Bilaga 1 – Krav på eduroam hos Skolfederations medlemmar

1. Bakgrund

I detta dokument beskrivs de krav som ställs på de medlemmar i Skolfederation som tecknat avtal om anslutning till eduroam (Medlem).

2. Gemensamma krav

- Alla Medlemmar skall uppfylla kraven I SWAMID 2.0.
- Medlem skall följa de krav på nätfunktion som ställs i *SWAMID eduroam Technology Profile*, som i sin tur regleras av *eduroam Policy Service Definition*.
- Medlem skall erbjuda nätverksåtkomst, dvs. alla Medlemmar som agerar IDP måste också agera SP.
- Medlem skall köra minst en RADIUS-server och bör av redundansskäl köra minst två RADIUS-servrar.
- Medlem skall vara behjälpliga med att lösa problem samt hantera roaming-relaterade incidenter.
- Medlem får inte ta betalt av användare som använder eduroam.

3. Utbyte av information

Medlem ska tillhandahålla följande information till IIS:

1) Sfär (realm/domain) som anslutningen avser (kan vara flera), (gäller endast för IDP)
2) IP-adresser för kundens RADIUS-servrar
3) RADIUS-hemlighet för anslutning

IIS ska tillhandahålla följande information till Medlem:

1) namn/adresser på Skolfederations RADIUS-servrar
2) RADIUS-hemlighet för anslutning

I de fall autentisering ska ske med protokollet RADSEC ska även certifikat och eventuella certifikatutfärdare utbytas mellan parterna.

Skolfederation

4. Identity Provider

Säkerhet

- Medlemmens sfär (*realm*) skall inkludera ett domännamn som ägs av Medlemmen. (Gäller endast för IDP)
- Domännamnet skall ligga under toppnivådomänen för Sverige – SE.
- IDP skall autentisera samtliga användare med hjälp av EAP (*Extensible Authentication Protocol*) över RADIUS enligt RFC 3580.
- Samtliga användare skall ges personliga och unika användaridentiteter.

Loggning

IDP skall vid nätverksåtkomst logga följande information (attribut):

- Datum och tid, spårbar till UTC
- Användarnamn (User-Name, inner EAP identity, Chargeable-User-Identity)
- MAC-adress (Calling-Station-Id)
- Operatör (Operator-Name, Called-Station-Id)

Loggar skall sparas så att IDP kan assistera SP vid incidenthantering. Skolfederations rekommendation är att loggar sparas i minst sex månader, men högst två år.

5. Service Provider

Nätverksåtkomst

SP skall erbjuda nätverksåtkomst i enlighet med eduroam *Policy Service Definition*. Detta betyder i korthet:

- Det trådlösa nätverkets namn skall vara “eduroam”
- Åtkomst via IPv4 skall erbjudas
- Åtkomst via IPv6 bör erbjudas
- Adressöversättning (NAT) av IPv4 bör undvikas

Nedanstående protokoll/portar skall vara öppna för samtliga besökande användare:

Tjänst	Protokoll	Riktning
IPsec	IP proto 50 (ESP)	in/ut
IPsec	IP proto 51 (AH)	in/ut
IPsec	UDP port 500 (IKE))	ut
OpenVPN	UDP port 1194	in/ut
IPv6 tunnel	IP proto 41	in/ut
IPsec NAT traversal	UDP port 4500	in/ut
Cisco IPsec over TCP	TCP port 10000	ut
PPTP VPN	IP proto 47 (GRE)	in/ut
PPTP VPN	TCP port 1723	ut

SSH	TCP port 22	ut
http	TCP port 80	ut
http	TCP port 443	ut
http	TCP port 3128	ut
http	TCP port 8080	ut
Skicka epost	TCP port 465	ut
Skicka epost	TCP port 587	ut
Ta emot e-post	TCP port 143	ut
Ta emot e-post	TCP port 993	ut
Ta emot e-post	TCP port 110	ut
Ta emot e-post	TCP port 995	ut
FTP (passive)	TCP port 21	ut

Nätverksåtkomst för besökande användare bör inte vara begränsat (dvs all trafik bör tillåtas). Om detta inte är möjligt skall trafik filtreras så lite som möjligt. SP bör inte använda sig av filtrering på applikationsnivå (*application inspection*) eller fångande reläer (*interception proxies*).

Loggning

SP skall vid nätverksåtkomst logga följande information (attribut):

- Datum och tid, spårbar till UTC
- Användarnamn (User-Name, outer EAP identity, Chargeable-User-Identity)
- MAC-adress (Calling-Station-Id)
- Operatör (Operator-Name, Called-Station-Id)

Loggar skall sparas så att SP kan assistera IDP vid incidenthantering. Skolfederations rekommendation är att loggar sparas i minst sex månader, men högst två år.

Säkerhet

- SP skall erbjuda kryptering enligt WPA2 (IEEE 802.11i/CCMP).
- SP ansvarar själv för att filtrera bort eventuella skadliga attribut, t.ex. för VLAN- och rolltilldelning, i RADIUS-svar från IDP.