Radiator
GBA/BSF

Open System Consultants Pty. Ltd.

Radiator GBA/BSF Support Module 1.2

27.1.2016

1. Introduction to GBA/BSF

GBA (generic bootstrapping architecture) is a technology which enables SIM-based service authentication for subscribers. It provides seamless authentication for supplementary services in VoLTE (voice over LTE), such as call forwarding, knocking, video call forwarding and other RCS (rich communication suite) services. The subscribers usually want to configure these services themselves even though the operator can preconfigure some of them.

Some of these services can be provided without GBA but, in this case, the service implementation requires the user to be switched to 3G network from LTE. This increases complexity and decreases the user experience due to possible lagging and interruptions in data connections and calls. Using GBA technology, these services can be implemented in LTE network without complex handovers.

In addition to VoLTE Supplementary Services, GBA technology can be extended for other services which require secure authentication. With GBA, it is possible to use the SIM-based authentication in any operator WWW services, for example, customer portals and prepaid charging. Furthermore, the authentication process is automatic and does not require any user actions. GBA does not require any specific communication technique but it can be used over Wi-Fi, LTE and other connections. Thus GBA technology can be used in, for example, remote devices and IoT (Internet of Things) devices.

VoLTE Supplementary Services use XCAP (XML configuration access protocol) over HTTP protocol for signalling. The authentication is done by bootstrapping a shared secret between a BSF (bootstrapping server functionality) and a UE (user equipment) which must have user credentials in a SIM card. GBA uses HTTP AKA (Authenticating Key Agreement) protocol for authenticating the entities. The authentication data is fetched from the HSS (Home Subscriber Server). When the HSS is used for identifying the user, there is no need for a separate user information database. The SIM-based authentication is a secure and easy way to reliably identify the subscriber as it does not require separate user names and passwords.

Figure 1 shows the basic architecture of a GBA-based authentication system. It consists of five network elements:

- Authentication Proxy (AP)
- Application Specific server (AS), for example, TAS (Telephone Application Services)
- BSF
- HSS
- UE

Sometimes the AP is not a separate entity itself but a part of the AS. In this case, the AS must support the needed 3GPP reference points and handle the operations of the AP. The AP communicates securely with the BSF. The BSF is a GBA-specific server, it facilitates the actual bootstrapping process between the UE and AP. The HSS contains subscriber data and manages the subscriber identity, access and security. It also has the same long-term master key Ki that is stored in the UE's SIM card.

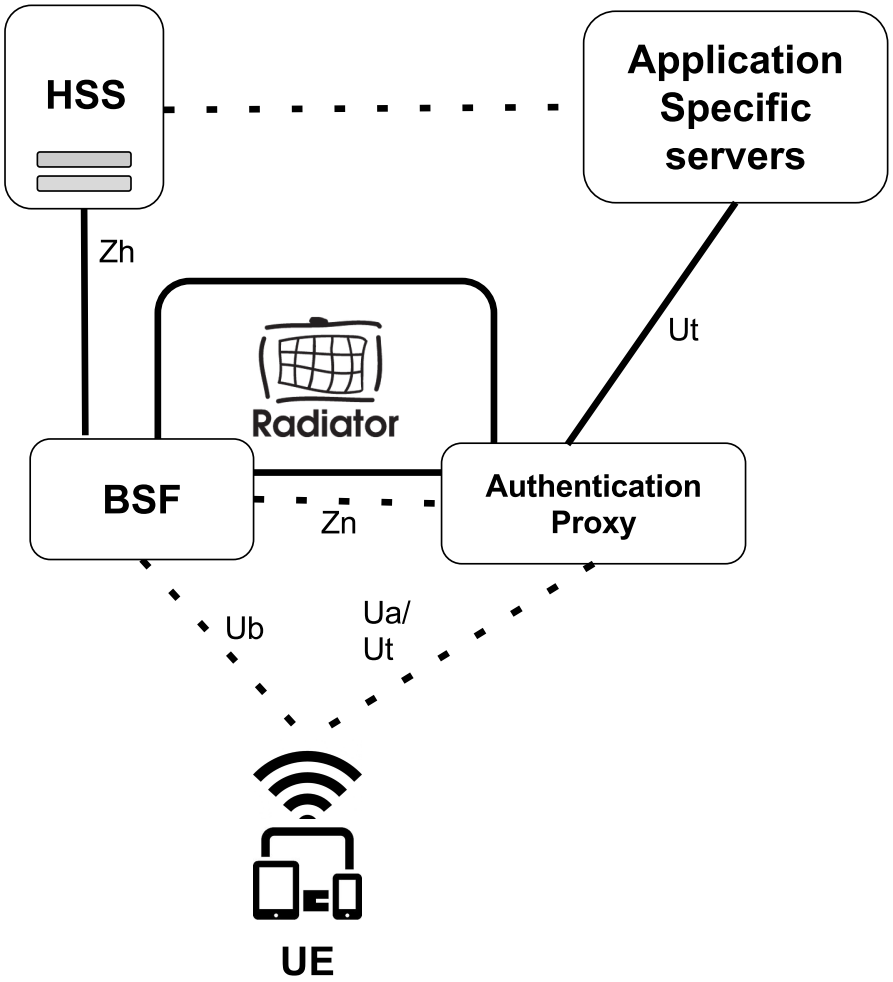

Figure 1. GBA architecture

2. Authentication procedure with GBA

In the GBA authentication process, the long-term master key Ki stored in the SIM card and HSS is used for generating a time-limited GMA master key Ks. Ks is shared between the BSF and UE. The BSF generates an AS-specific session key using Ks. This session key allows the mutual authentication.

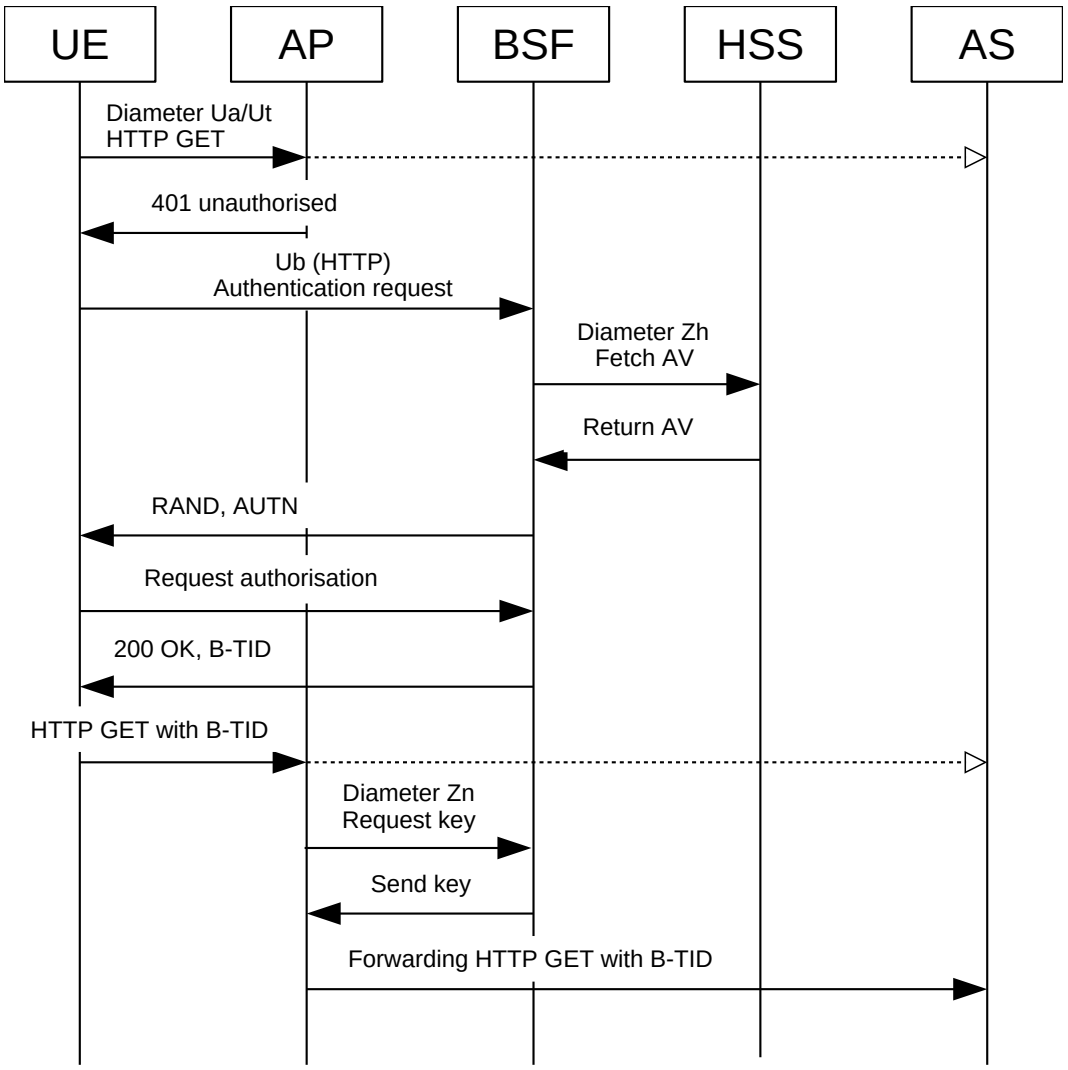

Figure 2. User authentication procedure with GBA

Figure 2 describes the bootstrapping procedure with GBA:

1. If the UE is not aware that the AS requires authentication, the UE tries to connect to the AS via the AP and sends an HTTP GET message using the Diameter Ua/Ut reference point.

2. The AP checks if the HTTP GET message contains HTTP digest authentication parameters. If they are missing or incorrect, the bootstrapping procedure starts and the AP sends an HTTP 401 (unauthorised) message back to the UE. Otherwise, the AP forwards the HTTP GET message to the AS (step 10).

3. The UE connects to the BSF using the Diameter Ub reference point and requests a user identity. The BSF address is derived from IMPI (IP multimedia private identity) or IMSI (international multimedia subscriber identity).

4. The BSF fetches the UE's AV (authentication vector) and GUSS (GBA user security settings) from the HSS via Diameter Zh. The GUSS contains several parameters, such as the key lifetime and alternative user ID's, for example, telephone number or email address. The AV contains the following parts:

   - RAND (random number)

   - AUTN (authentication token)

- XRES (expected response)
- CK (cipher key)
- IK (integrity key)

5. The BSF sends the RAND and AUTN to the UE.
6. The UE runs the HTTP AKA authentication algorithm.
7. The UE requests the authorisation digest from the BSF.
8. The BSF sends a 200 OK response message with B-TID (bootstrapping transaction identifier) to the UE.
9. When the UE has verified the response from the BSF, it sends another HTTP GET message to the AP. The message contains the B-TID.
10. The AP requests the authentication data from the BSF via Diameter Zn and compares it to the data the UE sent to the AP. If they match, the authentication is successful and the UE can request the services directly from the AS.

3. Radiator GBA/BSF Support Module

Radiator GBA/BSF Support Module implements the BSF functionality and AP. The authentication proxy feature is optional, the module can be used with operator's existing proxy. With Radiator GBA/BSF Support Module, you can easily implement seamless authentication for VoLTE Supplementary Services. Radiator GBA/BSF Support Module includes the HTTP Ua and Ub, and Diameter Zh and Zn interfaces.

Radiator GBA/BSF Support Module has been developed and field-tested together with operators and it is already used in operator networks. It is available from Open System Consultants and resellers around the world. For more information, contact the Open System Consultants sales team <info@open.com.au>.