Fraunhofer-Institut für Digitale Medientechnologie IDMT

Simple Certificate Enrollment Protocol

Ives Steglich

Munich, 12th October 2004

Fraunhofer Institut Digitale Medientechnologie

Overview

- SCEP Simple Certificate Enrollment Protocol
  - Goals
  - Basics
  - Message Format
  - Messages
  - Transaction Model
  - Requests
- Integration into OpenCA
  - Interface
  - Supported Operations
  - Open Issues

Overview

- SCEP Simple Certificate Enrollment Protocol
  - Goals
  - Basics
  - Message Format
  - Messages
  - Transaction Model
  - Requests
- Integration into OpenCA
  - Supported Operations
  - Open Issues

SCEP :: Goals

Primary

- CA and RA public key distribution
- Certificate enrollment
- Certificate revocation (manual)
- Certificate query
- CRL query

Secondary

- Certificate renewal
- CA rollover
- Confidantiality of internal networkdata ?

SCEP :: Basics

Transportprotocols

- HTTP (Get & POST)
- LDAP

Cryptographic Protocols & Containers

- PKCS#7 – Envelop and Confidentiality
- PKCS#10 – Certificate Requests

Cryptographic Algorithms

- RSA - no others supported till now for keys
- DES - used in PKCS#7 encryption portion
- MD5 - as digest for encrypted message part

Others

- Message based protocol: Request -> Response
- Actions always triggerd by Client

SCEP :: Messages

PKCSReq

CertRep

GetCertInitial

GetCert

GetCRL

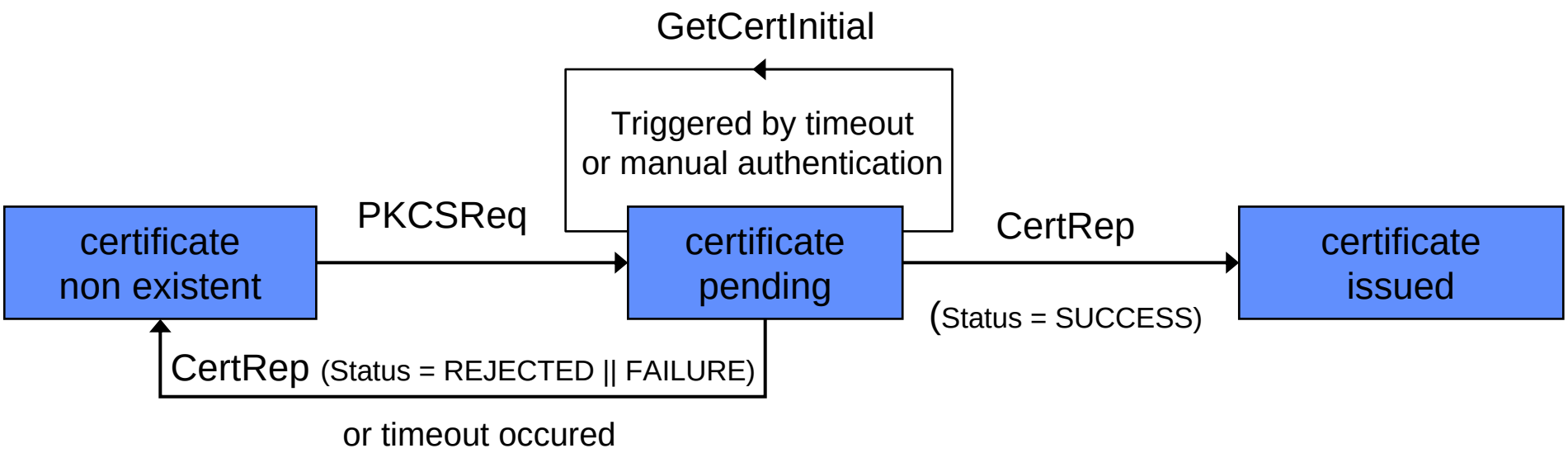
GetCACert

GetCACertChain (since rev. 3)

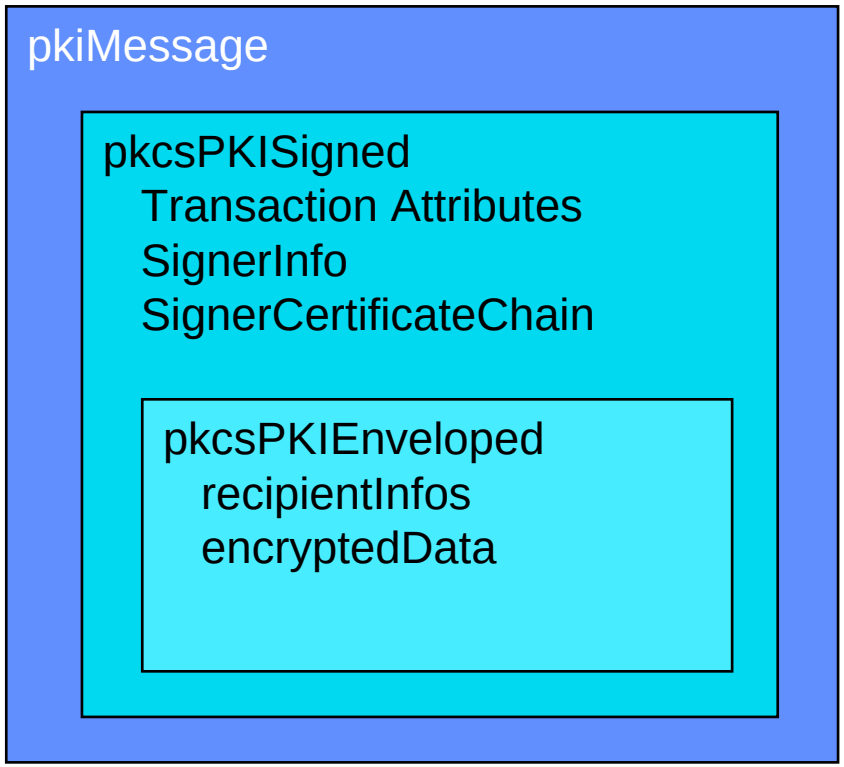
GetCACaps (since rev. 10)

GetNextCACert (since rev. 10)

SCEP :: Transaction Model



SCEP :: Basic Massageformat PKCS#7



pkiMessage:
outer PKCS#7 container

pkcsPKISigned
contains signed attributes
- transactin attributes
- etc.

pkcsPKIEnveloped
contains encrypted information
- PKCS#10 Request
- issued certificate
- crl
- empty
depending on request and reply
from the scep-interface

Messageformat :: Authenticated Transaction Attributes I

Authenticated Transaction Attributes

transactionID	unique transaction identifier - required
messageType	how to handle the content / what to expect - required
pkiStatus	only in response
failinfo	only in error condition
senderNonce	prevent reply attacs – required in request and response
recipientNonce	prevent reply attacs – required in response

Messageformat :: Authenticated Transaction Attributes II

messageTypes

PKCSReq (19)	Permits use of PKCS#10 certificate request
CertRep (3)	Response to certificate or CRL request
GetCertInitial (20)	Certificate polling in manual enrollment
GetCert (21)	Retrieve a certificate
GetCRL (22)	Retrieve a CRL or CRL-Distributionpoint

pkiStatus

SUCCESS (0)	request granted
FAILURE (2)	request rejected
PENDING (3)	request pending for manual approval.

Messageformat :: Failcodes

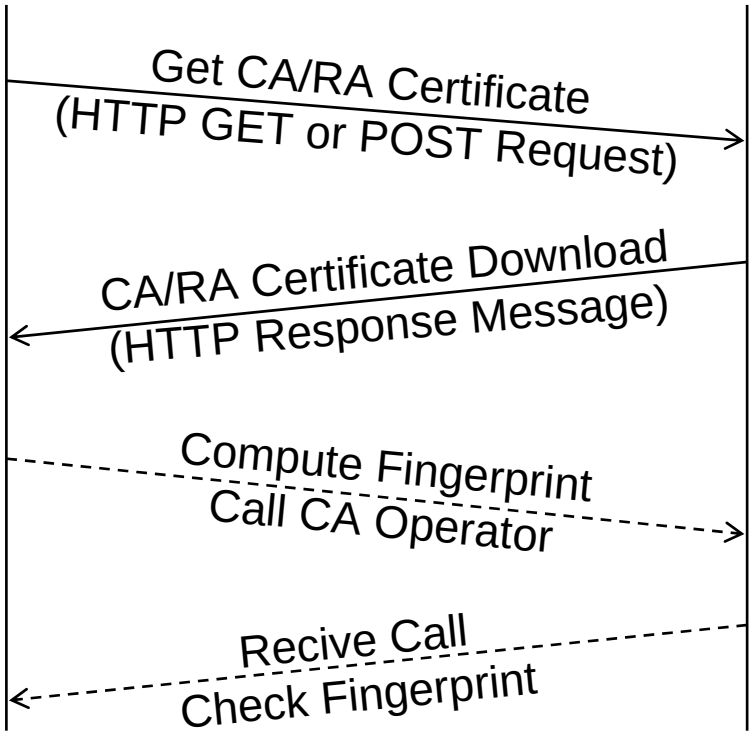
failinfo

badAlg (0)	Unrecognized or unsupported algorithm ident
badMessageCheck (1)	integrity check failed
badRequest (2)	transaction not permitted or supported
badTime (3)	Message time field was not sufficiently close to the system time
badCertId (4)	No certificate could be identified matching the provided criteria

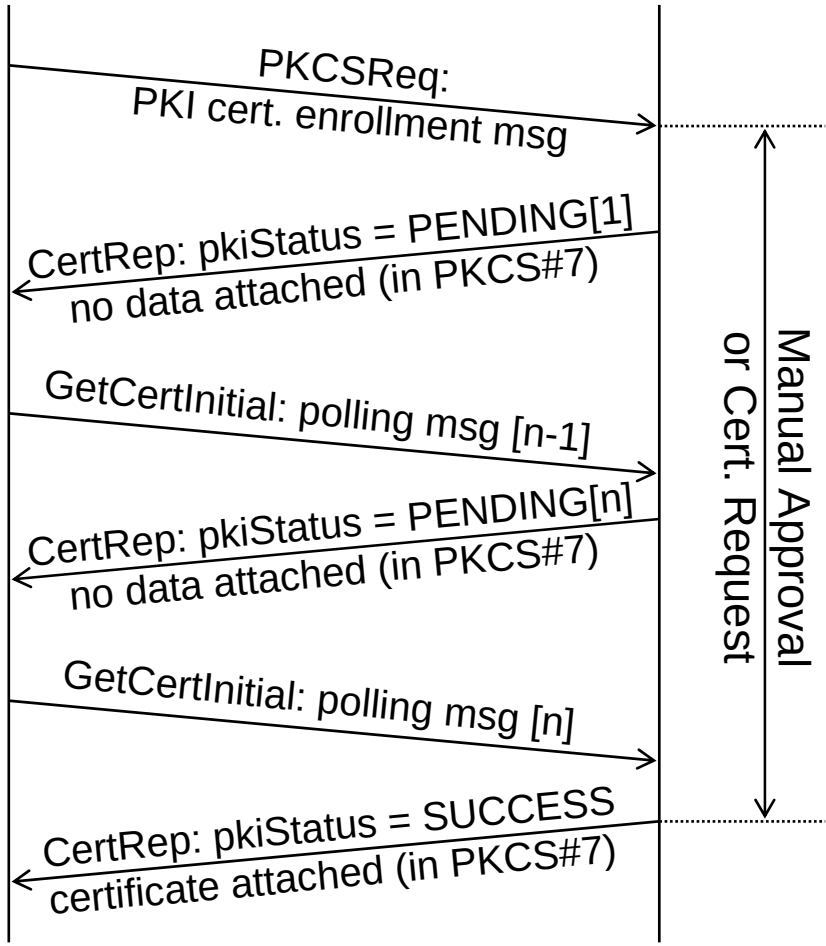
OpenCA mainly uses badRequest for ANY error inside OpenCA
so kind of problems may be difficult to trace on client-side

SCEP :: Communication Examples

CA/RA Certificate Distribution
(performed only once usaly)



Enrollment of an Certificate



SCEP :: Requests I

Based on PKCS#10 contains

- subject "the requestor's subject name“
- challengePassword
- extensions (x.509 v3)

ChallengePassword

- automatic enrollment;
  (requires preauthentication of clients)
- as revocation pin for verification against the ca

SCEP :: Requests II

Renewal

- if used issued Cert instead of selfsigned request should be handled as renewal

- if request is send after half of validity time may also be handled as renewal request

- behavior dependent on CA Policy

CA Rollover

- use newly introduced msg: GetNextCACert if supported by CA

Request New Cert for new CA/RA Cert

- use the new CA/RA cert in the requesting envelop instead of the actual CA/RA cert

Overview

- SCEP Simple Certificate Enrollment Protocol
  - Goals
  - Basics
  - Message Format
  - Messages
  - Transaction Model
  - Requests
- Integration into OpenCA
  - Supported Operations
  - Open Issues

Integration into OpenCA

cmdline based tookit openca-scep (c-code)

- can parse and create scep-conform pkcs#7 msg
- interface similar to openssl cmd-interfaces
- doesn’t do transaction or error handling

OpenCA created a new interface called SCEP

- consists of two functions
  - one for ca/ra certificate distribution
  - one for the operations itself
- transaction state and error checking managed inside those functions
- openca database keeps track of transactions

OpenCA :: Supported Operations

PKCSReq

CertRep

GetCertInitial

GetCert

GetCRL

GetCACert

GetCACertChain

GetCACaps (planed for 0.9.3)

GetNextCACert (planed for 0.9.3)

OpenCA :: Open Issues

Handling of renewals

- not implemented yet
- planed for 0.9.3

Preauthentication and automatic processing

- OpenCA backend doesn’t support automatic enrollment and preauthenticatin yet
- planed for 0.9.3

Crldistributionpoints

- sends back always CRL in response
- CDP instead of CRL not implemented yet
- planed as configuration option for 0.9.3

CA Rollover

- planed for 0.9.3