3GPP TSG SA WG3 Security — S3#37 **S3-050018**

21 - 25 February 2005

Sophia Antipolis, France

Title: **Discussion about Using OCSP to Check Validity of PDG Certificate in 3GPP IP Access**

Source: **ZTE Corporation**

Document for: **Discussion and decision**

Agenda Item:

Work Item: **WLAN-IW**

1 Introduction

In SA3#36 meeting, contribution S3-041100 introduced that UE is mandatory to support OCSP to check validity of PDG certificate. How to use OCSP in 3GPP IP Access is discussed in this contribution. Some suggestions are consequently put up.

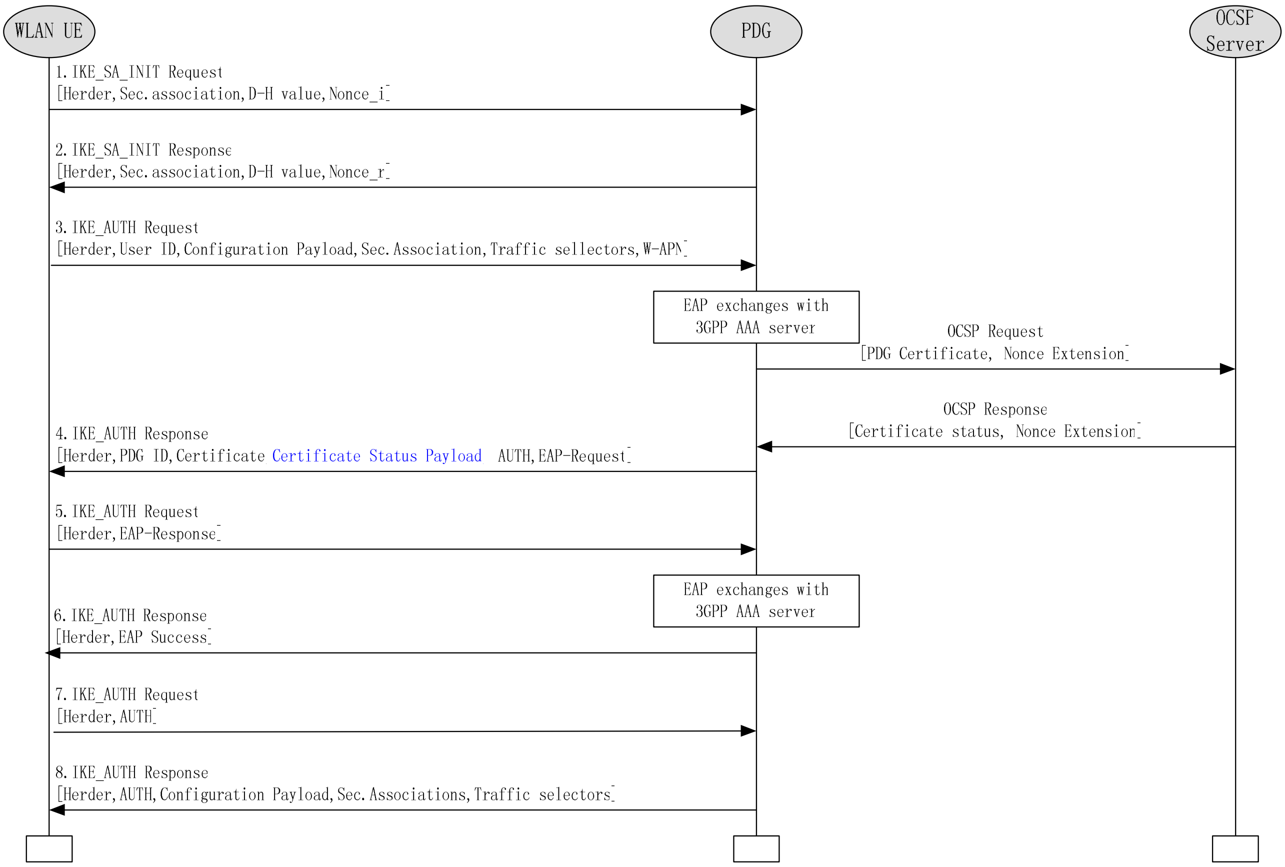
2 Discussion

A WLAN UE initiates 3GPP IP Access for the first time according to the tunnel full authentication and authorization procedure described by Figure7A in TS 33.234. WLAN UE may want to check the validity of PDG certificate but it can not gain access to Internet at present. It does happen when UE is not authorized to access to Internet through WLAN-AN directly. In this situation, valid check of PDG certificate using OCSP can be carried out in two ways as follow.

(1) After the UE initialled tunnel is successfully established and before user data is transmitted in the tunnel, UE may send an OCSP[2] request message to OCSP server. When UE receives OCSP response, it checks the certificate status. If the certificate of PDG is valid, UE will allow user data to be transmitted to PDG in the tunnel. If the certificate is not valid, UE should tear down the tunnel that is just established.

(2) During the tunnel establishing procedure, PDG may run OCSP message exchanges with OCSP server and push the certificate status signed by OCSP server to UE. UE checks the certificate status and the signature of OCSP server. If the certificate of PDG is valid, the establishment of tunnel will be continued. If the certificate is not valid, UE can terminate the 3GPP IP Access procedure through this PDG right now.

It is obvious that the second method is more efficient than the first one. Here the second method is discussed in more details. The following figure shows the message exchanges between WLAN UE and PDG. We omit the EAP/AKA details in order to focus on the IKEv2[3] and the OCSP exchanges. The 3rd IKEv2 message may contain Certificate Request payload if WLAN UE has no PDG's certificate. Before replying the 4th IKEv2 message, PDG can send its certificate in the OCSP Request message to OCSP server. OCSP server will reply response message with certificate status and generate a signature. PDG can envelop OCSP result (with the signature of OCSP server) in the 4th IKEv2 message and convey it to WLAN UE. When WLAN UE receives the 4th IKEv2 message, it will verify the signature of OCSP server and check the status of PDG's certificate. If the certificate status is good, then WLAN UE can trust the identity of PDG. If the certificate is revoked, WLAN UE can terminate tunnel establishment immediately.


WLAN UE
PDG
OCSF Server
1. IKE_SA_INIT Request
[Herder, Sec. association, D-H value, Nonce_i]
2. IKE_SA_INIT Response
[Herder, Sec. association, D-H value, Nonce_r]
3. IKE_AUTH Request
[Herder, User ID, Configuration Payload, Sec. Association, Traffic sellectors, W-APN]
EAP exchanges with 3GPP AAA server
OCSP Request
[PDG Certificate, Nonce Extension]
OCSP Response
[Certificate status, Nonce Extension]
4. IKE_AUTH Response
[Herder, PDG ID, Certificate Certificate Status Payload AUTH, EAP-Request]
5. IKE_AUTH Request
[Herder, EAP-Response]
EAP exchanges with 3GPP AAA server
6. IKE_AUTH Response
[Herder, EAP Success]
7. IKE_AUTH Request
[Herder, AUTH]
8. IKE_AUTH Response
[Herder, AUTH, Configuration Payload, Sec. Associations, Traffic selectors]

In order to prevent replay attacks, a random number specified by WLAN UE should be used as nonce extension in OCSP messages. So, the nonce_i sent by WLAN UE in the IKE_INIT_SA Request message can be used as the nonce in the OCSP request and response messages. The signature of OCSP server will cover the nonce extension. When Certificate Status Payload is enveloped in the 4th IKEv2 message, it should consist of three parts: PDG certificate status, nonce specified by UE and the signature generated by OCSP server.

An obstacle to deploy the above mechanism is that the definition of Certificate Status Payload is absent in IKEv2 draft. Whereas in TLS specifications, there is similar definition of Certificate Status Request Extension[4]. As the IKEv2 is often used as a mean of access control, in many cases terminals can only check the validity of access server's certificate after they are admitted to access network. If certificate status payload definition is introduced in IKEv2, certificate validity check can be accomplished during the access procedure. Thus the method is more efficient.

3 Conclusions

We propose that SA3 suggests IETF IPsec Working Group to consider enveloping certificate status in IKEv2 messages.

4 References

[1] 3GPP TS 33.234: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; WLAN Interworking Security".

[2] IETF RTC 2560: "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol (OCSP)".

.[3] draft-ietf-ipsec-ikev2-16.txt, September 2004: "Internet Key Exchange (IKEv2) Protocol".

.[4] IETF RTC 3546: "Transport Layer Security (TLS) Extensions".