

govroam NL

Service Policy



Version 1

20 January 2015

1. Introduction

1.1. Introduction to govroam

govroam (government roaming) is the secure roaming access service for local and national governmental organizations. govroam is based on eduroam, the world-wide roaming access service developed for the international research and education community. eduroam started as a project of the Trans-European Research and Education Networking Association (TERENA), which still oversees its operation worldwide. It was originated from The Netherlands and has spread to many countries.

1.2. govroam policy document

This govroam NL policy document describes the leading policies and principles on which basis govroam is governed. All organisations participating in govroam have to accept and act to this policy document with regards to govroam.

1.3. Definitions

A **govroam Identity Provider (IdP)** is responsible for authenticating its own users by checking the credentials against a local identity management system. IdPs assert the identity of their users to govroam Service Providers when required. As they hold information about the organization a user is affiliated with, IdPs are often referred to as a user's Home Organisation or Home Institution and the terms are sometimes used interchangeably.

A **govroam Service Provider (SP)** maintains a network and provides Internet access, usually wirelessly, to govroam visitors from other organisations once they are successfully authenticated. For this reason, Service Providers are often and interchangeably referred to as a user's Visited Organization or Visited Institution.

A **Roaming Operator** performs a coordinating role — it provides RADIUS proxy servers to ensure that authentication requests from the SP reach the right IdP, which in the future may involve passing them to other Roaming Operators in other countries. The Roaming Operator also maintains governance and oversight of govroam within the country in which they operate. In The Netherlands the Roaming Operator is the Foundation Government Roaming Nederland (the Foundation) . In the course of their on-going collaboration, the Foundation has assigned the provision of some aspects of the govroam services to SURFnet, who also performs operational tasks for the Roaming Operator of govroam.

Because other countries are also starting govroam services it is foreseen that, likewise the eduroam structure, a future Roaming Confederation (RC) may bring together a number of ROs serving a geographical region is. This is yet to be decided.

1.4. The govroam trust model

govroam is a loose federation of related organisations. In order to work successfully, it depends on an implicit tripartite trust relationship between an IdP, a SP and the RO. The IdP advertises the govroam service to its users, and trusts that the SP will provide the service in a manner consistent

with expectations, recognising that its users will sometimes rely on govroom services to the exclusion of making other arrangements. IdPs further trust that SPs will secure their users' credentials and respect the confidentiality of their users' communications.

SPs trust that the user identities asserted by an IdP are bona fide members of their organization in good standing, and that an IdP has a contractual hold over those users in the form of an acceptable use policy or equivalent. SPs trust that IdPs will take action in terms of their organizational policies should abuse be reported. Some SPs have legal or governance obligations to retain information about the people they provide their service to, and trust that IdPs will do so on their behalf in exchange for reducing the complexity of gaining access.

Both IdPs and SPs trust RO to both provide the necessary infrastructure and oversight, and to respect the privacy of their respective users and their communications.

1.5. The need for policy

In order for govroom to work, participating organisations must enter into the trust relationships described above. This can only occur when all parties have a clear understanding of their own responsibilities as well as the responsibilities of the other parties involved. Such understanding can be achieved informally in a small community, but is difficult to establish in situations where the parties involved may never have met each other or even be aware of each other's existence.

Therefore this policy exists to provide a basis for a mutual understanding of responsibilities; to make the boundaries of the trust relationship clear to all parties; and to reduce the risk that the relationship will break down as the result of inadvertent or malicious actions by a minority.

However, to be effective, a policy must provide a means for enforcement; it must allow for sanctions against people or organisations that do not comply, whether due to action or inaction. As the govroom services are not a commercial services and only a small amount of money to cover the cost of RO exchanges hands in providing govroom services, the only possible sanction for violating the trust foundation of the services is suspension or ejection from the community. The policy provides a mechanism for achieving this in a fair and equitable way.

2. Eligibility

2.1. It is the intention of this policy to be inclusive. Thus, should any ambiguity arise as to whether or not an organisation is eligible to provide a govroom service in The Netherlands, the board of the Foundation is decisive.

2.2. All organisations

- Registered in the "Staatsalmanak voor het Koninkrijk der Nederlanden" and published at <https://almanak.overheid.nl/> or

- Established by Dutch law (as a result of a bill set by the House of Representatives and the Senate or an "Algemene Maatregel van Bestuur [AMVB])

are eligible to become Identity Providers and / or Service Providers.

2.3. Notwithstanding 2.1 and 2.2, organisations not registered in the “Staatsalmanak voor het Koninkrijk der Nederlanden” are not eligible to become Identity Providers.

2.4. Any organization that is not eligible to become Identity Provider, but that assents to this policy may request to become a Service Provider. Such request must be addressed to the Foundation and the Foundation in agreement with the members council will decide on the acceptance of such organisations to be allowed as Service Provider.

3. Application process

3.1. Eligible organisations interested in providing a govroam service in The Netherlands should approach the Roaming Operator.

3.2. The Roaming Operator will require that an authorized representative of the prospective participant sign a statement of compliance with this policy before configuring the national RADIUS proxy servers to recognise their organization’s realm(s) and/or proxy RADIUS requests.

3.3. Limited test services may be provided on request and at the Roaming Operator's discretion for a period of no more than forty five (45) calendar days prior to requiring a signed compliance statement.

3.4. Separate compliance statements are required for each of the Identity Provider and Service Provider roles.

4. Responsibilities of parties

4.1. Responsibilities of Users

4.1.1. The responsibilities of Users of the govroam services are described in a separate govroam The Netherlands document.

4.1.2. All users of govroam services in The Netherlands are expected to be aware of and comply with those responsibilities.

4.2. Responsibilities of the Roaming Operator (RO)

4.2.1. The RO provides and maintains the RADIUS proxy servers and other technical infrastructure required to connect The Netherlands nationally.

4.2.2. The RO maintains a web site at <http://www.govroam.nl/> that provides information about govroam services in The Netherlands, including details of the IdPs and SPs.

4.2.3. The RO is responsible for coordinating communication between participating organisations and maintains one or more mailing lists for this purpose.

4.2.4. The RO monitors the govroam service and provides operational information on its web site.

4.2.5. The RO is not responsible for any impact as a result of a loss or disruption of service.

4.2.6. The RO may elect to outsource the provision and/or operation of some or all of the technical infrastructure to another party of its choosing (currently SURFnet).

Any reference to the RO in this document must be taken to include both the RO and/or its appointed agents as appropriate.

4.3 Responsibilities of a govroom Identity Provider (IdP; Home Organisation)

4.3.1. There is an expectation of reciprocity (IdPs should act as SPs) where feasible. However, it is acknowledged that this may not always be logical, desirable or technically possible.

4.3.2. IdPs may assert the identity of any user who is both directly affiliated with their organization and would normally be eligible to benefit from services of that organization. Internal policy within an organization may further limit the scope of eligibility.

4.3.3. Should a user cease to be affiliated with an IdP, the IdP must cease asserting their identity as soon as practically possible.

4.3.4. IdPs must ensure that any user whose identity they assert is bound by their organizational acceptable use policies. Such policies must allow for sanction in case of abuse irrespective of a user's geographic location at the time of the breach.

4.3.5. IdPs accept responsibility for those users whose identities they assert and must take appropriate action in accordance with their organizational acceptable use policies where incidents of abuse are reported by visited organizations.

4.3.6. IdPs must make any user who might make use of govroom services aware of the existence of the govroom The Netherlands User responsibilities document (for example by publishing a link to it from their web page describing govroom services).

4.3.7. IdPs are expected to act as first-line support for their own users; IdPs must publish up-to-date contact details for their help desk (or equivalent support structure) in the appropriate place on the RO's web site.

4.3.8. IdPs must meet or exceed the technical specifications described in Annex A.

4.3.9. IdPs must log the information detailed in Annex C and retain it for at least the minimum prescribed period.

4.3.10. Every IdP must nominate at least, and preferably more, technical contacts (people responsible for maintaining their RADIUS service), and provide up-to-date details of such to the RO. At least one contact must be subscribed to the relevant mailing list maintained by the RO.

4.3.11. There is an expectation that IdPs will cooperate with the RO.

4.4. Responsibilities of a govroom Service Provider (SP; Visited Organisation)

- 4.4.1. There is no expectation of reciprocity (SPs need not act as IdPs).
- 4.4.2. SPs must meet or exceed the technical specifications described in Annex B.
- 4.4.3. SPs must log the information detailed in Annex C and retain it for at least the minimum prescribed period.
- 4.4.4. SPs must provide govroam services free-of-charge to all eligible users, irrespective of Home Organization. For the avoidance of doubt, where an SP also acts as an IdP their users are not considered govroam users when using services provided by their home organization.
- 4.4.5. SPs must provide govroam services without any commercial purpose or any monetization. The collection of data on client devices and/or persons for any other purpose than for sound technical or legal reasons is not allowed.
- 4.4.6. SPs should assist IdPs in supporting their users when required, though the IdP must take primary responsibility.
- 4.4.6. SPs are encouraged to provide unfiltered and unrestricted Internet access. However, at a minimum they must provide the ability to browse the web, send & receive email, and use SSH (i.e. outgoing TCP ports 22, 80, 110, 143, 443, 465, 587, 993, and 995). Additionally, support for common VPN protocols should be provided if possible. Captive portals or other forms of walled garden must not be used; transparent proxies and NAT may be used.
- 4.4.7. Should an SP filter (firewall), restrict (shape, limit bandwidth, etc.) or monitor (log, intercept, etc.) Internet access, it must fully disclose its local policies on a dedicated web page. A link to such information must be provided in the appropriate place on the RO's web site.
- 4.4.8. Restrictions should only be imposed for sound technical or legal reasons, and must be reviewed at least once a year.
- 4.4.9. Should an SP wish to impose an acceptable use policy or other terms and conditions on visiting users it must publish the policy on its web site and provide a link in the appropriate place on the RO's web site.
- 4.4.10. Every SP must nominate at least one, preferably more, technical contacts (people responsible for maintaining their network service), and provide up-to-date details of such to the RO. At least one contact must be subscribed to the relevant mailing list maintained by the RO.
- 4.4.11. There is an expectation SPs will cooperate with the RO.

5. Occasion for sanctions

5.1. Sanctions by the Roaming Operator

- 5.1.1. The RO may refuse or limit service to an IdP or an SP based on their RADIUS realm.
- 5.1.2. When considering sanctions, the IdP and SP services provided by an organization must be considered separately — an IdP should not be restricted because of breaches of the SP requirements and vice versa.

5.1.3. Sanctions may be imposed when this policy is breached, when an IdP or SP does not cooperate with the RO, or where sound technical reasons exist to limit service.

5.1.4. The process leading to the imposition of sanctions must provide an IdP or SP with an opportunity to make representations to a clearly stated case for the imposition of the sanction(s).

5.1.5 The RO should work with the affected organization towards an effective long-term resolution.

5.1.6. Any sanction should be regularly reviewed. Service must be restored as soon as the RO is satisfied that the underlying cause has been adequately resolved.

5.2. Sanctions by Identity Providers

5.2.1. IdPs may withdraw an individual user's ability to use govroam by configuring their own authentication servers not to assert their identity.

5.2.2. Such sanctions would be imposed in terms of the IdP's internal policies and are outside the scope of this document.

5.2.3. There is an expectation that IdPs will impose those sanctions provided for in their organizational acceptable use policies should an SP provide evidence that a user has breached any law or relevant policy. There is no obligation to report the details of such sanctions to the SP.

5.3. Sanctions by Service Providers

5.3.1. SPs may limit or prevent use of their network by all users from a particular IdP by configuring their network to recognize (and reject) its RADIUS realm; in some cases SPs may also be able to block a single visiting user.

5.3.2. Such sanctions must only be imposed in response to abuse or for sound technical reasons (denial of service, excessive use, etc.).

5.3.3. Sanctions that limit service should be considered a short-term measure, and must be reviewed or removed as soon as possible.

5.3.4. If sanctions are to be imposed for more than one week, the SP must immediately notify the RO of the affected realm(s) and the reasons for such sanction.

5.3.5. As a matter of courtesy, the SP must notify the IdP responsible for the affected realm of the reasons for such sanction.

5.3.6. Where sanction is imposed in response to abuse, the SP must cooperate with the relevant IdP in any ensuing investigation.

5.3.7. Should an SP be of the opinion that an IdP is responsible for repeated infractions it must escalate the matter to the RO who will take appropriate action in accordance with this policy.

5.4. Other recourses

5.4.1. This policy does not limit or prevent either an SP or the RO from independently seeking legal recourse against a govroam user who is believed to have committed a sufficiently serious abuse or violation.

5.4.2. Such an action would normally be in addition to any sanction that may be imposed against the govroam user by their Home Organization, and should be considered accordingly.

5.4.3. The relevant IdP should be informed of such an action.

5.5. Disputes

5.5.1. In the event of a dispute between an IdP and an SP, the RO shall act as arbitrator and will give the final ruling. In such cases the RO will have internal procedures to follow which may include the consult of its Board

6. Authority and changes

6.1. The RO owns this policy document, the associated Annexes and User documents.

6.2. The RO may make changes to meet regulatory compliance or legislative requirements, or in response to changing technology, or as a result of feedback obtained from its user community. Wherever possible such changes shall be made in consultation with participating organizations.

6.3. Changes to this policy must be published on the RO's web site and distributed via the RO's mailing list(s) for IdPs and SPs.

6.4. Any policy change becomes effective thirty (30) days after publication.

6.5. Any IdP or SP that continues to make use of the govroam service after the effective date will be deemed to have accepted the revised policy.

Annex A Technical requirements for Identity Providers

A.1. IdPs must implement a RADIUS service to connect to the National govroam infrastructure. This service must be capable of supporting an Extensible Authentication Protocol (EAP) method for all of that organization's users that is suitable for use with both WPA2 and 802.1X, and supports mutual authentication and end-to-end encryption of credentials.

A.2. IdPs must configure their RADIUS servers to recognize a realm that mirrors the structure of a DNS name within a Dutch (.nl) domain delegated to their organization. Note that the realm does not need to be registered in DNS.

A.3. IdPs should create a test user to allow the RO to monitor their authentication services. The password associated with such a user should be randomly generated and must be provided to the RO. The test user account need only exist on govroam-facing RADIUS servers and should not be authorized to access any of the IdP's other services or infrastructure.

A.4. IdPs should only send RADIUS accept messages for valid authenticated local users; they must not send RADIUS accept messages for invalid or unauthenticated users, or for users in realms other than their own.

A.5 IdPs should provide support to their users. Any support matters may be escalated to the RO to coordinate and resolve.

Annex B Technical requirements for Service Providers

B.1. SP networks must implement 802.1X with a RADIUS interface to connect to the govroam infrastructure.

B.2. SPs must route all Extensible Authentication Protocol (EAP) messages destined for RADIUS realms other than their own to the RO's RADIUS proxy servers, and should not modify such messages in transit.

B.3. SPs may provide govroam services using any media, but at the very least wireless network access complying with IEEE 802.11b and/or 802.11g should be provided.

B.4. SP wireless networks must broadcast the SSID "govroam" — note that case is important, and govroam is specified entirely in lowercase.

B.5 SPs networks must provide IP address and DNS resolution auto-configuration infrastructure.

B.6 SPs should provide routable IP addresses, and MAY provide NAT translation.

B.7. SP wireless networks must support WPA2+AES, and may additionally support WPA/TKIP as a courtesy to users of older devices.

B.8. Where an SP provides wired govroam services on selected network ports, those ports should be clearly marked to identify them as such (for instance by labelling with the word "govroam" or displaying the govroam logo).

B.9. SPs should consider making use of a visitor VLAN for govroam -authenticated users, and should not share this with other network services.

Annex C Logging requirements

C.1. govroam IdPs must log all authentication attempts; the following information must be recorded:

C.1.1. timestamp of authentication requests and corresponding responses

C.1.2. the outer EAP identity in the authentication request (User-Name attribute)

C.1.3. the inner EAP identity (actual user identifier)

C.1.4. the MAC address of the connecting client (Calling-Station-Id attribute)

C.1.5. type of authentication response (i.e. Accept or Reject).

C.2. govroam SPs should keep sufficient logging information to be able to identify the responsible Identity provider for the logged-in user, by logging:

C.2.1. timestamp of authentication requests and corresponding responses

C.2.2. the outer EAP identity in the authentication request (User-Name attribute)

C.2.3. the MAC address of the connecting client (Calling-Station-Id attribute)

C.2.4. type of authentication response (i.e. Accept or Reject)

C.2.5. correlation information between a client's layer 2 (MAC) address and the layer 3 (IP) address that was issued after login if public addresses are used (e.g., ARP sniffing logs or DHCP logs)

C.3. Clocks used for logging timestamps must be synchronised via the Network Time Protocol (NTP; SNTP) or acceptable to the RO.

C.4. Logs must be retained for at least six months.

C.5. Users' right to privacy must be respected. Unless otherwise required by law, access to logs of govroam activities should be restricted to the SP's operational staff, the RO's staff, and the technical contacts of the relevant IdP (and then only to the extent necessary for the efficient functioning of govroam and the discharge of their responsibilities under this policy).

Information about a particular individual's use of the network should not be released to other parties without appropriate process.