

ENROLL
Internet-Draft
Expires: April 17, 2005

H. Tschofenig
D. Kroesenberg
Siemens
October 17, 2004

Next Steps for ENROLL
draft-tschofenig-enroll-next-steps-00.txt

Status of this Memo

This document is an Internet-Draft and is subject to all provisions of [section 3 of RFC 3667](#). By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she become aware will be disclosed, in accordance with [RFC 3668](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/lid-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on April 17, 2005.

Copyright Notice

Copyright (C) The Internet Society (2004).

Abstract

This document describes framework specific aspects relevant for the Credential and Provisioning (ENROLL) working group. State-of-the-art work with possible relevance for ENROLL is given with a special focus on the 3GPP Generic Authentication Architecture (GAA), which has a relationship to the Trusted Transitive Introduction (TTI) model. The main goal of this document is to initiate some discussions about the focus of the working group and possible next steps.

Internet-Draft

Next Steps for ENROLL

October 2004

Table of Contents

1.	Introduction	3
2.	Terminology	5
3.	Classification	6
3.1	Secret stored in device during manufacturing	6
3.2	Secret established over a secure network	6
3.3	Secret established over an insecure network	7
4.	Conclusion	10
5.	Security Considerations	13
6.	Acknowledgments	14
7.	References	15
7.1	Normative References	15
7.2	Informative References	15
	Authors' Addresses	17
A.	3GPP Generic Bootstrapping Architecture	19
A.1	Overview	19
A.2	The Generic Bootstrapping Architecture (GBA)	20
A.3	Application Security for HTTP Based Applications	22
A.3.1	Use of HTTP Digest Authentication	23
A.3.2	Use of TLS	23
	Intellectual Property and Copyright Statements	25

Internet-Draft

Next Steps for ENROLL

October 2004

1. Introduction

This document describes framework specific aspects relevant for the Credential and Provisioning (ENROLL) working group. State-of-the-art work with possible relevance for ENROLL is given with a special focus on the 3GPP Generic Authentication Architecture (GAA), which has a relationship to the Trusted Transitive Introduction (TTI) model defined in [[I-D.pritikin-ttimodel](#)].

The goal of this document is to discuss relevant scenarios for the work of the ENROLL group, and to provide some views to the discussion from the perspective of 3GPP networks. This explicitly does not consider the imprinting process for mobile operators of GSM or 3GPP networks, where SIM or USIM cards need to be initiated with security credentials (secret keys) and have to be issued to the mobile users by the network operators. This process is well-established; however, the trust relations between security domains related to mobile wireless networking tend to grow in complexity, and dynamic establishment of trust relations, or dynamic addition (and removal) of mobile users to new security domains seems to be the interesting case to be considered by ENROLL.

A number of terms are used in [[I-D.pritikin-ttimodel](#)] to define a model for introduction. One of them is out-of-band, which can, however, have quite different meanings in different contexts. For example, adding a mobile user by out-of-band means to a security domain can be the process where a network operator sends a letter with the initial credentials (USIM card, PIN) the user requires to get access to the wireless network. In a different scenario, this could be the dynamic, secure issuing of asymmetric credentials for access to services in a security domain requiring the use of such credentials. The user can receive such credentials either by the security domain hosting the service itself, or by a third party that has some trust relation in advance with both the security domain and the mobile user.

Hence, as a generic starting point for models relevant to ENROLL, the subsequent classification is taken from Section 4 of [\[I-D.hanna-zeroconf-seccfg\]](#) on security configuration mechanisms.

A simple architecture is based on two entities, Alice and Bob. In a more complex scenario three entities are considered. The two party scenario is shown in Figure 1 and the three party scenario is shown in Figure 2.

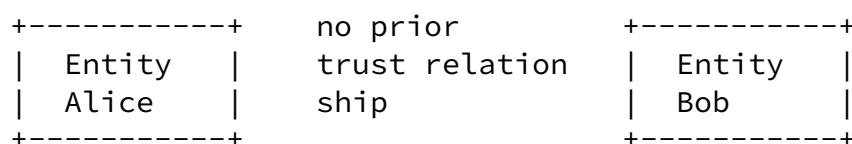


Figure 1: Two Party Scenario

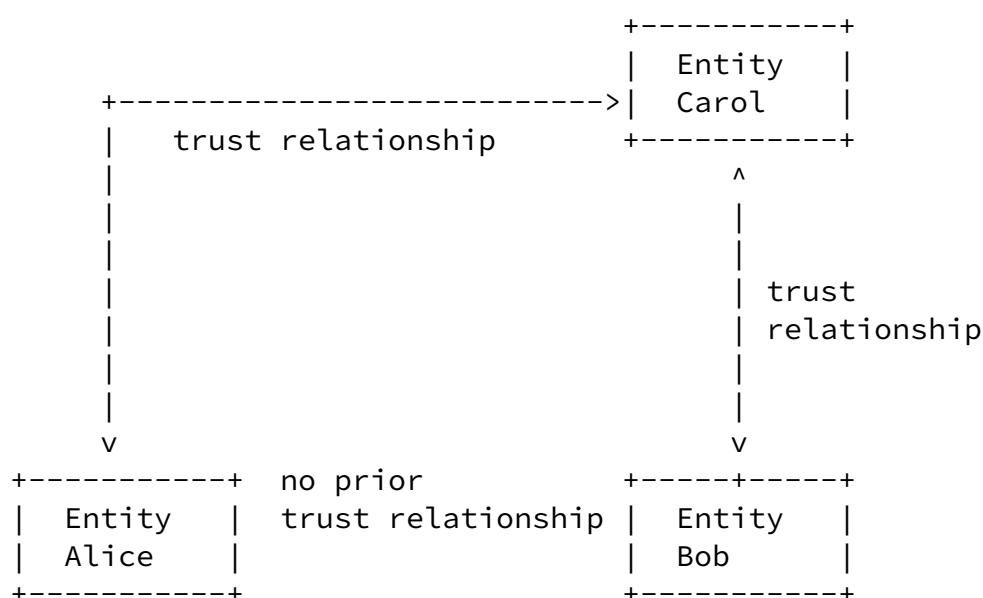


Figure 2: Three Party Scenario

In Figure 2 the existence of a third party, Carol, is used to

dynamically establish a security association between Alice and Bob to create a security association.

The relevance of these two models is shown in [Section 3](#).

[2](#). Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [\[RFC2119\]](#).

The cryptographic initialisation or what is also called imprinting, is a procedure of equipping the component with a secret value of a cryptographic parameter. The type of the parameter varies a lot depending on its subsequent use in security mechanisms. It may be an unstructured randomly generated string, from where future key material is derived. It may also be keying material related to an asymmetric cryptographic mechanism, in which case it has a well-defined structure.

In many mobile scenarios, the wireless link is the basic communication channel between the devices. It is inherently insecure, that is, passive eavesdropping, channel hi-jacking, as well as active impersonation and tampering of data is possible. The procedure of imprinting, where the initial secret cryptographic parameters are set in the component, is the most sensitive part of

the communication. If tampering or eavesdropping the imprinting step is possible, then the security of all future communication based on imprinting is ruined.

Considering the initial provision of credentials for allowing mobile users to access security domains, not only the term imprinting, but also enrollment, or bootstrapping frequently occur. The authors of this contribution are not aware of clear and commonly accepted definitions of these terms, but rather assume that these vary depending on the underlying use cases and scenarios where they are used.

Therefore, one goal of the ENROLL working group should be to leverage a common understanding of these terms.

[3.](#) Classification

This section defines a few classes of credential provisioning (or imprinting) scenarios.

[3.1](#) Secret stored in device during manufacturing

This scenario focuses on a cryptographic secret which is stored in the device during manufacturing. This secret generally cannot be changed and is made available to the user, e.g., by printing on a separate letter (off-line, out-of-band provisioning). Any entity possessing the password can change the configuration of the device. The security of the whole process depends on the shipment of the the letter with the relevant information.

This scenario in the view of the authors does not raise any specific issues relevant for the work in the ENROLL working group.

3.2 Secret established over a secure network

In this scenario it is assumed that Alice and Bob can communicate over a temporary secure channel or out-of-band channel. In this context, the secure channel can be based on one of the following technologies:

- o Fixed connection such as cable, USB interface, bar-code reader, smart-card reader
- o Human involvement, communication of passkeys, entering passkeys
- o Second wireless (e.g., infrared)
- o Other proximity based technology (low power channel)
- o Memory sticks (e.g., USB tokens)

An example for this approach is given with Windows Smart Network Key [WSNK] where the process of imprinting can be triggered at a new device (e.g., entity A in our example). As a result, Alice creates a key and the corresponding parameters and writes this information into an XML file and copies it to a USB stick. This USB stick is then used to carry the parameters to Bob to complete the imprinting procedure.

The content of the XML file heavily depends on the application domain. In the context of wireless LAN equipment security parameters used within IEEE 802.11i/802.11/802.1X are such as:

- o SSID
- o Encryption (WEP, TKIP, AES)
- o EAP Method (EAP-TLS, PEAP-EAP-MSCHAPv2, PEAP-EAP-TLS)

- o Authentication Type (open, shared, WPA, WPAPSK, WPA-NONE, WPA2, WPA2PSK)
- o IEEE 802.1X enabled?

and many non-security related parameters.

An approach to make this process generic for many application domains

is ambitious. As an example, the above parameter list includes a few EAP methods. Apart from the fact that the list is, by no means, complete it would also be necessary to specify a few parameters with relevance for each individual EAP method. Switching to a new application domain often requires to consider different types of identities.

3.3 Secret established over an insecure network

With this class there is no separate secure channel. Still a number of possibilities exist to establish a shared secret between Alice and Bob. Often, an approach similar to SSH is mentioned where the user has to compare a fingerprint of some exchanged parameters (e.g., the public key). This approach is described in [[SHAMAN](#)], in Section 4.3 of [[I-D.hanna-zeroconf-seccfg](#)] or with the Shared Secret Provisioning Protocol (SSPP) [[I-D.moskowitz-shared-secret-provprotocol](#)]. Thereby a Diffie-Hellman alike protocol is executed between the two entities, Alice and Bob. A cryptographic hash value computed over some payloads is displayed at both devices and compared. This fingerprinting approach is used to avoid man-in-the-middle attacks. The size of the solution space for such a protocol is affected by the type of environments where such a protocol is used and constraints such as computational requirements, requirements affected by the type of devices used, desired level of security, etc. Since SSPP is an abstract protocol mappings are provided, for example, to SNMP (see [[I-D.moskowitz-sspp-snmp](#)]). [[I-D.moskowitz-radius-client-kickstart](#)] describes how session keys can be established between RADIUS clients and RADIUS servers for Wireless LAN deployments.

Some architectures use a trusted third party to establish a security association between Alice and Bob. These protocols use the existence of a security association (and a trust relationship) between Alice and Bob and a trusted entity, Carol. Figure 2 depicts the architecture. A classic example of this architecture for network access authentication with the help of EAP and EAP methods is described in [[I-D.ietf-eap-keying](#)]. The same document describes the interaction between the different protocols and the keying framework.

In [[I-D.tschofenig-pana-bootstrap-kerberos](#)] a mechanism is described how to bootstrap Kerberos Ticket Granting Tickets based on an EAP network access authentication protocol run. Subsequently, Kerberos

service tickets can be requested for access to services.

In Figure 5 the 3GPP Generic Authentication Architecture (GAA) approach for establishing a security association between mobile users and services in a security domain the users are not initially part of, is described. [Appendix A](#) gives an overview of this architecture. There are a number of interesting differences between the EAP/AAA based approach and the 3GPP GAA framework that allows to leverage the established huge security infrastructure for mobile phone users

With a three party architecture two types of message exchanges are possible. We depict these two types in Figure 3 and in Figure 4.

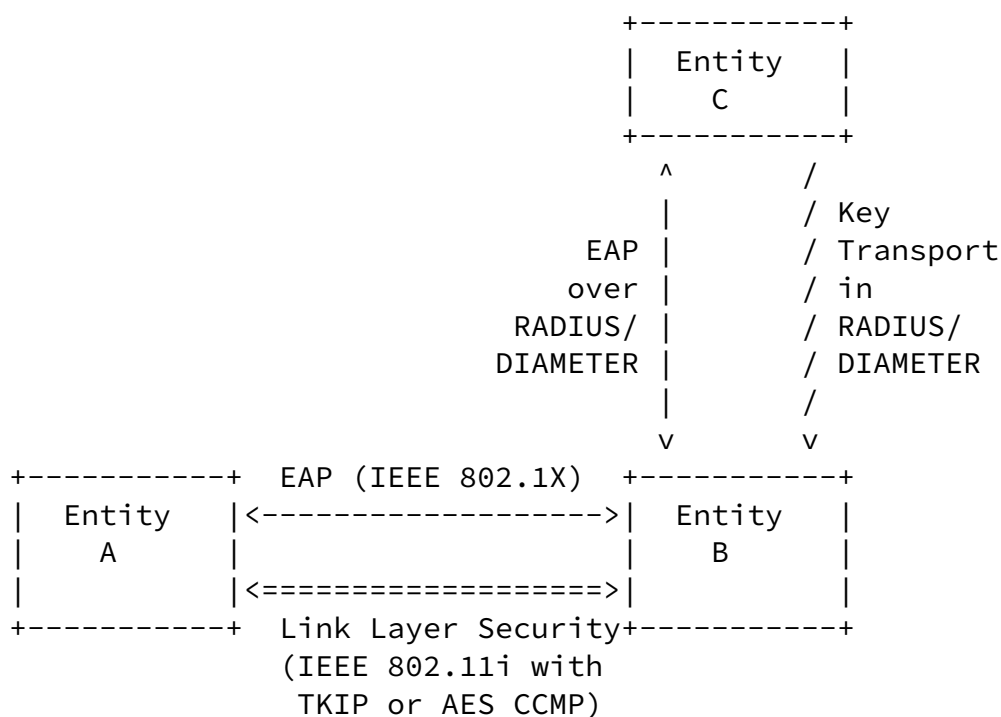


Figure 3: EAP based Architecture

With the message exchange in Figure 3 Alice starts interacting with Bob. Since there no relationship between Alice and Bob, it is necessary to forward the EAP exchange to Carol whereby Alice has a trust relationship with Carol. After a successful authentication and authorization session keys must be delivered to Bob for subsequent establishment of security associations. A number of protocols today use this architecture, such as IEEE 802.1X [[IEEE-802-1X-REV](#)] (and IEEE 802.11i), IKEv2 [[I-D.ietf-ipsec-ikev2](#)] or PANA [[I-D.ietf-pana-pana](#)]. These protocols just label the involved entities differently.

Internet-Draft

Next Steps for ENROLL

October 2004

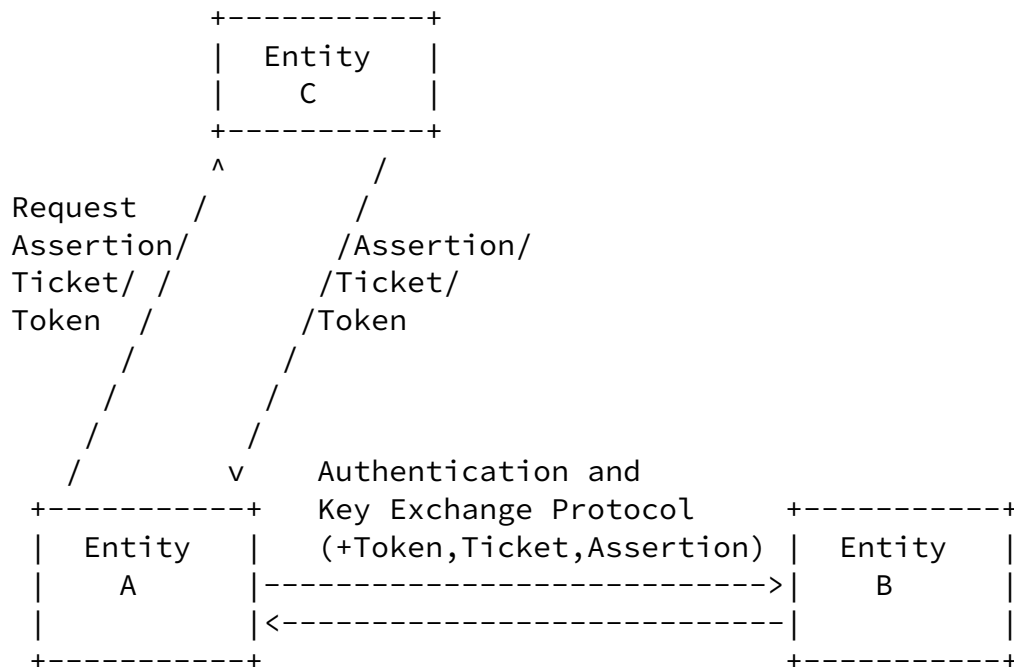


Figure 4: Token, Ticket, Assertion-based Architecture

With the architecture shown in Figure 4 Alice has to start communication with an Carol first, whereby a direct or indirect trust relationship between these two entities is assumed. First, some form of Token, Ticket or Assertion is requested. Different protocols label this item differently. This exchange typically requires mutual authentication and authorization to be finished before Alice receives the desired item. When a service access is required then Alice interacts with Bob and presents this Token, Ticket or Assertion. Kerberos (with the usage of Tickets) [[RFC1510](#)] and SAML (see for example, [[I-D.saml-tech-overview-1.1-03](#)], [[I-D.saml-core-1.1](#)], [[I-D.saml-bindings-1.1](#)]) with the usage of Assertions (or Artifacts which are references to Assertions) are protocol examples.

Internet-Draft

Next Steps for ENROLL

October 2004

[4.](#) Conclusion

The above sections give a number of sample classifications for scenarios relevant to the ENROLL group, and reference numerous examples. The main focus is on mobile scenarios, and on the "secret established over insecure network" processes that are considered the most interesting for current demands of introducing mobile users with appropriate credentials to access security domains offering services to the mobile users. Typically, a pre-established trust relation or security relation between such users and services cannot be assumed.

As an example that is considered relevant for the ENROLL working group, the 3GPP GAA is discussed in more detail in [Appendix A](#).

Although no thorough analysis of the GAA framework is provided in this initial draft version, a number of observations related to the different terminologies are given below.

The TTI model draft [[I-D.pritikin-ttimodel](#)] defines the term introduction as follows: 'When adding a device into a security domain the first task is to exchange cryptographic and configuration information between the security domain and the device. This process we term an Introduction.'

One question that arises is what exactly a "security domain" is? This, of course, heavily depends on the given usage scenario. For example, introduction to a security domain fundamentally differs (as well as the security domain does) for the use cases given in the above section (e.g., storing secret information in a device during manufacturing versus secret stored over insecure wireless link).

ENROLL needs to clearly state which types of security domains are covered, and which are not. This draft contributes to this clarification by providing additional use cases.

In 3GPP networks, a mobile device is 'added' to the home operator's

security domain as soon as the user gets the USIM card. In contrast, through the 3GPP GAA framework (see Annex A for a detailed overview) the mobile user is introduced to a service provider's security domain as soon as a new security context is initiated based on the existing security infrastructure of 3GPP networks.

The complexity described in [[I-D.pritikin-ttimodel](#)] for PKI enrollment is for instance solved by the GAA by the ability to dynamically issue public-key certificates to mobile users on demand, which offers the advantage that only those users receive certificate-based credentials who really request them. Issuing certificates to the complete, huge, user base of mobile phone

networks would unnecessarily increase initial costs and administrative effort. The 3GPP network operator, or some instance with an already established trust relationship with such an operator, can provide the role of an initiator in this case.

As it is not fully clear to the authors of this draft whether the definition of Introduction made by [[I-D.pritikin-ttimodel](#)] matches with the goals achieved by the 3GPP GAA, the related terms of a petitioner, an introducer and a Registrar are not used for the GAA example in Annex A. Instead, we use the roles of a mobile user, a home network (of the mobile user) and some service provider or application server as logical entities.

However, we expect that a good match for the different terminology would be to associate the mobile user with the petitioner, the home network with the introducer, and the application server with the registrar.

The 3GPP GAA may be considered as some form of authentication and authorization (AA) infrastructure the mobile user or petitioner is expected to enroll with. Although being a more complex example, this basically matches the 'pay for use' example in Section 4.5 of [[I-D.pritikin-ttimodel](#)] which describes the initiation of a trust relation between a mobile user and a public WLAN hotspot (provider of the service 'Internet access') through a credit card company as the initiator. [[TS22.934](#)] describes a similar scenario where a 3GPP network operator supports this initiation.

One result of matching the 3GPP GAA to the TTI model is that both the

introducer and the registrar may issue the credentials that are subsequently used by the petitioner for service access. This depends on the exact grouping of the processes:

- o If we just consider the process of issuing a certificate to the mobile user, where the user first contacts the BSF to authenticate and establish a new shared secret based trust relation with the NAF responsible for certificate issuing, this NAF may be considered as the Registrar issuing new credentials for subsequent service access.
- o If we consider service access and group the process of issuing credentials (i.e., the user's communication with the BSF and - based on this exchange - subsequently with the NAF, the network offering the GAA service may be considered as the initiator issuing credentials, and these are subsequently used with the registrar, i.e., some other NAF offering e.g. an HTTP-based service to the mobile user.

Although there is no clear terminology differentiating between these two examples given above, the authors of this draft tend to regard

the first example as introduction, or enrollment, and the second example as a bootstrapping process.

[5.](#) Security Considerations

The document discusses state-of-the-art security architectures and protocols. As such, it addresses a huge number of security issues. No additional specific security vulnerabilities, threat models or solutions are given in this section.

[6.](#) Acknowledgments

We would like to thank Wolfgang Buecker for his input to this document.

7.1 Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", March 1997.

7.2 Informative References

- [I-D.hanna-zeroconf-seccfg]
Hanna, S., "Configuring Security Parameters in Small Devices", [draft-hanna-zeroconf-seccfg-00](#) (work in progress), January 2002.
- [I-D.ietf-eap-keying]
Aboba, B., "Extensible Authentication Protocol (EAP) Key Management Framework", [draft-ietf-eap-keying-03](#) (work in progress), July 2004.
- [I-D.ietf-ipsec-ikev2]
Kaufman, C., "Internet Key Exchange (IKEv2) Protocol", [draft-ietf-ipsec-ikev2-16](#) (work in progress), September 2004.
- [I-D.ietf-pana-pana]
Forsberg, D., Ohba, Y., Patil, B., Tschofenig, H. and A. Yegin, "Protocol for Carrying Authentication for Network Access (PANA)", [draft-ietf-pana-pana-05](#) (work in progress), July 2004.
- [I-D.ietf-tls-psk]
Eronen, P. and H. Tschofenig, "Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)", [draft-ietf-tls-psk-01](#) (work in progress), August 2004.
- [I-D.moskowitz-radius-client-kickstart]
Moskowitz, R., "RADIUS Client Kickstart", [draft-moskowitz-radius-client-kickstart-01](#) (work in progress), October 2003.
- [I-D.moskowitz-shared-secret-provprotocol]
Moskowitz, R., "Shared Secret Provisioning Protocol", [draft-moskowitz-shared-secret-provprotocol-02](#) (work in progress), November 2003.
- [I-D.moskowitz-sspp-snmp]
Moskowitz, R., "SSPP over SNMP", [draft-moskowitz-sspp-snmp-01](#) (work in progress), October

2003.

- [I-D.pritikin-ttimodel]
Pritikin, M., "Trusted Transitive Introduction Model",
[draft-pritikin-ttimodel-01](#) (work in progress), July 2004.
- [I-D.saml-bindings-1.1]
Maler, E., Philpott, R. and P. Mishra, "Bindings and
Profiles for the OASIS Security Assertion Markup Language
(SAML) V1.1", September 2003.
- [I-D.saml-core-1.1]
Maler, E., Philpott, R. and P. Mishra, "Assertions and
Protocol for the OASIS Security Assertion Markup Language
(SAML) V1.1", September 2003.
- [I-D.saml-tech-overview-1.1-03]
Maler, E. and J. Hughes, "Technical Overview of the OASIS
Security Assertion Markup Language (SAML) V1.1", March
2004.
- [I-D.tschofenig-pana-bootstrap-kerberos]
Tschofenig, H., "Bootstrapping Kerberos",
[draft-tschofenig-pana-bootstrap-kerberos-00](#) (work in
progress), July 2004.
- [IEEE-802-1X-REV]
Institute of Electrical and Electronics Engineers, "DRAFT
Standard for Local and Metropolitan Area Networks:
Port-Based Network Access Control (Revision)", IEEE
802-1X-REV/D9, January 2004.
- [RFC1510] Kohl, J. and B. Neuman, "The Kerberos Network
Authentication Service (V5)", [RFC 1510](#), September 1993.
- [RFC3310] Niemi, A., Arkko, J. and V. Torvinen, "Hypertext Transfer
Protocol (HTTP) Digest Authentication Using Authentication
and Key Agreement (AKA)", [RFC 3310](#), September 2002.
- [SHAMAN] "Detailed technical specification of distributed mobile
terminal system security, Deliverable 10, Work Package 2,
IST-2000-25350 - SHAMAN", May 2002.
- [TR33.919]
3rd Generation Partnership Project, "3rd Generation
Partnership Project; Technical Specification Group

Internet-Draft

Next Steps for ENROLL

October 2004

Technical Specification 3GPP TR 33.919 V2.1.0 (2004-07),
July 2004.

[TS22.934]

3rd Generation Partnership Project, "3rd Generation
Partnership Project; Technical Specification Group
Services and System Aspects; Feasibility study on 3GPP
system to Wireless Local Area Network (WLAN) interworking
(Release 6)", Technical Specification 3GPP TS 22.934
V6.2.0 (2003-09), September 2003.

[TS33.220]

3rd Generation Partnership Project, "3rd Generation
Partnership Project; Technical Specification Group
Services and System Aspects; Generic Authentication
Architecture (GAA); Generic bootstrapping architecture
(Release 6)", Technical Specification 3GPP TS 33.220
V6.2.0 (2004-09), September 2004.

[TS33.221]

3rd Generation Partnership Project, "3rd Generation
Partnership Project; Technical Specification Group
Services and System Aspects; Generic Authentication
Architecture (GAA); Support for subscriber certificates
(Release 6)", Technical Specification 3GPP TS 33.221
V6.1.0 (2004-09), September 2004.

[WSNK]

"Windows Connect Now, Version 3, available at:
'<http://www.microsoft.com/whdc/device/netAttach/WSNK.msp>'
(Oct. 2004)", October 2004.

Authors' Addresses

Hannes Tschofenig
Siemens
Otto-Hahn-Ring 6
Munich, Bayern 81739
Germany

EMail: Hannes.Tschofenig@siemens.com

Tschofenig & Kroeselberg Expires April 17, 2005

[Page 17]

Internet-Draft

Next Steps for ENROLL

October 2004

Dirk Kroeselberg
Siemens
Otto-Hahn-Ring 6
Munich, Bayern 81739
Germany

EMail: Dirk.Kroeselberg@siemens.com

[Appendix A](#). 3GPP Generic Bootstrapping Architecture

[A.1](#) Overview

This chapter presents the concepts behind the Generic Authentication Architecture (GAA) specified in 3GPP [[TR33.919](#)] and the Generic Bootstrapping Architecture (GBA) specified in 3GPP [[TS33.220](#)]. This architecture is considered a relevant input scenario for ENROLL, since it supports introduction of mobile users (in the form of establishing shared secrets or public/private key pairs and certificates) for client access to security domains offering arbitrary (typically, but not limited to, HTTP-based) services. This process is based on the available security infrastructure in 3G mobile networks (i.e., on smartcard (USIM) based credentials).

The motivation for such an architecture arises from the fact that there are many services related to 3G mobile systems which all share a requirement for mutual authentication between a client (the mobile device) and an application server. While these authentication mechanisms might differ from application to application, they all require an a priori security relationship to be initiated either dynamically or statically. For all known authentication mechanisms this consists of either shared secret keys or the use of public key cryptography. For example, HTTP digest requires passwords (or shared secret keys) that have to be installed in the mobile user's device

before sending the first protected message. TLS assumes that the server and optionally the client are in possession of a TLS certificate before initiating a TLS-secured session.

The key issue with setting up initial security "credentials" between the mobile user's device and an application server is the possible complexity of the mobile (3GPP) scenario, where services can be provide by either the home or the visited network, or by 3rd party application providers with a relation to the home or visited network. In general, no initial relation between these parties exists.

This lead to the definition of a generic architecture for dynamically setting up security relations (in terms of shared secrets, or public-key certificates) between a mobile device and an application server, based on the existing security infrastructure of 3GPP networks. In such environments, all users are equipped with security credentials on a smartcard device (USIM), and the corresponding keys are stored in an entity called HSS (home subscriber server) in the home network that provides the USIM cards to mobile users.

The GAA provides means that allow a mobile user and an application server to establish either shared secrets or to establish a security relation based on user certificates. This generic "enrollment"

process is implemented in a unified, application independent architecture that relieves single applications from defining their specific ways of how to achieve a priori security relationships between clients and servers. Authentication is based on the well established AKA algorithm (e.g., used in EAP-AKA) so that the mobile network operator reuses the USIM cards that are expected to be largely spread among mobile phone users.

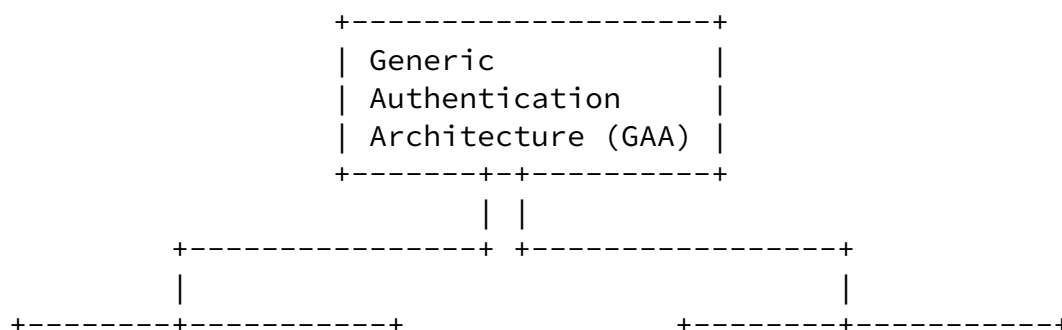




Figure 5: Components of the Generic Authentication Architecture

Thus, as shown in Figure 5, the GAA consists of two main components, one that aims at installing shared secrets in a mobile device and in an application server, and another who issues certificates to mobile devices. The two components are called the Generic Bootstrapping Architecture (GBA) [TS33.220], and Support for Subscriber Certificates (SSC) [TS33.221], respectively. In the following subsections we will discuss the architectural details of these components. As we will see, the support for subscriber certificates is just an example of an application that makes use of the GBA. Finally, we will illustrate the usage of the GBA for HTTP based services that perform client side authentication based on HTTP digest as a simple example.

A.2 The Generic Bootstrapping Architecture (GBA)

The elements of the Generic Bootstrapping Architecture are displayed in Figure 6. Apart from the mobile device and the HSS there are two additional elements:

The Bootstrapping Server Function (BSF): This represents an element that performs mutual authentication with the mobile user by means of the HTTP digest AKA protocol (see [RFC3310]). The authentication vectors required to run the AKA protocol are

fetches from the HSS (and are derived in the mobile device, or USIM card, in parallel). One result of the aka procedure is a pair of keys, IK and CK, from which keys are derived for later use by the mobile device and NAF to secure any application related communication.

The Network Application Function (NAF): This stands for a generic application server that provides any kind of service (application) to the mobile device. No assumptions are made about the protocol used between mobile device and NAF, though one candidate that is assumed to be used frequently is HTTP. The NAF fetches from the

BSF the key that resulted from the aka protocol run between BSF and mobile device, and uses it in securing the application related communication with the mobile device.

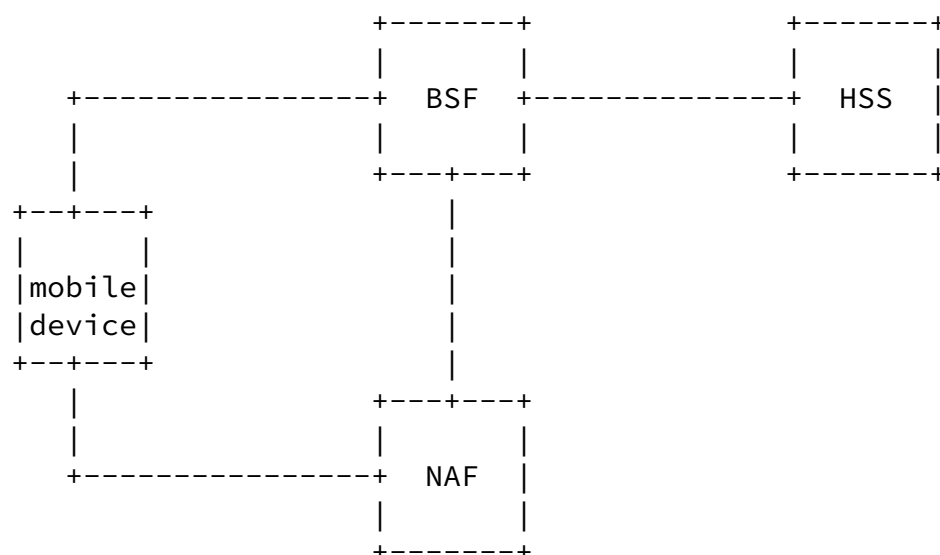


Figure 6: Elements of the Generic Bootstrapping Architecture

A high level view on the resulting information flow of the generic bootstrapping procedure is shown in Figure 7. In order to illustrate some of the concepts when the mobile device contacts several NAFs we have shown a communication flow where the mobile device addresses two different NAFs. The mobile device starts by sending a request to the first application server (NAF) indicating its intention to invoke some application (1). The concrete form of this request depends on the protocol used for this application. In general, the mobile device will not know whether GAA bootstrapping has to be performed in order to use the NAF. Therefore, the NAF indicates the use of bootstrapping in a response to the initial request and does not further process the request. After that the mobile device contacts the BSF and runs the HTTP digest aka protocol with the BSF based on the long term secret stored in the USIM located in the mobile device

(2). In the course of this procedure the BSF fetches one or more authentication vectors from the HSS which are required to perform the AKA protocol (3).

If the HTTP digest AKA protocol succeeds, the mobile device and BSF are in the possession of keys that are later used in securing messages exchanged between mobile device and NAF.

The mobile device now initiates a second attempt to send a request to the application server NAF. When the NAF receives the message, it requests the corresponding keys from the BSF (5). After having received the keys from the BSF, NAF is able to verify the request received by the mobile device and can henceforth use the keys to protect any further communication (6). Again, the details of the protection of these messages depend on the concrete protocol that is used by the application.

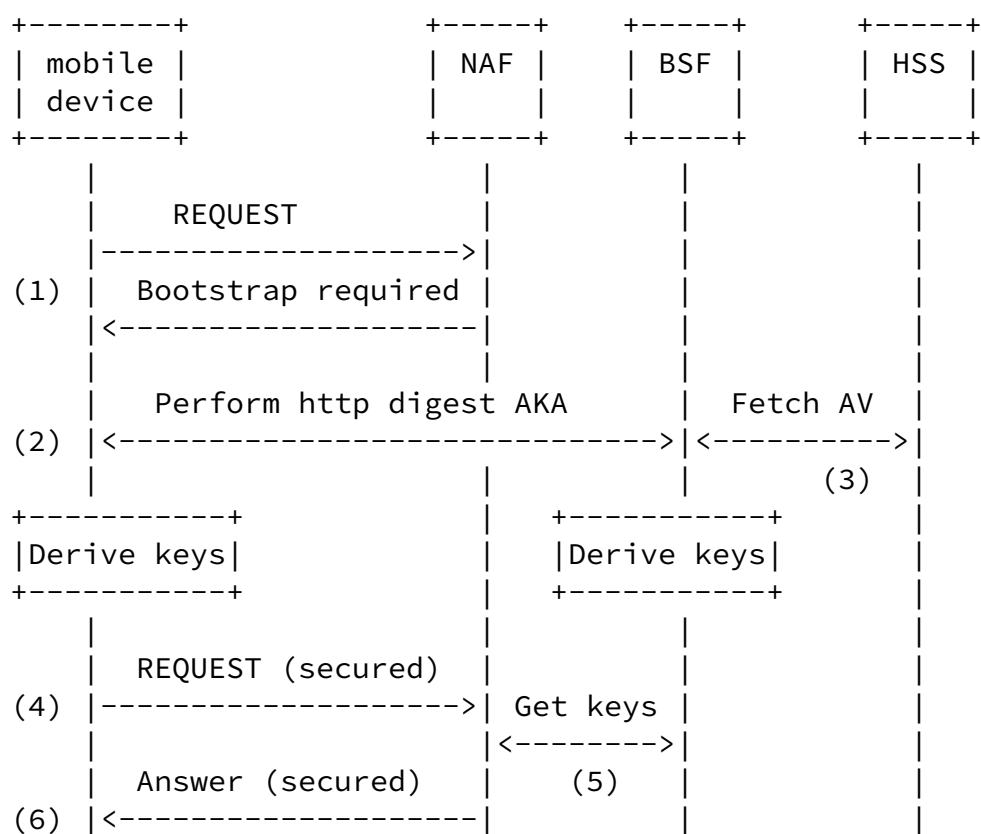


Figure 7: Elements of the Generic Bootstrapping Architecture

[A.3](#) Application Security for HTTP Based Applications

In the previous section we described how a security relation between a mobile device and an application server is established using the

Generic Bootstrapping Architecture. In this section we briefly illustrate the use of the Generic Bootstrapping mechanism in case the application protocol HTTP is run between the mobile device and the NAF.

In the simplest case the (mutual) authentication between mobile device and NAF can be performed using simple HTTP digest. In addition, TLS may be used which offers a higher level of security due to the encryption of the message exchange. TLS can either be used with server-only authentication, i.e., the server uses a TLS server certificate, and the client authenticates by other means like http digest through the TLS tunnel, or with the client authenticating with a TLS user certificate (mutual authentication).

[A.3.1](#) Use of HTTP Digest Authentication

If HTTP is used as protocol between a mobile device and an application server, HTTP Digest [[RFC2617](#)] is one natural candidate to perform simple client-only or mutual authentication between mobile device and application server. The role of the GBA in this scenario would be to provide the client and HTTP server (the NAF) with a http digest password (shared secret). Such information is not present for step (1) in Figure 7, since client and server do not have any initial security relation in place. After step (5) in Figure 7 has taken place, both the client in the mobile device and the NAF share a common secret to be used as http digest password.

[A.3.2](#) Use of TLS

When it comes to securing HTTP related communication, the use of TLS is another common option. Beyond authentication and integrity protection, it provides encryption of the communication packets. In a typical web scenario, the web server is authenticated using public key cryptography based on certificates. Following this, a secure tunnel, called the TLS record layer is established which carries all future communication between the client and the server. Frequently, the client is then authenticated by some separate protocol e.g. based on a password and some challenge-response mechanism like for instance HTTP Digest.

As already described in the above section the GBA can support this hybrid approach by initiating a security relation for http digest. The PKI-related aspects of the server-side PKI required for TLS operation are not considered here, and are independent of the functionality provided by the GBA.

Yet, TLS also offers the possibility for a client to present a

certificate on which the client authentication can be based.

However, today client certificates are often not used in the context of TLS as only few users of mobile devices bother to acquire certificates. There also exist proposals in the IETF to run TLS based on pre-shared keys not using certificates at all [[I-D.ietf-tls-psk](#)], i.e. both authentications (client to server and server to client) are based on symmetric techniques.

The 3GPP GAA allows to provide mobile users with such certificates on request. For this, the following steps are executed:

- (1) The mobile user uses the GBA as depicted in Figure 7, where the NAF is not the application server to be accessed via TLS, but a server allowing the client to request the issuing of (enrollment for) a Subscriber Certificate. Mutual authentication between the NAF providing Subscriber Certificates and the mobile user is based on the keys established after the user contacted the BSF. As a result, the mobile user requests a Subscriber certificate from the NAF.
- (2) The mobile user subsequently uses the Subscriber Certificate to authenticate the TLS session with the application server to be finally contacted.

The detailed specification for provisioning of Subscriber Certificates can be found in [[TS33.221](#)].

Internet-Draft

Next Steps for ENROLL

October 2004

Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in [BCP 78](#) and [BCP 79](#).

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at <http://www.ietf.org/ipr>.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Disclaimer of Validity

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED

WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Copyright Statement

Copyright (C) The Internet Society (2004). This document is subject to the rights, licenses and restrictions contained in [BCP 78](#), and except as set forth therein, the authors retain all their rights.

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.