ALU sets SCEP pre-study report

Author(s) : **Alex A CAO**

Approver(s) : **Jean Louis BOULET**

Ref. (Ed.) : **3AK_29000_0036_BEZZA(01)**

Date : **03.18.2013**

Distribution : Jean Michel LAURIOL, Jean Louis BOULET, Olivier KREET, Jean-Pierre KELLERMANN, Georges NOGUEIRA, Cecile BONNAUD, Michel MOUTON

Copies : Alex A CAO, Ada A WANG, Ting HE

Keywords : Prestudies NOE ICTouch

Abstract : This PPT contains the pre-study report of SCEP deployment of ALU IP sets.

Doc. Plan : ComSets R D

SubDocPlan :

Doc. Ref. :

Expandlist :

Simple Certificate Enrollment Protocol in ALU sets

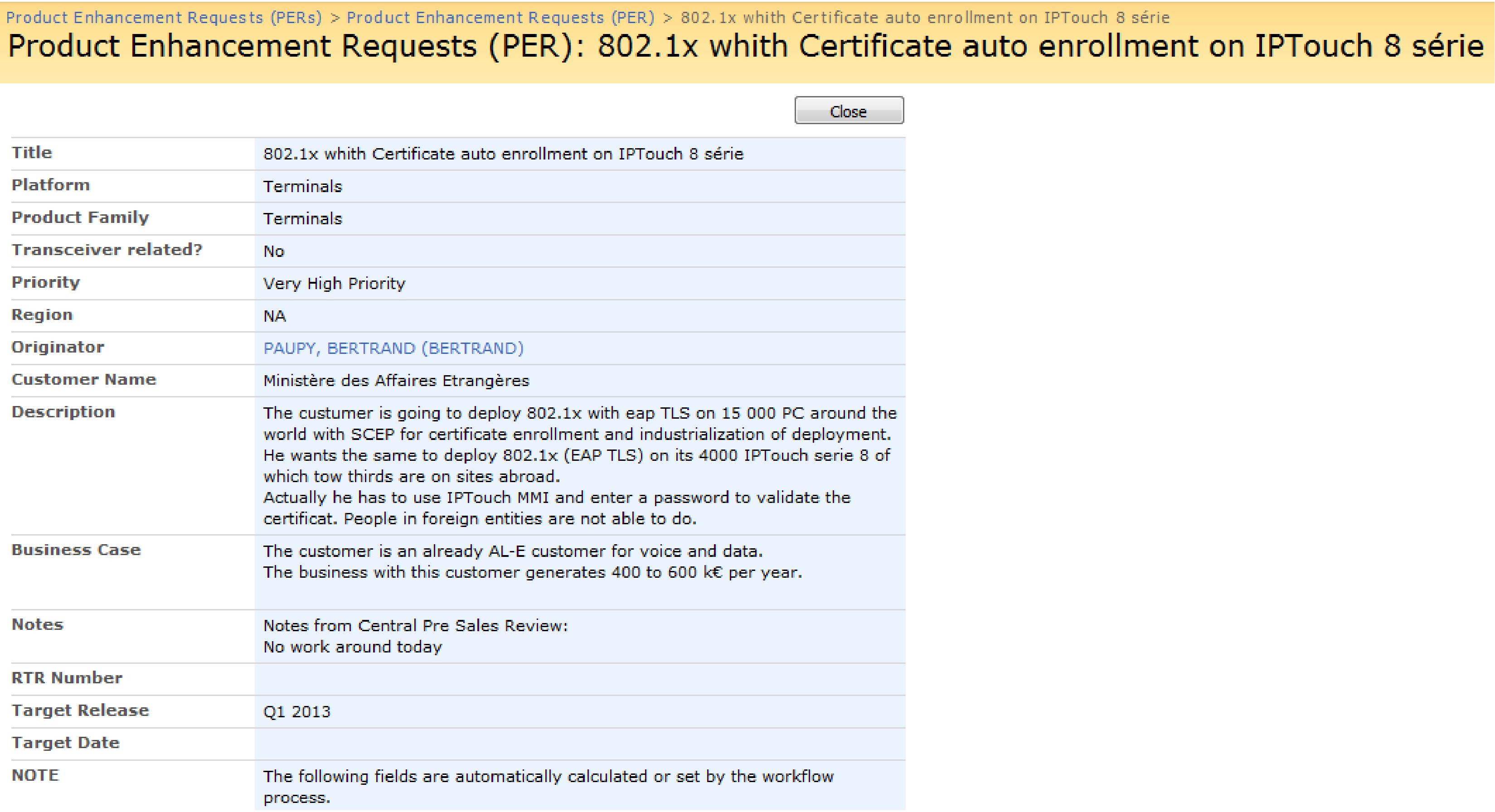
A.CAO

W1311.3

Agenda

- Problem we faced
- What is SCEP
- SCEP in ALU sets
- Complements

Problem we faced



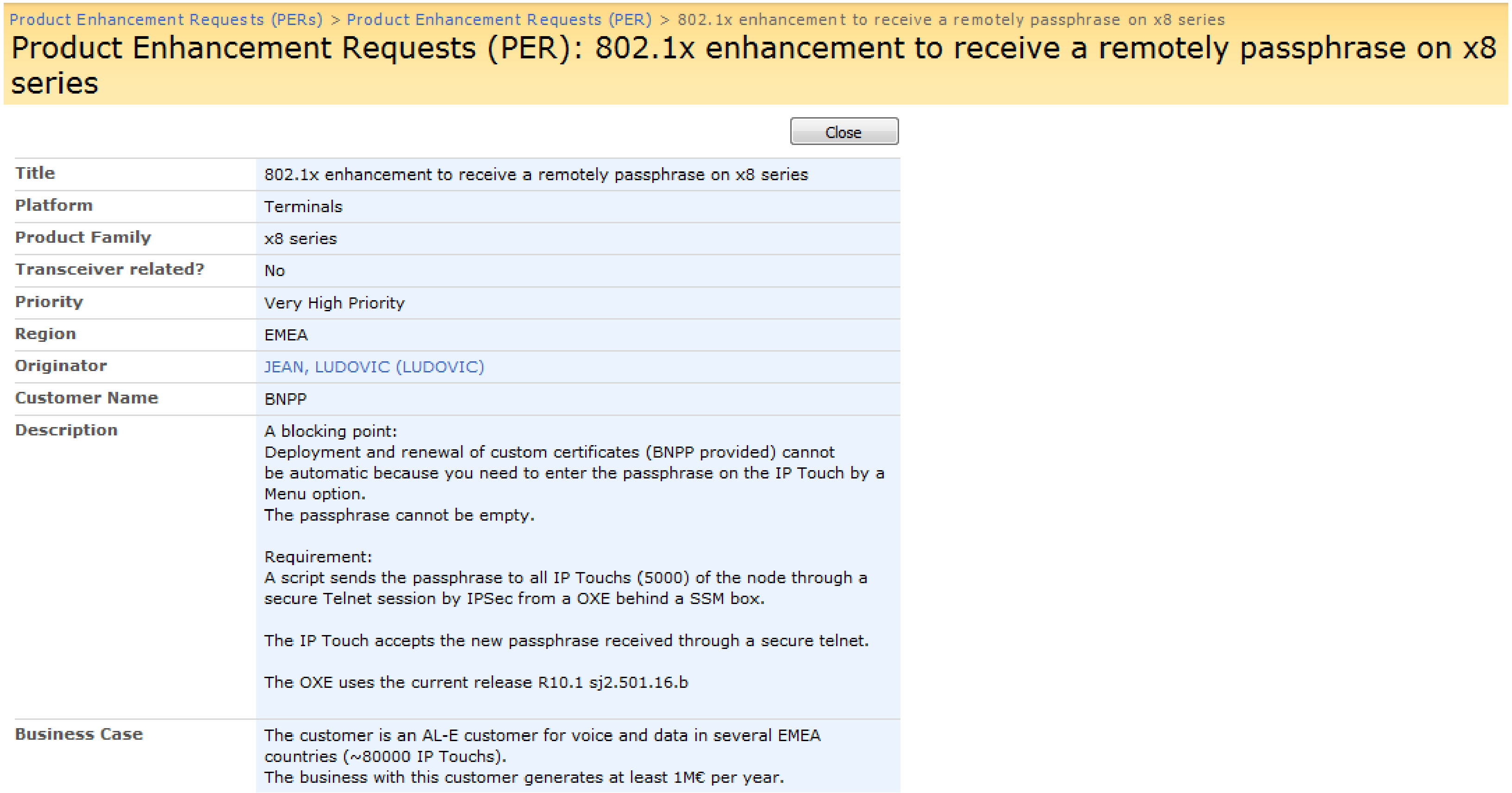
Product Enhancement Requests (PERs) > Product Enhancement Requests (PER) > 802.1x whith Certificate auto enrollment on IPTouch 8 série

Product Enhancement Requests (PER): 802.1x whith Certificate auto enrollment on IPTouch 8 série

Title	802.1x whith Certificate auto enrollment on IPTouch 8 série
Platform	Terminals
Product Family	Terminals
Transceiver related?	No
Priority	Very High Priority
Region	NA
Originator	PAUPY, BERTRAND (BERTRAND)
Customer Name	Ministère des Affaires Etrangères
Description	The custumer is going to deploy 802.1x with eap TLS on 15 000 PC around the world with SCEP for certificate enrollment and industrialization of deployment. He wants the same to deploy 802.1x (EAP TLS) on its 4000 IPTouch serie 8 of which tow thirds are on sites abroad. Actually he has to use IPTouch MMI and enter a password to validate the certificat. People in foreign entities are not able to do.
Business Case	The customer is an already AL-E customer for voice and data. The business with this customer generates 400 to 600 k€ per year.
Notes	Notes from Central Pre Sales Review: No work around today
RTR Number	
Target Release	Q1 2013
Target Date	
NOTE	The following fields are automatically calculated or set by the workflow process.

- http://uscals-sp.ind.alcatel.com/sites/PER/Lists/Product%20Enhanement%20Requests%20PER/DispForm.aspx?ID=2315

Problem we faced



Product Enhancement Requests (PERs) > Product Enhancement Requests (PER) > 802.1x enhancement to receive a remotely passphrase on x8 series

Product Enhancement Requests (PER): 802.1x enhancement to receive a remotely passphrase on x8 series

Title	802.1x enhancement to receive a remotely passphrase on x8 series
Platform	Terminals
Product Family	x8 series
Transceiver related?	No
Priority	Very High Priority
Region	EMEA
Originator	JEAN, LUDOVIC (LUDOVIC)
Customer Name	BNPP
Description	A blocking point: Deployment and renewal of custom certificates (BNPP provided) cannot be automatic because you need to enter the passphrase on the IP Touch by a Menu option. The passphrase cannot be empty. Requirement: A script sends the passphrase to all IP Touchs (5000) of the node through a secure Telnet session by IPSec from a OXE behind a SSM box. The IP Touch accepts the new passphrase received through a secure telnet. The OXE uses the current release R10.1 sj2.501.16.b
Business Case	The customer is an AL-E customer for voice and data in several EMEA countries (~80000 IP Touchs). The business with this customer generates at least 1M€ per year.

- http://uscals-sp.ind.alcatel.com/sites/PER/Lists/Product%20Enhanement%20Requests%20PER/DispForm.aspx?ID=2410

Problem we faced

Be simpler, NOE-2G set consider to allow customer to introduce their own certificates, replacing natively involved ALU certificates.
But due to the format(#PKCS12) limitation, customer must enter a password manually when downloading such kind of certificates.

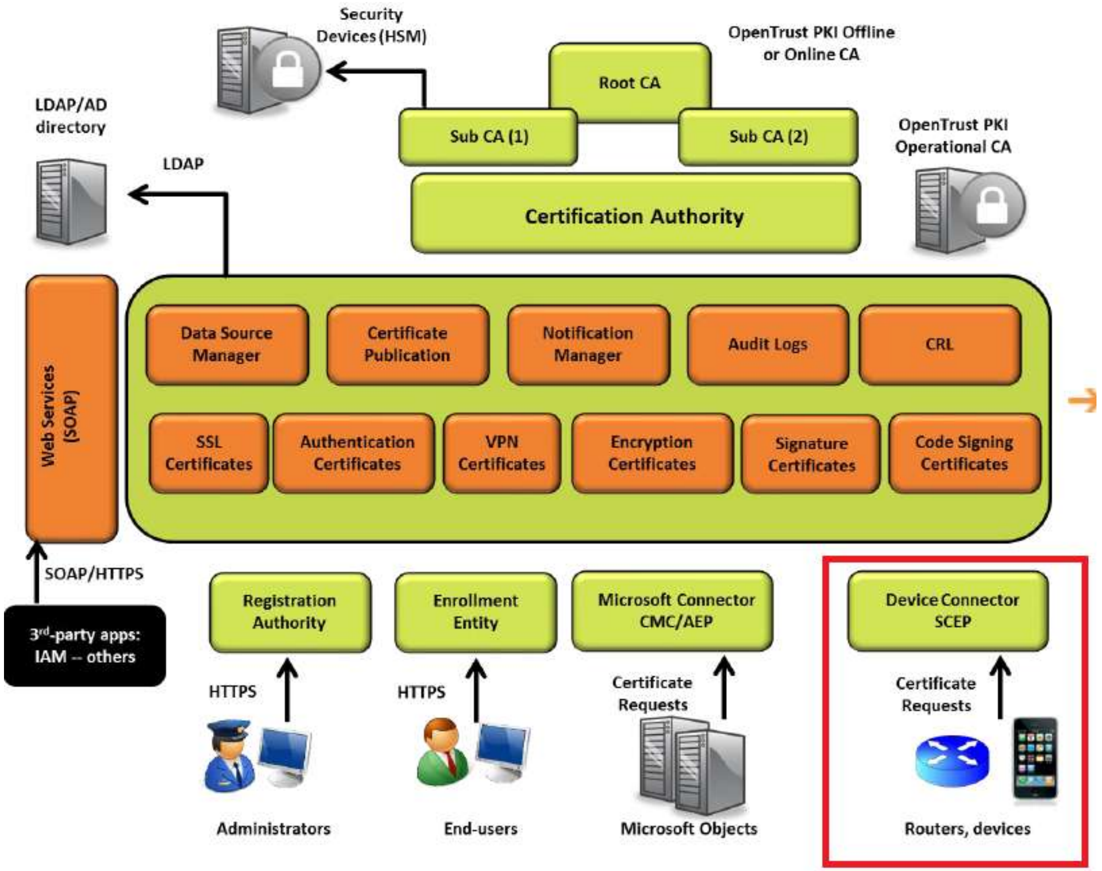
This certainly meets problems when there are a large number of NOE IP sets who need distribute customer certificates, it is impossible for TS to manually set password on every phone.

When sets run in NOE mode, it is possible to including PEM format private key/certificate/Root CA certificate data in lanpbx.cfg file to allow NOE get it from CS, but this solution is not suitable to SIP sets which does not support lanpbx.cfg downloading.

It is also a requirement that all serial ALU sets can support one uniform method to automatically distribute customer certificate without human operation.

Customer Requirement

Customer's network management applied OpenTRUST solution which applying automatically certificate enrollment and management through SCEP.
http://www.keynectis.com/en/certificate-based-identity-management



Customer Requirement

- ALU enterprise clients (hard phone/soft phone) need to work with SCEP servers so that ALU clients can enroll certificates through HTTP message exchange with OpenTrust.

- In 1st step, we only talk about the solution in clients side, no SCEP server or application will be added in server or OT side.

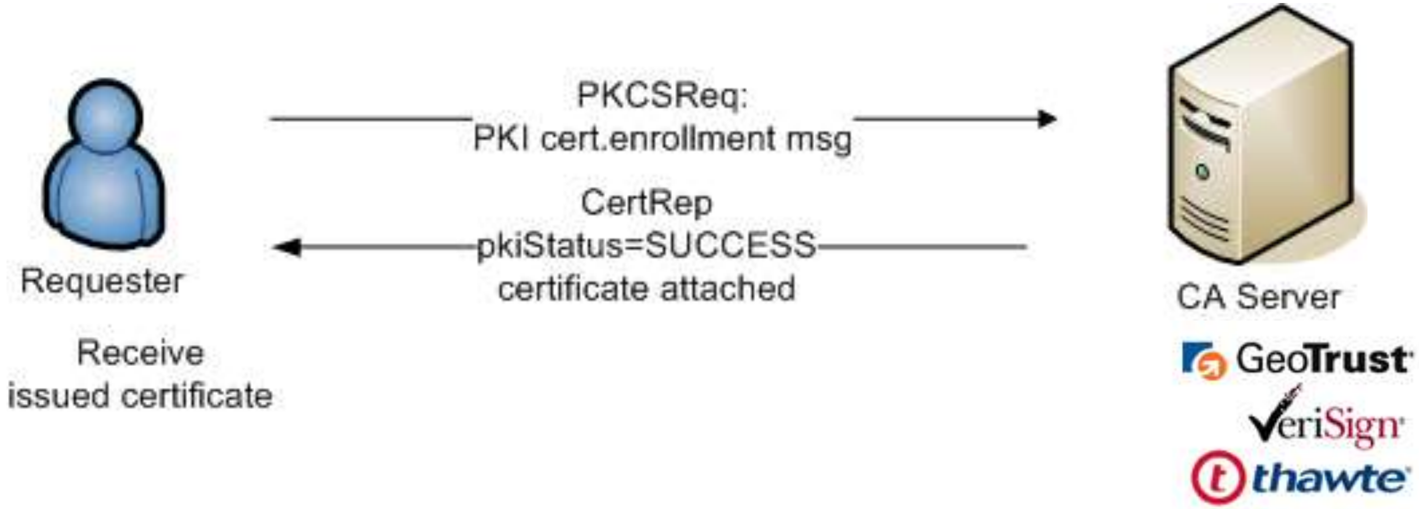
- Mandatory support must be provided to servers below:
  - OpenTRUST (OpenPKI)
  - Windows Server (2003/2008)
  - OpenSCEP

What is SCEP

- **S**imple **C**ertificate **E**nrollment **P**rotocol (SCEP), is a Public Key Infrastructure (PKI) communication protocol which leverages existing technology by using PKCS#7 and PKCS#10 over HTTP. SCEP is the evolution of the enrollment protocol developed by VeriSign, Inc. for Cisco Systems, Inc. It now enjoys wide support in both client and a Certification Authority implementations.

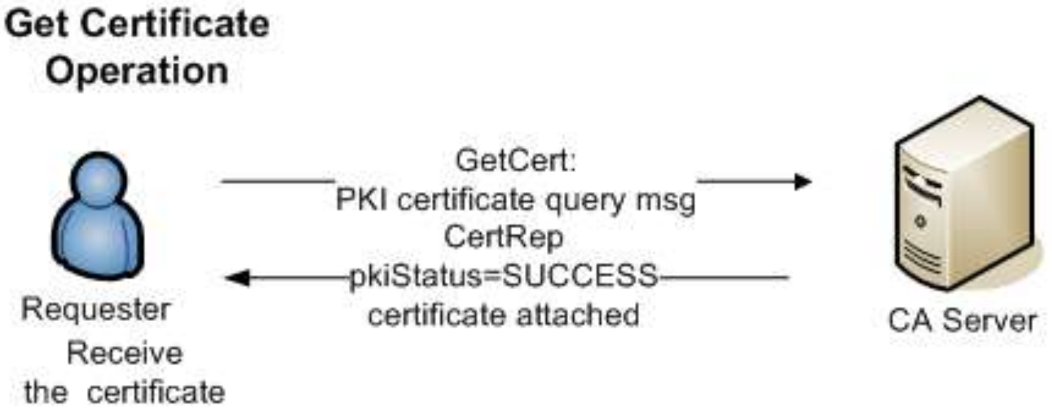
- The basic theory of SCEP is that client send a certificate request to CA server, then CA server automatically sign the certificate and response with signed certificate.

A successful transaction in automatic mode



- The certificate request in PKCSReq is coded as PKCS#10 format.
- The signed certificate in CERTRep is coded as PKCS#7b format.
- Message exchange are encoded and signed by PKCS#7 standard.

Other transaction in automatic mode



Get Certificate Operation

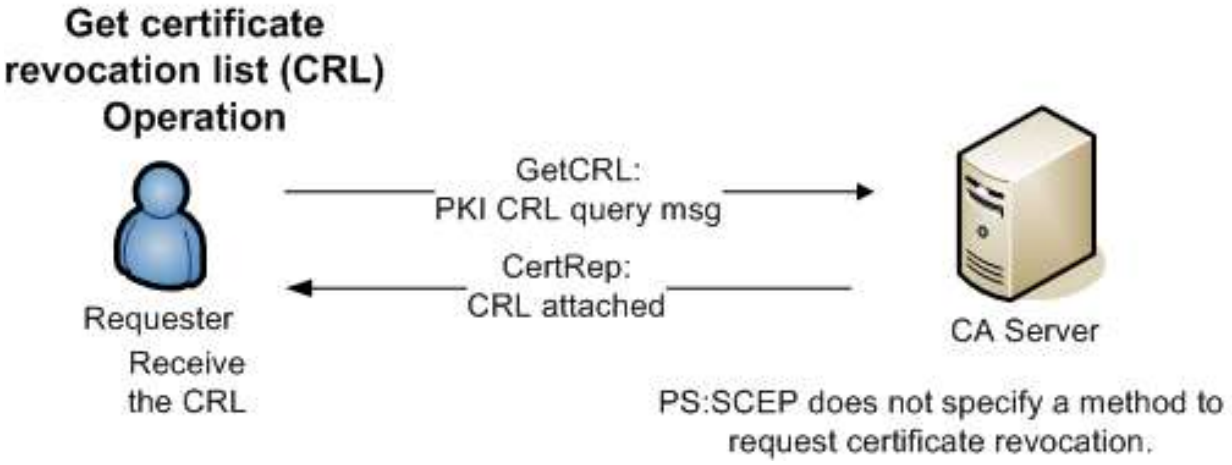
Requester

CA Server

GetCert:
PKI certificate query msg

CertRep
pkiStatus=SUCCESS
certificate attached

Receive
the certificate



Get certificate revocation list (CRL) Operation

Requester

CA Server

GetCRL:
PKI CRL query msg

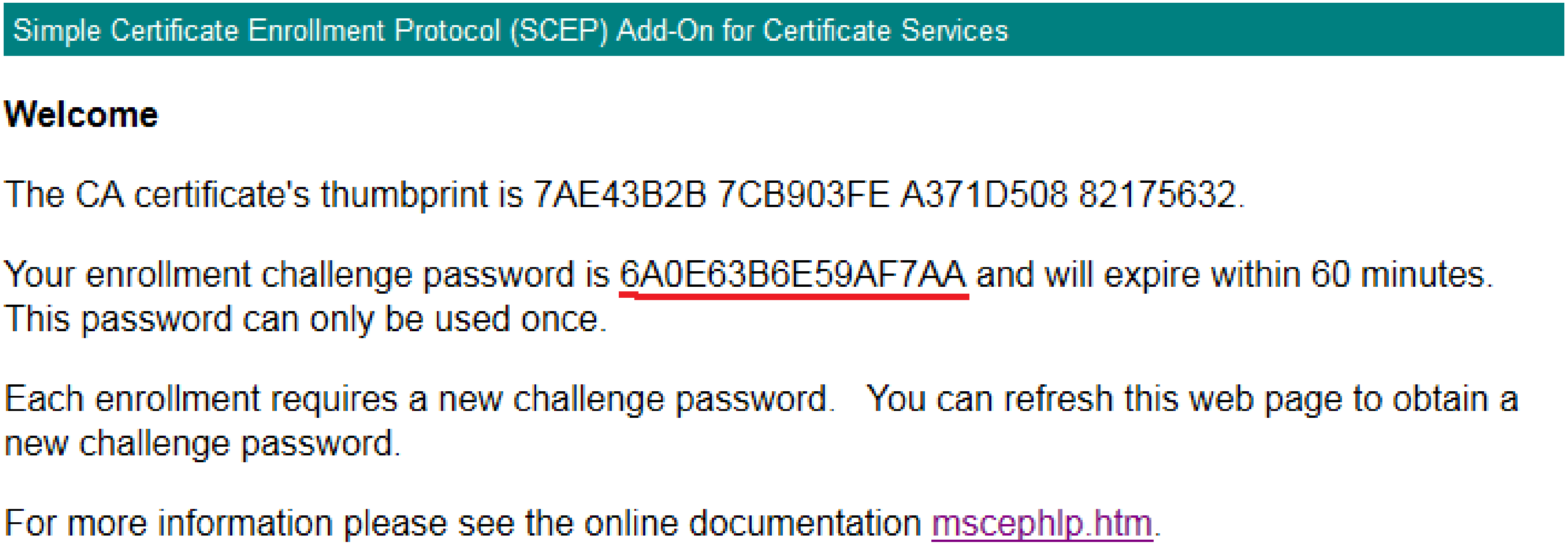
CertRep:
CRL attached

Receive
the CRL

PS:SCEP does not specify a method to
request certificate revocation.

Security issue in communication

- There is a optional Challenge Password (so called pre-shared-key) designed to prove the validation of the communication entities.
- Before client request certificate, optional it can get a challenge password from CA/RA server, this password will be included in certificate request.
- If the challenge mechanism is defined by server, then the same mechanism can also be applied during certificate revocation.
- The certificate renewal can also apply challenge password.



Simple Certificate Enrollment Protocol (SCEP) Add-On for Certificate Services

Welcome

The CA certificate's thumbprint is 7AE43B2B 7CB903FE A371D508 82175632.

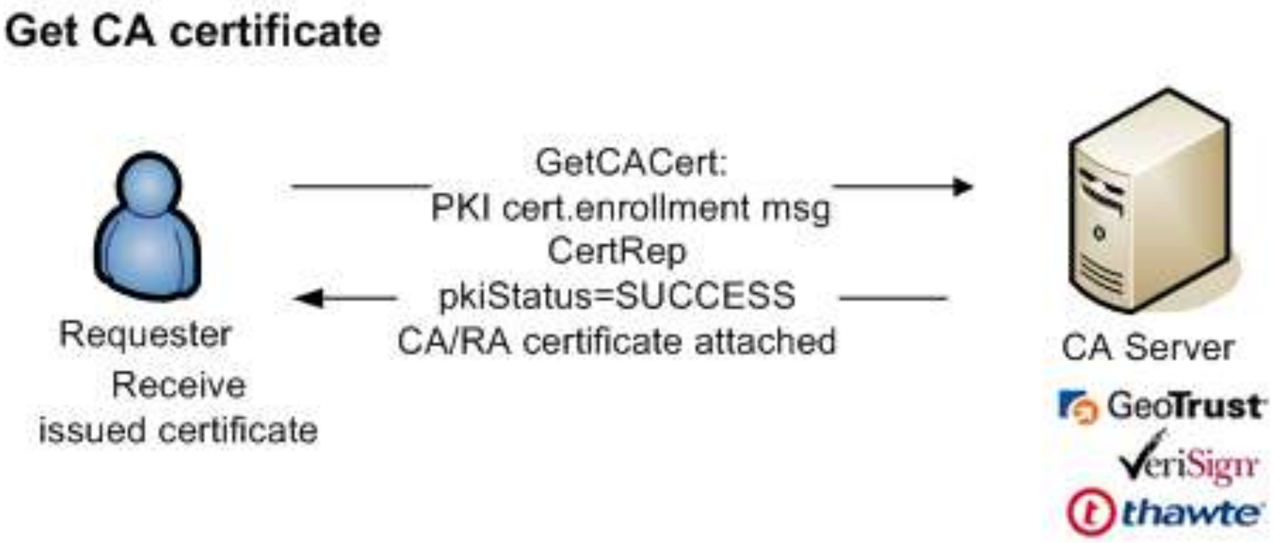
Your enrollment challenge password is 6A0E63B6E59AF7AA and will expire within 60 minutes. This password can only be used once.

Each enrollment requires a new challenge password. You can refresh this web page to obtain a new challenge password.

For more information please see the online documentation mscephlp.htm.

Security issue in communication

- When SCEP initializes, client must request for the certificate of CA/RA server. The public key existed in the CA will be applied to encrypt the messages during coming information exchange.



Security issue in communication

- The communication between the requester and the certification authority are secured using **SCEP Secure Message Objects** which specifies how PKCS#7 is used to encrypt and sign the data.

- ContentType = SignedData (called pkiMessage)
    - SignerInfo
        - Signature
            - authenticatedAttributes

  transactionID

  messageType

  pkiStatus

  failInfo

  senderNonce

  recipientNonce

  etc

  ContentInfo type = EnvelopedData (called pkcsPKIEnvelope; optional)
    - RecipientInfo
    - ContentInfo type = Data
        - messageData

Security issue in communication

- The first and second goals are met through the use of PKCS#7 and PKCS#10 encryption and digital signatures using authenticated public keys.

  - The CA's public key is authenticated via the checking of the CA fingerprint;
  - and the SCEP client's public key is authenticated through the manual authentication or pre-shared secret authentication.

- The third goal is met through the use of a challenge password for revocation, which is chosen by the SCEP client and communicated to the CA protected by the PKCS#7 encryptedData.

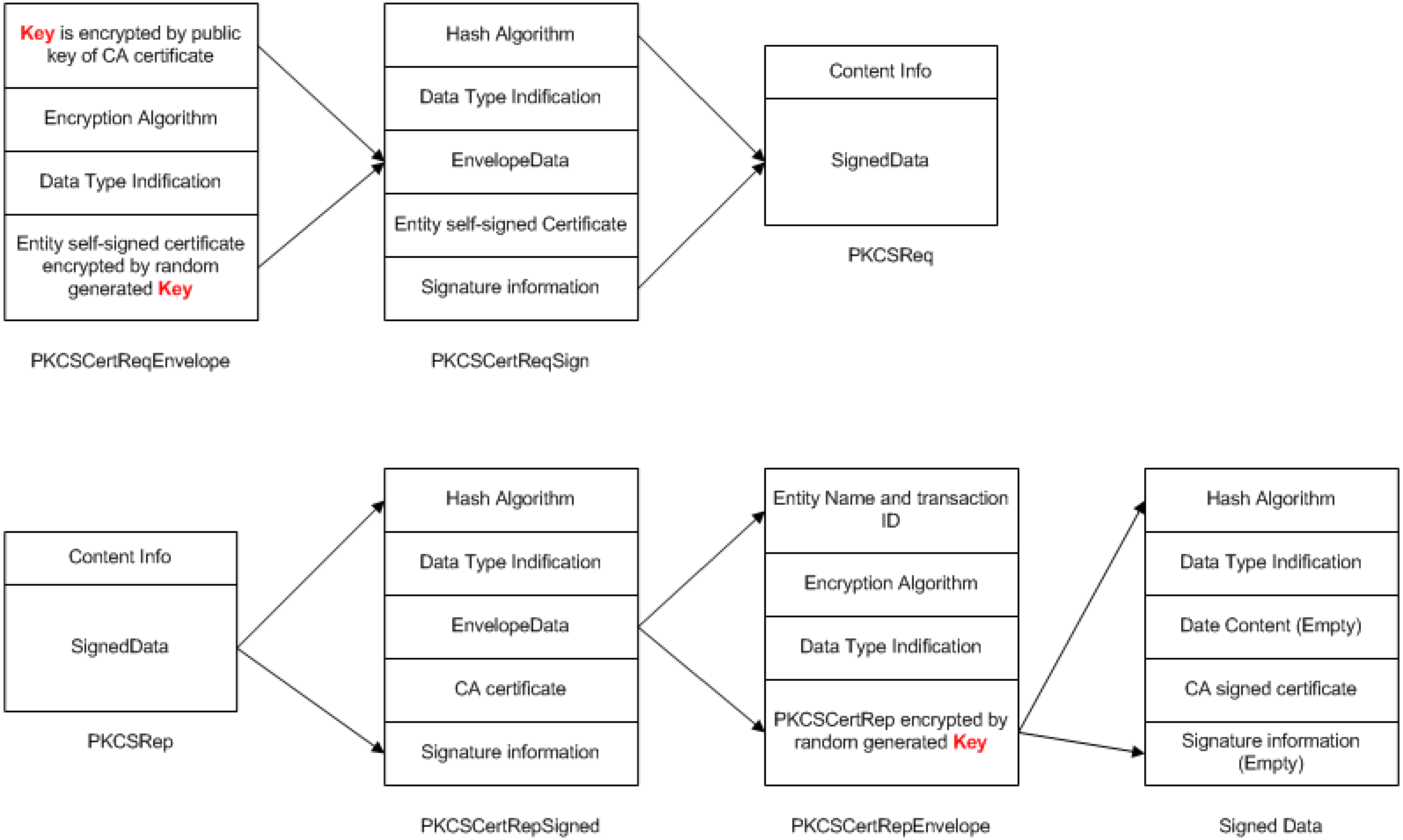
Security issue in communication

- In order to perform the signing operation the client uses an appropriate local certificate:

1. If the requesting system already has a certificate issued by the SCEP server, and the server supports renewal that certificate SHOULD be used.
2. If the requesting system has no certificate issued by the new CA, but has credentials from an alternate CA the certificate issued by the alternate CA MAY be used. Policy settings on the new CA will determine if the request can be accepted or not. This is useful when enrolling with a new administrative domain; by using a certificate from the old domain as credentials.
3. If the requester does not have an appropriate existing certificate, then a locally generated self-signed certificate MUST be used instead. The self-signed certificate MUST use the same subject name as in the PKCS#10 request.

- During the certificate enrollment, the requester MUST use the selected certificate's **keypair** when signing the PKCS#7. The server CertResp uses this signing certificate's public key when encrypting the response.
- When the certification authority creates the PKCS#7 envelope on the issued certificate, it SHOULD use the **public key, issuer name, and serial number** conveyed in the above included certificate. This will inform the end entity of which private key is needed to open the envelope. Note that when a client enrolls for separate encryption and signature certificates, it MAY use the signature certificate to sign both requests, and then expect its signature key to be used to encrypt both responses. In any case, the RecipientInfo on the envelope MUST reflect the key used to encrypt the request.

Message Organization



Key is encrypted by public key of CA certificate

Encryption Algorithm

Data Type Indification

Entity self-signed certificate encrypted by random generated Key

PKCSCertReqEnvelope

Hash Algorithm

Data Type Indification

EnvelopeData

Entity self-signed Certificate

Signature information

PKCSCertReqSign

Content Info

SignedData

PKCSReq

Content Info

SignedData

PKCSRep

Hash Algorithm

Data Type Indification

EnvelopeData

CA certificate

Signature information

PKCSCertRepSigned

Entity Name and transaction ID

Encryption Algorithm

Data Type Indification

PKCSCertRep encrypted by random generated Key

PKCSCertRepEnvelope

Hash Algorithm

Data Type Indification

Date Content (Empty)

CA signed certificate

Signature information (Empty)

Signed Data

Client Implementation

1. Client must be configured locally with:
   - The Certification Authority IP address or fully qualified domain name.
   - The Certification Authority HTTP CGI script path.
   - The identifying information that is used for authentication of the Certification Authority. This information MAY be obtained from the user, or presented to the end user for manual authorization during the protocol exchange (e.g. CA certificate who is trusted).
2. Manage locally for PKI exchange required material.
   - CA certificate
   - Key-pair
   - Certificate request
3. Extract public key of CA server, and apply SCEP procedures to send Cert request, and wait for certificate signed replied.
4. Install received signed certificate locally.

SCEP in ALU sets

- It is asked to apply unified solution to all range ALU sets of auto certificate distribution.
- Different level job is need to be done for this target.

ALU Phone	Platform OS Type	Required Job	Comment
NOE	Vxworks	1. Study how to generate private key/certificate request through OpenSSL library (no script supported). 2. Select a valid open source for implementing SCEP client (e.g. SSCEP). 3. Resolve the problem brought by no file system, 2nd dev on open source code. Some SCEP operation(GetCaps) need to be added. 4. Define when to do the enrollment (step 3?). When to renew certificate? 5. Interaction with initialization procedure. 6. Local configuration for HTTP URL mentioned above (or from lanpbx.cfg/own configuration file).	NOE-2G NOE-3G NOE-SIP
VHE	Linux	1. Study how to generate private key/certificate request through Openssl commands. 2. Select a valid open source for implementing SCEP client (e.g. SSCEP). 3. Define when to do the enrollment, related to the interchange with main initialization procedure probably. 4. Local configuration for HTTP URL mentioned above.	8082 MIP
VLE	Vxworks	Refer to NOE.	8002/8012 OTDP

Obsoleted

Alcatel·Lucent

AT THE SPEED OF IDEAS™

Some new requirements

1. Certificate renewal requirement

Current enterprise solution don’t support dynamic certificate renew mechanism, in SCEP draft, there is related description.

Appendix C. **CA Capabilities**

Example: GET /cgi-bin/pkiclient.exe?operation=GetCACaps&message=myca might return: GetNextCACert<LF>POSTPKIOperation

Appendix D. **Client Certificate Renewal**

An enrollment request that occurs more than halfway through the validity period of an existing certificate for the same subject name and key usage MAY be interpreted as a re-enrollment or renewal request and be accepted. A new certificate with new validity dates can be issued, even though the old one is still valid, if the CA policy permits. The server MAY **automatically revoke the old client certificate**. Clients MUST use **GetCACaps** (see Appendix C) to determine if the CA supports renewal. Clients MUST support servers that do not implement renewal, or that reject renewal requests.

To renew a client certificate, the client uses the **PKCSreq message and signs it with the existing client certificate**. The client SHOULD use a new keypair when requesting a new certificate. The client MAY request a new certicate using the old keypair.

Some new requirements

2. Certificate revoke requirement

SCEP **does not specify a method** to request certificate revocation.

In order to revoke a certificate, the requester **must contact the CA server operator using a non-SCEP defined mechanism**. Although the PKCS#10 [RFC2986] challengePassword is used by SCEP for enrollment authorization (see Enrollment authorization (Section 2.3)) this does not inhibit the CA server from maintaining a record of the challengePassword to use during subsequent revocation operations as implied by [RFC2985].

Open Points:

•May refer to last slide, through a renewal operation trigger?

•Terminal need local clock time to decide whether the certificate is out of date, if true, then follow the process in last slide.

•OCSP can be applied to check the status of certificate, supported by OpenPKI, is it applied in customer network configuration? http://www.ietf.org/rfc/rfc2560.txt

SCEP in solutions

- Add HTTP server service which support SCEP. (Independent server probably, used by NOE sets and SIP sets)
- Add certificate sign mechanism , Certificate Authorization server is needed.
- PKI configuration?
- OpenSCEP includes SCEP server (scepd), please double check on FOSS to see whether it is OK to apply it.
- Server must support **GetCACaps** method if renewal feature is required.
- Possible to add revocation support.
- To be add…

Client interface

- For local checking and implementation, add new settings in local MMI menu:

Checkbox:	SCEP: On/Off	*Start SCEP when up?*
Checkbox:	Challenge Password Required?	*Apply challenge password?*
Text Box:	SCEP URL: http://<SCEP server IP/FQDN>/PATH	*SCEP URL*
~~Button:~~	~~Launch SCEP~~	~~*Start SCEP lively*~~

- For centralized management, add configuration parameters in:

DM configuration files (MIP, VLE)

lanpbx.cfg files (NOE)

Which should involve:

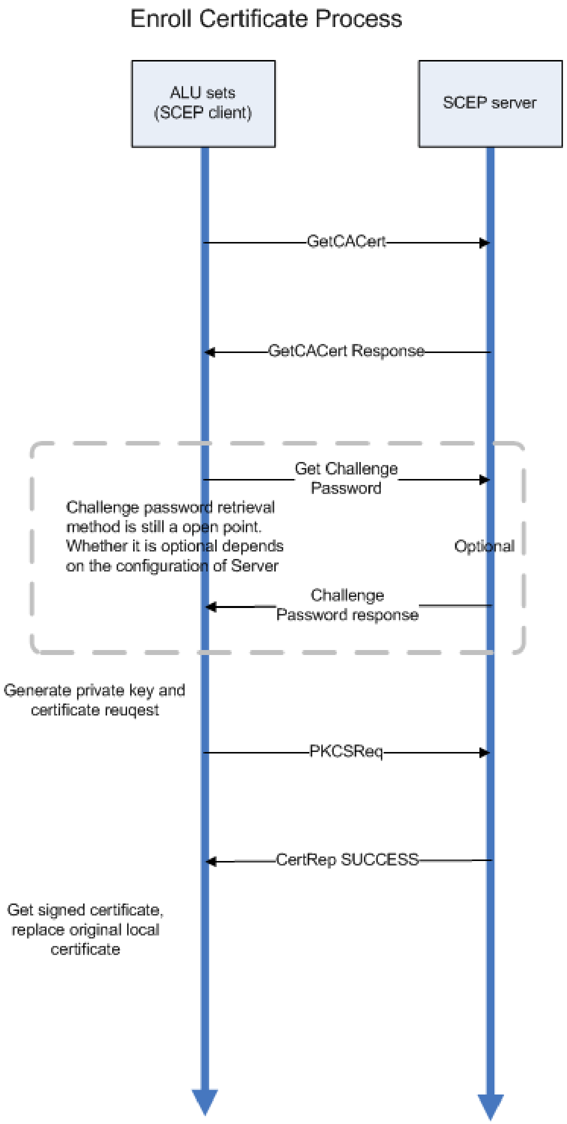
scep_run = [yes|no]	*Start SCEP when up?*
scep_challenge_password = [yes|no]	*Apply challenge password?*
scep_url = string	*SCEP URL*

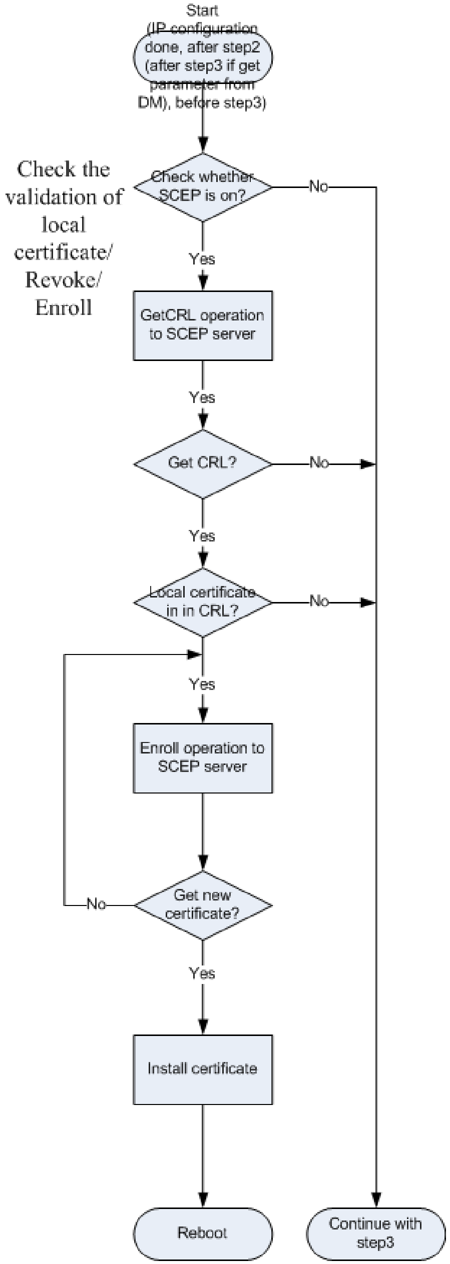
Open Point:

We by default name the certificate CN with its MAC address? It is used to generate a certificate request e.g. 00809F59E1A0

SCEP procedure for certificate enrollment

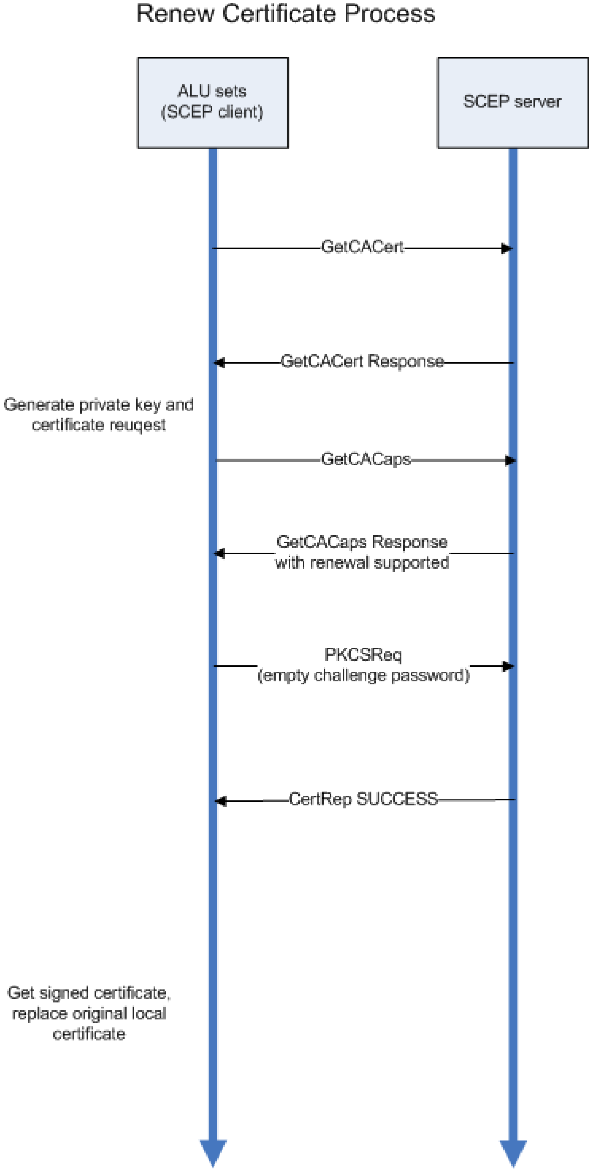
- This happened after terminal has feasibility to connect to SCEP server, terminal can check CRL from CA, if it is revoked, enroll a new one.
- The revocation procedure is also included during this procedure.


Enroll Certificate Process
ALU sets (SCEP client)
SCEP server
GetCACert
GetCACert Response
Get Challenge Password
Challenge password retrieval method is still a open point. Whether it is optional depends on the configuration of Server
Optional
Challenge Password response
Generate private key and certificate reuqest
PKCSReq
CertRep SUCCESS
Get signed certificate, replace original local certificate


Start (IP configuration done, after step2 (after step3 if get parameter from DM), before step3)
Check the validation of local certificate/ Revoke/ Enroll
Check whether SCEP is on?
No
Yes
GetCRL operation to SCEP server
Yes
Get CRL?
No
Yes
Local certificate in in CRL?
No
Yes
Enroll operation to SCEP server
Get new certificate?
No
Yes
Install certificate
Reboot
Continue with step3

SCEP procedure for certificate renew

- This one happened after terminal get correct date (For SIP sets, date is got from SNTP, for NOE sets, from call server), if local certificate is expired, renew it.



Renew Certificate Process

ALU sets (SCEP client)

SCEP server

GetCACert

GetCACert Response

Generate private key and certificate reuqest

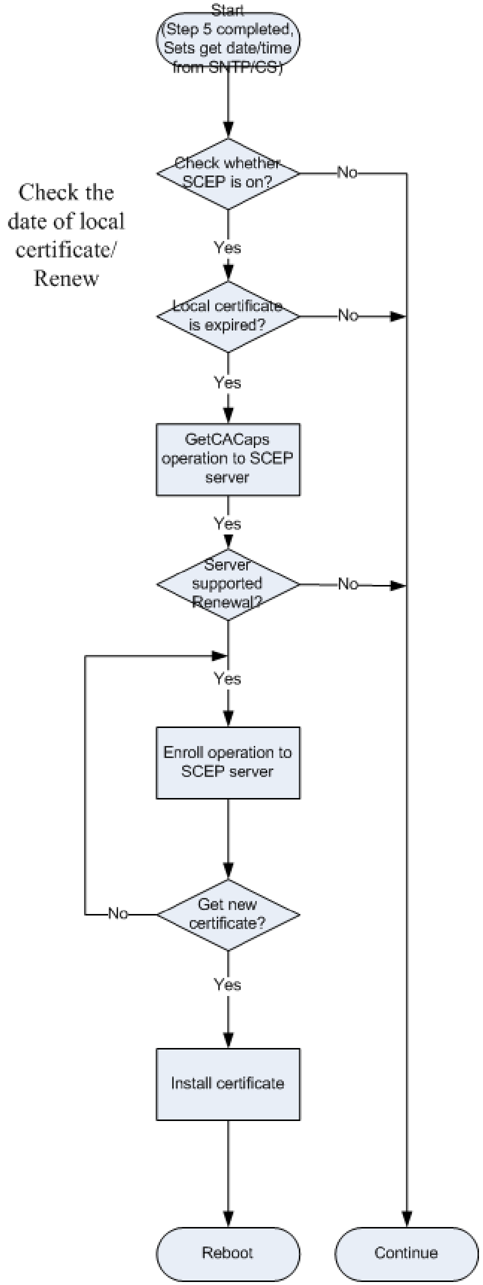
GetCACaps

GetCACaps Response with renewal supported

PKCSReq (empty challenge password)

CertRep SUCCESS

Get signed certificate, replace original local certificate



Check the date of local certificate/ Renew

Start (Step 5 completed, Sets get date/time from SNTP/CS)

Check whether SCEP is on?

No

Yes

Local certificate is expired?

No

Yes

GetCACaps operation to SCEP server

Yes

Server supported Renewal?

No

Yes

Enroll operation to SCEP server

Get new certificate?

No

Yes

Install certificate

Reboot

Continue

Customer network analysis

- To support standard SCEP with customer's network management system, need more time to study how customer network works like (OPENTRUST, Enterprise PKI).
- As slide 7th mentioned, we need to analyze different type of SCEP solutions to ensure the implementation in client side can satisfy the requirement.

Solution (Server)	From	Progress Description	Cost
OPENTRUST Enterprise PKI	KEYNECTIS OPENTRUST	Only few introduction doc, no evaluation software yet. ☹	?
Microsoft Windows Server 2003 Windows Server 2008	Microsoft	Tested on Win2003, works well with CA retrieval/certificate enrollment/CRL retrieval/certificate search, still need to check the feasibility of certificate renewal. ☺	1MW
OpenSCEP	open source™	Old support (openssl version must be earlier than 0.9.7 which is version of 2000). Kind of difficult to build the test environment.(to make it work, need to install /configure many library and servers) 😐	2MW
		Sum	>5MW

* Very possibly that OpenSCEP is not in the list we need to supported for the moment according to Georges' information.

Status of pre-study/PoC (1)

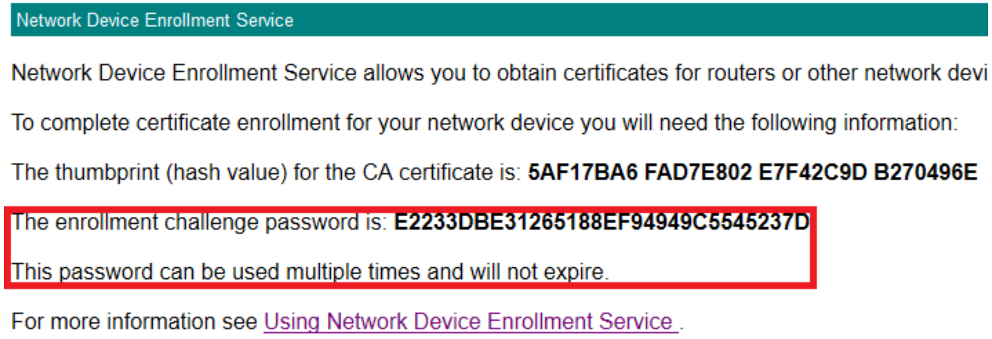
- OpenSCEP solution has been abandoned because seems there is no such requirement from market needs.
- According to latest news update from BNPP, the main solution is focused on MS SCEP server. OpenPKI is mentioned but obviously not be applied for SCEP.

- I use **VLE R100** software to do the SSCEP PoC, since the software of VLE is much same as the one of NOE IP, so it is much more meaningful to do it on VLE currently.
- The functions has been verified work well and correct with Windows2003 SCEP server.
  - Local Key-Pair generation.
  - Local p7 format request generation.
  - GETCA operation. -- require CA/RA certificate from SCEP server
  - ENROLL operation. -- request certificate from SCEP server
  - GETCRL operation. -- require CRL from SCEP server
  - GETCERT operation. -- require certificate from SCEP server according to serial number of certificate.
- Try to test renew feature then found Windows 2003 SCEP does not support "GetCACaps" operation, which means draft defined renewal operation cannot work with MS server.

* Very possibly that OpenSCEP is not in the list we need to supported for the moment according to Georges' information.

Status of pre-study/PoC (2)

- **Also found difference when try windows 2008:**
  - Windows 2008 allow to configure one password which can be re-used (verified in lab).



Network Device Enrollment Service

Network Device Enrollment Service allows you to obtain certificates for routers or other network devi

To complete certificate enrollment for your network device you will need the following information:

The thumbprint (hash value) for the CA certificate is: **5AF17BA6 FAD7E802 E7F42C9D B270496E**

The enrollment challenge password is: **E2233DBE31265188EF94949C5545237D**

This password can be used multiple times and will not expire.

For more information see Using Network Device Enrollment Service .

  - Windows 2008 by default and recommend open the SCEP server through HTTPS.
  - When SSCEP work with Win2008 SCEP server, not work for operation GETCRL, there is same issues reflect in internet but no fix yet, the only method from internet is to roll-back the SCEP server to 2003. ☹
    http://social.technet.microsoft.com/Forums/en-US/winserversecurity/thread/ac159186-219a-47ee-a55e-575f99a89ebe/
  - Win2003 does not support renewal function, Win2008 R2 SP1 need hotfix (http://support.microsoft.com/kb/2483564) to support “GetCACaps” ,both GetCACaps & renewal is verified work well.

Status of pre-study/PoC (3)

- **So we may need more detail information about customer environment.**
  - Is HTTPS required in customer side? (current PoC is based SSCEP which does not support http natively, we need to report https implementation in NOE-SIP if needed for HTTPs support, further effort is needed.)
  - Win2003 or Win2008 deployed? (Win2003 does not support renewal, win2008 need hotfix to support it)
  - GetCRL operation is not supported by SSCEP implementation currently with Win2008.

SCEP DEV in ALU hard sets (VxWorks Based)

- It is asked to apply unified solution to all range ALU sets of auto certificate distribution.
- Different level job is need to be done for this target. The cost evaluation (DEV/DOC only) is also provided below:

ALU Phone	Platform OS Type	Required Job	Cost
NOE (NOE-2G NOE-3G NOE-SIP VLE/VLE+)	Vxworks	Study how to generate private key/certificate request through OpenSSL library (no script supported).	2MW
		Select a valid open source for implementing SCEP client (e.g. SSCEP).	2MW
		Resolve the problem brought by no file system, 2nd dev on open source code. Some SCEP operation(GetCACaps) need to be added.*	3MW
		Define when to do the enrollment (step 3?). When to renew certificate?	1MW
		Interaction with initialization procedure.	2MW
		Local configuration in MMI	1MW
		Dev for new DM parameter	1MW
		Sum	12MW

*SSCEP has included http implementation, considered that no need to support https (depend on customer configuration policy).

SCEP DEV in ALU hard sets (Linux Based)

ALU Phone	Platform OS Type	Required Job	Cost
MIP (8082 VHE)	Linux	Study how to generate private key/certificate request through Openssl commands.	1MW
		Select a valid open source for implementing SCEP client (e.g. SSCEP).	2MW
		2nd dev on open source code. Some SCEP operation(GetCACaps) need to be added.	3MW
		Define when to do the enrollment (step 3?). When to renew certificate?	1MW
		Define when to do the enrollment, related to the interchange with main initialization procedure probably.	2MW
		Local configuration in MMI	1MW
		Dev for new DM parameter	1MW
		Sum	11MW

SCEP DEV in other ALU SW clients …

ALU Phone	Platform OS Type	Required Job	Cost
OTC PC?			

TBC

Open point

- How to deal with date/time validation problem when terminal don't has date/time information? Now we don't have date information at least before step 4, which means there is no date validation for certificate (server authentication) before step 4.

  [Closed]: For SIP phone, date/time check after step3(count on when sntp start); For NOE phone, date/time check after step5 (connected to system)
- Possibly to reuse ALU certificate key-pair to generate certificate request? Is it OK to use ALU key-pair instead of generate automatically? (enrollment of customer certificate in a terminal with ALU certificate only)

  [Closed]: Prefer to apply new key-pair since this function is mainly to customer certificate deployment for security reason.
- How to transmit challenge phrase? How to transmit it securely?
- SCEP don't design a mechanism to notify client about the certificate expiration problem, only way is terminal to check it during initialization, anyone has better method?

  [Closed] Terminal decide itself according the date/time information it get.
- How to trigger set to launch SCEP client when working with OXE if there is special requirement to deploy new certificates , design a new message in OXE?

- There is a interesting document which mentioned some advices about the authentication of untrusted devices, should it be taken account in our server plan (requester authentication):

http://www.css-security.com/wp-content/uploads/2012/05/*SCEP-and-Untrusted-Devices*.pdf

- …

Helpful link

- SCEP draft* link:

http://tools.ietf.org/html/draft-nourse-scep-23

- OpenSCEP** link:

http://openscep.othello.ch/
http://openscep.othello.ch/download/openscep-0.4.2.tar.gz

- SSCEP*** link:

ftp://ftp.freebsd.org/pub/FreeBSD/ports/distfiles/sscep.tgz
https://github.com/certnanny/sscep

- FOSS link:

http://foss.app.alcatel-lucent.com/foss/products/display/1244/
http://foss.app.alcatel-lucent.com/foss/products/display/5964/

* The newest draft version is 23
** OpenSCEP is based on GPL ☹; Support most of draft version 5.
*** SSCEP is based on BSD ☺; Support draft version 6&11 (**TBC**).

Complements

- Customer requirements
- Use case story

Customer serviceability requirements

Device certificates customization required for 802.1x TLS authentication

- BNPP (PER2410)
  - **PKI? SCEP? To confirm**
  - **30k** IPTouch serie 8
  - 1M€ business per year

- French Foreign Ministry (PER2315)
  - OpenTrust PKI
  - Autoenrollment on 15000 Linux equipments, required for **4k** IPTouch serie 8
  - SCEP with PSK
  - No web based autoenrollment portal
  - 400k to 600k€ business per year

- SOE/Cubicon (to be expected soon)
  - Microsoft CA
  - 802.1X. TLS + customized device certificate for approx. **xTBC** IPTouch serie 8 devices
  - Current deployment done manually

BNPP detail requirement 22/2/2013

① BNPP told us that they accepted SCEP; it seems to be the best solution for the voice part, BNPP uses the auto-enrollment via the Microsoft mechanisms for their Desktop, laptop and domain controllers.

② PKI used by BNPP : OpenTrust

③ The certificates will be used for NAc (802.1x) but BNPP wants to know if it's possible to use the certificates for the encryption.

④ BNPP uses certificates for their tablets, laptops, desktops and Microsoft servers

⑤ BNPP is waiting an automatic and secure process for the auto-enrollment.

⑥ BNPP is waiting an automatic and secure process for the renewal

SCEP impact on Device Configuration

- For IPTouch only, follow with impact analysis on
  - OXE config management: lanpbx.cfg for integrating
    - URL
    - PSK
    - Enrollment/Renewal/Revokation flag
  - 8770
    - Support of new OXE config parameters

- For MyIC phone, follow with impact analysis on
  - OpenTouch OAM&P
  - 8770

A- Enrollment use case

The device has a default factory cert, customer decides to replace by its own customer certificate

User PoV

- No interaction with user

Admin PoV

1- Autoenrollment based on PSK

- Telephony admin provides SCEP server URL on device configuration
- Telephony admin configures SCEP pre-shared key(PSK or challengePassword) on SCEP server and in device configuration
- Telephony admin triggers autoenrollment phase remotely (enrollment flag in device configuration?)
- Device creates its key pair and certificate request
- Device sends its certificate request to the SCEP server
- SCEP server checks PSK, and if OK automatically approves requests
- PKI CA signs the certificate requests
- PKI CA sends back signed certificate to the device
- Device associates the received signed certificate with its key pair

2- Enrollment with explicit PKI approbation, without PSK

- Telephony admin provides SCEP server URL on device configuration
- Telephony admin triggers autoenrollment phase remotely (enrollment flag in device configuration?)
- Device creates its key pair and certificate request
- Device sends its certificate request to the SCEP server
- SCEP server relays the request to the Registration Authority (RA)
- PKI admin checks the certificate requests and approves (one by one or bunch of them...)
- PKI CA signs approved certificate requests
- PKI CA sends back signed certificate to the device
- Device associates the received signed certificate with its key pair

B- Renewal use case

Device has a customer certificate cert#1 that comes close to expiration. The device must request a new customer certificate in replacement.

User PoV
- No interaction with user

Admin PoV
Previous key pair reuse depends on the server capability to support GetCACaps options, described in Appendix C. of SCEP Draft.

1- Automatic renewal with current key pair
- Telephony admin provides SCEP server URL on device configuration
- Telephony admin triggers autoenrollment phase remotely (enrollment flag in device configuration?)
- Device creates its key pair and certificate request
- Device sends certificate request signed with current keys to the SCEP server
- SCEP server checks that request comes from an already known end entity, and if OK automatically approves requests
- PKI CA signs the certificate requests
- PKI CA sends back signed certificate to the device
- Device associate the received signed certificate with its key pair

2- if no renewal support, we can replay scenario A.1 or A.2.

C- Certificate revocation

The customer certificate must be revoked by the PKI admin:
Two possible ways:

- either we support SCEP revocation procedures
- or, because the device key store can only contains 1 certificate at at time, revocation can be seen as a simple certificate renewal

We recommend second case:

1. GetCRL when SCEP configuration is on, check whether own certificate is listed in CRL, then revoke it locally and do A.1 or A.2.
2. Inquiry the status of the validation of local certificate by OCSP (I noticed that OCSP is supported by OpenPKI)
3. When terminal get date/time information, check the valid time duration of current certificate, if it is out of time (expired I supposed, need to check not yet case?), revoke it locally and do A.1 or A.2.

User PoV

- No interaction with user

Admin PoV

- PKI admin requests a certificate revokation on PKI servers side
- Device does not need to know or perform anything

AT
THE
SPEED
OF
IDEAS™

www.alcatel-lucent.com