TITAN.IUM

ACCESS AND SESSION MANAGEMENT

Product Data Sheet

Ut-Proxy Subscriber Self Administration

Business Benefits

- Enhanced security for users when accessing Supplementary Services
- Protection of the core network from possible attacks and fraudulent accesses
- Improves network operations and subscriber satisfaction
- Authentication for new services using temporary credentials
- Flexible options for routing to support different deployment scenarios saving time and money

TITAN.IUM

Product Data Sheet

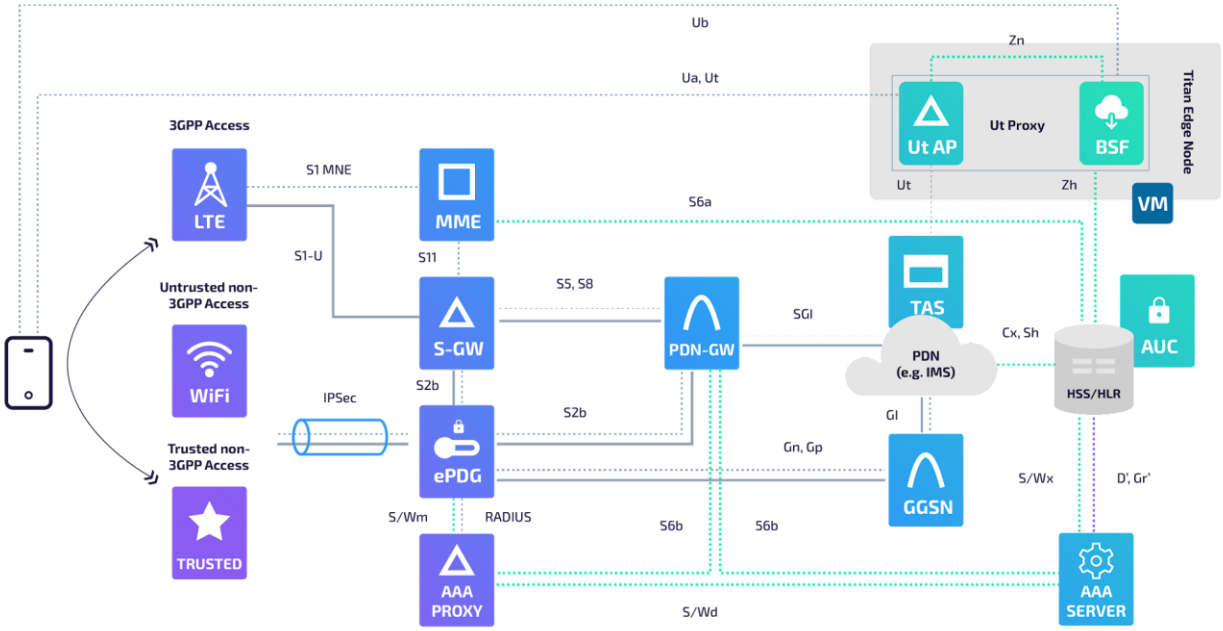
Ut-Proxy Subscriber Self Administration

The Challenge

As VoLTE and Rich Communication Services (RCS) services continue to evolve in the Communications Service Providers' (CSPs) network, the ability for subscribers to securely self configure the services they want to use (e.g., call forwarding, blocking, etc.) becomes very important to the overall user experience. Older proprietary solutions that are limited and costly to maintain are now being replaced by IETF-defined standards based on the HTTP XCAP protocol (XML Configuration Markup Language Configuration Access Protocol RFC4825) across the 3GPP standard Ut interface. The new XCAP based approach, combined with Generic Bootstrapping Architecture (GBA) authentication is being utilized by more mobile devices every month. Thus, supporting older, proprietary approaches that utilize specific firmware has become too costly to continue to be deployed.

The Titan.ium Solution

The Titan.ium Ut-Proxy is a next-generation Subscriber Self Administration (SSA) solution that is part of the Titan and Titan.ium architectures. These enable the most flexible and intelligent Ut-Proxy solution, making it possible to combine with other products like HSS, HLR, DSC, SLF, STP, SFW (depending on the chosen platform), providing common functions and a uniform look and feel GUI and API for its administration.



To authenticate Ut messages, Ut-Proxy is deployed to take this authentication task for the AS, and the Generic Bootstrapping Authentication (GBA) is applied to avoid provisioning an additional shared secret between UE and network. As a result, the Ut messages can be authenticated in any access network with the existing shared secret between the UE and operator. This is also applicable for authentication of any HTTP-based traffic, e.g., in IoT deployments, as long as the IoT devices can support GBA-based authentication. For devices not supporting GBA based authentication, Titan.ium Ut-Proxy can also use native HTTP Digest defined in RFC2617 to authenticate the devices.

TITAN.IUM

Product Data Sheet

Ut-Proxy Subscriber Self Administration

The Titan.ium Solution (continued)

Titan.ium Ut-Proxy consists of the two functional blocks of the GBA solution: the Bootstrapping Server Function (BSF) and the Authentication Proxy (AP) acting as a combination of a Network Application Function (NAF) and reverse HTTP proxy. One or both functions can be simultaneously activated in the same Titan Edge/Titan.ium cluster. BSF is deployed in the home PLMN and utilizes the Home Subscriber Server (HSS) as a subscriber profile repository (HSS only) and authentication center (AuC). The AP is optimized for the routing of Ut/XCAP requests from the UE towards the IMS application servers and can be deployed in the home or visited PLMN.

Business Benefits

The Ut-Proxy acts as a gateway between untrusted User Equipment (UEs) and the trusted core network that is hosting TAS, HSS, protecting the core network from being corrupted improving network operations and subscriber satisfaction.

In addition, the Ut-Proxy provides authentication for any new services, including 3rd party services, by deriving new temporary credentials from the GBA. Furthermore, the Ut-Proxy provides flexible routing options to support different deployment scenarios saving time and money.

Key Capabilities

Initiation of Bootstrapping
The Ut Authentication Proxy (AP) will request the UE to initiate bootstrapping with the Bootstrapping Server Function (BSF) if the UE indicates support of Generic Bootstrapping Architecture (GBA) in the HTTP request to the AP, and the request does not include any bootstrapping data or the included bootstrapping data is expired. GBA ME, GBA U, and GBA Digest modes can be used by the UE to get access to the IMS AS via AP.

Authentication
The authentication procedure applied to a bootstrapping request initiated by the UE and received by the BSF re-uses the Digest AKA and SIP Digest authentication procedures utilized by the IMS core. The Digest AKA procedure is applied to SIM- based UE, while the SIP Digest procedure is applied to SIM-less UE. Transport Layer Security (TLS) is mandatory during the authentication procedure for the SIM-less UE in order to generate the shared session key. For SIM-based UE, the session key is generated from the UMTS authentication vector.

Profile Download
During the bootstrapping procedure, the BSF downloads the GBA User Security Settings (GUSS) profile of the subscriber from the home HSS and deliver relevant information to AP so that they can be forwarded to AS. Titan.ium's Ut-Proxy also supports the use case where HSS doesn't provide GUSS profile.

TITAN.IUM

Product Data Sheet

Ut-Proxy Subscriber Self Administration

Key Capabilities (continued)

Bootstrapping Usage

The UE will use the bootstrapped security association when sending HTTP requests to the application server located in the IMS network. The Authentication Proxy intercepts the HTTP traffic and authorizes the received request. If needed, the AP communicates with the BSF to obtain the bootstrapped data, and also the AP-specific user security settings (USS) downloaded as part of the GUSS profile from the HSS.

Flexibility

The Authentication Proxy provides flexible routing criteria to select IMS Application Server (AS). AP can determine the target AS by mapping the request URI of the initial HTTP request to an ordered list of applications server identities. Alternatively, the HTTP Host header is used for the AS selection, or the source of incoming HTTP request. If the selected AS requests the AP to retarget the HTTP traffic, the AP uses the URI of the new AS from the non-recursive 305 redirect response.

Different configuration options are available to adjust the Ut- Proxy's behavior for different deployment scenarios. Diameter based Zn interface allows multiple Ut-Proxy instances in the same deployment, where AP and BSF on different Ut-Proxy instances can either be connected directly, or via a DRA indirectly. It is also configurable whether the lifetime value in GUSS profile or the locally configured value is used, or which user identity or flag in GUSS profile shall be forwarded to AS. And Ut-Proxy supports multi-realm deployment so that the same Ut-Proxy deployment can support a deployment with multiple PLMNs.

Contact Titan.ium Today

Please visit www.titaniumplatform.com for product or solution information. For configuration and pricing details, please contact your local account representative via sales@titaniumplatform.com

About Titan.ium

Titan.ium Platform is a leader in signaling, routing, subscriber data management, and security software and services.
Our solutions are deployed in more than 80 countries by over 180 companies, including eight of the world's top ten communications service providers and all of the top five. Titan.ium supports any network, domain, signaling protocol, and infrastructure with advanced routing capabilities and a unified end-user experience.

DISCOVER THE POSSIBILITIES.
INNOVATION AT YOUR FINGERTIPS