

TERENA TF Mobility
20th meeting 20 oct 2009



Support for the development of



Report from GN3:

Multi-Domain User Applications Research
Task 1: Roaming developments

Issues being worked on



- RadSec
 - Standardisation
 - Improving implementations
- Chargeable-User-Identity: recognising a user on re-entry
- „Don't Fragment“ issue on Linux: debugging, back to the roots
- Watching brief on standards: IEEE 802.1X
- We're having a ... deliverable: DJ3.1.1
„Development of RadSec and definition of eduroam extensions“

RadSec



■ Well... RTFM :-)

□ A number of Internet-Drafts

- TCP transport
- DTLS transport
- TLS encryption
- Dynamic Discovery
- CA for operations

□ Implementations

- JRadius: welcome to the club

□ Deployment

- A few countries use the eduGAIN CA for bidirectional RadSec up-/downlinks
- Many countries use own CA for intra-country connections



Chargeable-User-Identity (CUI)



- Well... RTFM :-)
- A standard RADIUS attribute, but almost unimplemented (until GN3 ...)
- Opaque, persistent identifier for a user
 - SP can request a CUI
 - IdP can generate one on the way back
 - We define some extras for better privacy
 - CUI shouldn't be global, but different per SP
 - Need an SP Identifier
 - Combine CUI with „Operator-Name“ attribute
 - If Operator-Name is not sent, no CUI for you



Don't Fragment



- A Linux-only issue
 - Linux sends all UDP packets with „DF“ bit set
 - Supposed to help with PMTU discovery
 - Good goal, but: discards(!) packets if PMTU would be needed
 - EAP payloads with much bulk data transfer would suffer most (notably EAP-TLS, but not exclusively)
- Workaround: disable PMTU system-wide
- Fix: manipulate socket to disable DF
 - We provided fixes for FreeRADIUS, Radiator, radsecproxy, wpa_supplicant (eapol_test)





This page intentionally left blank.