S3-020486

Architectural choices for Subscriber Certificates

NOKIA

Introduction

- S3-020378 (Nokia contribution, July 2002) describes security and other requirements for subscriber certificates
- LS to SA1 and SA2 (S3-020447, July 2002, Helsinki) identifies four choices on connecting cellular network to the Certification Authority (CA): SGSN, GGSN, IMS, and a new “gateway” type element.
- In this contribution we discuss the pros and cons of each choice. For each choice (SGSN, GGSN, IMS and New Element):
  - Idea and Benefits
  - Required New Functionality
  - Drawbacks and Possible Stumbling Blocks
- Overall conclusion: the four architectural choices are more or less equal from security point of view.

SGSN Alternative: Idea and Benefits

- What?
  - The CA is connected to the SGSN.
  - UE sends the certificate request always to SGSN. UE indicates within the request message the network (home or visited) from which it wants the certificate.
- Benefits
  - Existing secure communication channel with UE used (no need to define new security procedures).
  - SGSN is always located in visited network, so addressing of local CA is easy.
  - SGSN can handle easily the subscriber information check (or deliver the needed info to CA), as subscriber profile is downloaded to SGSN.

SGSN Alternative: Required New Functionality

- SGSN needs to support new UE signaling.
- SGSN needs to check where the certificate request is routed to and add needed parameters (e.g. parameters from subscriber profile) to it.
- SGSN may need to check in the subscriber data whether issuing of certificate is allowed or not.
- SGSN needs to support new interface to CA.

SGSN Alternative: Drawbacks and Possible Stumbling Blocks

- The interoperator interface between visited SGSN and home CA might be problematic from operator's point of view.
- Addressing CA in home network when user is roaming requires either that address of home CA is stored to UE, or added to subscriber profile.
- Requires standardization of signaling messages (in layer 3).

GGSN Alternative: Idea and Benefits

- What?
  - The CA is connected to the GGSN.
  - UE selects the network from which it wants the certificate by selecting the correct GGSN (home or visited).
  - The certificate request and response could be in new messages between UE and GGSN.
- Benefits
  - Existing secure communication channel with UE used (no need to define new security procedures).
  - GGSN is a ”natural” element from which to go to network elements that are external to PS domain.

GGSN Alternative: Required New Functionality

- GGSN needs to support new interface to CA.
- GGSN needs to decide based on subscriber data whether issuing of certificate is allowed or not (also CA could do this if data is delivered to it).
- New signaling messages for certificate request.
  - UE, SGSN and GGSN need to support those new messages.

GGSN Alternative: Drawbacks and Possible Stumbling Blocks

- Standardization of new messages between UE and GGSN is required.
- Certificate issuing from visited network is coupled with other services (e.g. getting internet access) through the visited network's GGSN, because UE and visited GGSN can communicate only if they share a PDP context.

IMS Alternative: Idea and Benefits

- What?
  - IMS system to act as the authenticator of the subscriber during certificate requests, and CA is connected to an IMS element.
  - Before certificate request is done, normal IMS registration (including P-CSCF discovery, S-CSCF selection and authentication) is done.
- Benefits
  - Allows that check for issuing subscriber certificate is done always in home operator’s network (added flexibility for checking parameters).
  - Subscriber certificates could be obtained over any access network that provides access to IMS.

IMS Alternative: Required New Functionality

- P-CSCF needs to identify SIP message carrying the certificate request, and add address of the local CA to that message.
- S-CSCF needs to check in the subscriber data whether issuing of certificate is allowed or not.
- S-CSCF needs to support new interface to CA (possibly extension of ISC interface).

IMS Alternative: Drawbacks and Possible Stumbling Blocks

- Would make subscriber certificates, and services based on them, restricted to IMS subscribers.
- If P-CSCF is in home network, then **the local CA can not be used** and local services that require agreement between local operator and service provider can not be supported.
- May require IETF standardization.
- Requires changes to P-CSCF and S-CSCF.
  - P-CSCF needs to identify SIP message containing certificate request.

New ”Gateway” Type Element Alternative: Idea and Benefits

- What?
  - A new network element to act as the authenticator of the subscriber during certificate requests
- Benefits
  - Technically feasible
  - No arbitrary constraints
    - in theory, anything can be specified and designed in a new element
  - Access independence for certificate requests
  - Synergies with WLAN interworking security solutions possible
  - Changes to application layer easier to build on top of legacy terminals (supporting e.g. WIM and USIM)

New Element Alternative: Required New Functionality

- Terminal must support the new authentication mechanism
  - e.g., PIC, EAP, and EAP AKA
- New element needs an interface to HSS
    - either directly, using the MAP-based roaming infrastructure
    - or indirectly, using a DIAMETER-based roaming infrastructure
  - needs an interface to the CA
    - but may be possible to use some existing standard RA <-> CA interface

New Element Alternative: Drawbacks and Possible Stumbling Blocks

- Terminals have to support PIC, EAP, and EAP AKA
  - Alternative: HTTP Digest AKA, but then protocol messages in addition to HTTP Digest needed
- How does UE find the authenticator? (when certificates are issued by visited networks)
  - Service Location Protocol can be used; but then network and terminal should support SLP
- A new independent domain that consumes authentication vectors is needed
- Home operator control over certificate issuing requires new attributes in subscriber profile and retrieval of subscriber profile to a new element has to be arranged