Regolamento della Federazione Italiana Eduroam

Versione 1.4

Gennaio 2009

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], riportato in **Appendice "A"**.

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 e alle altre reti ad essa connesse agli utenti mobili (*roaming users*) delle organizzazioni partecipanti (**servizio Eduroam**).

La **Federazione** è coordinata dal **Consortium GARR** (anche **GARR,** nel seguito), che la rappresenta presso le altre federazioni e confederazioni.

Questo documento contiene le regole che devono essere seguite dalle organizzazioni che vogliono far parte delle **Federazione** e gli impegni e responsabilità del **GARR**. Il modulo di sottoscrizione, che fa parte integrante di questo documento, è contenuto nell'Appendice B e deve essere firmato dai rappresentanti legali del **GARR** e dell'organizzazione. Se un'organizzazione desidera uscire dalla Federazione è sufficiente che lo comunichi alla Segreteria del **GARR**.

Eduroam è un marchio registrato di TERENA, ed è l'abbreviazione di Educational Roaming. Maggiori informazioni sono reperibili all'indirizzo http://www.eduroam.org.

2.2 Principi base

I principi base della **Federazione Italiana Eduroam** sono i seguenti:

- offrire agli utenti dei propri membri, che si trovino presso un'altra delle organizzazioni partecipanti, l'accesso alla rete GARR (ed alle altre reti ad essa connesse), attraverso l'infrastruttura di rete dell'organizzazione ospite, utilizzando le credenziali di accesso utilizzate dalla propria organizzazione (servizio Eduroam);
- garantire la protezione delle credenziali di accesso e dei dati scambiati dai *roaming user.*

2.3 Partecipazione alla Federazione Italiana Eduroam

L'accesso alla **Federazione Italiana Eduroam** è riservato esclusivamente alle organizzazioni afferenti alla rete realizzata e gestita dal **Consortium GARR** (rete GARR).

2.4 Confederazione Europea Eduroam

La **Federazione Italiana Eduroam** è un membro della **Confederazione Europea Eduroam**, le cui regole sono definite in [3] e sono state sottoscritte dal **Consortium GARR** a nome della **Federazione**. Lo scopo della **Confederazione Europea Eduroam** è di estendere a livello internazionale i servizi forniti ai propri membri dalle federazioni nazionali Eduroam, con regole di utilizzo il più possibile omogenee, compatibilmente con le differenze imposte dalle legislazioni nazionali. Le specifiche tecniche della **Confederazione Europea Eduroam** sono in [4].

2.5 *Peering* con altre federazioni non Eduroam

La **Federazione Italiana Eduroam** PUÒ anche stabilire accordi di *peering* con altre federazioni che non fanno parte della **Confederazione Europea Eduroam**, ma che forniscono servizi di mobilità equivalenti. In tal caso la **Federazione** DEVE stabilire le politiche di *peering* che verranno adottate. Tali accordi di *peering* non si estendono alle federazioni che appartengono alla **Confederazione Europea Eduroam** e ai relativi servizi.

2.6 Accesso ai servizi della Federazione Italiana Eduroam

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 Europea 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 alcuni 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 User 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 ad esse contrari, anche se permessi in altre sedi.

3 Ruoli e Responsabilità

Esistono quattro ruoli fondamentali nel servizio Eduroam:

1. **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).

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 della 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 alle federazione, l'interruzione dei peering, qualora le ritenga necessarie per preservare l'integrità e la sicurezza del servizio stesso.

I compiti del **Consortium GARR** consistono in:

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

Il **GARR** è responsabile:

- della gestione del supporto tecnico di secondo livello che copre l'assistenza nella fase di pre-connessione 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 le organizzazioni che partecipano al servizio Eduroam, in modo tale che le policy e procedure indicate nel presente documento siano adottate dai membri della federazione in tempi rapidi.

Il **GARR** interagisce con il contatto tecnico designato della organizzazione partecipante per collaudare uno o più dei seguenti aspetti:

- connettività iniziale;
- processo di autenticazione ed autorizzazione;
- i servizi autorizzati offerti;
- le attività di monitoraggio (log service);
- le principali configurazioni dei server di autenticazione in modo che siano conformi alle policy del servizio.

Come ultimo mezzo per la risoluzione di inadempienze, il **Consortium GARR** ha il diritto di imporre sanzioni tecniche alle organizzazioni non adempienti.

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, l'organizzazione di appartenenza dell'utente del servizio Eduroam (*Home Organization*), è di agire in qualità di fornitore di cre-

denziali d'identificazione per il proprio personale, nonché per tutti coloro che hanno diritto di accesso alla rete GARR, come definito dalle AUP in vigore (ivi compresi quindi anche gli studenti regolarmente iscritti, ove applicabile).

Sempre come stabilito dalle 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 **Consortium GARR** e/o delle pubbliche autorità, di fornire in tempi rapidi l'identità personale dell'utente a cui corrispondono le credenziali indicate;
- rendere pubblica la propria procedura di identificazione ed assegnazione delle credenziali;
- nominare una persona responsabile del servizio Eduroam in qualità di 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 le AUP della rete GARR, nonché con le politiche di sicurezza della rete GARR e la legislazione in vigore;
- utilizzare nomi utenti conformi a RFC4282 e appartenenti al proprio realm;
- utilizzare almeno un server di autenticazione che rispetti le specifiche di RFC2685 (RADIUS) e RFC2866 (RADIUS Accounting), che DEVE rispondere a eventuali ICMP Echo Request inviati dai processi di monitor installati dal **GARR** e DEVE accettare 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 (log) secondo le modalità indicate nella sezione 4.

L'identity Provider agisce anche come supporto tecnico e di servizio per i suoi utenti che vogliono accedere presso gli altri Resource Provider ai servizi Eduroam. Come indicato nella 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 **Consortium GARR** o presso le altre organizzazioni partecipanti alla **Federazione Eduroam**.

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 si assume alcuna responsabilità 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 (ed alle reti ad essa collegate) agli utenti Eduroam che si siano autenticati in modo valido 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) in entrata e in uscita e UDP/500 (IKE);
- OpenVPN: UDP/1194;
- IPv6 Tunnel Broker service: protocollo IP 41 in entrata e in uscita;
- IPsec NAT-Traversal: UDP/4500;
- Cisco IPSec VPN over TCP: TCP/10000 in uscita;
- PPTP VPN: protocollo IP 47 (GRE) in entrata e in uscita e TCP/1723 in uscita;
- SSH: TCP/22 in uscita;
- HTTP e HTTPS: TCP/80 e TCP/443 in uscita;
- IMAP4 e IMAPS: TCP/143 e TCP/993 in uscita;
- IMAP3: TCP/220 in uscita;
- POP3 e POP3S: TCP/110 e TCP/995 in uscita;
- (S)FTP passivo: TCP/21 in uscita;
- SMTPS: TCP/465 in uscita;
- SMTP submission via STARTTLS: TCP/587 in uscita;
- RDP: TCP/3389 in 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” (salvo eventuali conflitti con reti vicine che si sovrappongono: in tal caso il Resource Provider DEVE concordare con il **GARR** il SSID da utilizzare e DEVE mettere in atto le misure necessarie per informare del diverso SSID gli utenti);
- supportare il protocollo IEEE 802.1X e almeno WPA/TKIP;
- 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 e Policy, nonché il testo stesso di questo documento;
    - i dettagli del SSID Eduroam che viene utilizzato (in broadcast o non in broadcast);
    - i dettagli dei servizi autorizzati agli utenti Eduroam;

    - i riferimenti del Resource Provider locale (punto di contatto);
    - il logo Eduroam ed il suo trademark statement originale;
    - il collegamento al servizio della Federazione Italiana Eduroam;
- 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 (log) secondo le modalità indicate nella sezione 4.

Il Resource Provicer DOVREBBE fornire indirizzi IP pubblici agli utenti Eduroam; se disponibili, POSSONO essere forniti anche indirizzi Ipv6.

Il Resource Provider non si assume alcuna responsabilità 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 conoscenza 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 registrate almeno le seguenti informazioni :

- data e ora di ogni operazione (richiesta di autenticazione; assegnazione di indirizzo IP, …);
- il risultato dell'autenticazione restituito dall'authentication server;
- per gli Identity Provider: l'identità interna della richiesta, anche quando viene trasmessa via rete un'identità fittizia;
- per i Resource Provider: l'accoppiamento tra l'indirizzo hardware dell'apparato usato dall'utente e l'indirizzo IP assegnato.

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] AUP della rete GARR - http://www.garr.it/reteGARR/aup.php?idmenu=collegare

[3] *European Eduroam Confederation Policy*, GN2-07-328 http://preview.tinyurl.com/4brvvt

[4] Eduroam Service Definition and Implementation Plan, GN2-07-327v2 http://preview.tinyurl.com/3p7j2d

Versioni

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
RFC2119

Network Working Group S. Bradner
Request for Comments: 2119 Harvard University
BCP: 14 March 1997
Category: Best Current Practice

Key words for use in RFCs to Indicate Requirement Levels

Status of this Memo

This document specifies an Internet Best Current Practices for the Internet Community, and requests discussion and suggestions for improvements. Distribution of this memo is unlimited.

Abstract

In many standards track documents several words are used to signify the requirements in the specification. These words are often capitalized. This document defines these words as they should be interpreted in IETF documents. Authors who follow these guidelines should incorporate this phrase near the beginning of their document:

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

Note that the force of these words is modified by the requirement level of the document in which they are used.

1. MUST This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification.

2. MUST NOT This phrase, or the phrase "SHALL NOT", mean that the definition is an absolute prohibition of the specification.

3. SHOULD This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.

4. SHOULD NOT This phrase, or the phrase "NOT RECOMMENDED" mean that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.

5. MAY This word, or the adjective "OPTIONAL", mean that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item. An implementation which does not include a particular option MUST be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein an implementation which does include a particular option MUST be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides.)

6. Guidance in the use of these Imperatives

Imperatives of the type defined in this memo must be used with care and sparingly. In particular, they MUST only be used where it is actually required for interoperation or to limit behavior which has potential for causing harm (e.g., limiting retransmissions) For example, they must not be used to try to impose a particular method on implementors where the method is not required for interoperability.

7. Security Considerations

These terms are frequently used to specify behavior with security implications. The effects on security of not implementing a MUST or SHOULD, or doing something the specification says MUST NOT or SHOULD NOT be done may be very subtle. Document authors should take the time to elaborate the security implications of not following recommendations or requirements as most implementors will not have had the benefit of the experience and discussion that produced the specification.

8. Acknowledgments

The definitions of these terms are an amalgam of definitions taken from a number of RFCs. In addition, suggestions have been incorporated from a number of people including Robert Ullmann, Thomas Narten, Neal McBurnett, and Robert Elz.

9. Author's Address

Scott Bradner
Harvard University
1350 Mass. Ave.
Cambridge, MA 02138
phone - +1 617 495 3864
email - sob@harvard.edu

Appendice B
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 1.4,* 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)