Mobility Task Force

Deliverable I

TF-Mobility roaming policy document

Version 1.2

Authors: Licia Florio, James Sankar, David Simonsen, Klaas Wierenga.

Contributions: TF-Mobility members

Introduction

This document is based on discussions that have taken place within the TERENA Mobility taskforce. This document provides guidelines necessary to ensure roaming services that support transparent guest network access services can continue to be accepted and scale (wired and/or wireless). This work does not attempt to research any nation state or European Union legislation, nor does it attempt to harmonise national legislation from nation states within the European Union in any way.

The document falls in three parts: a general introduction to roaming, a policy for participating NREN's and a policy for participating institutions.

Aims

The overall aim of this work is to assist in fostering trust between academic institutions and between NRENs so that these critical relationships can encourage active participation, and the development of roaming services (transparent guest access).

Also this document seeks to formalize roaming guidelines that cover the supply and receipt of roaming services and provide details of the processes needed to effectively manage roaming services and guest users.

The vision

The vision of the TF-Mobility taskforce is to create a collaborative environment where academic guest users can visit other institutions either nationally or internationally and be offered an automated network access service. The service should be recognizable as an academic roaming service and offer a minimum agreed level of security. Some institutions may make available a range of security options to the guest / roaming user, however it is the responsibility of the guest / roaming user to respect the acceptable use policy of the *visited* institution as well as, of course, to follow the AUP of their *home* institution.

Once authenticated credentials have been sent to the guest /roaming users home institution authentication server and have been successfully processed, the visited institution will “trust” the response from the guest / roaming user’s home authentication server and grant a level of network access based on the visited institutions local site policy. All authentication sessions and network access sessions must be logged for auditing purposes to ensure that any breaches of the local acceptable use policy can be traced and appropriate remedial action can be taken in a timely manner that is acceptable to all participants.

Ideally the guest or roaming user should not have to do anything in addition to what he/she would normally do if physically located at their home institution. It will be necessary for home institutions to educate their own users participating in this service to ensure that they abide by policies contained herein and contact the appropriate person(s) for technical support related matters.

Roaming Services - General Principles

- The obvious security requirement is that the roaming access must only be available to authorized users, which should include all users authorized for Internet access at the participating NRENs and their institutions.

- All roaming users are required to authenticate at their home institution in order to be granted network access at the visited institution.

- All roaming users are responsible for their own credentials (and transmission thereof) and must abide by the roaming AUP (see section 1.1 hereafter) that has been agreed on behalf of the user by their home institution.

- The visited institution must be able to prove that the network access service has access to the roaming service so that roaming users can recognise and take advantage of it.

- The visited institution must clearly state that the mechanism for the transmission of user credentials is secure. If not secure the visited institution must (if requested) be able to support a user-initiated solution typically from the guest user’s client device so that a securer solution is possible.

- The visited institution has the right to block any roaming user, academic institution or NREN from accessing its local area network access provision.

- The visited institution will determine the authorisation of the network access provision.

- The home institution will be responsible for supporting their guest users including educating users on service support issues and abiding to relevant policies.

- Participants should provide feedback to their institutions on the roaming service and if necessary escalate any issues to their NREN who in turn on rare occasions may escalate a matter onto Terena to either log or resolve.

Benefits of roaming services

- There will be a lower administrative burden supporting guest / roaming users.
- Users will ideally be able to gain reasonably secure transparent network access in a less complex and timelier manner without changes required to their client devices and ideally no need for additional user credentials.
- More pervasive transparent and secure guest or roaming access should result in greater opportunities for collaborative research and academic work groups between academic organisations both nationally and internationally.
- The use of authentication servers with logging facilities should provide a better system of traceability than the current solution of manually allocating guest access.
- Some roaming services can also be of local value for local users at the home institutions, i.e. user authentication services.

Policies

To facilitate the interest shown in roaming services it is important that policies are put in place at appropriate levels to ensure that benefits remain whilst threats and risks are minimized and managed within acceptable levels. The following sections will list policies that relate to different levels of control and responsibility within a hierarchy of trust.

Roaming Services – Intra-NREN roaming Policy

1. TERENA level policy (agreements for participation between NRENs and TERENA)

TERENA will adopt this document as the TERENA roaming policy. All participating NRENs connecting to or wishing to connect to the TERENA authentication servers (European top level RADIUS servers) to participate in inter-NREN roaming must abide by the following as a minimum

1.1. Participating NRENs must abide by this “roaming” service agreement contained herein.

1.2. NRENs are responsible for ensuring that their national authentication servers can provide a secure means of transferring user credentials to and from other proxy authentication servers as required.

1.3. NRENs must have signed agreements in place with their academic institutions to participate in the supply and receipt of national and inter-NREN roaming services.

1.4. NRENs must have the following procedures in place to handle

1.4.1. National authentication server support and maintenance.
1.4.2. Security issues. It is advisable that the NRENs keep their CERT groups informed of development work and have channels in place to work together on issues that affect both parties
1.4.3. Fraudulent use of the roaming service by users or groups of users.
1.4.4. A monitoring facility to show the status of the national authentication servers so that home institutions can use this information as part of any guest user fault reporting activity.
1.4.5. A mechanism for providing feedback on the roaming service so that guest or roaming users can identify participating institutions and their service offering.

1.5. Ideally, NRENs should have a minimum of two authentication servers at different locations on their core network for resilience and redundancy.

1.6. The NREN must mandate their participating institutions to notify guest users on the level of security offered for the transmission of user credentials.

1.7. The NREN must mandate their participating institutions to educate their users in the roaming service and ensure that any technical support issues are handled at the home institution only. If the home institution determines the fault lies at the visited institution, only then should the issue be raised with the visited organisation technical support team.

1.8. The NREN must mandate their participating institutions to log authentication sessions and network access sessions so that they can trace a user for both security and capacity planning purposes.

1.9. The NREN must mandate their participating institutions to report any security issues or fraudulent activities to their NREN and manage and resolve such matters accordingly and report these to TERENA.

1.10. NRENs are not expected to provide privacy against casual snoopers; it is therefore the responsibility of the home institution and the guest user to have appropriate end-to-end privacy solutions in place to secure communications.

1.11. NRENs should have written guidelines for participating institutions to assist them in drafting local site and user policies to ensure compliance with the roaming service agreements with their NREN.

2. NREN level policy (agreements for participation between NRENs and their institutions)

A national policy framework must be in place so that all participating institutions have signed acceptance to that agree to the following as a minimum

2.1. Participating academic institutions must abide by the “roaming” service agreement contained herein.

2.2. Participating academic institutions are responsible for educating their users to respect the local AUP of the visited institution that their users that have been granted network access to and are obliged to help resolve any issues that relate to their users.

2.3. Participating academic institutions must provide a secure authentication server that can securely process and forward user credentials as required.

2.4. Participating academic institutions should communicate to guest or roaming users on whether and how they offer the roaming service.

2.5. Participating academic institutions should inform guest users of the level(s) of security offered for the transmission of user credentials.

2.6. Participating academic institutions must educate their users in the roaming service and ensure that any technical support issues are handled at the home organisation only. If the home organisation determines the fault lies at the visited institution, only then should the issue be raised with the visited organisation technical support team.

2.7. Participating academic institutions must log authentication sessions and network access session and be able to trace a user for both security and capacity planning purposes.

2.8. Participating academic institutions must report any security issues or fraudulent activities to their NREN to manage and resolve accordingly.