SIP Identity Usage in Enterprise Scenarios

IETF #64 Vancouver, 11/2005

Steffen Fries, Siemens AG, ✉ steffen.fries@siemens.com
Hannes Tschofenig, Siemens AG, ✉ hannes.tschofenig@siemens.com
Siemens AG, Corporate Technology, CT IC 3
81730 Munich, Germany

draft-fries-sipping-identity-enterprise-scenario-01.txt

Problem Description

- End2end authentication, identity provision, and security parameter bootstrapping are interesting for several scenarios (e.g., media data security)
- User credentials from Enterprises often limited
  - Username and password ◊ may be used for service access within the Enterprise only
  - Corporate PKI solutions ◊ certificates may not be signed by a globally trusted root certificate and thus not easily verifiable by third parties
  - If corporate PKI used, user credentials often provided on dedicated security devices (like smart cards) ◊ may not interface with devices like IP Phones
- Enterprise devices may already be bound to corporate PKI through device certificates (e.g., applying IEEE 802.1x)
- Problem: How to provide a trusted certificate to be used for secure interactions with an external party?

Problem Description (cont.)

- SIP Identity and SIPPING Certs help, but do not explicitly provide solution for binding an identity to a device certificate or self-signed certificate for session duration

- SIP Identity ID (draft-ietf-sip-identity-06.txt) introduces Authentication Service
    - Basic idea is signing the FROM field and some other headers as well as SDP body after authenticating the user
    - Does not talk about SDP body content associations with the assertion (except integrity)

- SIPPING Certs ID (draft-ietf-sipping-certs-02.txt) introduces Credential Server
    - Suitable for an enterprise environment to provide credential (certificate) information to end hosts and end users via a credential server
    - Unclear if interaction with external parties using a public certificate server is realistic (corporate directory often only accessible from within the enterprise)
    - Requires AoR matching of certificate (won’t work e.g., with device certificates)

Solution Approach

- draft-fries-sipping-identity-enterprise-scenario-01.txt builds on the Identity ID by proposing the following for BCP:
  - Upon INVITE initiator provides certificate within the SDP body, e.g., by using new MIKEY method draft-ietf-msec-mikey-rsa-r-00.txt or plain RFC3261 S/MIME key exchange (draft currently takes device certs as example, may be also self-signed)
  - Handling of Authentication Service (following SIP Identity ID)
    - Provides signature over certain header fields and SDP body after authenticating the user
    - Creates an implicit session binding for the identity provided in FROM field with the certificate sent in the body
  - Receiver stores provided identity and certificate for duration of session
  - Certificate may be used to negotiate further session security parameter
  - Saves interaction with other peers like a certificate server

Next Steps

- Propose to take ID as WG item for BCP
- Adoption as WG item?