3GPP TSG SA WG3 Security — S3#26 **S3-020636**

19 – 22 November 2002

Oxford, UK

Source: **Siemens**

Title: **Bootstrapping for subscriber certificates**

Document for: **Discussion**

Agenda Item: **7.7 (Support for subscriber certificates)**

Abstract

This contribution proposes that 3GPP should concentrate their work on defining a bootstrapping protocol, based on AKA, which establishes a shared secret between a UE and an appropriate network server. This shared secret could then be used in certificate requests to authenticate the client. 3GPP should also consider to standardise certificate formats/profiles and an inter-operator PKI. 3GPP should leave the standardisation of the actual certificate management protocols to other bodies. An architecture to support the proposed approach is sketched, and a first overview of candidates for a bootstrapping protocol is given. The bootstrapping protocol should be sufficiently generic to be able to support also other application scenarios.

---

1. Introduction

Since the work item on subscriber certificates was approved at SA3#21 one year ago, SA3 has seen many detailed contributions on the subject, investigating a variety of issues. The work was originally planned to be completed by SA#17 (Sept 2002), but SA3 does not seem to have agreed on a way forward yet. However, two tendencies seem to be emerging: a preference for access network independent solutions, and a preference for certificates issued by the home operator. Instead of adding to the number of detailed investigations of particular issues, this contribution tries to take a step back and look at what 3GPP SA3 should and could be doing in the context of subscriber certificates. It then proceeds to propose an approach to solve the identified tasks.

2. Scope of 3GPP work on subscriber certificates

At a first glance, it does not seem obvious why 3GPP should deal with subscriber certificates at all. True, there are many useful applications of subscriber certificates, among them digital signatures in m-commerce, location services security and key management for end-to-end encryption, but application issues are not typically addressed by 3GPP, but by other bodies, such as WAP (now OMA) or W3C.

The latter organisations have worked indeed, and are still working, on certificate request procedures which are optimised to reduce the load on clients (see earlier Siemens contribution to SA3#24 S3-020365, and a companion contribution submitted by Siemens to this meeting). In addition, the IETF has provided certificate management protocols (CMP, PIC). It is questionable whether 3GPP should add another new certificate request protocol to the list of available protocols, or even, select one of those already existing. However, the security of all these protocols rests on the availability of a shared secret or a password known to both the subscriber and the CA/PKI portal. The problem is, however, that this shared secret or password is, in general, not available in an automated way, rather, it has to be provided out-of-band via O&M measures which tend to be costly. This is called the bootstrapping problem.

3GPP can usefully come into play to solve the bootstrapping problem in an automated way, without using out-of-band measures. The 3GPP security infrastructure could be employed to bootstrap subscriber certificate requests.

The following elements are needed for the provision and use of a subscriber certificate:

1. The provision of bootstrapping information: a shared secret/password or a pre-installed certificate (device certificate). The bootstrapping problem could be solved by 3GPP defining a generic bootstrapping protocol based on AKA.

2. A certificate request protocol using this bootstrapping information to authenticate the subscriber

3. A mechanism to provide confidentiality and/or integrity to certificate request messages (this mechanism may or may not be integrated with the certificate request protocol)

4. A standardised format (a profile of an existing standard) for the subscriber certificate to ensure interoperability

5. An inter-operator PKI if it is required that an application provider needs to verify subscriber certificates issued in a different domain.

Proposal for future 3GPP work on subscriber certificates: It is proposed that 3GPP standardises item 1. 3GPP may consider standardising items 4 and 5, or it may decide to leave this to other bodies (e.g. GSMA). 3GPP should not standardise items 2 and 3.

Justification of the proposal: As already mentioned, WAP/OMA, W3C and the IETF are providing protocols covering item 2, so there is no need for 3GPP to compete with them and invent yet another such protocol. Neither is a need seen for 3GPP to standardise such a protocol, if certificates are issued by the home operator which seems to be the current preference of 3GPP groups. It may be advisable to see which certificate request protocol will enjoy widespread support in implementations, as 3GPP may not be the dominant market force in the area of PKI management. The specifications under consideration in WAP/OMA, W3C and the IETF (WAP 1.2, XKMS, CMP, PIC, possibly others) also indicate how these protocols could be secured (item 3 above). In all cases, the existence of a shared secret and (in most cases) the ability of the client to verify a server certificate, seems sufficient to provide that security. The security may be provided at application layer or at transport layer.

In some more detail, the mentioned specifications are secured in the following way (item 3 above):

- WAP 1.2 uses WTLS with server authentication;

- XKMS uses XML security, possibly in addition to TLS with server authentication;

- CMP [2] mandates support for a basic authentication scheme (see section 2.2.2.2 in [2]). This scheme uses an initial authentication key IAK that is established by out-of-band distribution to authenticate the initial certification request. As the PKI message protection mechanism, a “PKIProtection” structure defined by [2] may be used that allows to protect the CMP messages based on preshared secrets, or external protection mechanisms like PKCS#7 or Security Multiparts [RFC1847] encapsulation may be used.
  Regarding the bootstrapping, the key IAK may be provided as the result of a run of the generic bootstrapping protocol.

- PIC uses its in-built security, based on ISAKMP, server authentication is done using server certificates, client authentication is done using an EAP method.

3. A generic bootstrapping protocol

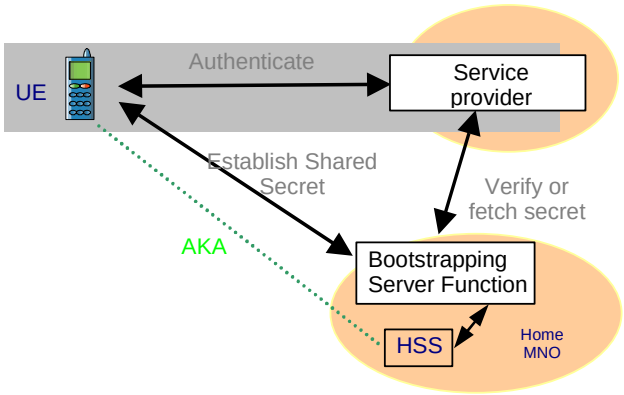
Possible uses of a generic bootstrapping protocol

Although this document discusses the bootstrapping issue specifically for subscriber certificates, we assume that a generic bootstrapping protocol provided by the MNO may be used in other contexts as well, e.g. for http security (Nokia’s contribution S3-020528), presence services security, or for MBMS when an application layer solution is chosen. The following general model for a generic bootstrapping function provided by the MNOs is envisaged:

If the UE wants to access an MNO-based service that requires authentication, it establishes a shared secret between itself and the bootstrapping server function of its home operator. Based on a run of the bootstrapping protocol, the established shared secret will be used subsequently for authentication with the MNO-based service the UE tries to access.

The MNO providing the service requires some interaction with the bootstrapping server function issuing the shared secret, in order to be able to successfully run the authentication process with the UE. This interaction may consist in

retrieving the shared secret in a secure way, or in the bootstrapping server function supporting the requesting service by verifying user credentials, e.g. using RADIUS or DIAMETER.



The bootstrapping function in the home MNO itself needs to interface with the HSS, to fetch AKA authentication vectors.

Note, that the definition of the service itself (like the application protocol and the specific authentication mechanism used) should be complementary to the generic bootstrapping protocol. This reduces the dependency between the certificate provision and the 3G system to the support for client authentication provided by the 3G system to the service provider. The grey shaded area in the above figure does not depend on 3GPP standards. Many different solutions could be adopted there. This is seen as an advantage of the proposed solution, as it does not limit the ways in which certificate provision may be achieved. Please also note that the service may be provided either in the home domain or in the visited domain, whereas the bootstrapping server function is assumed to be in the home domain. However, if the service provider is located in the visited domain then trust issues between the service provider and the home operator have to be addressed. This may involve the definition of an inter-operator PKI and a broker function (e.g. a broker AAA server provided by the visited operator). The interface between the service provider and the bootstrapping server has to be adequately secured.

Requirements on a generic bootstrapping function

1. It should provide a mutually authenticated client and a bootstrapping server function in the home network with a shared secret

2. It should leverage the current 3GPP security infrastructure, i.e. it should use the AuC, USIM and the AKA protocol.

3. It should be access network independent (i.e. should not depend on a particular link layer technology such as GPRS or WLAN).

4. It should allow the separation of different uses of the protocol (in order to avoid protocol interaction attacks). I.e. different shared secrets should be made available for different uses.

Candidate protocols:

To fulfill the second requirement, the candidate protocols discussed below are limited to those using the AKA protocol as the central mechanism for authentication and key agreement. The list includes obvious candidates, but it is not claimed that the list is exhaustive.

1. AKA according to 3G Rel'99
   The AKA protocol itself only operates over UMTS CS/PS access. It fulfills requirements 1 and 2 of the above requirements, but does not fulfill requirement 3 for access network independence.
   As this is not supported, we assume that this approach will not further be considered.

2. EAP/AKA
   An EAP/AKA based bootstrapping protocol, depending on its realization, could match the above requirements. However, it depends on an environment that supports EAP (transport) as currently WLAN or PPP (which would

clearly conflict with requirement 3). EAP is not generally available over IP transport; only specific solutions as PIC using a newly defined ISAKMP-EAP payload are available.
It is not considered an option for 3GPP to specify its own EAP transport solution, as this would need standardization within the IETF, which would be unlikely to meet the 3GPP schedule for subscriber certificates.

3. IMS-AKA, digest aka over SIP: works only in IMS, SIP
   IMS-AKA is limited to IMS users and network entities. Although it may be used over any access network technology it may be argued that the provision of subscriber certificates should not be limited to IMS subscribers.

4. http digest aka
   This candidate is very similar to digest aka over SIP, but is carried within http messages instead. It may be run between the UE and an independent http server in the operator's network. The similarity to components of the IMS could be exploited for implementation: the S-CSCF already provides a standardized interface towards the HSS (a subset of Cx could be used for supporting the general bootstrapping), and the S-CSCF already implements functionality required for digest aka.

Evaluation:

Candidate 4 based on http digest aka seems to be the most promising one. It is very close to existing IMS functionality and seems to allow reuse of already existing components, if an IMS system is part of the operator's network. http is assumed to be available on the terminal.

Therefore it is suggested to study this candidate with priority. But certainly, further work is needed.

Conclusions

It is proposed that 3GPP standardises a bootstrapping protocol based on AKA to support the provision of subscriber certificates. This bootstrapping protocol should be as generic as possible, so that it can be used for other application scenarios as well. Further possible applications for this protocol should be investigated to identify requirements on such a bootstrapping protocol.

We suggest to study the http digest aka proposed in section 3 of this document, as a candidate for the generic bootstrapping protocol, with priority.

3GPP should decide whether to standardise a certificate profile and/or and inter-operator PKI of a standardized certificate format itself, or to leave this to other bodies (e.g. GSMA).

3GPP should not standardise a new certificate request protocol, or protection (integrity, confidentiality) mechanisms for such a protocol.

Furthermore, depending on the agreement reached by SA3, an updated work item description would be needed.

References

[1] http digest aka (rfc3310)
[2] IETF PKIX group (March 1999): RFC2510, "Certificate Management Protocols"