3GPP TSG WG3 S3#17bis Tdoc S3z010047
Madrid, Spain
27th April, 2001

Agenda Item: TBD

Source: TSG SA3

Title: Working assumptions and HSS/S-CSCF concerns

Document for: Discussion and decision

1 Scope and objectives

The scope for this document is to discuss with and inform SA2 on the current status in SA3 on aSIP and termination of authentication.

2 Working assumptions

Session establishment

It is the working assumption of the aSIP ad hoc group that the hop-by-hop integrity protection of session establishment (INVITEs) and the option to authenticate the user during re-registrations and the ability of the Network to force re-registration, provide adequate protection for session establishment. The re-registration timer can be reset to a new value when forcing a re-registration.

Confidentiality Protection of SIP signalling

It is the working assumption of the aSIP ad hoc group that the confidentiality of SIP signalling between the UE and P-CSCF is optional for implementation. Confidentiality of SIP signalling can rely on existing mechanisms, or mechanisms which will be provided by NDS.

3 HSS/S-CSCF concerns

23.228 created to make HSS a "dumb" database ?

- Delay of re-authentication (fetching Auth Vectors)
  - Cases of Re-authentication are: Re-registrations~~, during long calls~~

  TO BE REMOVED BECAUSE OF WORKING ASSUMPTION ON SESSION EST.

  HSS performs functionality per user authentication (+ higher data storage requirement)
  - Introduction of VLR functionality in the HSS

- DoS attack risk ?
  - Bogus user concerns ?

    RELATED TO DATA STORAGE CONCERN
  - Dealing with identified DoS attacks

Concerns with S-CSCF solution:

- Introduction of VLR functionality in S-CSCF
- Early allocation of S-CSCF resources
  - DoS attack risk ?
    - Bogus user concerns ?
    - many resources allocated to unauthenticated users
    - Extra signalling overhead on Failure

- HSS storage of S-CSCF addresses solution needs to be checked for feasibility