organisations can have unexpected effects and result in problems. In particular, those specified in Requirement 14 may be disruptive to the recipient organisation and MUST NOT be included. See 3.6.2 for more information.

Detailed logging of authentication requests (and accounting requests if applicable) is necessary for problem resolution and the tracking of network abuse. Note that the govroam Service Definition (available from the Jisc govroam website) states that Visited organisations have responsibilities in relation to the online activities of visitors, and consequently it is in the interests of the Visited service provider to ensure that this logging is accurate and complete.

The IP addresses of the NRPSs and the govroam Portal are provided as part of the boarding process.

RADIUS accounting is not relevant in govroam outside of participants' networks, and receiving and responding to these by the NRPS consumes processing resources that could be better utilised. In addition, the configuration of ORPS to forward accounting messages to the NRPS represents unnecessary complication. It is therefore a mandatory requirement that ORPS MUST NOT forward accounting messages to the NRPS.

2.5 Govroam Service Information Website

2.5.1 Requirements

19. If a govroam information webpage is available, organisations MUST ensure that their govroam information webpage meets the international WCAG 2.1 AA standard for accessibility.

2.5.2 Recommendations

4. Participants SHOULD publish a govroam service information webpage which SHOULD be generally accessible from the Internet and, if applicable, within the organisation to allow visitors to access it easily on site. The webpage SHOULD include the following information as a minimum:

4.1. The text of, or a link to, the participant's acceptable use policy (AUP), where applicable.

4.2. A link to the govroam Policy Service Definition.

4.3. The govroam logo linking to the govroam website.

4.4. The type of service offered where the scope of the govroam service is limited, such as Visited-only or Home-only; and the operational status of the service if the web page is

published before the service becomes operational, or in the event of local maintenance.

2.5.2 Discussion

The participant's govroam service information website is used to publish relevant information to help visitors and local users at the organisation connect to and make use of the participant's govroam service.

Since users will have a reasonable expectation of being able to connect to govroam wherever the govroam SSID is broadcast, any limitation affecting users' ability to utilise the service, such as Visited-only and Home-only service types, must be advertised on the organisation's govroam website.

Note that Visited organisations' govroam service information websites are subject to further requirements; these are set out in that section of this specification.

3. Home Organisation Requirements and Recommendations

This section outlines the service requirements and recommendations for Home organisations.

A home organisation authenticates affiliated users when they attempt to connect at a visited organisation.

This section focuses on setting up EAP-PEAP authentication. If your organisations is considering an alternative authentication type, such as EAP-TLS, contact the govroam team to discuss further (govroam@jisc.ac.uk).

3.1 User Names

3.1.1 Requirements

20. Home organisations' govroam user names MUST conform to the Network Access Identifier (NAI) specification (RFC 4282[5]), i.e. comprise identity name, @ symbol, and realm components.

21. The realm component MUST conclude with participant's realm name, which MUST be a domain name in the global Domain Name System (DNS) that the Home organisation administers, either directly or by delegation.

3.1.2 Discussion

The purpose of the NAI is to specify a user name format for use within roaming services. Compliance with this requirement reduces the likelihood of problems arising from applications (such as RADIUS proxies) parsing user names in unexpected ways. Note that the use of privacy-preserving anonyms or pseudonyms is permitted, although care must be taken to ensure that the identity of the end user can always be established by the Home organisation.

One of the major elements of the govroam ethos is that users should be able to connect to govroam services in a seamless manner, without the user having to alter credentials in supplicant software. The requirement that only RFC 4282 compliant user names are permitted for use with govroam,

5 B. Aboba, M. Beadles, J. Arkko, P. Eronen, RFC4282 - The Network Access Identifier, 2005

whether at the user's Home site or when roaming, ensures that users are more readily able to connect wherever an govroam service is encountered.

3.2 Logging

3.2.1 Requirements

22. Home organisations MUST log all authentication attempts; the following information MUST be recorded:

    22.1. The time that the authentication request was received.

    22.2. The authentication result returned by the authentication database.

    22.3. The reason given, if any, if the authentication was denied or failed.

    22.4. User-Name in the outer-EAP and the User-Name from the inner-EAP (if a tunneled EAP method is used).

    22.5. Chargeable-User-Identity (CUI) if one was generated.

    22.6. Calling-Station-ID.

    22.7. Operator-Name if one was present in the Access-Request.

3.2.2 Discussion

Detailed logging of authentication is necessary for problem resolution and investigation of network abuse.

3.3 EAP Authentication

3.3.1 Requirements

23. Home organisations MUST configure their RADIUS server to authenticate one or more Extensible Authentication Protocol[6] (EAP) types.

24. Home organisations MUST select an EAP type, or EAP types, for which their RADIUS server will generate symmetric keying material for encryption ciphers and encapsulate the keys, following section 3.16 of RFC 3580[7], within RADIUS Access-Accept packets.

3.3.2 Recommendations

5. Home organisations SHOULD choose a type, or types, that fulfill all or most of the 'mandatory requirements' section of RFC 4017[8].

6 B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, H. Levkowetz, Ed., RFC3748 – Extensible Authentication Protocol (EAP), 2004
7 P. Congdon, B. Aboba, A. Smith, G. Zorn, J. Roese, RFC3580 - IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines, 2003
8 D. Stanley, J. Walker, B. Aboba, RFC4017 - Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs, 2005

5.1. The EAP types TLS[9], PEAP[10], and TTLS[11] are recommended.

3.3.3 Discussion

RFC 4017 defines requirements for EAP types used on IEEE 802.11[12] LANs. While it is recommended that Home organisations select an EAP type (or types) that fulfills as many of these requirements as possible, it is mandatory that the 'Generation of symmetric keying material' requirement is met, and that the keys are returned in the RADIUS Access-Accept packet.

3.4 Test Account

3.4.1 Requirements

25. If the Home organisation has chosen to support PEAP or TTLS type methods, the organisation MUST create and issue to the govroam team an authenticatable test account per realm registered and the relevant methods MUST be supported by this test account; additionally PAP may be used.

26. If the password for this account is changed then the govroam team MUST be notified immediately to reflect this change. If it is believed the password has been compromised then the password MUST be changed immediately and the govroam team updated as soon as possible.

3.4.2 Recommendations

6. The test account SHOULD be created in the organisation's primary user database. If more than one user database exists, it SHOULD be created in the user database that is likely to be most authenticated against.

7. Other privileges SHOULD NOT be assigned to the test account.

8. The test account SHOULD be configured to allow at least five consecutive failed authentication attempts without the account being locked.

3.4.3 Discussion

A test account is required for monitoring and test purposes by the govroam team. The EAP method selected by the participating organization for this account should match the method most commonly used by the organisation. The credentials for the test account will only be known by the govroam team and the Home organisation. The test account credentials should be supplied to govroam team and should be updated there whenever changes are made.

3.5 User Security Awareness

3.5.1 Recommendations

9. Home organisations SHOULD educate their users around secure use of the service.

---

9 B. Aboba, D. Simon, RFC2716 - PPP EAP TLS Authentication Protocol, 1999
10 Ashwin Palekar, Dan Simon, Glen Zorn, S. Josefsson, Protected EAP Protocol (PEAP), 2003
11 Paul Funk, Simon Blake-Wilson, EAP Tunneled TLS Authentication Protocol Version 0 (EAP-TTLSv0), 2005
12 IEEE Computer Society, Supplement to 802.11-1999,Wireless LAN MAC and PHY specifications: Higher speed Physical Layer (PHY) extension in the 2.4 GHz band, 1999

3.5.2 Discussion

Home organisations should be mindful of the fact that their users' communications are forwarded over networks with unknown security characteristics, and that govroam does not provide any guarantees regarding the privacy of this data. **The use of VPN is strongly recommended.**

3.6 RADIUS Hosts

3.6.1 Requirements

27. Home organisations MUST attempt to authenticate all authentication requests forwarded from the NRPS.

3.6.2 Recommendations

10. 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 Access-Accept reply SHOULD NOT contain dynamic VLAN or vendor-specific 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.

11. If the Home RADIUS server supports Chargeable-User-Identity (CUI) then Access-Accept replies SHOULD contain the CUI attribute, where CUI is solicited in the authentication request from the Visited organisation, as described in RFC 4372[13].

3.6.3 Discussion

It is common for organisations to apply filters to drop authentication requests where the NAS-Port-Type attribute does not match 'Wireless - IEEE 802.11' and/or Service-Type = 'Framed-User' in standard deployments. However, for govroam purposes, some NASs do not send such attributes and there is no requirement to do so within this Technical Specification. **All authentication requests forwarded by the NRPSs are valid and therefore MUST NOT be filtered.**

A response MUST be sent to all authentication requests. RADIUS servers are configured to mark other RADIUS servers as unavailable if they fail to respond to an authentication request. If an ORPS of an individual organisation is marked as unavailable by a NRPS then any authentication request for users at that site will be automatically rejected. More seriously, if ORPS connected to a RRPS fail to respond to authentication requests sent to the RRPS from the NRPS then the RRPS will be marked as unavailable by the NRPS, thus rejecting any further authentication to the Federation as a whole.

4. Visited Organisation Requirements and Recommendations

This section outlines the service requirements and recommendations for visited organisations.

A visited organisation provides authenticated visitors with access to a visitor LAN.

This section focuses on setting up EAP-PEAP authentication. If your organisations is considering an alternative authentication type, such as EAP-TLS, contact the govroam team to discuss further (govroam@jisc.ac.uk).

13 IETF, RFC 4372 Chargeable User Identity, http://www.ietf.org/rfc/rfc4372.txt

The engineering standards table below summarises and highlights the standards and features of greatest impact on users:

SSID	govroam	***Application Proxy***	MAY
WPA/ TKIP	MUST NOT	***Port Restrictions***	MAY
WPA2/AES	MUST	***IPv6***	SHOULD
WPA3	MAY	***Injection of O-N***	SHOULD
NAT	MAY		

4.1 Network Presentation

4.1.1 Requirements

28. Visited organisations MUST implement the engineering standards defined in this specification.

29. Visited organisations MUST ensure that is not possible for a non-govroam service to be mistaken by visitors for the participant's govroam service.

30. The word 'govroam' MUST NOT be used in an SSID for a non-compliant network.

31. Visited organisations' govroam networks MUST NOT be shared with any other network service, including eduroam.

32. Visited organisations MUST NOT offer visitors any wireless media other than IEEE 802.11.

4.1.2 Discussion

Some participants may wish to deploy a non-govroam wireless service, in addition to a govroam service. For example, a participant's own users may require access to a wireless network that should remain inaccessible to visitors. Participants may offer such services; for example, by using another Service Set Identifier (SSID). However, visitors should not be able to confuse these services with the participant's govroam service.

Note that it is permissible for a participant to place their own users onto a network which does not comply with govroam policy (e.g. one which has greater port/protocol restrictions), even if they have connected to an SSID bearing the name 'govroam'; it is not permissible to do this to visitors.

It is anticipated that organisations will use VLAN technology to segregate networks; however, this is not mandatory and participating organisations may choose to realise the necessary segregation through other means (such as physical isolation).

Eduroam and Govroam very similar services and are implement almost identically. However, they are two different services with different user bases, stakeholders and policy documents. It would contravene both the policies and the common understanding underpinning both services to allow devices to mix freely on the same network (VLAN). Thus the expectation is that there are separate VLANs, address space and NATed external addresses (where applicable) for each service.

While it is anticipated that IEEE 802.11 will be the dominant access media for govroam, participants are permitted to use other media, such as wired Ethernet, providing that the other technical requirements are adhered to. With the same proviso, the mixing of media on the same network is also permitted.

At present this specification prohibits the use of non-IEEE 802.11 wireless media, such as Bluetooth, because their suitability for govroam has not yet been adequately explored. These media may be considered for inclusion in subsequent revisions of this specification if interest in their use is expressed.

4.2 RADIUS Forwarding

4.2.1 Requirements

33. Visited organisations MUST forward RADIUS requests originating from govroam Network Access Servers (NASs) which contain user names with non-local realms to a NRPS via an ORPS. A non-local realm name is defined as one that is neither associated with the participant nor the participant's partner where a service is provided in partnership with another organisation. Requests containing local realm names (those associated with the participant or partner organisation) MUST NOT be forwarded to the NRPS.

    33.1. RADIUS Access-Requests MUST be sent to port UDP/1812.

    33.2. Access-Requests using RadSec MUST be sent to port TCP/2083.

34. Visited organisations MUST NOT forward requests containing user names which do not include a realm nor any which are non-NAI compliant.

35. Visited organisations MUST NOT forward requests that have originated from NASs that do not conform to the requirements of this specification.

36. Visited organisations MAY configure additional realms to forward requests to other internal RADIUS servers, but these realms MUST NOT be derived from any domain in the global DNS that the participant or a partner organisation does not administer.

37. In situations where a participating organisation is in partnership with another participating organisation to provide managed Visited services at sites belonging to the partner and where that partner operates its own Home service, the managed Visited service provider MUST forward requests containing user names with a realm associated with the partner directly to the RADIUS server of that partner and MUST NOT forward those requests to the NRPS.

38. In situations where the organisation providing the managed Visited service is also working as a partner with further participating organisations, the Visited organisation MUST ensure that requests originating from a managed site of such an organisation are NOT forwarded to any other partner.

39. Visited organisations MUST NOT otherwise forward requests directly to other govroam participants.

4.2.2 Recommendations

12. Visited organisations SHOULD configure their ORPS to load balance between the NRPS servers.

13. Visited organisations MAY configure their ORPS to fail-over between the NRPS servers.

13.1. If the fail-over algorithm has a configurable timer that specifies the length of time after which an unresponsive server is considered unreachable, this timer SHOULD be configured to zero seconds (or as low a value as possible).

14. The Visited organisation SHOULD configure their ORPS to insert the Operator-Name attribute, accurately composed for their realm, into all Access-Request packets forwarded to the NRPS.

15. Visited organisations SHOULD request Chargeable-User-Identity (CUI) in Access-Request packets forwarded to the NRPS if CUI is supported by the ORPS.

16. If an ORPS is capable of using Status-Server (RADIUS Code 12) to detect the operational state of the NRPS, then it SHOULD be configured to do so.

17. If an ORPS is capable of being queried by Status-Server then that functionality SHOULD be enabled so that the NRPS are able to make a more informed decision on the operational status of the ORPS. If Status-Server is enabled, then it MUST listen on port 1812 and respond with an Access-Reject.

4.2.3 Discussion

In the future (and by mutual agreement with participants), govroam in the UK may join the wider international govroam confederation, which consists of organisations holding domain names derived from many of the top level Domain Name Service[14] (DNS) domains. Consequently it is necessary to ensure that the RADIUS realm and DNS name-spaces used in the UK remain congruent; otherwise, RADIUS requests may not be routed correctly.

The NRPS MUST NOT be used as a general-purpose authentication system. At the present time, only NASs that conform to the requirements of this specification may use the NRPS.

Given the regional federation structures that support most govroam participants, wherein one member organization may provide govroam services for another through a formal agreement (which may be commercially based) and where both partners are full members of the govroam federation, the issue of routing of RADIUS messages needs clarification: the potential exists for the routing of all requests to the NRPS, including those for users from the partnered organisations. This would effectively turn the NRPS into an off-campus relay for a large proportion of an organisation's home users, a task for which the NRPS were never designed. Requests arising from users who are members of the partnered organisation must be routed directly to the partner's ORPS and not to the NRPS.

Chargeable-User-Identity attribute is useful in troubleshooting When a Visited organisation sets a NUL character in a CUI attribute included an Access-Request, the Home organisation's RADIUS server, if it supports CUI, can (and should be configured to) return an identifier (although not necessarily the identity), of the user via CUI in the Access-Accept to the Visited organisation ORPS. The values of CUI may be included in RADIUS logs.

With reference to 3.6.3, Status-Server mitigates for the scenario where RADIUS servers are marked as unavailable due to a lack of response. Status-Server can be thought of as a 'RADIUS Ping'. Simple Status-Server requests sent to a RADIUS server can be responded to with an Access-Reject which indicates the presence of a working RADIUS server. This is a much more reliable method of determining the status of a RADIUS than using authentication request timeouts.

14 P. Mockapetris, RFC1034 - Domain names - concepts and facilities, 1988

4.3 NAS Requirements

4.3.1 Requirements

40. NASs MUST implement IEEE 802.1X15 authentication.

41. On receipt of a RADIUS Access-Accept, the NAS and network MUST immediately forward traffic to, and from, the visitor according to the requirements set out in section 4.5; no form of local authorisation is permitted that would deny this to the visitor except in the case where network abuse has been detected.

42. Wireless IEEE 802.11 NASs MUST support symmetric keying using keys provided by the Home organisation within the RADIUS Access-Accept packet, in accordance with section 3.16 of RFC 3580.

43. A NAS port MUST NOT connect more than one user unless the NAS is not capable of being configured other than to use the same port for the connection of multiple users and the NAS maintains client traffic separation by other means.

44. All NASs that are deployed by Visited organisations to support govroam MUST include the following RADIUS attributes within Access-Request packets.

    44.1. Calling-Station-ID attribute containing the supplicant's MAC address.

    44.2. NAS-IP-Address attribute containing the NAS's IP address.

4.3.2 Discussion

With modern wireless controller equipment the NAS is the controller, which in most implementations just uses a single port. Security relies on client traffic being separated internally by the controller. Note that this restriction may prohibit the use of some gateway devices that provide IEEE 802.1X authentication to multiple users over a single NAS port.

Knowledge of supplicants' MAC and NAS's IP addresses allows detailed logging of authentication and accounting that is necessary for problem resolution, the tracking of network abuse and trend analysis.

Participants MUST NOT use other network access control technologies to restrict a visitor's connection i.e. captive portal pages.

4.4 Securing Host Network Configuration

4.4.1 Recommendations

18. Visited organisations SHOULD configure the network to prevent a visitor from masquerading as an authorised Dynamic Host Configuration Protocol[16] (DHCP) server or router.

19. Visited organisations SHOULD configure the wireless network to place clients into their own broadcast domains, where possible.

---

15 IEEE Computer Society, Port-Based Network Access Control, 2004

16 R. Droms, RFC 2131 - Dynamic Host Configuration Protocol, 1997

4.4.2 Discussion

A visitor's client, once authenticated, requires information about the visitor network. DHCP and Address Resolution Protocol (ARP) are used for this purpose in IPv4; DHCPv6 and Neighbourhood Discovery (ND) in IPv6. However, most implementations of these protocols do not provide a mechanism for authenticating the sender. Hence, a concern arises from the introduction of devices that act as 'rogue routers'.

Such a router can perform a man-in-the-middle attack by issuing DHCP responses, gratuitous ARP requests or ND Router Advertisements (RA) that indicate that it is the default gateway for the network. All of the client's subsequent communications are sent to the rogue router. It might also forward them on to a masquerading target such as a faked banking service.

While there are no standards that address this problem directly for IPv4, most vendors have implemented proprietary solutions which participants should use, if available, to prevent the abuse of ARP, DHCP and RAs.

Many wireless vendors provide functionality which allows clients to be placed in their own broadcast domain and thus are isolated from their neighbors with the same subnet.

4.5 IP Forwarding

Many wireless vendors provide functionality which allows clients to be placed in their own broadcast domain and thus are isolated from their neighbours with the same subnet.

4.5.1 Requirements

45. Visited organisations MAY implement IPv4 and IPv6 filtering between the visitor network and other networks, providing that this permits the forwarding of the following mandatory protocols to external networks:

VPN

IPSec NAT traversal:	UDP/4500 egress and established.
Cisco IPSec NAT traversal:	UDP/10000 & TCP/10000 egress and established.
	UDP/1701 egress and established.
OpenVPN:	UDP/1194 & TCP/1194 egress and established.
ESP:	IP protocol 50 egress and established.
AH:	IP protocol 51 egress and established.
ISAKMP and IKE:	UDP/500.

Email

IMAP4:	TCP/143 egress and established.
SMTPS:	TCP/465 egress and established.
Message submission:	TCP/587 egress and established.
IMAPS:	TCP/993 egress and established.
POP3S:	TCP/995 egress and established.

Web

HTTP:	TCP/80 egress and established.
HTTPS:	TCP/443 egress and established.
HTTP Proxy:	TCP/8080 egress and established.

Multimedia

Teams:	UDP/3478-3481 egress and established.
Zoom:	UDP/8801-8810 egress and established.
	TCP/8801-8802 egress and established.
XMPP:	TCP/5222 egress and established.

Other

SSH:	TCP/22 egress and established.
NTP:	UDP/123 egress and established.

4.5.2 Recommendations

20. Visited organisations MAY implement arbitrary IP filtering of packets addressed to other hosts on the Visited organisation's own network.

21. Visited organisations SHOULD provide visitors with unimpeded access to the Internet, where local policy permits.

4.5.3 Discussion

An important aim of govroam is to provide visitors with unimpeded access to the Internet. This maximises the probability of a visitor's applications working as expected, thereby improving the visitor's experience of the service and reducing the support burden on the Home organisation.

However, participants may wish to implement some filtering of IP traffic entering and leaving the visitor network. For example, a participant may wish to limit the usage of bandwidth by potentially demanding applications, and so forth. This is permitted provided that the filtering policy allows the forwarding of the protocols laid out above.

Content filtering, whilst deprecated on govroam networks, is permitted. If content filtering is implemented, this must be stated on the organisation's govroam information website.

Filtering of packets addressed to other hosts on the Visited organisation's own internal network is permitted.

4.6 Application and Interception Proxies

4.6.1 Requirements

46. Visited organisations deploying application or 'interception' proxies on their govroam network MUST publish this fact on their govroam service information website.

47. Transport Layer Security (TLS)/Secure Sockets Layer (SSL) interception proxies MUST NOT be used for govroam visitors.

4.6.2 Recommendations

22. Non-transparent proxies SHOULD NOT be deployed but if one is, then the Visited organisation MUST also provide documentation on the configuration of applications to use the proxy on their Govroam website.

Discussion

Applications commonly require special configuration to use a proxy, which reduces usability and may increase the support burden. The presence of a proxy may also break some applications. Likewise 'interception' proxies, often used by intrusion and virus detection systems, may result in the user experiencing unexpected network behaviour. A TLS/SSL interception proxy represents an unacceptable security risk and breach of user privacy.

Whilst TLS interception proxies are not permitted on the govroam network onto which visitors are connected, at the home site organisations may connect their own users to non-govroam network services to which this requirement does not apply.

4.7 Govroam Service Information Webpage

4.7.1 Requirements

48. If a govroam information webpage is available, visited organisations MUST ensure the following, in addition to the recommendations detailed in section 2.5:

    48.1. The provision of sufficient information to enable visitors to identify and access the service; at a minimum this must include the locations covered.

    48.2. Where applicable, the inclusion of information specified in section 4.6 regarding application and interception proxies.

4.7.2 Recommendations

23. Visited organisations MAY publish the IP forwarding policies imposed on the visitor network.

4.7.3 Discussion

Publishing the IP forwarding policies imposed on the visitor network may assist Home organisations in supporting their users without needing to contact local support staff at the Visited organisation.

4.8 SSID

4.8.1 Requirements

49. Operational govroam Wi-Fi services, as described in this specification, MUST use a broadcast SSID of 'govroam' in lower case characters only.

50. Organisations that are in the process of developing Home or Visited services but are not yet offering operational services MUST NOT broadcast the 'govroam' SSID, and should instead use an appropriate test SSID of their choosing.

51. Organisations (including third parties) MUST provide an SSID for testing which MUST NOT be able to be confused with the production 'govroam' SSID. e.g. 'Test'.

4.8.2 Discussion

Since users have a reasonable expectation of being able to connect to govroam wherever the govroam SSID is visible, during the development stage of implementing govroam when an operational

service is not available at an organisation, the possibility of users detecting a broadcast govroam SSID must be minimised.

When in the process of configuring the RADIUS servers it's important to be able to test end to end authentication. Administrators engaged in this activity MUST be able to provide a way to test devices and credentials and to demonstrate that they are able to authenticate visitors.

4.9 Network Addressing

4.9.1 Requirements

52. Visited organisations MUST allocate IPv4 addresses to visitors using DHCP.

53. Visited organisations MUST log the IPv4 addresses allocated to visitors and the corresponding MAC addresses.

54. If NAT is used as part of a govroam implementation, visited organisations MUST log NAT address mappings,

4.9.2 Discussion

The DHCP server logs are required to enable participants to correlate DHCP leases to users in the course of investigating an issue. This requires the cooperation of both Home and Visited sites.

4.9.3 Recommendations

24. Govroam networks MAY make use of NAT.

25. Participants SHOULD implement IPv6 and allow routing of IPv6 on the govroam network.

26. If using IPv6 participants MUST allocate IPv6 addresses using SLAAC or DHCPv6.

27. Participants MUST log the IPv6 addresses allocated to visitors and the corresponding MAC addresses.

28. Participants SHOULD NOT use NAT with IPv6 but, if used, MUST log the address mappings.

29. Participants SHOULD provide IPv6 DNS services

4.9.4 Discussion

IPv6 is the next generation Internet Protocol. Increasing adoption of IPv6 by service providers means that there is a benefit to participants in offering IPv6 connectivity to visitors. It is strongly recommended that visited sites implement IPv6 wherever possible. Support for IPv6 has improved significantly in recent years and Govroam is encouraging its adoption wherever possible. Either SLAAC or DHCPv6 are acceptable ways to assigns addresses. NAT SHOULD be avoided as IPv6 should not need it. NAT should not be used as a security feature and only where address space is limited, which is not an issue with IPv6.

Please consider providing suitable IPv6 DNS servers.

4.10 WPA

4.10.1 Requirements

55. The WPA specification MUST NOT be supported and the TKIP algorithm MUST NOT be employed in govroam services.

4.11 WPA2

4.11.1 Requirements

56. Govroam Visited Wi-Fi services MUST implement at least WPA2 Enterprise with the use of the CCMP (AES) algorithm.

4.11.2 Discussion

WPA2 Enterprise is the Wi-Fi Alliance's interoperability compliance certification scheme for IEEE 802.11 security features. This is regarded as the strongest WLAN security specification available.

WPA2 Enterprise is mandatory for govroam services, as it contributes towards a higher security context and is the only permitted standard in the UK.

The Wi-Fi Alliance specifies both WPA2 and WPA2 with Protected Management Frames (WPA2 with PMF). Currently there is no requirement regarding which WPA2 standard must be used (WPA2 or WPA2 with PMF) for govroam. However, participants deploying WPA2 with PMF should be aware this may cause interoperability issues with clients which are not certified for WPA2 with PMF.

4.12 WPA3

4.12.1 Recommendations

30. Govroam Visited Wi-Fi services MAY implement WPA3 Enterprise if possible. If WPA3 Enterprise is implemented then 192-bit security MUST be disabled

31. Protected Management Frames (PMFs) SHOULD be implemented but MUST be set to 'Supported' rather than 'Required'.

4.12.2 Discussion

WPA3 Enterprise offers enhanced security over WPA2 but the main one, 192-Bit security, requires changes to the IdPs on all sites so Visited Sites MUST NOT use it. It would be hard to debug authentication failures will occur if they do.

5. Appendices

5.1 Appendix I – Summary of Requirements

5.1.1 Common requirements

1. All participating organisations MUST observe the requirements set out in section 2 of this document.

2. Participants that choose to participate as a Home organisation MUST observe the requirements set out in section 3 of this document.

3. Participants that choose to participate as a Visited organisation MUST observe the requirements set out in section 4 of this document.

4. Participants MUST designate a technical contact that can be contacted using e-mail and telephone during normal business hours. The contact may be either a named individual or an organisational unit. Arrangements must be made to cover for absence of a named technical contact owing to eventualities such as illness and holidays.

5. Every log entry MUST state the date and time it was logged, derived from a reliable time source. The timestamp MUST be in UTC.

6. Logs MUST be kept for a minimum period of three months.

7. Regional Federation Organisations MUST forward logs to a syslog server specified by Jisc.

    7.1. The syslog log MUST be in RFC 5424 format.

    7.2. The syslog log MUST contain a message body in FTICKS format.

    7.3. There MUST only be one syslog log per roaming event.

    7.4. There MUST NOT be syslog logs sent for unsuccessful authentications, only successful ones.

    7.5. There MUST NOT be syslog logs sent for authentication requests originating from, or being proxied to, the NRPS.

    7.6. There MUST NOT be syslog logs sent for authentication requests originating and terminating within the same realm.

8. Participants' RADIUS (Remote Authentication Dial In Service) clients and servers MUST comply with RFC 2865 and RFC 2866 .

9. Participants' RADIUS clients' and servers' clocks MUST be configured to synchronise regularly with a reliable time source

10. Participants MUST deploy at least one ORPS (organisational RADIUS proxy server).

11. The ORPS operated by a Federation MUST be reachable from the govroam National RADIUS Proxy Servers (NRPS) and MUST be configured to listen on port UDP/1812 (or 2083 if using RADSEC).

12. The ORPS operated by Individual Organisations MUST be reachable from the govroam National RADIUS Proxy Servers (NRPS) and MUST be configured to listen on port UDP/1812 (or 2083 if using RADSEC).

13. Participants using RADSEC MUST use X.509 certificates to identify their ORPS.

14. The ORPS operated by a Federation and the ORPS operated by Individual Organisations MUST respond to Internet Message Control Protocol (ICMP) Echo requests received from NRPS.

15. The following RADIUS attributes MUST be forwarded unaltered by all participant's ORPS (Sites, Federation or Individual Organisation) if present in the RADIUS Access-Request, Access-Challenge, Access-Accept or Access-Reject messages:

    15.1. User-Name

    15.2. Reply-Message

    15.3. State

    15.4. Class

    15.5. Message-Authenticator

    15.6. Proxy-State

    15.7. EAP-Message

    15.8. MS-MPPE-Send-Key

    15.9. MS-MPPE-Recv-Key

    15.10. Calling-Station-Id

    15.11. Operator-Name

    15.12. Chargeable-User-Identity

16. The following RADIUS attributes MUST NOT be forwarded by participants' ORPS:

    16.1. Tunnel-Type

    16.2. Tunnel-Medium-Type

    16.3. Tunnel-Private-Group-ID

    16.4. Airespace-Interface-Name

    16.5. Aruba-User-Role

    16.6. Aruba-User-VLAN

17. Participants MUST NOT forward accounting messages to the NRPS.

18. Participants' ORPSs MUST log all RADIUS authentication requests exchanged with the NRPS; the following information must be recorded.

18.1. The value of the user name attribute in the request (i.e. the anonymous outer identity).

18.2. The value of the Calling-Station-Id attribute in the request.

19. If a govroam information webpage is available, organisations MUST ensure that their govroam information webpage meets the international WCAG 2.1 AA standard for accessibility.

5.1.2 Home organisation requirements

26. Home organisations' govroam user names MUST conform to the Network Access Identifier (NAI) specification (RFC 4282), i.e. comprise identity name, @ symbol, and realm components.

21. The realm component MUST conclude with participant's realm name, which MUST be a domain name in the global Domain Name System (DNS) that the Home organisation administers, either directly or by delegation.

22. Home organisations MUST log all authentication attempts; the following information MUST be recorded:

22.1. The time that the authentication request was received.

22.2. The authentication result returned by the authentication database.

22.3. The reason given, if any, if the authentication was denied or failed.

22.4. User-Name in the outer-EAP and the User-Name from the inner-EAP (if a tunneled EAP method is used).

22.5. Chargeable-User-Identity (CUI) if one was generated.

22.6. Calling-Station-ID.

22.7. Operator-Name if one was present in the Access-Request.

23. Home organisations MUST configure their RADIUS server to authenticate one or more Extensible Authentication Protocol (EAP) types.

24. Home organisations MUST select an EAP type, or EAP types, for which their RADIUS server will generate symmetric keying material for encryption ciphers and encapsulate the keys, following section 3.16 of RFC 3580 , within RADIUS Access-Accept packets.

25. If the Home organisation has chosen to support PEAP or TTLS type methods, the organisation MUST create and issue to the govroam team an authenticatable test account per realm registered and the relevant methods MUST be supported by this test account; additionally PAP may be used.

26. If the password for this account is changed then the govroam team MUST be notified immediately to reflect this change. If it is believed the password has been compromised then the password MUST be changed immediately and the govroam team updated as soon as possible.

27. Home organisations MUST attempt to authenticate all authentication requests forwarded from the NRPS.

5.1.3 Visited organisation requirements

28. Visited organisations MUST implement the engineering standards defined in this specification.

29. Visited organisations MUST ensure that is not possible for a non-govroam service to be mistaken by visitors for the participant's govroam service.

30. The word 'govroam' MUST NOT be used in an SSID for a non-compliant network.

31. Visited organisations' govroam networks MUST NOT be shared with any other network service, including eduroam.

32. Visited organisations MUST NOT offer visitors any wireless media other than IEEE 802.11.

33. Visited organisations MUST forward RADIUS requests originating from govroam Network Access Servers (NASs) which contain user names with non-local realms to a NRPS via an ORPS. A non-local realm name is defined as one that is neither associated with the participant nor the participant's partner where a service is provided in partnership with another organisation. Requests containing local realm names (those associated with the participant or partner organisation) MUST NOT be forwarded to the NRPS.

    33.1. RADIUS Access-Requests MUST be sent to port UDP/1812.

    33.2. Access-Requests using RadSec MUST be sent to port TCP/2083.

34. Visited organisations MUST NOT forward requests containing user names which do not include a realm nor any which are non-NAI compliant.

35. Visited organisations MUST NOT forward requests that have originated from NASs that do not conform to the requirements of this specification.

36. Visited organisations MAY configure additional realms to forward requests to other internal RADIUS servers, but these realms MUST NOT be derived from any domain in the global DNS that the participant or a partner organisation does not administer.

37. In situations where a participating organisation is in partnership with another participating organisation to provide managed Visited services at sites belonging to the partner and where that partner operates its own Home service, the managed Visited service provider MUST forward requests containing user names with a realm associated with the partner directly to the RADIUS server of that partner and MUST NOT forward those requests to the NRPS.

38. In situations where the organisation providing the managed Visited service is also working as a partner with further participating organisations, the Visited organisation MUST ensure that requests originating from a managed site of such an organisation are NOT forwarded to any other partner.

39. Visited organisations MUST NOT otherwise forward requests directly to other govroam participants.

40. NASs MUST implement IEEE 802.1X authentication.

41. On receipt of a RADIUS Access-Accept, the NAS and network MUST immediately forward traffic to, and from, the visitor according to the requirements set out in section 4.5; no form of local authorisation is permitted that would deny this to the visitor except in the case where network abuse has been detected.

42. Wireless IEEE 802.11 NASs MUST support symmetric keying using keys provided by the Home organisation within the RADIUS Access-Accept packet, in accordance with section 3.16 of RFC 3580.

43. A NAS port MUST NOT connect more than one user unless the NAS is not capable of being configured other than to use the same port for the connection of multiple users and the NAS maintains client traffic separation by other means.

44. All NASs that are deployed by Visited organisations to support govroam MUST include the following RADIUS attributes within Access-Request packets.

    44.1. Calling-Station-ID attribute containing the supplicant's MAC address.

    44.2. NAS-IP-Address attribute containing the NAS's IP address.

45. Visited organisations MAY implement IPv4 and IPv6 filtering between the visitor network and other networks, providing that this permits the forwarding of the following mandatory protocols to external networks:

VPN

IPSec NAT traversal:	UDP/4500 egress and established.
Cisco IPSec NAT traversal:	UDP/10000 & TCP/10000 egress and established.
	UDP/1701 egress and established.
OpenVPN:	UDP/1194 & TCP/1194 egress and established.
ESP:	IP protocol 50 egress and established.
AH:	IP protocol 51 egress and established.
ISAKMP and IKE:	UDP/500.

Email

IMAP4:	TCP/143 egress and established.
SMTPS:	TCP/465 egress and established.
Message submission:	TCP/587 egress and established.
IMAPS:	TCP/993 egress and established.
POP3S:	TCP/995 egress and established.

Web

HTTP:	TCP/80 egress and established.
HTTPS:	TCP/443 egress and established.
HTTP Proxy:	TCP/8080 egress and established.

Multimedia

Teams:	UDP/3478-3481 egress and established.
Zoom:	UDP/8801-8810 egress and established.
	TCP/8801-8802 egress and established.
XMPP:	TCP/5222 egress and established.

Other

SSH:	TCP/22 egress and established.
NTP:	UDP/123 egress and established.

46. Visited organisations deploying application or ‘interception’ proxies on their govroam network MUST publish this fact on their govroam service information website.

47. Transport Layer Security (TLS)/Secure Sockets Layer (SSL) interception proxies MUST NOT be used for govroam visitors.

48. If a govroam information webpage is available, visited organisations MUST ensure the following, in addition to the recommendations detailed in section 2.5:

    48.1. The provision of sufficient information to enable visitors to identify and access the service; at a minimum this must include the locations covered.

    48.2. Where applicable, the inclusion of information specified in section 4.6 regarding application and interception proxies.

49. Operational govroam Wi-Fi services, as described in this specification, MUST use a broadcast SSID of ‘govroam’ in lower case characters only.

50. Organisations that are in the process of developing Home or Visited services but are not yet offering operational services MUST NOT broadcast the ‘govroam’ SSID, and should instead use an appropriate test SSID of their choosing.

51. Organisations (including third parties) MUST provide an SSID for testing which MUST NOT be able to be confused with the production ‘govroam’ SSID. e.g. ‘Test’.

52. Visited organisations MUST allocate IPv4 addresses to visitors using DHCP.

53. Visited organisations MUST log the IPv4 addresses allocated to visitors and the corresponding MAC addresses.

54. If NAT is used as part of a govroam implementation, visited organisations MUST log NAT address mappings,

55. The WPA specification MUST NOT be supported and the TKIP algorithm MUST NOT be employed in govroam services.

56. Govroam Visited Wi-Fi services MUST implement at least WPA2 Enterprise with the use of the CCMP (AES) algorithm.

5.2 Appendix II - Summary of Recommendations

5.2.1 Common recommendations

1. Participants SHOULD observe the recommendations set out in this document.

2. Syslog MAY use TLS encryption (RFC5425) to communicate with the syslog server.

3. Participants SHOULD deploy a secondary ORPS.

4. Participants SHOULD publish a govroam service information webpage which SHOULD be generally accessible from the Internet and, if applicable, within the organisation to allow visitors to access it easily on site. The webpage SHOULD include the following information as a minimum:

    4.1. The text of, or a link to, the participant's acceptable use policy (AUP), where applicable.

    4.2. A link to the govroam Policy Service Definition.

    4.3. The govroam logo linking to the govroam website.

    4.4. The type of service offered where the scope of the govroam service is limited, such as Visited-only or Home-only; and the operational status of the service if the web page is published before the service becomes operational, or in the event of local maintenance.

5.2.2 Home organisation recommendations

5. Home organisations SHOULD choose a type, or types, that fulfill all or most of the 'mandatory requirements' section of RFC 4017 .

    5.1. The EAP types TLS , PEAP , and TTLS are recommended.

6. The test account SHOULD be created in the organisation's primary user database. If more than one user database exists, it SHOULD be created in the user database that is likely to be most authenticated against.

7. Other privileges SHOULD NOT be assigned to the test account.

8. The test account SHOULD be configured to allow at least five consecutive failed authentication attempts without the account being locked.

9. Home organisations SHOULD educate their users around secure use of the service.

10. 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 Access-Accept reply SHOULD NOT contain dynamic VLAN or vendor-specific 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.

11. If the Home RADIUS server supports Chargeable-User-Identity (CUI) then Access-Accept replies SHOULD contain the CUI attribute, where CUI is solicited in the authentication request from the Visited organisation, as described in RFC 4372 .

5.2.3 Visited organisation recommendations

12. Visited organisations SHOULD configure their ORPS to load balance between the NRPS servers.

13. Visited organisations MAY configure their ORPS to fail-over between the NRPS servers.

    13.1. If the fail-over algorithm has a configurable timer that specifies the length of time after which an unresponsive server is considered unreachable, this timer SHOULD be configured to zero seconds (or as low a value as possible).

14. The Visited organisation SHOULD configure their ORPS to insert the Operator-Name attribute, accurately composed for their realm, into all Access-Request packets forwarded to the NRPS.

15. Visited organisations SHOULD request Chargeable-User-Identity (CUI) in Access-Request packets forwarded to the NRPS if CUI is supported by the ORPS.

16. If an ORPS is capable of using Status-Server (RADIUS Code 12) to detect the operational state of the NRPS, then it SHOULD be configured to do so.

17. If an ORPS is capable of being queried by Status-Server then that functionality SHOULD be enabled so that the NRPS are able to make a more informed decision on the operational status of the ORPS. If Status-Server is enabled, then it MUST listen on port 1812 and respond with an Access-Reject.

18. Visited organisations SHOULD configure the network to prevent a visitor from masquerading as an authorised Dynamic Host Configuration Protocol (DHCP) server or router.

19. Visited organisations SHOULD configure the wireless network to place clients into their own broadcast domains, where possible.

20. Visited organisations MAY implement arbitrary IP filtering of packets addressed to other hosts on the Visited organisation’s own network.

21. Visited organisations SHOULD provide visitors with unimpeded access to the Internet, where local policy permits.

22. Non-transparent proxies SHOULD NOT be deployed but if one is, then the Visited organisation MUST also provide documentation on the configuration of applications to use the proxy on their Govroam website.

23. Visited organisations MAY publish the IP forwarding policies imposed on the visitor network.

24. Govroam networks MAY make use of NAT.

25. Participants SHOULD implement IPv6 and allow routing of IPv6 on the govroam network.

26. If using IPv6 participants MUST allocate IPv6 addresses using SLAAC or DHCPv6.

27. Participants MUST log the IPv6 addresses allocated to visitors and the corresponding MAC addresses.

28. Participants SHOULD NOT use NAT with IPv6 but, if used, MUST log the address mappings.

29. Participants SHOULD provide IPv6 DNS services

30. Govroam Visited Wi-Fi services MAY implement WPA3 Enterprise if possible. If WPA3 Enterprise is implemented then 192-bit security MUST be disabled

31. Protected Management Frames (PMFs) SHOULD be implemented but MUST be set to 'Supported' rather than 'Required'.

5.3 Appendix III – Glossary

Term	Definition
802.11	See IEEE 802.11.
802.1X	See IEEE 802.1X.
AAA	Authentication, Authorisation, Accounting.
Accounting	The process of reporting the utilisation of a NAS to an accounting server.
Application proxy	An intermediary host which acts as both a server and a client for the purpose of making requests on behalf of other clients. Requests from clients are serviced internally or by passing them, with possible translation, on to other servers. Web proxies, which fetch web pages on behalf of web browser, are amongst the commonest type.
Authentication	The process of a supplicant attempting to confirm its identity to a NAS.
Authorisation	The process of enforcing the privileges accorded to an identity, and restricting access to resources accordingly.
Bluetooth	A specification for seamless wireless short-range communications of data and voice between both mobile and stationary devices.
Broadcast	See Broadcast SSID.
Broadcast SSID	An SSID that is advertised by a WAP.
Credentials	Information, such as a password or user certificate, that is used by an authentication protocol to establish a claimed identity.

DHCP	See Dynamic Host Configuration Protocol.
DHCPv6	See Dynamic Host Configuration Protocol for IPv6.
Dynamic Host Configuration Protocol	A protocol used to assign IP configuration information, such as an IP address, to hosts dynamically.
Dynamic Host Configuration Protocol for IPv6	A protocol used to assign IPv6 configuration information, such as an IP address, to hosts dynamically.
EAP	See Extensible Authentication Protocol.
EAP-PEAP	An EAP type implementing TLS to secure a tunnel in which a second EAP type is used to provide authentication.
EAP-TLS	An EAP type implementing authentication using certificates.
EAP-TTLS	An EAP type implementing TLS to secure a tunnel in which a Diameter-based transaction is performed to provide authentication.
Govroam	*Govroam* is a federated roaming service that provides secure network access by authenticating a user with their own credentials issued by their Identity Provider. The UK govroam federation is governed and supported by Jisc which provides technical support services, national RADIUS proxy infrastructure and defines this Technical Specification.
Extensible Authentication Protocol (EAP)	An authentication framework that supports multiple authentication types, including passwords, token cards, and certificates. EAP is specified in RFC2284 [10].
Home organisation	An organisation with affiliated users that can authenticate them when they attempt to authenticate at a Visited organisation.
ICMP	See Internet Control Message Protocol.
IEEE 802.11	A family of specifications for wireless LANs.
IEEE 802.11i	An amendment to the 802.11 standard specifying improved security mechanisms for IEEE 802.11 LANs.

IEEE 802.1X	A specification for port-based network access control, part of the IEEE 802 (802.1) group of protocols. It provides authentication to supplicants attached to a LAN port, establishing a network connection or preventing access from that port if authentication fails.
Internet Control Message Protocol	An IP protocol for reporting errors and other information relevant to IP packet processing.
IPv4	The most commonly deployed version of IP.
IPv6	The next generation version of IP. It includes a much larger address space, amongst other significant improvements.
Jisc	Jisc manages the operation and development of Janet, the UK's education and research network.
Man in the middle	An attack in which an attacker is able to read, insert and modify at will, messages between two parties without either party knowing that the link between them has been compromised.
NAI	See Network Access Identifier.
NAS	See Network Access Server.
ND	See Neighbour Discovery.
Neighbour Discovery	IPv6 Neighbour Discovery is an IPv6 protocol that determines relationships between other hosts on the LAN.
Network Access Identifier (NAI)	The NAI is used to address a user within a specific realm using the general format user@realm. The NAI is specified by RFC4282 (supersedes 2486).
Network Access Server (NAS)	A router or bridge that provides network access to a locally attached network for authenticated supplicants.
NREN	National Regional Education Network.
NRPS	National RADIUS Proxy Server. A host managed by Jisc that forwards packets between govroam participants' ORPSs and the eduroam top-level RADIUS proxies.

ORPS	Organisational RADIUS Proxy Server. A host managed by a participant that forwards RADIUS packets between the NRPS and internal RADIUS clients and servers.
Proxy	See RADIUS proxy or Application proxy.
Public Key Infrastructure	The framework in which digital certificates are created and used, based on a public and private keys.
RA	See Router advertisement.
RADIUS	Remote Authentication Dial-In User Service. A protocol for carrying authentication, authorisation, accounting and configuration information between a Network Access Server which desires to authenticate its links and a shared Authentication Server. RADIUS authentication is specified in RFC2865 and RADIUS accounting in RFC2866.
RADIUS proxy	A RADIUS server that can receive RADIUS requests from RADIUS clients and perform a decision to determine which RADIUS server the request should be forwarded onto for processing.
Router advertisement	An ND message used by routers to advertise their presence on the LAN.
Service Set Identifier	An identifier that a WAP and wireless stations use to communicate with each other.
Supplicant	A party requesting authentication from a NAS in order to access a network.
SSID	See Service Set Identifier.
Visited organisation	An organisation that provides authenticated visitors with access to a visitor LAN.
WAP	See Wireless Access Point.
Wireless Access Point	A bridge that enables forwarding between its associated wireless stations, and hosts on a directly-connected wired network.
WPA	A subset of the features offered by IEEE 802.11i and profiled by the WiFi Alliance. WPA is a less complete profile of IEEE 802.11i than is WPA2.

WPA2	A subset of the features offered by IEEE 802.11i and profiled by the WiFi Alliance. WPA2 is a more complete profile of IEEE 802.11i than is WPA.
WPA3	A subset of the features offered by IEEE 802.11i and profiled by the WiFi Alliance. WPA3 includes additional security protocols.