End-to-End Wi-Fi Roaming Test Cases
Version 4.0
11 May 2012

*This is a **Non-binding** Permanent Reference Document of the GSMA.*

Security Classification – NON CONFIDENTIAL GSMA MATERIAL

Antitrust Notice
The information contain herein is in full compliance with the GSM Association's antitrust compliance policy.

Table of Contents

1. Summary

The following document outlines test cases for Remote Authentication Dial In User Service (RADIUS)-based username-password, Extensible Authentication Protocol (EAP) for GSM Subscriber Identity Module (EAP-SIM), EAP for UMTS Authentication and Key Agreement (EAP-AKA), EAP-Tunnelled Transport Layer Security (EAP-TTLS) and EAP-Transport Layer Security (EAP-TLS) authenticated Wi-Fi roaming. The roaming environment is defined in PRD IR.61 Wi-Fi Roaming Guidelines.

2. Introduction

2.1. Scope of document

This document specifies a set of test cases for a Wi-Fi roaming service to confirm that it complies with PRD IR.61 Wi-Fi Roaming Guidelines. RADIUS shall be the protocol to be used for passing Authentication, Authorization and Accounting data, (AAA).

Whilst it is expected that Wi-Fi roaming will be a bilateral activity between two Wi-Fi Service providers (SP), please note that this document is written in a unidirectional context. Hence Roaming is taking place by a Mobile Terminal MT(a) to Visited Wi-Fi Service Provider network SP(b) only. There is no reference to a Mobile Terminal MT(b) visiting Home Wi-Fi Service Provider network SP(a).

To complete End-to-end Wi-Fi Roaming tests for bilateral roaming, it is necessary to perform the tests in this document twice: the second time the real identities of SP (a) and SP (b) are swapped.

Note: Billing cycles will not be part of these tests. However, the production of valid RADIUS accounting data that is used in the billing cycle is tested in a similar method as the generation of Call Data Records (CDRs) described in IR.35 End – to – End Functional Capability Test Specification for Inter-PLMN GPRS Roaming.

The Wi-Fi roaming environment shall be as described in PRD IR.61.

2.2. Strategy for Testing

To complete the test cases efficiently, the amount of simultaneous joint activity between Home SP (a) and Visited SP (b) should be minimized.

To this effect, testing program forms three separate components:

- Home SP (a) issues Test User Accounts and programmes Authentication Servers accordingly
- Visited SP (b) performs tests
- Visited SP (b) and Home SP (a) exchange data and discuss results

3. Username/Password Test Cases (Web-login)

The test cases are divided into four groups:

- Access tests:
  Login procedure and authentication, routing to correct server, Realm functionality in each proxy.
- Accounting tests:
  Validating that RADIUS accounting logs match.
- Service Failure tests
- User Experience tests

Pre-requisites for Username/Password Testing

- A GSMA Wi-Fi Roaming Guidelines (PRD IR.61) compliant Wi-Fi roaming test environment implemented.
- RADIUS configuration information shared (Realms, IP addresses of proxies, etc. via IR.21, RADIUS Shared Secret via secure means).
- List of active/valid test accounts made available by the Home SP (a) to Visited SP (b) for testing purposes. Three (3) accounts to each roaming partner.
- One barred user account provided to Visited SP (b) for the tests.
- Relevant system logs identified. The Visited SP (b) has to collect RADIUS messages going to Home SP (a) network server for to be able to validate RADIUS accounting data.

A File Transfer Protocol (FTP) location established from where the test file of a known size may be downloaded in data transfer testing.

3.1. Access Tests

3.1.1. Valid Roaming Authentication

Action: Enter a valid Home SP (a) username and a valid password using the Visited SP (b) network.

Result: Home SP (a) user should be granted access and get full network capabilities.

3.1.2. Valid Username, Invalid Password

Action: Enter a valid Home SP (a) username and an invalid password using the Visited SP (b) network.

Result: Home SP (a) user should be denied access.

3.1.3. Invalid Username

Action: Enter an invalid username and password using the Visited SP (b) network.

Result: User should be denied access.

3.1.4. Operator Determined Barring

Background: The Home SP (a) decides which object-relational mapping system, ODB ´s should stop the customer from using Wi-Fi (for example, Barring of GPRS, Barring of Roaming, Barring of outgoing calls, or other/way of barring).

Action: Enter a valid but barred Home SP (a) Username and a valid Password using the Visited SP (b) network.

Result: User access should be denied by the home SP (a).

3.1.5. Operator Determined Barring While Session Open

Background: This feature requires a RADIUS Change of Authorisation message implementation according to RFC 5176 on the Core Network side and on the Access Network.

Action: Perform a successful authentication. The Home SP (a) removes Wi-Fi capability from the user at issue by sending a Radius Change of Authorisation message. Consequently, the next authentication should fail.

Result: The session is closed and cannot be re-established.

3.2. Accounting Tests

3.2.1. RADIUS Accounting Data Generation (Session Time)

Action: Login with a valid Home SP (a) username in Visited SP (b) network, logout after set time.

Result: RADIUS accounting log should reflect the set time.

Comments: If Interim RADIUS accounting messages are used, the set time should be longer than the interim interval and interim message(s) should be generated during this test.

3.2.2. RADIUS Accounting Data Generation (Data Transferred)

Action: Login with a valid Home SP (a) username in Visited SP (b) network, download a test file of known size, upload a test file of known size, and logout.

Result: RADIUS accounting log Bytes-In and Bytes-Out fields should reflect the transferred file size and some network overhead.

Comments: If Interim RADIUS accounting messages are used, the transferred file should be big enough that interim message(s) are generated during this test.

3.2.3. Verifying RADIUS Accounting Logs

Action: Exchange RADIUS session logs of the accounting tests between Home SP (a) and Visited SP (b)

Result: Both accounting logs should have the same values in correct fields for the accounting tests. Also verify that proxy-state attributes are logged and that the values are correct.

3.3. Service Failure Tests

3.3.1. Implicit Logout

Action: Login with a valid Home SP (a) username in Visited SP (b) network, disconnect the Wi-Fi card or switch off the Mobile Terminal (a). Wait for set time, re-insert card or switch on the Mobile Terminal (a).

Result: Access should be denied to the user without a new login and the accounting session should be closed.

Comments: The wait time depends on the access controller configuration.

3.3.2. Inactivity Logout

Action: Login with a valid Home SP (a) username in Visited SP (b) network and leave the Mobile Terminal (a) idle.

Result: An automatic logout should occur after a pre-determined length of time.

Comments: The idle-timeout time depends on the used system. Normal accounting data should be generated after an automatic logout.

3.4. User Experience Tests

While conducting Access and Accounting tests, some user experience related issues should also be checked.

3.4.1. Login Page

Action: Visited SP (b)'s login page is displayed after association with Visited SP Network.

Result: Yes/No.

3.4.2. Help Page

Action: Visited SP (b)'s help page is available on the login page and is displayed before login.

Result: Yes/No.

3.4.3. Start Page

Action: Visited SP (b)'s start page and/or session status window are displayed after a successful login.

Result: Yes/No.

3.4.4. Unsuccessful Login

Action: An error message is displayed after an unsuccessful login.

Result: Yes/No.

3.4.5. Successful Login

Action: Logout method is clearly displayed after a successful login.

Result: Yes/No.

3.4.6. Logout Confirmation

Action: Logout confirmation is displayed after explicit and inactivity logouts.

Result: Yes/No.

3.5. Test Evaluation

- Accounting logs to be prepared to check that they match between all participants.
- Analyse failures.
- Produce Test Report:
  – Completed Test cases
  – Experiences
  – Problems
  – Solutions
  – Proposals

4. Extensible Authentication Protocol for GSM Subscriber Identity Module (EAP-SIM) Test Cases

The test cases are divided into four groups:

- Access tests
  – Login procedure and authentication, routing to correct server, Realm functionality in each proxy.
- Accounting tests
  – Validating that RADIUS accounting logs match.
- Service Failure tests
- User Experience tests

Pre-requisites for EAP-SIM Testing

- A GSMA Wi-Fi Roaming Guidelines (PRD IR.61) compliant Wi-Fi roaming test environment implemented.
- RADIUS configuration information shared (Realms, IP addresses of proxies, etc. via IR.21, RADIUS Shared Secret via secure means).
- List of active/valid test Subscriber Identity Modules (SIMs) made available by the Home SP (a) to Visited SP (b) for testing purposes. Three (3) SIMs to each roaming partner. SIM can be either SIM card, or Universal Integrated Circuit Card (UICC) with SIM application.
- One barred SIM (SIM-card with no Wi-Fi service) provided to Visited SP (b) for the tests.
- Relevant system logs identified. The Visited SP (b) has to collect RADIUS messages going to Home SP (a) network server for to be able to validate RADIUS accounting data.
- An FTP location established from where a test file of a known size may be downloaded in data transfer testing.
- Pseudonym and realm together are according to the 3GPP TS 23.003 specification
- It is suggested that Visited SP (b) sets re-authentication period maximum to 30 minutes. This is due to a new security key delivery.

Note: Next test cases refer to re-authentication, meaning that during the user session the client is authenticated and the security keys are exchanged. Re-authentication can be Full authentication (EAP-SIM server fetches the triplets from Home Location Register (HLR)) or Fast re-authentication (no HLR query).

4.1. Access Tests

4.1.1. Valid Roaming Authentication using IMSI as an identity

Action: Configure client to use International Mobile Subscriber Identity (IMSI) as an identity. Enter a valid Home SP (a) SIM-card to the terminal and enter the correct PIN-code using the Visited SP (b) network.

Result: Home SP (a) user should be granted access and access full network capabilities.

4.1.2. Valid Roaming Authentication using pseudonym as identity

Background: In order to use pseudonym identity, at least one successful authentication with IMSI must be performed. The usage of pseudonyms must be enabled in the Home SP (a) network.

Action: Configure client to use pseudonym as an identity. Enter a valid Home SP (a) SIM-card to the terminal and enter the correct PIN-code using the Visited SP (b) network.

Result: A Home SP user should be granted access and get full network capabilities.

4.1.3. Valid Roaming Authentication using fast re-authentication mechanism

Background: Fast Re-authentication mechanism allows the authentication to be completed without querying Home SP (a) HLR. The usage of fast re-authentication must be enabled in the Home SP (a) network.

Action: Perform successful authentication with mechanism described either in 2.1.1 or 2.1.2. While authenticated, push re-authenticate or similar button in your client to make fast re-authentication.

Result: A Home SP user should be granted access and access full network capabilities.

4.1.4. Periodical re-authentication

Background: Home SP (a) network can require periodically re-authentications. After a configured time period the client must authenticate itself to Home SP (a) network either by using fast re-authentication or full authentication mechanism.

Action: Perform successful authentication with mechanisms described either in 2.1.1 or 2.1.2. Wait for an agreed time period and examine if re-authentication occurs.

Result: A Home SP (a) user should be granted access and access full network capabilities.

4.1.5. Handover

Background: When moving from Access Point (AP) coverage to another AP coverage, the client should make automatically a new authentication or fast re-authentication depending on the client features

Action: Session is active; change your position so that a handover occurs.

Result: Handover succeeds; check the authentication type.

4.1.6. Operator Determined Barring

Background: The Home SP (a) decides how to stop the customer from using Wi-Fi.

Action: Enter a valid Home SP (a) SIM-card to the terminal and enter the correct PIN-code using the Visited SP (b) network.

Result: User access should be denied by the Home SP (a).

4.1.7. Operator Determined Barring While Session Open

Background: This feature requires RADIUS Change of Authorisation message implementation according to RFC 5176 on Core Network side and on a Access Network.

Also re-authentication mechanism could be used to implement barring mechanism. If the user account gets barred between two sequential authentications, the next authentication attempt will fail.

Action: Perform a successful authentication. A Home SP (a) removes Wi-Fi capability from the user at issue by sending Radius Change of Authorisation message. Consequently the next re-authentication (full authentication) should fail.

Result: The session is closed and cannot be re-established.

4.1.8. Removing a SIM-Card During User Session

Background: Removing the SIM-card during the session should terminate the session.

Action: Remove the Universal Serial Bus (USB) or Personal Computer Memory Card International Association (PCMCIA) smart card reader during the session.

Result: The session is terminated in the time period of two (2) seconds.

4.2. Accounting Tests

4.2.1. RADIUS Accounting Data Generation (Session Time)

Action: Login with a valid Home SP (a) SIM card in Visited SP (b) network and logout after a set time (with the help of Session timeout attribute).

Result: RADIUS accounting log should reflect the set time.

Comments: If Interim RADIUS accounting messages are used, the set time should be longer than the interim interval and interim message(s) should be generated during this test.

4.2.2. RADIUS Accounting Data Generation (Data Transferred)

Action: Login with a valid Home SP (a) SIM card in Visited SP (b) network, download a test file of known size, upload a test file of known size, and logout.

Result: RADIUS accounting log Bytes-In and Bytes-Out fields should reflect the transferred file size and some network overhead.

Comments: If Interim RADIUS accounting messages are used, the transferred file should be big enough that interim message(s) are generated during this test.

4.2.3. Verifying RADIUS Accounting Logs

Action: Exchange RADIUS session logs of the accounting tests between Home SP (a) and Visited SP (b).

Result: Both accounting logs should have the same values in correct fields for the accounting tests. Also verify that proxy-state attributes are logged and that the values are correct.

4.2.4. Handover

Background: In case the user is moving from one AP's coverage to another AP's coverage the ongoing accounting session may be altered.

Action: Session is active; change your position so that a handover occurs.

Result: Handover succeeds; check the Accounting session. Current accounting session may remain after the handover. Alternatively a new accounting session is created after successful handover and the old accounting session gets terminated.

4.2.5. Chargeable User Identity (CUI)

Background: The usage of the pseudonym creates the accounting problem for the Visited SP (b), as it does not recognise the real user and which identity that would be usable with the existing inter-operator billing systems. CUI is solving this problem. The visited SP (b) must send back the CUI received in the authentication accept message back to the Home SP (a) in the format the Home SP (a) sent it.

Action: Home SP (a) sends CUI to the visited SP (b) in the predefined format (IMSI, MSISDN, NAI...) in an Access-Accept message

Result: Visited SP (b) sends the CUI back in the same format it was received (refer to the IR.61 to see which packet may include CUI). Visited SP (b) is able to use CUI for the accounting purposes.

4.3. Service Failure Tests

4.3.1. Implicit Logout

Action: Login with a valid Home SP (a) SIM card in Visited SP (b) network, disconnect the WLAN card or switch off the Mobile Terminal (a). Wait for set time, re-insert card or switch on the Mobile Terminal (a).

Result: Access should be denied to the user without a new login and the accounting session should be closed.

Comments: The wait time depends on the access controller configuration.

4.3.2. Inactivity Logout

Action: Login with a valid Home SP (a) SIM in Visited SP (b) network and leave the Mobile Terminal (a) idle.

Result: An automatic logout should happen after a pre-determined time period.

Comments: The idle-timeout time depends on the used system. Normal accounting data should be generated after an automatic logout.

4.4. User Experience Tests

While conducting Access and Accounting tests, some user experience related issues should also be checked. These issues are mainly pointing to the 1X-client features, and may not include the visited SP (b) network features.

4.4.1. Help Page

Action: Visited SP (b)'s help page (or link) is available on the start page of the visited SP (b).

Result: Yes/No.

4.4.2. Start Page

Action: Visited SP (b)'s start page appears after browser opening and/or session status might be visible in the EAP-SIM client.

Result: Yes/No.

4.4.3. Unsuccessful Login

Action: An error message is displayed after an unsuccessful login in the client.

Result: Yes/No.

4.4.4. Successful Login

Action: The successful login is clearly displayed by the client after successful login.

Result: Yes/No.

4.4.5. Logout Confirmation

Action: Logout confirmation is displayed after explicit and inactivity logouts.

Result: Yes/No.

4.5. Test Evaluation

- Accounting logs to be prepared to check that they match between all participants
- Analyse failures
- Produce Test Report:
  – Completed Test cases
  – Experiences
  – Problems
  – Solutions
  – Proposals

The client used for the tests to be mentioned (name, version etc.)

5. EAP-AKA Test Cases

Extensible Authentication Protocol for UMTS Authentication and Key Agreement (EAP-AKA) test cases are the same as for the EAP-SIM. The only difference when testing is that it requires a 3G SIM card in this document is referred as UICC, instead of the 2G SIM card that only supports EAP-SIM.

The test cases are divided into four groups:

- Access tests
  - Login procedure and authentication, routing to correct server, Realm functionality in each proxy.
- Accounting tests
  - Validating that RADIUS accounting logs match.
- Service Failure tests
- User Experience tests

Pre-requisites for EAP-AKA Testing

- A GSMA Wi-Fi Roaming Guidelines (PRD IR.61) compliant Wi-Fi roaming test environment implemented.
- RADIUS configuration information shared (Realms, IP addresses of proxies, etc. via IR.21, RADIUS Shared Secret via secure means).
- List of active/valid test UICCs made available by the Home SP (a) to Visited SP (b) for testing purposes. Three (3) UICCs to each roaming partner.
- One barred UICC (UICC-card with no Wi-Fi service) provided to Visited SP (b) for the tests.
- Relevant system logs identified. The Visited SP (b) has to collect RADIUS messages going to Home SP (a) network server for to be able to validate RADIUS accounting data.
- An FTP location established from where test file of a known size may be downloaded in data transfer testing.
- Pseudonym and realm together are according to the 3GPP TS 23.003 specification
- It is suggested that Visited SP (b) sets re-authentication period at a max. 30 minutes. This is because of a new security key delivery.

Note: Next test cases refer to re-authentication, Meaning that during the user session the client is authenticated and the security keys are exchanged. Re-authentication can be Full authentication (EAP-AKA server fetches the quintets from HLR) or Fast re-authentication (no HLR query).

5.1. Access Tests

5.1.1. Valid Roaming Authentication using IMSI as an identity

Action: Configure client to use IMSI as an identity. Enter a valid Home SP (a) UICC-card to the terminal and enter the correct PIN-code using the Visited SP (b) network.

Result: Home SP (a) user should be granted access and get full network capabilities.

5.1.2. Valid Roaming Authentication using pseudonym as identity

Background: In order to use pseudonym identity, at least one successful authentication with IMSI must be performed. The usage of pseudonyms must be enabled in the Home SP (a) network.

Action: Configure client to use pseudonym as an identity. Enter a valid Home SP (a) UICC-card to the terminal and enter the correct PIN-code using the Visited SP (b) network.

Result: Home SP (a) user should be granted access and get full network capabilities.

5.1.3. Valid Roaming Authentication using fast re-authentication mechanism

Background: Fast Re-authentication mechanism allows the authentication to be completed without querying Home SP (a) HLR. The usage of fast re-authentication must be enabled in the Home SP (a) network.

Action: Perform successful authentication with the mechanisms described either in 4.1.1 or 4.1.2. While authenticated, push re-authenticate or similar button in your client to make fast re-authentication.

Result: Home SP (a) user should be granted access and get full network capabilities.

5.1.4. Periodical re-authentication

Background: Home SP (a) network can require periodically re-authentications. After a configured time period, the client must authenticate itself to Home SP (a) network either by using fast re-authentication or full authentication mechanism.

Action: Perform successful authentication with mechanism described either in 4.1.1 or 4.1.2. Wait for an agreed time period and examine if re-authentication occurs.

Result: Home SP (a) user should be granted access and access full network capabilities.

5.1.5. Handover

Background: When moving from AP coverage to another AP coverage, the client should make automatically a new authentication or fast re-authentication depending on the client features

Action: Session is active; change your position so that a handover occurs.

Result: Handover succeeds; check the authentication type

5.1.6. Operator Determined Barring

Background: The Home SP (a) decides how to stop the customer from using Wi-Fi.

Action: Enter a valid Home SP (a) UICC-card to the terminal and enter the correct PIN-code using the Visited SP (b) network.

Result: User access should be denied by the Home SP (a).

5.1.7. Operator Determined Barring While Session Open

Background: This feature requires RADIUS Change of Authorisation message implementation according to RFC 5176 on Core Network side as well on Access Network.

Also Re-authentication mechanism could be used to implement barring mechanism. If the user account gets barred between two sequential authentications, the next authentication attempt will fail.

Action: Perform a successful authentication. The Home SP (a) removes Wi-Fi capability from the user at issue by sending a RADIUS Change of Authorisation message. Consequently, the next re-authentication (full authentication) should fail.

Result: The session is closed and cannot be re-established.

5.1.8. Removing UICC-Card During User Session

Background: Removing UICC-card during the session should terminate the session.

Action: Remove USB or PCMCIA smart card reader during the session

Result: The session is terminated in a two (2) second time period.

5.2. Accounting Tests

5.2.1. RADIUS Accounting Data Generation (Session Time)

Action: Login with a valid Home SP (a) UICC card in Visited SP (b) network, logout after a set time (with the help of Session timeout attribute).

Result: RADIUS accounting log should reflect the set time.

Comments: If Interim RADIUS accounting messages are used, the set time should be longer than the interim interval and interim message(s) should be generated during this test.

5.2.2. RADIUS Accounting Data Generation (Data Transferred)

Action: Login with a valid Home SP (a) UICC card in Visited SP (b) network, download a test file of a known size, upload a test file of a known size, and logout.

Result: RADIUS accounting log Bytes-In and Bytes-Out fields should reflect the transferred file size and some network overhead.

Comments: If Interim RADIUS accounting messages are used, the transferred file should

be big enough that interim message(s) are generated during this test.

5.2.3. Verifying RADIUS Accounting Logs

Action: Exchange RADIUS session logs of the accounting tests between Home SP (a) and Visited SP (b)

Result: Both accounting logs should have the same values in correct fields for the accounting tests. Also verify that proxy-state attributes are logged and that the values are correct.

5.2.4. Handover

Background: In case the user is moving from one AP's coverage to another AP's coverage the on-going accounting session may be altered.

Action: Session is active; change your position so that a handover occurs.

Result: Handover succeeds; check the Accounting session. Current accounting sessions may remain after the handover. Alternatively a new accounting session is created after a successful handover and the old accounting session becomes terminated.

5.2.5. Chargeable User Identity (CUI)

Background: The usage of the pseudonym creates the accounting problem for the visited SP (b), because it does not recognise the real user and which identity would be usable with the existing inter-operator billing systems. CUI is solving this problem. The Visited SP (b) must send back the CUI received in the authentication accept message back to the Home SP (a) in the format the Home SP (a) sent it.

Action: Home SP (a) sends CUI to the Visited SP (b) in the predefined format (IMSI, MSISDN, NAI...) in an Access-Accept message.

Result: Visited SP (b) sends the CUI back in the same format it was received (refer to the IR.61 to see which packet may include CUI). Visited SP (b) is able to use CUI for the accounting purposes.

5.3. Service Failure Tests

5.3.1. Implicit Logout

Action: Login with a valid Home SP (a) UICC card in Visited SP (b) network, disconnect the WLAN card or switch off the Mobile Terminal (a). Wait for set time, re-insert card or switch on the Mobile Terminal (a).

Result: Access should be denied to the user without a new login and the accounting session should be closed.

Comments: The wait time depends on the access controller configuration.

5.3.2. Inactivity Logout

Action: Login with a valid Home SP (a) UICC in Visited SP (b) network and leave the Mobile Terminal (a) idle.

Result: An automatic logout should happen after a pre-determined time.

Comments: The idle-timeout time depends on the used system. Normal accounting data should be generated after an automatic logout.

5.4. User Experience Tests

While conducting Access and Accounting tests, some user experience related issues should also be checked. These issues are mainly pointing to the 1X-client features, not so much to the Visited SP (b) network features.

5.4.1. Help Page

Action: Visited SP (b)'s help page (or link) is available on the start page of the Visited SP (b).

Result: Yes/No.

5.4.2. Start Page

Action: Visited SP (b)'s start page appears after browser opening and/or session status might be seen in the EAP-AKA client.

Result: Yes/No.

5.4.3. Unsuccessful Login

Action: An error message is displayed after an unsuccessful login in the client.

Result: Yes/No.

5.4.4. Successful Login

Action: The successful login is clearly displayed by the client after successful login.

Result: Yes/No.

5.4.5. Logout Confirmation

Action: Logout confirmation is displayed after explicit and inactivity logouts.

Result: Yes/No.

5.5. Test Evaluation

- Accounting logs to be prepared to check that they match between all participants.

- Analyse failures
- Produce Test Report:
  - Completed Test cases
  - Experiences
  - Problems
  - Solutions
  - Proposals
- The client used for the tests to be mentioned (name, version etc.)

6. EAP-TTLS Test Cases

The Extensible Authentication Protocol - Tunnelled Transport Layer Security test cases are divided into four groups:

- Access tests
  - Login procedure and authentication, routing to correct server, Realm functionality in each proxy
- Accounting tests
  - Validating that RADIUS accounting logs match.
- Service Failure tests
- User Experience tests

Pre-requisites for Username/Password Testing

- A GSMA Wi-Fi Roaming Guidelines (PRD IR.61) compliant Wi-Fi roaming test environment implemented.
- RADIUS configuration information shared (Realms, IP addresses of proxies, etc via IR.21, RADIUS Shared Secret via secure means).
- List of active/valid test accounts made available by the Home SP (a) to Visited SP (b) for testing purposes. Three (3) accounts to each roaming partner.
- One barred user account provided to Visited SP (b) for the tests.
- Relevant system logs identified. The Visited SP (b) has to collect RADIUS messages going to Home SP (a) network server for to be able to validate RADIUS accounting data.

An FTP location established from where a test file of a known size may be downloaded in data transfer testing.

6.1. Access Tests

6.1.1. Valid Roaming Authentication

Action: Enter a valid Home SP (a) username and a valid password to EAP-TTLS client using the Visited SP (b) network.

Result: Home SP (a) user should be granted access and get full network capabilities.

6.1.2. Valid Username, Invalid Password

Action: Enter a valid Home SP (a) username and an invalid password to EAP-TTLS client using the Visited SP (b) network.

Result: Home SP (a) user should be denied access.

6.1.3. Invalid Username

Action: Enter an invalid username and password to EAP-TTLS client using the Visited SP (b) network.

Result: User should be denied access.

6.1.4. Operator Determined Barring

Background: The Home SP (a) decides which ODB ´s should stop the customer from using Wi-Fi (for example Barring of GPRS, Barring of Roaming, Barring of outgoing calls, or other kind / way of barring).

Action: Enter a valid but barred Home SP (a) Username and a valid Password using the Visited SP (b) network.

Result: User access should be denied by the home SP (a).

6.1.5. Operator Determined Barring While Session Open

Background: This feature requires RADIUS Change of Authorisation message implementation according to RFC 5176 on Core Network side as well as on the Access Network.

Action: Perform a successful authentication. The Home SP (a) removes Wi-Fi capability from a user at issue by sending Radius Change of Authorisation message. Subsequently, the next authentication should fail.

Result: The session is closed and can not be re-established.

6.2. Accounting Tests

6.2.1. RADIUS Accounting Data Generation (Session Time)

Action: Login with a valid Home SP (a) username in Visited SP (b) network, logout after a set time period of time.

Result: RADIUS accounting log should reflect the set time.

Comments: If Interim RADIUS accounting messages are used, the set time should be longer than the interim interval and interim message(s) should be generated during this test.

6.2.2. RADIUS Accounting Data Generation (Data Transferred)

Action: Login with a valid Home SP (a) username in Visited SP (b) network, download a test file of a known size, upload a test file of known size, and logout.

Result: RADIUS accounting log Bytes-In and Bytes-Out fields should reflect the transferred file size and some network overhead.

Comments: If Interim RADIUS accounting messages are used, the transferred file should

be big enough that the interim message(s) are generated during this test.

6.2.3. Verifying RADIUS Accounting Logs

Action: Exchange RADIUS session logs of the accounting tests between Home SP (a) and Visited SP (b)

Result: Both accounting logs should have the same values in the correct fields for the accounting tests. Also verify that the proxy-state attributes are logged and that the values are correct.

6.3. Service Failure Tests

6.3.1. Implicit Logout

Action: Login with a valid Home SP (a) username in Visited SP (b) network, disconnect the WLAN card or switch off the Mobile Terminal (a). Wait for set time, re-insert the card or switch on the Mobile Terminal (a).

Result: Access should be denied to the user without a new login and the accounting session should be closed.

Comments: The wait time depends on the access controller configuration.

6.3.2. Inactivity Logout

Action: Login with a valid Home SP (a) username and password in Visited SP (b) network and leave the Mobile Terminal (a) idle.

Result: An automatic logout should happen after a pre-determined time.

Comments: The idle-timeout time depends on the used system. Normal accounting data should be generated after an automatic logout.

6.4. User Experience Tests

While conducting Access and Accounting tests, some user experience related issues should also be checked. These issues are mainly pointing to the 1X-client features, and does not include the visited SP (b) network features.

6.4.1. Help Page

Action: Visited SP (b)’s help page (or link) is available on the start page of the visited SP (b).

Result: Yes/No.

6.4.2. Start Page

Action: Visited SP (b)’s start page appears after the browser opening and/or session status might be seen in the EAP-TTLS client.

Result: Yes/No.

6.4.3. Unsuccessful Login

Action: An error message is displayed after an unsuccessful login in the client.

Result: Yes/No.

6.4.4. Successful Login

Action: The successful login is clearly displayed by the client after successful login.

Result: Yes/No.

6.4.5. Logout Confirmation

Action: Logout confirmation is displayed after explicit and inactivity logouts.

Result: Yes/No.

6.5. Test Evaluation

- Accounting logs to be prepared to check that they match between all participants
- Analyse failures
- Produce Test Report:
  - Completed Test cases
  - Experiences
  - Problems
  - Solutions
  - Proposals
- The client used for the tests to be mentioned (name, version etc.)

7. EAP-TLS Test Cases

EAP-TLS test cases are the same as for the EAP-TTLS. The only difference is that EAP-TLS requires a unique certificate to the test terminal. Exchange of the certificates must be agreed between Home SP (a) and Visited SP (b) case by case.

Since the test cases are the same as with EAP-TTLS, those are not described here.

Document Management

Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
0.1	June 6th, 2002	First draft created in WLAN TF ("version A")		
0.2	June 7th, 2002	Version after WLAN TF Stockholm meeting ("version B")		
0.3	July 4th, 2002	Version after WLAN TF conference call (4th of July) ("version C")		
1.0	August 22nd, 2002	Version after WLAN TF conference call ("version D"), presented to IREG plenary in Singapore		
2.0.0	September 19th, 2002	Version based on discussions and agreements in WLAN TF /(IREG) Singapore meeting ("version E")		
3.0.0	September 27th, 2002	Version approved by WLAN TF in Portland ("version F"), presented to Packet WP in Madrid (November 2002)		
3.0.1	January 17th, 2003	Version after Packet WP ad-hoc in Düsseldorf		
3.1.0	February 11th, 2003	Version after Packet WP Yokohama meeting (IREG Doc 026/03 Rev 1)		
3.2.	April 23rd, 2003	Approved by EMC		
4.0	May 11th, 2012	DAG documents 092_025, 92_026, 92_027, 92_028, incorporated	DAG 92	Jalkanen Tero/Keisala Ilkka/TeliaSonera

Other Information

Type	Description
Document Owner	IREG
Editor / Company	Marko Onikki / TeliaSonera

Feedback

It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You may notify us at prd@gsm.org
Your comments or suggestions & questions are always welcome.

APPENDIX A

Wi-Fi SP Name: [1]	
Wi-Fi SP Country (Abbreviated according to ISO 3166):	
Testing Personnel's Name:	
Test Execution Date:	

A.1 Test Results for Username/Password

8.1. Access Tests

8.1.1. Valid Roaming Authentication

Username Used in Test	
Date	
Start Time	
End Time	
Test Result (Pass/Fail)	
Description	Enter valid roaming username and password
Status/Comments/Expectations	Username should be in the proper format. User should be granted access and have full network capabilities.

8.1.2. Valid Username, Invalid Password

Username Used in Test	
Date	
Start Time	
End Time	
Test Result (Pass/Fail)	
Description	Enter valid roaming username and invalid password
Status/Comments/Expectations	Access denied. No network access.

8.1.3. Invalid Username

Username Used in Test	
Date	
Start Time	
End Time	
Test Result (Pass/Fail)	

[1] Maximum 22 letters. This field is only used for administrative purposes, however, it must always be filled in order to identify the operator.

Description	Enter invalid roaming username and password
Status/Comments/Expectations	Username should be in the proper format. User should be denied access and have no network capabilities.

8.1.4. Operator Determined Barring

Username Used in Test	
Date	
Start Time	
End Time	
Test Result (Pass/Fail)	
Description	Enter a valid roaming username and password of an account that has been barred by Home SP (a)
Status/Comments/Expectations	Access denied. No network access.

8.1.5. Operator Determined Barring While Session Open

Username Used in Test	
Date	
Start Time	
End Time	
Test Result (Pass/Fail)	
Description	Enter a valid roaming username and password. When the session is open, the SP (a) should assign a barring to this subscriber using functionality according to RFC 5176.
Status/Comments/Expectations	The session should be cancelled automatically a pair of seconds later (quasi-online).

8.2. Accounting Tests

8.2.1. RADIUS Accounting Data Generation (Session Time)

Username Used in Test	
Date	
Start Time	
End Time	
Test Result (Pass/Fail)	
Test Verification Result [2]	
Description	Login, Logoff after a set time
Status/Comments/Expectations	Accounting logs should reflect the connection time.

8.2.2. RADIUS Accounting Data Generation (Data Transferred)

Username Used in Test	
Date	
Start Time	
End Time	
Volume (Amount of transferred data)	
Test Result (Pass/Fail)	

[2] Test Verification Result field is used for verifying test result against Home SP RADIUS messages. Home SP Testing Personnel should check that RADIUS logs correspond to values mentioned in this testing document.

Test Verification Result [2]	
Description	Login, download test file, upload test file and Logoff
Status/Comments/Expectations	Bytes-In and Bytes-Out in Accounting Logs should be values which are approximately the size of the test file + some network overhead.

8.2.3. Verifying RADIUS Accounting Logs

Username Used in Test	
Date	
Start Time	
End Time	
Volume (Amount of transferred data)	
Test Result (Pass/Fail)	
Test Verification Result[2]	
Description	Verify that both accounting logs have the same results for all of the accounting tests. Specially, verify that proxy-state attributes are logged and that values are correct.
Status/Comments/Expectations	Session logs to be exchanged along with a copy of the test plan used (for username/time resolution per test).

8.3. Service Failure Tests

8.3.1. Implicit Logout

Username Used in Test	
Start Time	
End Time	
Test Result (Pass/Fail)	
Test Verification Result[2]	
Description	Disconnect Wi-Fi card or turn off computer while connected. Wait a set time. Re-insert card or turn on computer.
Status/Comments/Expectations	Accounting should show a closed session and the user should have no network access.

8.3.2. Inactivity Logout

Username Used in Test	
Start Time	
End Time	
Test Result (Pass/Fail)	
Test Verification Result	
Description	The Wi-Fi connection is left idle, an automatic log-off should happen after a pre-determined time.
Status/Comments/Expectations	Absence time-out.

8.4. User Experience Tests

8.4.1. Login Page

Username Used in Test	
Test Result (Yes/No)	

Description	User's welcome page is displayed after association to network.
Status/Comments/Expectations	

Help Page

Username Used in Test	
Test Result (Yes/No)	
Description	Help-page displayed by clicking on link at Login page.
Status/Comments/Expectations	

8.4.2. Start Page

Username Used in Test	
Test Result (Yes/No)	
Description	Local Start-page and session window are displayed after successful login
Status/Comments/Expectations	

8.4.3. Unsuccessful Login

Username Used in Test	
Test Result (Yes/No)	
Description	Error message shown after unsuccessful login.
Status/Comments/Expectations	

8.4.4. Successful Login

Username Used in Test	
Test Result (Yes/No)	
Description	Logout method is clearly displayed after successful login.
Status/Comments/Expectations	

8.4.5. Logout Confirmation

Username Used in Test	
Test Result (Yes/No)	
Description	Logout confirmation is displayed after explicit and inactivity logouts.
Status/Comments/Expectations	

Wi-Fi SP Name: [3]	
Wi-Fi SP Country (Abbreviated according to ISO 3166):	
Testing Personnel's Name:	
Test Execution Date:	

A.2 Test Results for EAP-SIM

9.1. Access Tests

9.1.1. Valid Roaming Authentication using IMSI as identity

SIM (IMSI, MSISDN) Used in Test	
Date	
Start Time	
End Time	
Test Result (Pass/Fail)	
Description	Enter valid PIN code to the client.
Status/Comments/Expectations	User should be granted access and have full network capabilities.

9.1.2. Valid Roaming Authentication using pseudonym as identity

SIM (IMSI, MSISDN) Used in Test	
Date	
Start Time	
End Time	
Test Result (Pass/Fail)	
Description	Configure client to use pseudonym as an identity, Enter valid PIN code.
Status/Comments/Expectations	User should be granted access and have full network capabilities.

9.1.3. Valid Roaming Authentication using fast re-authentication mechanism

SIM (IMSI, MSISDN) Used in Test	
Date	
Start Time	
End Time	
Test Result (Pass/Fail)	
Description	Press fast re-authentication button or similar in the client.
Status/Comments/Expectations	User should be granted access and have full network capabilities.

[3] Maximum 22 letters. This field is only used for administrative purposes, however, it must always be completed to identify the operator.

9.1.4. Periodical re-authentication

SIM (IMSI, MSISDN) Used in Test	
Date	
Start Time	
End Time	
Test Result (Pass/Fail)	
Description	While session opens, periodical re-authentication should happen.
Status/Comments/Expectations	User should be granted access and have full network capabilities.

9.1.5. Handover

SIM (IMSI, MSISDN) Used in Test	
Date	
Start Time	
End Time	
Test Result (Pass/Fail)	
Description	Move between 2 APs so that a handover occurs.
Status/Comments/Expectations	Handover succeeds, check authentication type.

9.1.6. Operator Determined Barring

SIM (IMSI, MSISDN) Used in Test	
Date	
Start Time	
End Time	
Test Result (Pass/Fail)	
Description	Operator Determined Barring
Status/Comments/Expectations	The user access should be denied by Home SP (a).

9.1.7. Operator Determined Barring While Session Open

SIM (IMSI, MSISDN) Used in Test	
Date	
Start Time	
End Time	
Test Result (Pass/Fail)	
Description	Operator is barring the session while session is open.
Status/Comments/Expectations	The user access should be denied by SP (a). This is up to SP (a) implementation.

9.1.8. Removing SIM-Card During User Session

SIM (IMSI, MSISDN) Used in Test	
Date	
Start Time	
End Time	
Test Result (Pass/Fail)	
Description	Remove SIM-card during user session.

Status/Comments/Expectations	The session is terminated in time period of two (2) seconds.

9.2. Accounting Tests

9.2.1. RADIUS Accounting Data Generation (Session Time)

SIM (IMSI, MSISDN) Used in Test	
Date	
Start Time	
End Time	
Test Result (Pass/Fail)	
Test Verification Result [4]	
Description	Login, Logoff after a set time.
Status/Comments/Expectations	Accounting logs should reflect the connection time.

9.2.2. RADIUS Accounting Data Generation (Data Transferred)

SIM (IMSI, MSISDN) Used in Test	
Date	
Start Time	
End Time	
Volume (Amount of transferred data)	
Test Result (Pass/Fail)	
Test Verification Result	
Description	Login, download test file, upload test file and Logoff.
Status/Comments/Expectations	Bytes-In and Bytes-Out in Accounting Logs should be values which are approximately the size of the test file + some network overhead.

9.2.3. Verifying RADIUS Accounting Logs

SIM (IMSI, MSISDN) Used in Test	
Date	
Start Time	
End Time	
Volume (Amount of transferred data)	
Test Result (Pass/Fail)	
Test Verification Result	
Description	Verify that both accounting logs have the same results for all of the accounting tests. Specially, verify that proxy-state attributes are logged and that values are correct.
Status/Comments/Expectations	Session logs to be exchanged along with a copy of the test plan used (for IMSI/MSISDN/time resolution per test).

9.2.4. Handover

SIM (IMSI, MSISDN) Used in Test	

[4] Test Verification Result field is used for verifying test result against Home SP RADIUS messages. Home SP Testing Personnel should check that RADIUS logs correspond to values mentioned in this testing document.

Date	
Start Time	
End Time	
Volume (Amount of transferred data)	
Test Result (Pass/Fail)	
Test Verification Result	
Description	Move so that handover occurs during an open session.
Status/Comments/Expectations	The user session continues, or there may be two separate accounting sessions.

9.2.5. Chargeable User Identity (CUI)

SIM (IMSI, MSISDN) Used in Test	
Date	
Start Time	
End Time	
Volume (Amount of transferred data)	
Test Result (Pass/Fail)	
Test Verification Result	
Description	Login with a valid SIM card
Status/Comments/Expectations	Home SP (a) sends CUI to the Visited SP (b). Check that Visited SP (b) sends CUI back to the Home SP (a) in the same format it was received.

9.3. Service Failure Tests

9.3.1. Implicit Logout

SIM (IMSI, MSISDN) Used in Test	
Start Time	
End Time	
Test Result (Pass/Fail)	
Test Verification Result	
Description	Disconnect Wi-Wi card or turn off computer while connected. Wait a set time. Re-insert card or turn on computer.
Status/Comments/Expectations	Accounting should show a closed session and user should have no network access.

9.3.2. Inactivity Logout

SIM (IMSI, MSISDN) Used in Test	
Start Time	
End Time	
Test Result (Pass/Fail)	
Test Verification Result	
Description	The Wi-Fi connection is left idle, an automatic log-off should happen after a pre-determined time.
Status/Comments/Expectations	Absence time-out.

9.4. User Experience Tests

9.4.1. Help Page

SIM (IMSI, MSISDN) Used in Test	
Test Result (Yes/No)	
Description	User's welcome page is displayed after successful login and opening the browser.
Status/Comments/Expectations	This functionality is up to Visited SP (b) implementation.

9.4.2. Start Page

SIM (IMSI, MSISDN) Used in Test	
Test Result (Yes/No)	
Description	Help-page displayed by clicking on link at Login page.
Status/Comments/Expectations	This functionality is up to Visited SP (b) implementation.

9.4.3. Unsuccessful Login

SIM (IMSI, MSISDN) Used in Test	
Test Result (Yes/No)	
Description	Error message shown after unsuccessful login.
Status/Comments/Expectations	An error message is displayed after an unsuccessful login in the client. This might be related to the client features.

9.4.4. Successful Login

SIM (IMSI, MSISDN) Used in Test	
Test Result (Yes/No)	
Description	The successful login is clearly displayed by the client after successful login.
Status/Comments/Expectations	This might be related to the client features.

9.4.5. Logout Confirmation

SIM (IMSI, MSISDN) Used in Test	
Test Result (Yes/No)	
Description	Logout confirmation is displayed after explicit and inactivity logouts by the client.
Status/Comments/Expectations	This might be related to the client features.

Wi-Fi SP Name: [5]	

[5] Maximum 22 letters. This field is only used for administrative purposes, however, it must always be filled in in order to identify the operator.

Wi-Fi SP Country (Abbreviated according to ISO 3166):	
Testing Personnel's Name:	
Test Execution Date:	

A.3 Test Results for EAP-AKA

10.1. Access Tests

10.1.1. Valid Roaming Authentication using IMSI as identity

UICC (IMSI, MSISDN) Used in Test	
Date	
Start Time	
End Time	
Test Result (Pass/Fail)	
Description	Enter valid PIN code to the client.
Status/Comments/Expectations	User should be granted access and have full network capabilities.

10.1.2. Valid Roaming Authentication using pseudonym as identity

UICC (IMSI, MSISDN) Used in Test	
Date	
Start Time	
End Time	
Test Result (Pass/Fail)	
Description	Configure client to use pseudonym as an identity, Enter valid PIN code.
Status/Comments/Expectations	User should be granted access and have full network capabilities.

10.1.3. Valid Roaming Authentication using fast re-authentication mechanism

UICC (IMSI, MSISDN) Used in Test	
Date	
Start Time	
End Time	
Test Result (Pass/Fail)	
Description	Press fast re-authentication button or similar in the client.
Status/Comments/Expectations	User should be granted access and have full network capabilities.

10.1.4. Periodical re-authentication

UICC (IMSI, MSISDN) Used in Test	
Date	
Start Time	
End Time	
Test Result (Pass/Fail)	

Description	While session opens, periodical re-authentication should happen.
Status/Comments/Expectations	User should be granted access and have full network capabilities.

10.1.5. Handover

UICC (IMSI, MSISDN) Used in Test	
Date	
Start Time	
End Time	
Test Result (Pass/Fail)	
Description	Move between two (2) APs so that handover occurs.
Status/Comments/Expectations	Handover succeeds, check authentication type.

10.1.6. Operator Determined Barring

UICC (IMSI, MSISDN) Used in Test	
Date	
Start Time	
End Time	
Test Result (Pass/Fail)	
Description	Operator Determined Barring
Status/Comments/Expectations	The user access should be denied by Home SP (a).

10.1.7. Operator Determined Barring While Session Open

UICC (IMSI, MSISDN) Used in Test	
Date	
Start Time	
End Time	
Test Result (Pass/Fail)	
Description	Operator is barring the session while session is open.
Status/Comments/Expectations	The user access should be denied by Home SP (a). This is up to SP (a) implementation.

10.1.8. Removing SIM-Card During User Session

UICC (IMSI, MSISDN) Used in Test	
Date	
Start Time	
End Time	
Test Result (Pass/Fail)	
Description	Remove SIM-card during user session.
Status/Comments/Expectations	The session is terminated in time period of two (2) seconds.

10.2. Accounting Tests

10.2.1. RADIUS Accounting Data Generation (Session Time)

UICC (IMSI, MSISDN) Used in Test	
Date	
Start Time	
End Time	
Test Result (Pass/Fail)	
Test Verification Result [6]	
Description	Login, Logoff after a set time
Status/Comments/Expectations	Accounting logs should reflect the connection time.

10.2.2. RADIUS Accounting Data Generation (Data Transferred)

UICC (IMSI, MSISDN) Used in Test	
Date	
Start Time	
End Time	
Volume (Amount of transferred data)	
Test Result (Pass/Fail)	
Test Verification Result	
Description	Login, download test file, upload test file and Logoff.
Status/Comments/Expectations	Bytes-In and Bytes-Out in Accounting Logs should be values which are approximately the size of the test file + some network overhead.

10.2.3. Verifying RADIUS Accounting Logs

UICC (IMSI, MSISDN) Used in Test	
Date	
Start Time	
End Time	
Volume (Amount of transferred data)	
Test Result (Pass/Fail)	
Test Verification Result	
Description	Verify that both accounting logs have the same results for all of the accounting tests. Specially, verify that proxy-state attributes are logged and that values are correct.
Status/Comments/Expectations	Session logs to be exchanged along with a copy of the test plan used (for IMSI/ MSISDN/time resolution per test).

10.2.4. Handover

UICC (IMSI, MSISDN) Used in Test	
Date	
Start Time	
End Time	
Volume (Amount of transferred data)	

[6] Test Verification Result field is used for verifying test result against Home SP RADIUS messages. Home SP Testing Personnel should check that RADIUS logs correspond to values mentioned in this testing document.

Test Result (Pass/Fail)	
Test Verification Result	
Description	Move so that handover occurs during an open session.
Status/Comments/Expectations	The user session continues, or there may be two separate accounting sessions.

10.2.5. Chargeable User Identity (CUI)

UICC (IMSI, MSISDN) Used in Test	
Date	
Start Time	
End Time	
Volume (Amount of transferred data)	
Test Result (Pass/Fail)	
Test Verification Result	
Description	Login with a valid SIM card.
Status/Comments/Expectations	Home SP (a) sends CUI to the Visited SP (b). Check that Visited SP (b) sends CUI back to the Home SP (a) in the same format it was received.

10.3. Service Failure Tests

10.3.1. Implicit Logout

UICC (IMSI, MSISDN) Used in Test	
Start Time	
End Time	
Test Result (Pass/Fail)	
Test Verification Result	
Description	Disconnect Wireless LAN card or turn off computer while connected. Wait a set time. Re-insert card or turn on computer.
Status/Comments/Expectations	Accounting should show a closed session and user should have no network access.

10.3.2. Inactivity Logout

UICC (IMSI, MSISDN) Used in Test	
Start Time	
End Time	
Test Result (Pass/Fail)	
Test Verification Result	
Description	The Wi-Fi connection is left idle, an automatic log-off should happen after a pre-determined time.
Status/Comments/Expectations	Absence time-out.

10.4. User Experience Tests

10.4.1. Help Page

UICC (IMSI, MSISDN) Used in Test	
Test Result (Yes/No)	
Description	User's welcome page is displayed after successful login and opening the browser.

Status/Comments/Expectations	This functionality is up to Visited SP (b) implementation.

10.4.2. Start Page

UICC (IMSI, MSISDN) Used in Test	
Test Result (Yes/No)	
Description	Help-page displayed by clicking on link at Login page.
Status/Comments/Expectations	This functionality is up to Visited SP (b) implementation.

10.4.3. Unsuccessful Login

UICC (IMSI, MSISDN) Used in Test	
Test Result (Yes/No)	
Description	Error message shown after unsuccessful login.
Status/Comments/Expectations	An error message is displayed after an unsuccessful login in the client. This might be related to the client features.

10.4.4. Successful Login

UICC (IMSI, MSISDN) Used in Test	
Test Result (Yes/No)	
Description	The successful login is clearly displayed by the client after successful login.
Status/Comments/Expectations	This might be related to the client features.

10.4.5. Logout Confirmation

UICC (IMSI, MSISDN) Used in Test	
Test Result (Yes/No)	
Description	Logout confirmation is displayed after explicit and inactivity logouts by the client.
Status/Comments/Expectations	This might be related to the client features.

Wi-Fi SP Name: [7]	
Wi-Fi SP Country (Abbreviated according to ISO 3166):	
Testing Personnel's Name:	
Test Execution Date:	

A.4 Test Results for EAP-TTLS

11.1. Access Tests

11.1.1. Valid Roaming Authentication

Username/Password Used in Test	
Date	
Start Time	
End Time	
Test Result (Pass/Fail)	
Description	Enter valid roaming username and password.
Status/Comments/Expectations	Username should be in the proper format. User should be granted access and have full network capabilities.

11.1.2. Valid Username, Invalid Password

Username/Password Used in Test	
Date	
Start Time	
End Time	
Test Result (Pass/Fail)	
Description	Enter valid roaming username and invalid password.
Status/Comments/Expectations	Access denied. No network access.

11.1.3. Invalid Username

Username/Password Used in Test	
Date	
Start Time	
End Time	
Test Result (Pass/Fail)	
Description	Enter invalid roaming username and password.
Status/Comments/Expectations	Username should be in the proper format. User should be denied access and have no network capabilities.

[7] Maximum 22 letters. This field is only used for administrative purposes, however, it must always be completed to identify the operator.

11.1.4. Operator Determined Barring

Username/Password Used in Test	
Date	
Start Time	
End Time	
Test Result (Pass/Fail)	
Description	Enter a valid roaming username and password of an account that has been barred by Home SP (a).
Status/Comments/Expectations	Access denied. No network access.

11.1.5. Operator Determined Barring While Session Open

Username/Password Used in Test	
Date	
Start Time	
End Time	
Test Result (Pass/Fail)	
Description	Enter a valid roaming username and password. When the session is open, the SP (a) should assign a barring to this subscriber using functionality according to RFC 5176.
Status/Comments/Expectations	The session should be cancelled automatically a pair of seconds later (quasi-online).

11.2. Accounting Tests

11.2.1. RADIUS Accounting Data Generation (Session Time)

Username/Password Used in Test	
Date	
Start Time	
End Time	
Test Result (Pass/Fail)	
Test Verification Result [8]	
Description	Login, Logoff after a set time.
Status/Comments/Expectations	Accounting logs should reflect the connection time.

11.2.2. RADIUS Accounting Data Generation (Data Transferred)

Username/Password Used in Test	
Date	
Start Time	
End Time	
Volume (Amount of transferred data)	
Test Result (Pass/Fail)	
Test Verification Result[9]	
Description	Login, download test file, upload test file and Logoff.

[8] Test Verification Result field is used for verifying test result against Home SP RADIUS messages. Home SP Testing Personnel should check that RADIUS logs correspond to values mentioned in this testing document.

[9, 11] Test Verification Result field is used for verifying test result against Home SP RADIUS messages. Home SP Testing Personnel should check that RADIUS logs correspond to values mentioned in this testing document.

Status/Comments/Expectations	Bytes-In and Bytes-Out in Accounting Logs should be values which are approximately the size of the test file + some network overhead.

11.2.3. Verifying RADIUS Accounting Logs

Username/Password Used in Test	
Date	
Start Time	
End Time	
Volume (Amount of transferred data)	
Test Result (Pass/Fail)	
Test Verification Result10	
Description	Verify that both accounting logs have the same results for all of the accounting tests. Specially, verify that proxy-state attributes are logged and that values are correct.
Status/Comments/Expectations	Session logs to be exchanged along with a copy of the test plan used (for username/time resolution per test).

11.3. Service Failure Tests

11.3.1. Implicit Logout

Username/Password Used in Test	
Start Time	
End Time	
Test Result (Pass/Fail)	
Test Verification Result12	
Description	Disconnect Wireless LAN card or turn off computer while connected. Wait a set time. Re-insert card or turn on computer.
Status/Comments/Expectations	Accounting should show a closed session and user should have no network access.

11.3.2. Inactivity Logout

Username/Password Used in Test	
Start Time	
End Time	
Test Result (Pass/Fail)	
Test Verification Result13	
Description	The Wi-Fi connection is left idle, an automatic log-off should happen after a pre-determined time.
Status/Comments/Expectations	Absence time-out.

11.4. User Experience Tests

11.4.1. Help Page

Username/Password Used in Test	

Test Result (Yes/No)	
Description	Help-page displayed by clicking on link at Start page.
Status/Comments/Expectations	This functionality is up to Visited SP (b) implementation.

11.4.2. Start Page

Username/Password Used in Test	
Test Result (Yes/No)	
Description	Local Start-page and session window are displayed after successful login.
Status/Comments/Expectations	This functionality is up to Visited SP (b) implementation.

11.4.3. Unsuccessful Login

Username/Password Used in Test	
Test Result (Yes/No)	
Description	Error message shown after unsuccessful login.
Status/Comments/Expectations	This functionality is up to client feature.

11.4.4. Successful Login

Username/Password Used in Test	
Test Result (Yes/No)	
Description	Logout method is clearly displayed after successful login.
Status/Comments/Expectations	This functionality is up to client feature.

11.4.5. Logout Confirmation

Username/Password Used in Test	
Test Result (Yes/No)	
Description	Logout confirmation is displayed after explicit and inactivity logouts.
Status/Comments/Expectations	This functionality is up to client feature.