**eduroam(UK) Technical Specification v1.4 – Summary of Recommendations Checklist**

The following tables summarise the eduroam deployment recommendations made in the Technical Specification. When implemented in conjunction with the mandatory requirements, the resulting service will conform to best current practice.

|  |  |  |  |
| --- | --- | --- | --- |
| **O.R. no.** | **Description** | **Compliance notes** | **Tick box Y/N** |
| **Common Recommendations – both Home (IdP) and Visited (SP)** | | | |
| 1. | Participants SHOULD observe the recommendations set out in this document |  |  |
| 2. | Participants SHOULD deploy a secondary ORPS |  |  |
| 3. | Participants SHOULD NOT forward accounting messages to the NRPS |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **O.R. no.** | **Description** | **Compliance notes** | **Tick box Y/N** |
| **Home (IdP) Organisation Recommendations** | | | |
| 4. | Home organisations SHOULD choose a type, or types, that fulfil all or most of the ‘mandatory requirements’ section of RFC 4017 [16] |  |  |
| 4.1. | The EAP types TLS [17], PEAP [18], and TTLS [19] are recommended |  |  |
| 5. | The test account SHOULD be created in the organisation’s primary user database. If more than one user database exists, it SHOULD be created in the user database that is likely to be most authenticated against |  |  |
| 6. | Other privileges SHOULD NOT be assigned to the test account |  |  |
| 7. | The test account SHOULD be configured to allow at least five consecutive failed authentication attempts without the account being locked |  |  |
| 8. | Home organisations SHOULD educate their users to use protocols that provide appropriate levels of security when using eduroam |  |  |
| 9. | Where an authentication request is received from a NRPS, as opposed to being received from an internal RADIUS client or NAS, a Home organisation’s Access-Accept reply SHOULD NOT contain dynamic VLAN assignment attributes, unless a mutual agreement is in place with the Visited organisation. This may be achieved by the Home organisation filtering out dynamic VLAN assignment attributes if present in Access-Accept packets sent to the NRPS. |  |  |
| 10. | If the Home RADIUS server supports Chargeable-User-Identity (CUI) then Access-Accept replies SHOULD contain the CUI attribute, where CUI is solicited in the authentication request from the Visited organisation, as described in RFC 4372 [22] |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **O.R. no.** | **Description** | | | **Compliance notes** | **Tick box Y/N** |
| **Visited (SP) Organisation Recommendations** | | | | | |
| 11. | | Where possible Visited organisations SHOULD implement the enhanced features/advanced level engineering standards in preference to the base engineering standards for their eduroam networks |  | |  |
| 12. | | Visited organisations SHOULD configure their ORPS to load balance between the NRPS servers |  | |  |
| 13. | | Visited organisations MAY configure their ORPS to fail-over between the NRPS servers |  | |  |
| 13.1. | | If the fail-over algorithm has a configurable timer that specifies the length of time after which an unresponsive server is considered unreachable, this timer SHOULD be configured to zero seconds (or as low a value as possible) |  | |  |
| 14. | | Visited organisation SHOULD configure their ORPS to insert the Operator-Name attribute, accurately composed for their realm, into all Access-Request packets forwarded to the NRPS |  | |  |
| 15. | | Visited organisations SHOULD request Chargeable-User-Identity (CUI) in Access-Request packets forwarded to the NRPS if CUI is supported by the ORPS |  | |  |
| 16. | | If an ORPS is capable of using Status-Server (RADIUS Code 12) to detect the operational state of the NRPS, then it SHOULD be configured to do so |  | |  |
| 17. | | If an ORPS is capable of being queried by Status-Server then that functionality SHOULD be enabled so that the NRPS are able to make a more informed decision on the operational status of the ORPS |  | |  |
| 18. | | Visited organisations SHOULD configure the network to prevent a visitor from masquerading as an authorised Dynamic Host Configuration Protocol (DHCP) [27] server or router |  | |  |
| 19. | | Visited organisations MAY implement arbitrary IP filtering of packets addressed to other hosts on the Visited organisation’s own network |  | |  |
| 20. | | Visited organisations SHOULD provide visitors with unimpeded access to the Internet and vice versa, where local policy permits |  | |  |
| 21. | | Visited organisations SHOULD NOT deploy application or ‘interception’ proxies on the eduroam network |  | |  |
| 22. | | Visited organisations SHOULD ensure that their eduroam information website is accessible using small form-factor devices |  | |  |
| 23. | | Visited organisations MAY publish the IP forwarding policies imposed on the visitor network |  | |  |
| 24. | | As part of the enhanced features/advanced level standard, participants are recommended to implement IPv6 and allow routing of IPv6 on the eduroam network |  | |  |

For references refer to full Technical Specification document.