3GPP TSG SA WG3 Security — S3#29 **S3-030355**
15 –18 July 2003
San Francisco, USA

Source: **SchlumbergerSema**

Title: **Support for Subscriber Certificates**

Document for: **Discussion and Decision**

Agenda Item: **Support for Subscriber Certificates**

Table of Content:

1. EXISTING STANDARDS

OMA (Open Mobile Alliance) has existing specifications that deal with Wireless PKI and the WIM (Wireless Identification Module). There also exist draft specifications, in a very advanced stage, for on-board key generation in the WIM and for certificates enrollment. These specifications provide generic mechanisms that can be integrated into the 3GPP work item on “Bootstrapping of application security and support for subscriber certificates”.
Currently the only PKI identity token that is standardized is the WIM, which is an application that can be implemented on the UICC card next to the USIM application. This application provides all the necessary functionality for digital signatures creation, certificates storage and other features that a PKI systems needs. It will also include the needed interfaces for on-board key generation and the mechanisms to generate an authenticated certificate request.
It is proposed to refer to this security token in the above 3GPP work item and not to reinvent or redefine another PKI security token.

2. OMA SPECIFICATIONS FOR ISSUING CERTIFICATE

OMA current draft specifications on “certificate enrollment” are in a very advanced stage (should be finalized in September 2003). In this section we describe the basic mechanisms that are proposed in these specifications in order to enable the 3GPP SA3 to validate the parts that can be reused and integrated in its solution for “support for subscriber certificates”.
When demanding a certificate the UE need to supply sufficient information to the remote server to identify the PKI security token and the subscriber. This is done by supplying the WIM serial number (unique for every WIM) to the remote server (PKI Portal, NAF etc.). The procedure for applying for a certificate also accommodate authentication of the remote server, as is demanded by the WI in the 3GPP SA3.
The scenario for a certificate request, that demands a remote server authentication, is depicted below (figure 1). It is done when the user connect to the PKI portal with a WAP or Internet browser, and receives xHTML page that embed the ECMA script for the key enrollment. However, the same

mechanism can be adapted for other kind of protocols, which the 3GPP SA3 may choose to implement. In the first invocation the demand for key enrollment for a certificate is refused by the WIM since it needs to authenticate the remote server. It returns the WIM serial number and a 20 bytes challenge that is generated in the WIM. The remote server can use the WIM serial number in order to get information about the needed authentication keys and potentially other data about the subscriber. It then reformats a new enrollment request along with the challenge signed (a MAC) with the session key. The WIM will accept the request if authentication is successful. The ME will format the PKCS#10 certificate request and include in it the attributes that prove that the key is kept in a tamper resistant device (e.g. WIM). Signing the public key with a long lasting key in the WIM does the proof of origin. This signing key can be an asymmetric or symmetric key (MAC) that is personalized in the WIM. The proof of origin is done E2E and is not dependent on session keys in the ME, but rather on keys that are safely stored in the WIM itself. This overcomes a possible vulnerability of the ME for key storage.

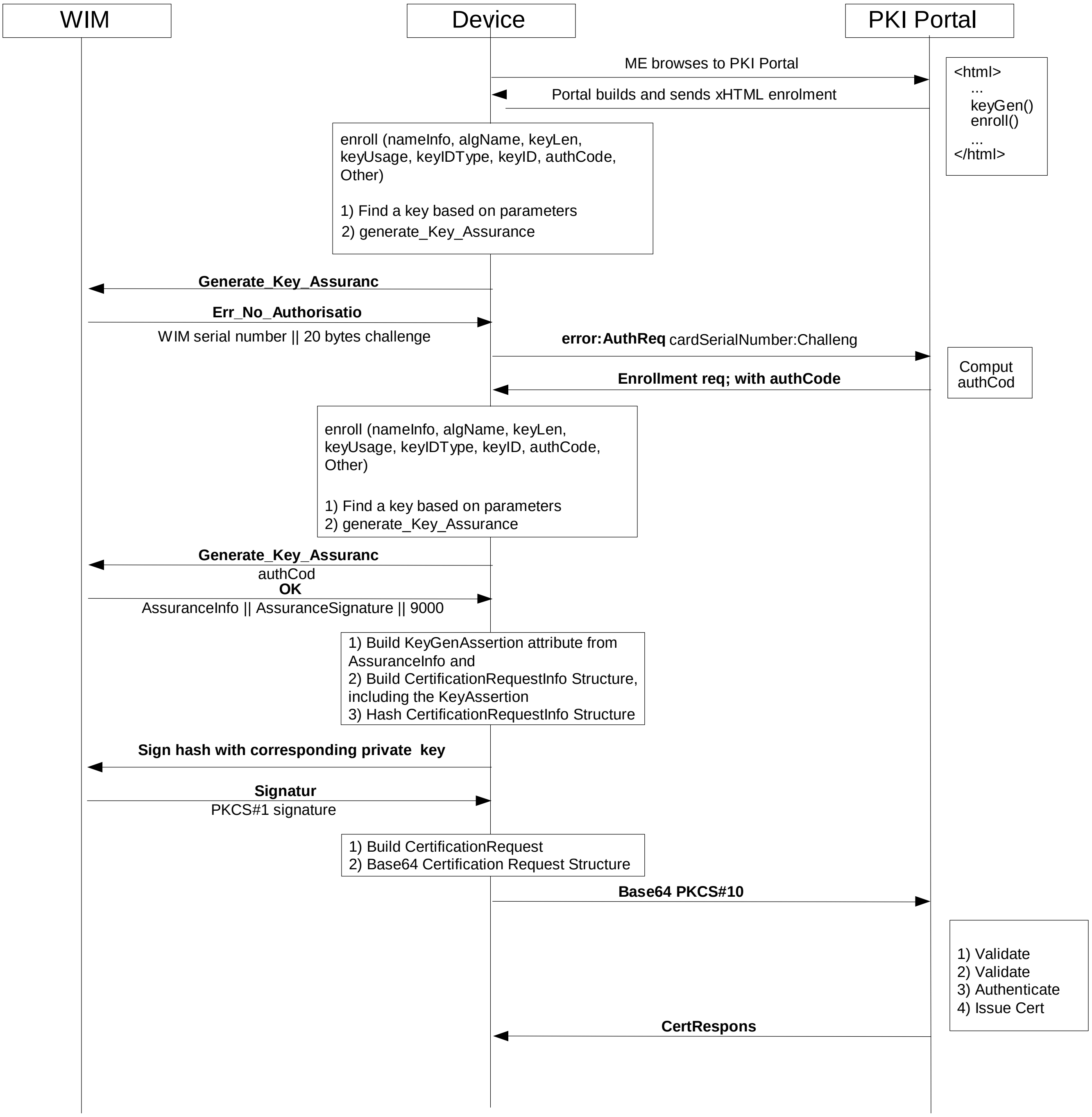

WIM
Device
PKI Portal
ME browses to PKI Portal
Portal builds and sends xHTML enrolment
<html>
...
keyGen()
enroll()
...
</html>
enroll (nameInfo, algName, keyLen, keyUsage, keyIDType, keyID, authCode, Other)
1) Find a key based on parameters
2) generate_Key_Assurance
Generate_Key_Assuranc
Err_No_Authorisatio
WIM serial number || 20 bytes challenge
error:AuthReq cardSerialNumber:Challeng
Comput authCod
Enrollment req; with authCode
enroll (nameInfo, algName, keyLen, keyUsage, keyIDType, keyID, authCode, Other)
1) Find a key based on parameters
2) generate_Key_Assurance
Generate_Key_Assuranc
authCod
OK
AssuranceInfo || AssuranceSignature || 9000
1) Build KeyGenAssertion attribute from AssuranceInfo and
2) Build CertificationRequestInfo Structure, including the KeyAssertion
3) Hash CertificationRequestInfo Structure
Sign hash with corresponding private key
Signatur
PKCS#1 signature
1) Build CertificationRequest
2) Base64 Certification Request Structure
Base64 PKCS#10
1) Validate
2) Validate
3) Authenticate
4) Issue Cert
CertRespons

Figure 1: interactions for subscriber certificate request

The **GenEnrollReq** ECMA script will return an error or a well-formed enrollment request. The Enroll Request take the form of a PKCS#10 certificate request as defined in [2].
In addition, the specification defines mechanisms to indicate to the PKI an assurance as to how the key was generated and stored. This assurance may indicate that the key was generated on trusted hardware (such as a WIM). This assurance is provided through the inclusion of an attribute in the attributes field of the CertificationRequestInfo structure. The assurance information MUST be one of:

- Digital signature using a public key formatted as a CMS message.
- An HMAC using a symmetric key formatted as a CMS message.

The data on which the HMAC or digital signature is calculated include the public key for which an assertion is provided as well as an indication of the type of assertion that is made.

3. OMA SPECIFICATIONS FOR ON-BOARD KEY GENERATION

The key generation in the WIM is done with similar mechanisms. The scenario for on-board key generation, that demands a remote server authentication, is depicted below (figure 2). It is done when the user connects to the PKI portal (or other authorized remote server) with a WAP or Internet browser, and receives the xHTML page that embed the ECMA script for the key generation. However, the same mechanism can be adapted for other kind of protocols, which the 3GPP SA3 may choose to implement.
In the first invocation the demand for key generation is refused by the WIM since it needs to authenticate the remote server. It returns the WIM serial number and a 20 bytes challenge that is generated in the WIM. The remote server can use the WIM serial number in order to get information about the needed authentication keys. It then reformats a new XHTML page with the ECMA script for key generation along with the challenge signed (a MAC) with the authentication key. The WIM will accept the request if authentication is successful. The WIM will generate the keys internally and return the public key hash as an identifier for the key.

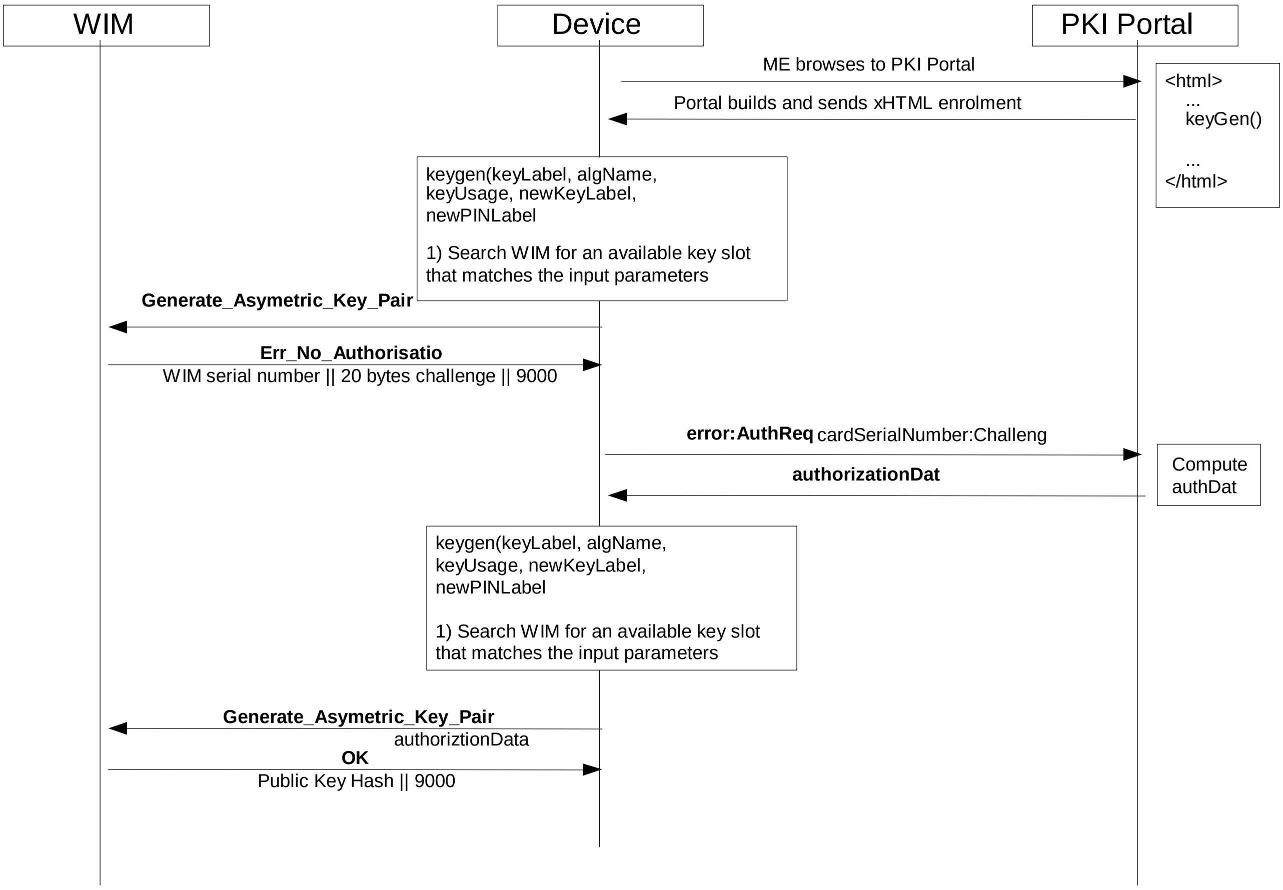
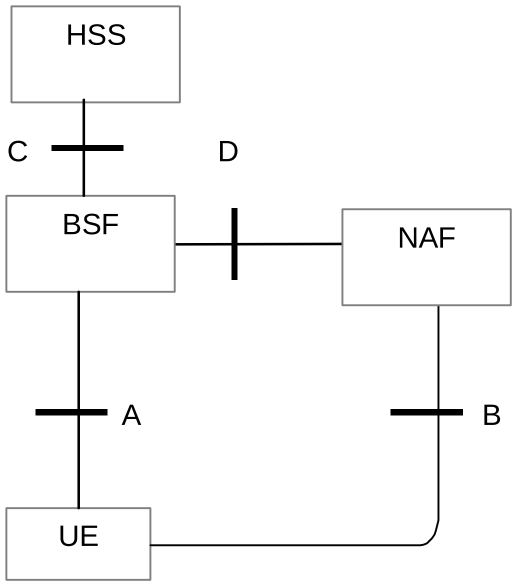

WIM
Device
PKI Portal
ME browses to PKI Portal
Portal builds and sends xHTML enrolment
<html>
...
keyGen()
...
</html>
keygen(keyLabel, algName, keyUsage, newKeyLabel, newPINLabel
1) Search WIM for an available key slot that matches the input parameters
Generate_Asymetric_Key_Pair
Err_No_Authorisatio
WIM serial number || 20 bytes challenge || 9000
error:AuthReq cardSerialNumber:Challeng
authorizationDat
Compute authDat
keygen(keyLabel, algName, keyUsage, newKeyLabel, newPINLabel
1) Search WIM for an available key slot that matches the input parameters
Generate_Asymetric_Key_Pair
authoriztionData
OK
Public Key Hash || 9000

Figure 2: interactions on-board key generation

4. MATCHING OMA SPECIFICATIONS AND 3GPP BOOTSTRAPPING ARCHITECTURE

The OMA specifications for on-board key generation and key enrollment (subscriber certificate) can be integrated in the current work of 3GPP SA3. There is no need to reinvent other solutions and the possibility to leverage on existing work can accelerate the work. The current network model that is involved in the bootstrapping approach is depicted below:



The NAF represents the PKI portal (or equivalent) in the OMA architecture. The transaction identifier for the interaction between the UE and the NAF is the “WIM serial number”. This will enable the NAF to get the needed authentication key and subscriber information from the BSF to be used for the certificate request. The B protocol can either be the WAP or Internet protocol with xHTML browsing as in OMA, or another protocol that is decided by the SA3 group. It should preserve the end to end authentication with the WIM and the ability to generate the same events, with the relevant parameters, in both sides.

5. WAY FORWARD

It is proposed that the 3GPP SA3 group send a liaison statement to the OMA Security group for the exchange of documents and relevant information. An ad-hoc joint meeting can also be arranged in order to check the possibility to collaborate for advancing a coherent solution that take advantage of existing specifications.

6. REFERENCES

[1] OMA specifications on Key Generation and Key Enrollment

[2] PKCS #10 v1.7: Certification Request Syntax Standard, RSA Laboratories, May 26, 2000, http://www.rsasecurity.com/rsalabs/pkcs/pkcs-10/index.html