Regolamento della Federazione Italiana eduroam

Versione 2.1

Maggio 2016

1 Definizione dei termini

Le parole chiave utilizzate in questo documento, sempre scritte in maiuscolo ed indicate nella tabella di seguito con a fianco la loro versione originale in lingua inglese, devono essere interpretate secondo le definizioni originali in lingua inglese specificate nel documento RFC2119 [1].

DEVE	MUST / SHALL
NON DEVE	MUST NOT / SHALL NOT
OBBLIGATORIO	REQUIRED
DOVREBBE	SHOULD
NON DOVREBBE	SHOULD NOT
CONSIGLIABILE	RECOMMENDED
POTREBBE / PUÒ	MAY
FACOLTATIVO	OPTIONAL

2 Definizioni generali

2.1 Scopo

Lo scopo della **Federazione Italiana eduroam** (anche **Federazione**, nel seguito) è di facilitare l'accesso alla rete GARR agli utenti mobili (*roaming*) delle organizzazioni partecipanti.

La **Federazione** è coordinata dal **Consortium GARR** (anche **GARR,** nel seguito), che la rappresenta presso la **Confederazione Europea eduroam**.

Questo documento contiene le regole che devono essere seguite dalle Organizzazioni membri della **Federazione** e gli impegni e le responsabilità del **GARR**.

Il modulo di sottoscrizione è contenuto nell'**Appendice A** e deve essere firmato dal Direttore del **GARR** e dal rappresentante legale dell'Organizzazione.

Se un'Organizzazione desidera uscire dalla Federazione è sufficiente che lo comunichi alla Segreteria del **GARR**.

eduroam è un marchio registrato della **GÈANT Association**, ed è l'abbreviazione di Educational Roaming. Maggiori informazioni sono reperibili agli indirizzi http://www.eduroam.it/ e http://www.eduroam.org/.

2.2 Federazione Italiana eduroam

La **Federazione Italiana eduroam** ha lo scopo di:

- offrire agli utenti dei propri membri, che si trovino presso un'altra delle organizzazioni partecipanti, l'accesso alla rete GARR e alle altre reti a essa connesse, attraverso l'infrastruttura di rete dell'Organizzazione ospitante, utilizzando le credenziali di accesso della propria Organizzazione;
- garantire la protezione delle credenziali di accesso e dei dati scambiati.

2.3 Confederazione Europea eduroam

La **Federazione Italiana eduroam** è un membro della **Confederazione Europea eduroam** (anche **Confederazione**, nel seguito), le cui regole [3], nell'ambito del progetto GÈANT, sono state sottoscritte da **GARR**.

Le specifiche tecniche della **Confederazione** sono in [4].

2.4 Servizio Mondiale eduroam

La **Confederazione Europea eduroam** è collegata a tutte le altre Confederazioni eduroam a livello mondiale, costituendo il **Servizio Mondiale eduroam**, il cui scopo è di estendere a livello internazionale i servizi forniti ai propri membri dalle Federazioni nazionali, con regole di utilizzo il più possibile omogenee, compatibilmente con le differenze imposte dalle legislazioni nazionali.

2.5 *Peering* con altre Federazioni

La **Federazione** PUÒ anche stabilire accordi di *peering* con altre Federazioni che non facciano parte della Confederazione o del Servizio Mondiale eduroam, ma che forniscano servizi di mobilità equivalenti. In tal caso la **Federazione** DEVE stabilire le politiche di *peering* che verranno adottate. Tali accordi non si estendono alle Federazioni che appartengono alla Confederazione e ai relativi servizi.

2.6 Accesso ai servizi della Federazione

Il servizio di accesso alla rete per utenti *roaming* fornito dalla **Federazione** è disponibile a tutti gli utenti finali delle Organizzazioni membro, agli utenti delle altre Federazioni che hanno aderito alla Confederazione, al Servizio Mon-

diale eduroam e alle altre Federazioni con cui esista un accordo di *peering*.

I membri della **Federazione** POSSONO limitare l'accesso ai servizi forniti alle altre Federazioni nel caso in cui le politiche praticate da queste, o da alcuni dei loro membri, non siano in grado di garantire dei requisiti previsti dalla legislazione in vigore in Italia o non rispettino i requisiti minimi di sicurezza richiesti dalla **Federazione**.

I partecipanti alla **Federazione** DEVONO comunicare al **GARR** le eventuali limitazioni all'accesso che essi stabiliscono, nonché ogni loro modifica.

2.7 Gestione e risoluzione dei problemi

In caso di problemi, gli utenti *roaming* devono, in prima istanza, rivolgersi alla propria Organizzazione; se necessario, sarà il personale di questa a contattare e coinvolgere l'Organizzazione ospitante.

2.8 Acceptable Use Policy locali

I membri della **Federazione** devono rendere disponibili le proprie *Acceptable Use Policy* (AUP) agli utenti ospitati, che sono tenuti a rispettarle, astenendosi da comportamenti a esse contrari, anche se permessi in altre sedi.

3 Ruoli e Responsabilità

Esistono quattro ruoli fondamentali nel servizio eduroam:

1. **eduroam Service Provider**: l'organizzazione che coordina e gestisce a livello nazionale il servizio eduroam;
2. **Identity Provider**: le Organizzazioni che partecipano al servizio fornendo ai propri utenti le credenziali necessarie per poter accedere alla rete;
3. **Resource Provider**: le Organizzazioni che partecipano al servizio fornendo gli apparati e l'infrastruttura di rete che permette agli utenti di accedere alla rete;
4. **User**: l'utente finale del servizio.

In molti casi le organizzazioni svolgono allo stesso tempo il ruolo di *Identity Provider* (per i propri utenti) e *Resource Provider* (per tutti gli utenti del servizio eduroam, compresi i propri).

La partecipazione alla **Federazione Italiana eduroam** in qualità di *Identity Provider* è riservato **esclusivamente** alle Organizzazioni afferenti alla rete realizzata e gestita dal **Consortium GARR**.

La partecipazione in qualità di **solo** Resource Provider è consentito a qualsiasi Organizzazione che metta gratuitamente a disposizione l'accesso alla propria rete ai membri della Federazione, della Confederazione e del Servizio Mondiale eduroam.

3.1 eduroam Service Provider

Il **Consortium GARR** è l'organizzazione responsabile in Italia del servizio nazionale eduroam (**eduroam Service Provider**). Il **GARR** agisce nel ruolo di autorità per l'attuazione delle policy della **Federazione Italiana eduroam**, in accordo con quella della **Confederazione Europea eduroam** [3].

Il **GARR** PUÒ intraprendere misure urgenti, ivi compresa la disconnessione del servizio, l'esclusione di un partecipante dalla Federazione e l'interruzione dei *peering*, qualora le ritenga necessarie per preservare l'integrità e la sicurezza del servizio stesso.

I compiti del **GARR** consistono in:

- coordinare il servizio eduroam a livello nazionale, dando supporto ai contatti tecnici designati dalle Organizzazioni partecipanti alla **Federazione**;
- mantenere i collegamenti con le altre Federazioni eduroam europee e con i relativi server di autenticazione;
- contribuire allo sviluppo della **Federazione** e dei servizi offerti;
- mantenere e sviluppare la rete dei server di autenticazione nazionali, che connettono le Organizzazioni partecipanti.

Il **GARR** è responsabile:

- della gestione del supporto tecnico di secondo livello che copre l'assistenza nella fase di preconnessione alla **Federazione** e l'assistenza tecnica alle Organizzazioni connesse;
- del mantenimento di un sito web con informazioni tecniche, di servizio, di policy e procedurali;
- del mantenimento delle mailing list dedicate al servizio eduroam;
- del coordinamento delle comunicazioni tra i membri della **Federazione**, in modo tale che le policy e le procedure indicate in questo documento siano adottate in tempi rapidi.

Il **GARR** interagisce con i contatti tecnici designati dalle Organizzazioni partecipanti per collaudare uno o più dei seguenti aspetti:

- connettività iniziale;
- processo di autenticazione ed autorizzazione;
- i servizi offerti;
- le attività di monitoraggio;
- le conformità delle configurazioni dei server di autenticazione alle policy del servizio.

Come ultimo mezzo per la risoluzione di eventuali inadempienze, il **GARR** ha il diritto di imporre sanzioni tecniche alle Organizzazioni coinvolte.

Il **GARR** non si assume alcuna responsabilità per danni o problemi che derivino dall'abuso, da interruzioni o da malfunzionamenti del servizio eduroam.

3.2 Identity Provider

Il ruolo dell'Identity Provider, gestito dall'Organizzazione di appartenenza dell'utente (*Home Organization*), è di fornire le credenziali d'identificazione per il proprio personale e per tutti coloro che hanno diritto di accesso alla rete GARR, come definito dalla Acceptable Use Policy in vigore.

Sempre come stabilito dalla AUP, l'Identity Provider DEVE

- mettere in atto una procedura di assegnazione credenziali che preveda l'accertamento dell'identità personale dell'utente a cui vengono assegnate;
- essere in grado, su richiesta del **GARR** o delle pubbliche autorità, di fornire in tempi rapidi l'identità dell'utente a cui corrispondono le credenziali indicate;
- rendere pubblica la propria procedura di identificazione e assegnazione delle credenziali;
- nominare almeno una persona come referente ufficiale presso il **GARR**;
- collaborare con il **GARR** nel caso di abusi, incidenti di sicurezza o altri problemi che derivino dal servizio eduroam stesso, in accordo con l'AUP della rete GARR, nonché con le politiche di sicurezza della rete GARR e la legislazione in vigore;
- utilizzare identità EAP **esterne** della forma <*name*>`@realm`, dove `realm` è un dominio DNS gestito dall'Organizzazione e <*name*> è una stringa arbitraria;
- utilizzare almeno un server di autenticazione, che
  - rispetti le specifiche di RFC2685 (RADIUS) e RFC2866 (RADIUS Accounting);
  - rispondere alle eventuali ICMP Echo Request inviati dai processi di monitor installati dal **GARR;**
  - accetti almeno un tipo di autenticazione EAP;
- creare, su richiesta del **GARR**, un "test account eduroam" (credenziali di accesso al servizio) messo a disposizione del **GARR** per finalità di test e debugging del servizio;
- conservare le informazioni relative agli accessi secondo le modalità indicate nella sezione 4;
- agire come supporto tecnico e di servizio per i propri utenti: come indicato nel paragrafo 2.7, solamente i responsabili locali possono scalare le problematiche di supporto tecnico, di servizio o di sicurezza a nome dei propri utenti presso il **GARR** o presso le altre Organizzazioni.

Gli Identity Provider sono anche responsabili del buon comportamento dei propri utenti, nonché della loro informazione sul rispetto delle policy in vigore.

L'Identity Provider non può essere ritenuto responsabile per danni o problemi

che derivino dall'abuso, da interruzioni o da malfunzionamenti del servizio eduroam.

3.3 Resource provider

Il ruolo di un Resource Provider consiste nel fornire connettività ed accesso alla rete GARR agli utenti eduroam che si siano autenticati secondo le modalità stabilite.

Il Resource Provider DEVE fornire accesso ad *almeno* le seguenti porte e protocolli:

- IPSec VPN: protocolli IP 50 (ESP) e 51 (AH) (entrata e uscita) e UDP/500 (IKE) (uscita);
- OpenVPN 2.0: UDP/1194 (entrata e uscita);
- IPv6 Tunnel Broker service: protocollo IP 41 (entrata e uscita);
- IPsec NAT-Traversal: UDP/4500 (entrata e uscita);
- Cisco IPSec VPN over TCP: TCP/10000 (uscita);
- PPTP VPN: protocollo IP 47 (GRE) (entrata e uscita) e TCP/1723 (uscita);
- SSH: TCP/22 (uscita);
- HTTP e HTTPS: TCP/80, TCP/443, TCP/3128, TCP/8080 (uscita);
- IMAP4 e IMAPS: TCP/143 e TCP/993 (uscita);
- POP3 e POP3S: TCP/110 e TCP/995 (uscita);
- (S)FTP passivo: TCP/21 (uscita);
- SMTPS: TCP/465 (uscita);
- SMTP submission via STARTTLS: TCP/587 (uscita).

Inoltre il Resource Provider DEVE:

- offrire *almeno* servizi wireless LAN IEEE 802.11b, mentre è CONSIGLIATO IEEE 802.11g e PUÒ essere fornito anche IEEE 802.11a;
- utilizzare e annunciare il SSID "eduroam": nel caso di conflitti con reti vicine, PUO' utilizzare un SSID del tipo "eduroam-...";
- supportare IEEE 802.1X;
- supportare WPA2/AES (WPA/TKIP PUO' essere supportato);
- nominare almeno una persona responsabile del servizio, comunicandone il nominativo al **GARR**;
- assicurarsi che i sistemi utilizzati dagli utenti roaming siano configurati e mantenuti secondo i correnti standard di sicurezza, in modo da non mettere in pericolo la sicurezza propria e delle altre Organizzazioni;
- predisporre una pagina web che contenga la propria AUP e le informazioni necessarie per la connessione, tra cui **almeno**:

    - un testo che conferma l'adesione del Resource Provider a questo Regolamento;
    - i dettagli del SSID che viene utilizzato;
    - i dettagli dei servizi autorizzati agli utenti eduroam;
    - l'eventuale presenza di proxy;
    - i riferimenti del Resource Provider locale (punto di contatto);
- collaborare con l'Organizzazione a cui appartengono gli utenti del servizio roaming per risolvere eventuali problemi;
- collaborare con il **GARR** per la risoluzione di eventuali incidenti di sicurezza;
- conservare le informazioni relative agli accessi secondo le modalità indicate nella sezione 4.

Il Resource Provider DOVREBBE

- oltre alle porte e ai protocolli sopra indicati, consentire tutte le connessioni in uscita;
- evitare l'uso del NAT;
- fornire connettività IPV6.

Il Resource Provider NON DOVREBBE utilizzare un *application* o *interception proxy*: se lo fa NON DEVE utilizzarlo per richiedere agli utenti dati personali.

Il Resource Provider non può essere ritenuto responsabile per danni o problemi che derivino dall'abuso, da interruzioni o malfunzionamenti del servizio eduroam.

3.4 Utenti

L'utente del servizio eduroam è una persona che utilizza il servizio di accesso eduroam presso un Resource Provider.

L'utente è responsabile per il buon uso e la conservazione delle proprie credenziali di accesso e DEVE:

- mettere in atto ogni misura volta ad impedirne l'abuso e la loro divulgazione a terzi: le credenziali sono strettamente personali;
- verificare che si sta connettendo ad un autentico eduroam Resource Provider, ad esempio esaminando il certificato del RADIUS server di autenticazione e collegandosi soltanto a reti protette dal servizio 802.1X;
- informare immediatamente il proprio Identity Provider se sospetta che ci siano state violazioni di sicurezza.

4 Logging

Sia l'Identity Provider sia il Resource Provider DEVONO registrate tutte le richieste di accesso e di autenticazione. In particolare DEVONO essere registra-

te almeno le seguenti informazioni :

- data e ora di ogni operazione;
- il Calling-station-id nelle richieste di autenticazione;
- il risultato dell'autenticazione restituito dall'authentication server;
- le identità interna ed esterna della richiesta (per gli Identity Provider);
- l'accoppiamento tra l'indirizzo hardware dell'apparato usato dall'utente e l'indirizzo IP assegnato (per i Resource Provider).

I sistemi di logging DEVONO avere data ed ora sincronizzate con sistemi affidabili.

Le informazioni registrate DEVONO essere mantenute per un periodo minimo di 6 (sei) mesi, o maggiore se prescritto dalla legislazione in vigore.

5 Bibliografia

[1] *RFC 2119*, http://www.ietf.org/rfc/rfc2119.txt

[2] *Acceptable Use Policy – AUP*, http://www.garr.it/utenti/regole-di-accesso/acceptable-use-policy-aup

[3] *European Confederation eduroam Policy*, https://www.eduroam.org/wp-content/uploads/2016/05/GN3-12-194_eduroam-policy-for-signing_ver2-4_1_18052012.pdf

[4] e*duroam Policy Service Definition*, https://www.eduroam.org/wp-content/uploads/2016/05/GN3-12-192_eduroam-policy-service-definition_ver28_26072012.pdf

Versioni

2.1

Aggiornamento in seguito al passaggio da TERENA a GÈANT.

Chiarificazioni.

2.0

Aggiornamento in seguito al rilascio della nuova versione della *eduroam Policy Service Definition* e della *European Confederation eduroam Policy*.

1.4

Aggiunta la richiesta che i partecipanti forniscano la URL di una pagina con le informazioni necessarie per il collegamento ad eduroam, come indicato nella sezione 3.3.

Appendice A
Adesione alla Federazione Italiana eduroam

Organizzazione partecipante: _____

☐ Partecipa come Resource Provider;

☐ Partecipa come Identity Provider per i seguenti “realm”:

_____

_____

_____

Contatto Tecnico 1: Nome _____

E-mail _____

Tel: _____

Contatto Tecnico 2: Nome _____

E-mail _____

Tel: _____

Informazioni locali (URL): _____

Dichiaro di aver preso visione e di accettare integralmente il *Regolamento della Federazione Italiana eduroam, Versione 2.1,* di cui il presente modulo è parte sostanziale.

Data: _____

Per l’organizzazione partecipante: Per il Consortium GARR

_____ _____

(nome, titolo e firma) (nome, titolo e firma)