PGW may retain the IMS secret in cases where the UE only disconnects from the IMS network, but while it is still connected to the 4G network. This process should not lower the level of security.

Another aspect is the process of mobility. As long as the mobile device is located in the 4G access network, the PGW is the ultimate connectivity anchor point for the UE, its address does not change, unless the UE re-connects. Same thing is valid for the hybrid 3G-4G networks where the core network is 4G-EPC, because the PGW is the central entity there as well. If the access is non-3GPP, PGW continues to be the entity that handles the IP provisioning.

6. Conclusions and Future work

This paper presented the overall 4G and IMS architectures, using one of the scenarios most commonly encountered, where the UE is in the home-network. The UE authenticates to the 4G network, using MME as a proxy to the HSS. Then, when trying to access an application server, it may use the GAA architecture, either in GBA mode – using a shared secret located on the UICC and on the HSS, or using SSC – a PKI portal that assigns digital certificates to the UICC.

This paper also presented the classic IMS-SIP-AKA procedure, an HTTP-like method for authenticating the SIP endpoint to the IMS network (HSS), via the CSCF servers available here. It presents as well a proposed authentication model for the IMS system, which is designed to provide faster and secure access to the IMS system, while relying on the security features of the 4G system, without producing relevant changes to the IMS core.

7. References

[1] RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP) - http://www.ietf.org/rfc/rfc3455.txt (Access date: September, 2010)

[2] RFC 3329 Security Mechanism Agreement for the Session Initiation Protocol (SIP) - http://www.faqs.org/rfcs/rfc3329.html (Access date: September, 2010)

[3] TS 33.401 - 3GPP SAE - Security architecture - http://www.3gpp.org/ftp/Specs/archive/33_series/33.401/ (Access date: September, 2010)

[4] TS 33.402 - 3GPP SAE - Security aspects of non-3GPP accesses - http://www.3gpp.org/ftp/Specs/archive/33_series/33.402/ (Access date: September, 2010)

[5] TS 33.203 - Access security for IP-based services - http://www.3gpp.org/ftp/Specs/archive/33_series/33.203/ (Access date: September, 2010)

[6] TS 33.210 – Network Domain Security; IP network layer security - http://www.3gpp.org/ftp/Specs/archive/33_series/33.210/ (Access date: September, 2010)

[7] TS 33.310 – Network Domain Security; Authentication Framework - http://www.3gpp.org/ftp/Specs/archive/33_series/33.310/ (Access date: September, 2010)

[8] "IP Multimedia Subsystem (IMS) signaling core security" - Ivan Tirado Kennesaw State University, Kennesaw, GA, 2008 (Access date: September, 2010)

[9] "Security issues with the IP multimedia subsystem (IMS)" - Michael T. Hunter, Russell J. Clark, Frank S. Park - Georgia Institute of Technology, Atlanta, GA, 2007 (Access date: September, 2010)

[10] "Seamless mobility and standards" - David Binet France Telecom, Rennes – 2009 (Access date: September, 2010)

[11] Tech-Invite: http://tech-invite.com/ (Access date: August, 2010)

[12] TS 29.294 – Tunneling Protocol for Control plane (GTPv2-C) http://www.3gpp.org/ftp/Specs/archive/29_series/29.274/ (Access date: September, 2010)

[13] TS 33.220 – Generic Authentication Architecture; Generic Bootstrapping Authentication http://www.3gpp.org/ftp/Specs/archive/33_series/33.220/ (Access date: September, 2010)

[14] TS 33.246 – Security of Multimedia Broadcast/Multicast Service http://www.3gpp.org/ftp/Specs/archive/33_series/33.246/ (Access date: August, 2010)

[15] TR 33.919 – Generic Authentication Architecture – System Overview http://www.3gpp.org/ftp/Specs/archive/33_series/33.919/ (Access date: August, 2010)

[16] TS 33.221 – Support for Subscriber Certificates http://www.3gpp.org/ftp/Specs/archive/33_series/33.221/ (Access date: September, 2010)

[17] OpenIMSCore Project http://www.openimscore.org/ (Access date: September, 2010)

[18] "One-Pass Authentication and Key Agreement Procedure in IP Multimedia Subsystem for UMTS" - Chung-Ming Huang and Jian-Wei Li (Access date: February, 2011)

