Javaslat az NIIF eduroam dokumentáció frissítésére 1.0->2.0

1. Indoklás, célok

Az NIIF eduroam dokumentáció aktuális, 1.0 változata 2008-ban készült. Azóta

- változtak a WLAN technikai lehetőségek,
- napvilágra kerültek új WLAN biztonsági problémák,
- fejlődött a (nemzetközi) eduroam infrastruktúra,
- változtak a nemzetközi eduroam szabályzatok.

A fentiek indokolttá teszik az NIIF eduroam szabályzat és az eduroam ismertető frissítését. (A harmadik ide tartozó dokumentum az eduroam föderációs szerződés, ennek módosítása nem szükséges.)

A frissítés célja, hogy a dokumentáció ismét megfeleljen az aktuális műszaki és szabályozási környezetnek.

A változások rövid említése természetesen mindkét dokumentum végén megtalálható „Verziókövetés” táblázatban. Emellett az eszközölt módosítások részletes felsorolása is megtalálható a jelen dokumentum „Változások” című fejezetében.

2. Ütemezés

A dokumentumok közül a szabályzat esetében lényeges a módosítás ütemezése. Az alább javasolt ütemezés két fő szempontra épül: A magyarországi eduroam infrastruktúra mielőbb érje el az új szabályzat szerinti korszerű állapotot, de a tagintézményeknek ez ne jelentsen aránytalanul nagy terheket.

Az alábbi lépéseknél zárójelben megadtunk egy példát az ütemezésre.

1. Az ismertető és a szabályzat **tervezett új verziójának megküldése** az NIIF Műszaki Tanácsnak és az eduroam tagintézmények illetékeseinek véleményezésre. (Pl. 2016. április 11.)
2. A szabályzattervezet **megvitatása, esetleges módosítása**, véglegesítése. Határidő: a megküldés után egy hónappal. (Pl. 2016. május 11.)
3. Az új ismertető és a véglegesített **új szabályzat publikálása az NIIF Intézet által** a http://www.eduroam.hu/ alatt. Az NIIF Intézet egyúttal írásban tájékoztatja a föderáció tagintézményeit az új szabályzatról. Határidő: a véglegesítés után egy héttel. (Pl. 2016. május 17.)
4. A magyarországi **föderáció tagjai** az új szabályzat elfogadása esetén **publikálják** azt a saját intézményükben és tájékoztatják róla saját felhasználóikat; vagy az új szabályzat el nem fogadása esetén értesítik erről a döntésükről az NIIF Intézetet. Határidő: az új változatok NIIFI általi publikálását követő hónap 15. napja. (Pl. 2016. június 15.)
5. Az **új szabályzat hatályba lép** az NIIFI általi publikálását követő második hónap elején. A föderációs szerződést az új szabályzat NIIFI általi **publikálása után aláíró intézmények, a központi infrastruktúra üzemeltetője, és a felhasználók számára** az új szabályzat szerinti működés **a hatályba lépéstől kötelező**. (Pl. 2016. július 1.)

6. Mindenki más, így a magyarországi föderációhoz az 5. pontban meghatározottnál **korábban csatlakozott eduroam tagintézmények számára kötelező**vé válik az új szabályzat szerinti működés a szabályzat hatályba lépése után 8 hónappal. (Pl. 2017. március 1.)

A fenti 3., 5., és 6. pont szerinti határidő konkrét dátuma bekerül a szabályzatba.

3. Változások

3.1. A szabályzat 2.0 változatának újdonságai (az 1.0-hoz képest)

[pontosítás] A felhasználói jogosítvány fogalmának tisztázása, és használatának módosítása az egész dokumentumban eszerint: A jogosítvány nem egy titkos adat, hanem a felhasználó azonosítóját tartalmazó publikus, valamint egy érzékeny részből áll – ez utóbbi titkos, és birtoklása igazolja a felhasználó azonosságát.

A központi infrastruktúra üzemeltetője nemzetközi viszonylatban a hagyományos RADIUS/UDP mellett RADIUS/TLS-t (RadSec) is használhat. (Hazai viszonylatban marad változatlanul a RADIUS/UDP.)

[pontosítás] A 3.1.3.4. új követelménypont előírja az EAP authentikáció felhasználó és saját intézménye közti lebonyolításához szükséges RADIUS attribútum érintetlenül történő proxyzását.

[központi infrastruktúra: új és módosított követelmények] A RADIUS authentikációra vonatkozó 3.1.3.1-2. pontok általánosabbra módosultak, UDP és TLS feletti RADIUS esetén egyaránt alkalmazhatók. A korábbi 3.1.3.3. előírás átkerült az általános fejezetből változatlan tartalommal az intézményekre vonatkozó fejezetbe (3.2.5.1.), módosított – a RADIUS/TLS esetet is tartalmazó – tartalommal pedig a központi infrastruktúrára vonatkozó fejezetbe (3.3.3.1.).

[központi infrastruktúra: új követelmények] A központi RADIUS infrastruktúrára vonatkozó fejezet új pontokkal (3.3.2.2-6.) bővült, melyek kötelezővé teszik nemzetközi viszonylatban a RADIUS üzenetek TLS feletti fogadását, és javasolják TLS feletti küldését, valamint ez utóbbi esetben előírják az F-Ticks statisztikai üzenetek küldését.

[intézmények: módosított követelmény] A módosított 3.2.1.2. pont lehetővé teszi nem `.hu` végződésű eduroam domain név használatát is, bár ez nem ajánlott.

[intézmények: új követelmény] Az új 3.2.4.5. pont szerint az intézmények számára javasolt a RADIUS/TLS-hez szükséges NAPTR DNS bejegyzés létrehozása. Így a saját felhasználóik külföldi vendéglátó intézményben történő csatlakozásakor az authentikációs kommunikáció történhet a magyarországi központi infrastruktúráig RADIUS/TLS segítségével is. (A központi infrastruktúra és a saját intézmény közt változatlanul RADIUS/UDP marad ezután is.)

[központi infrastruktúra: módosított követelmény] A módosított 3.2.5.8. és 3.3.4.2. pontok értelmében nem elegendő a PAP authentikáció használata a központi infrastruktúra üzemeltetője részéről a felügyeletben, hanem a valós problémák nagyobb részét felfedő EAP (EAP-TTLS vagy PEAP) authentikációt kell erre a célra használnia.

[intézmények: új követelmény] Az új 3.2.5.9-10. pontok értelmében a saját felhasználók authentikációjakor kötelező a Chargeable User Identity használata, amennyiben azt a vendéglátó intézmény jelzi.

[intézmények: új követelmény] Az új 3.2.5.11. pont értelmében a gyakori hibát okozó VLAN attribútumokat csak előre egyeztetett esetben szabad küldeni az authentikációs folyamat során.

[intézmények: pontosítás] Az intézmények által üzemeltetett WLAN access pointokra vonatkozó előírások módosultak a 3.2.6.1. és a 3.2.6.3. pontokban az IEEE 802.11 szabvány fizikai és adatkapcsolati réteget leíró részei fejlődésének türkében.

[intézmények: módosított követelmény] A WPA/TKIP időközben napvilágra került biztonsági problémái miatt a korábban csak ajánlottként megadott WPA2/AES kötelezővé vált. Ennek megfelelően a 3.2.6.5-6. pontokat a módosított 3.2.6.5. pont váltotta fel, és ezzel összhangban módosult a 3.2.6.1. pont.

[intézmények: új követelmény] A felhasználói jogosítványok illetéktelen kezekbe kerülésének megakadályozása érdekében kiegészült a 3.2.3.3. pont a RADIUS tanúsítvány pontos ellenőrzési módjának kötelező ismertetésével, és új ajánlottként bekerültek a 3.2.4.3-4. pontok.

[intézmények: módosított követelmény] Több intézmény térben egymást átfedő eduroam WLAN szolgáltatásának problémája elkerülése érdekében kötelezővé vált ezekben az esetekben eltérő SSID-k használata. Az ilyen esetek kezelésére módosultak és kiegészültek a korábbi 3.2.6.7-9. pontok az aktuális 3.2.6.6-10. pontokra.

[intézmények: módosított követelmény] A 3.2.7.3. pontban leírt kötelezően átengedendő forgalom módosult. Bekerült a HTTP-hez használt 3128-as és 8080-as TCP portra, valamit az XMPP-hez használt 5222-es TCP portra irányuló forgalom, az FTP, továbbá az IPsec AH és ESP.

[intézmények és központi infrastruktúra: új követelmény] Az új 3.2.2.9. és 3.3.1.3. pontok szerint nyilván kell tartani a szolgáltatási helyszíneket az eduroam központi térképes adatbázisában.

[módosított követelmény] A módosított 3.1.3.2., 3.2.5.1., 3.3.3.1. pontok értelmében a RADIUS accounting üzeneteket nem kell proxyzni.