ITU-T / ATIS Workshop
"Next Generation Technology and Standardization"
Las Vegas, 19-20 March 2006

End-to-End Authentication Requirements for NGNs

Ray P. Singh
Telcordia Technologies

ITU-T

Alliance for Telecommunications Industry Solutions

Overview

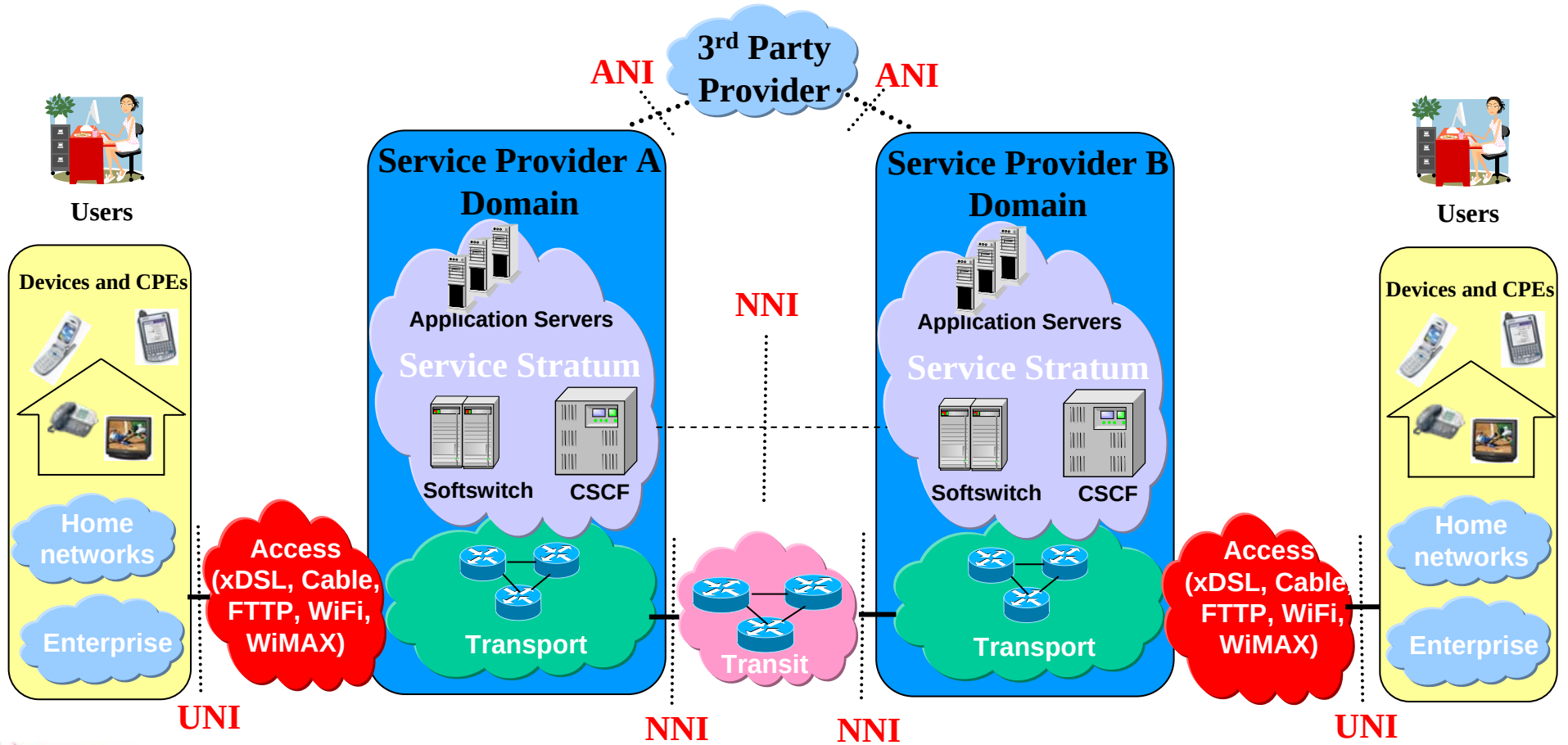
- What is the problem?
  - Full security capabilities need to be specified for NGNs
    - Lack of requirements for capabilities to authenticate various entities (e.g., users, devices, network elements, networks, service providers, etc) in multi-network environment
- What has to be done
  - Identify authentication capabilities to be supported
  - Develop and specify requirements
- Why is it important
  - Protection of NGN infrastructure and services
    - Authentication is the first line of defense against unauthorized access
  - Necessary for accounting/billing, law enforcement and other purposes
  - Better to specify and support authentication capabilities initially as opposed to retro fitting deployed NGNs

ITU-T Recommendation X.805

- Authentication Security Dimension Definition
  - The authentication security dimension serves to confirm the identities of communicating entities.
  - Authentication ensures the validity of the claimed identities of the entities participating in communication (e.g., person, device, service or application) and provides assurance that an entity is not attempting a masquerade or unauthorized replay of a previous communication.

End-to-End View (1 of 2)

Authentication of communicating entities in multi-network environment



End-to-End View (2 of 2)

- Authentication across UNI, NNI and ANI in a multi-network environment
  - Access networks (xDSL, Cable, WiFi, WiMAX, etc)
  - Core networks
    - Transport stratum
    - Service/control stratum
  - 3rd party application providers
  - Transit network providers
  - Customer domains (e.g., terminals, home and enterprise networks)
- Identity management across multiple service providers and administrative domains

Organization of Authentication Functions

- Network Access Authentication
- Service/Application Authentication
- Network-to-Network Authentication
- User Peer-to-Peer Authentication
- User Authentication of Network
- 3rd Party Provider Authentication

Network Access Authentication (UNI)

- Authentication of customer domain entities to obtain network access connectivity
  - End user devices and terminals
  - Home network gateways
  - Enterprise network gateways
- Factors to consider
  - Identification of customer domain entities
  - Trust relations and information sharing across multiple administrative domains
    - Identity management
    - Mobility
    - Privacy of user information
  - Authentication mechanisms to be supported

Service / Application Authentication

- Authentication of user, device, and user/device combination to obtain
  - Access to NGN services and features (e.g., Voice)
  - Access to unique or special services (e.g., ETS)
- Factors to consider
  - Multiple user identities (e.g., user name, telephone number, email address)
  - Trust relations across multiple administrative domains
    - Identity management
    - Mobility
    - Privacy of user information
  - Authentication mechanisms (e.g., Using SIP signaling or Web based (http))

Network-to-Network Authentication

- Authentication across Network-to-Network Interface (NNI)
  - Transport authentication
    - Authentication of communicating entities in the transport network (e.g., transport network elements for bearer traffic)
  - Service/control authentication
    - Authentication of communicating entities in the service stratum (e.g., signaling and control network elements such as SBCs, CSCFs, etc)
  - Management authentication
    - Authentication of communicating entities in the management plane (e.g., for exchange of management or accounting information)
- Factors to consider
  - Identification of network elements and communicating entities
  - Trust relations across multiple administrative domains
  - Authentication mechanisms

User Peer-to-Peer Authentication

- Peer-to-peer authentication of communicating end users and devices
  - Calling user authentication of called user
  - Called user authentication of calling user
  - User authentication of data origin source
- Factors to consider
  - Feature may be provided as a service
  - May involve a 3rd party verification (e.g., service provider)
  - Authentication mechanisms

User Authentication of Network

- User authentication of the NGN
  - User authentication of the connected NGN (e.g., access network)
  - User authentication of the NGN service provider
- Factors to consider
  - Feature may be provided as a service
  - May involve a 3rd party verification (e.g., service provider)
  - Network and service provider identity
  - Trust relations across multiple administrative domains
  - Authentication mechanisms

3rd Party Provider Authentication

- Two separate issues to be addressed
  - 3rd party application provider
  - 3rd party authentication provider
- 3rd party application provider
  - Authenticating 3rd party application providers for access
  - Authentication of communicating signaling/control, transport and management entities across ANI
- 3rd party authentication provider
  - Allow for possible use 3rd party providing authentication service
- Factors to consider
  - Authentication mechanisms for ANI
  - Trust relations across multiple administrative domains

Abbreviations and Acronyms

- ANI – Access Network Interface
- CPE – Customer Premise Equipment
- CSCF – Call Session Control Function
- DSL – Digital Subscriber Loop
- ETS – Emergency Telecommunications Service
- FTTP – Fiber To The Premise
- NGN – Next Generation Network
- NNI – Network-to-Network Interface
- UNI – User Network Interface
- SBC – Session Border Controller