

OMA DM: VPN Client PKI Management Object Specification

Version 1.0; April 30, 2008

OMA Device
Management

NOKIA

Copyright © 2008 Nokia Corporation. All rights reserved.

Nokia and Forum Nokia are trademarks or registered trademarks of Nokia Corporation. Other product and company names mentioned herein may be trademarks or trade names of their respective owners.

Disclaimer

The information in this document is provided “as is,” with no warranties whatsoever, including any warranty of merchantability, fitness for any particular purpose, or any warranty otherwise arising out of any proposal, specification, or sample. This document is provided for informational purposes only.

Nokia Corporation disclaims all liability, including liability for infringement of any proprietary rights, relating to implementation of information presented in this document. Nokia Corporation does not warrant or represent that such use will not infringe such rights.

Nokia Corporation retains the right to make changes to this document at any time, without notice.

License

A license is hereby granted to download and print a copy of this document for personal use only. No other license to any other intellectual property rights is granted herein.

Contents

1	Introduction.....	6
1.1	Documentation conventions.....	6
1.2	Supported management operations.....	6
1.3	Supported manageable data.....	6
1.4	Long-lasting commands.....	6
2	PKI management object nodes.....	7
2.1	List of management nodes.....	7
2.2	General.....	8
2.2.1	NokiaPKI.....	8
2.2.2	NokiaPKI/Logon.....	8
2.2.3	NokiaPKI/Logoff.....	9
2.2.4	NokiaPKI/KeyStore.....	9
2.2.5	NokiaPKI/CertStore.....	9
2.2.6	NokiaPKI/General.....	10
2.2.7	NokiaPKI/General/CertApplications.....	10
2.3	Certificates.....	10
2.3.1	NokiaPKI/Cert.....	10
2.3.2	NokiaPKI/Cert/<X>.....	11
2.3.3	NokiaPKI/Cert/<X>/Type.....	11
2.3.4	NokiaPKI/Cert/<X>/Format.....	11
2.3.5	NokiaPKI/Cert/<X>/SerialNumber.....	11
2.3.6	NokiaPKI/Cert/<X>/IssuerName.....	12
2.3.7	NokiaPKI/Cert/<X>/FingerprintAlg.....	12
2.3.8	NokiaPKI/Cert/<X>/FingerprintValue.....	12
2.3.9	NokiaPKI/Cert/<X>/ValidityBegin.....	12
2.3.10	NokiaPKI/Cert/<X>/ValidityEnd.....	13
2.3.11	NokiaPKI/Cert/<X>/SubjectName.....	13
2.3.12	NokiaPKI/Cert/<X>/SubjectAltName.....	13
2.3.13	NokiaPKI/Cert/<X>/KeyURI.....	13
2.3.14	NokiaPKI/Cert/<X>/KeyID.....	14
2.3.15	NokiaPKI/Cert/<X>/KeyUsage.....	14
2.3.16	NokiaPKI/Cert/<X>/Deletable.....	14
2.3.17	NokiaPKI/Cert/<X>/Trusted.....	15
2.3.18	NokiaPKI/Cert/<X>/Applicability.....	15
2.3.19	NokiaPKI/Cert/<X>/Content.....	15
2.4	Certificate signing requests.....	15
2.4.1	NokiaPKI/CertReq.....	16
2.4.2	NokiaPKI/CertReq/<X>.....	16
2.4.3	NokiaPKI/CertReq/<X>/SubjectName.....	16

2.4.4	NokiaPKI/CertReq/<X>/RFC822Name	17
2.4.5	NokiaPKI/CertReq/<X>/KeyURI.....	17
2.4.6	NokiaPKI/CertReq/<X>/KeyLength.....	18
2.4.7	NokiaPKI/CertReq/<X>/Content.....	18
2.5	Private keys	18
2.5.1	NokiaPKI/PrivKey.....	18
2.5.2	NokiaPKI/PrivKey/<X>.....	19
2.5.3	NokiaPKI/PrivKey/<X>/KeyType.....	19
2.5.4	NokiaPKI/PrivKey/<X>/KeyLength	19
2.5.5	NokiaPKI/PrivKey/<X>/KeyID.....	19
2.6	PKCS #12.....	20
2.6.1	NokiaPKI/PKCS12	20
2.6.2	NokiaPKI/PKCS12/<X>	20
2.6.3	NokiaPKI/PKCS12/<X>/Password	20
2.6.4	NokiaPKI/PKCS12/<X>/Deletable.....	21
2.6.5	NokiaPKI/PKCS12/<X>/Applicability.....	21
2.6.6	NokiaPKI/PKCS12/<X>/Content.....	21
3	Management object usage.....	22
3.1	General.....	22
3.2	Certificate management (Cert node)	22
3.3	Certificate request management (CertReq node).....	23
3.4	Private key management (PrivKey node).....	24
3.5	PKCS #12 management (PKCS12 node).....	25
4	Terms and abbreviations.....	26
5	References	27
6	Evaluate this resource	28

Change history

April 30, 2008	Version 1.0	Initial document release

1 Introduction

This document describes an OMA Device Management (DM) [2] management object for the management of PKI data related to the use of the Nokia Mobile VPN Client software [3]. This document is applicable for S60 3rd Edition, Feature Pack 1.

Although the goal in the design of the PKI management object has been to fulfill the PKI management needs of the Nokia Mobile VPN Client software, the idea has also been to keep the PKI management object as generic as possible and thus applicable to any PKI management needs.

Support for the PKI management object is optional. This means that a mobile device that supports OMA DM does not necessarily support the PKI management object. However, if a mobile device does support the PKI management object, then the device must support all management nodes that make up the management object.

1.1 Documentation conventions

Code is written in the `Courier` font.

Dynamic name of a management node is denoted with '<X>'. The name must be unique among its siblings. For OMA DM server-added PKI objects, the OMA DM server selects the names for the nodes according to server specific rules. The client automatically creates the names for all PKI objects that are configured to the system via non OMA DM mechanisms. For such nodes, the name of the node is a random number formatted as a string and prefixed with the string "cli", for example "cli123".

1.2 Supported management operations

Management servers can use the PKI management object to:

- List, get, add, update, and delete CA and user certificates.
- List, get, create (cause the device to create), and delete certificate requests.
- List and delete private keys.
- Add PKCS #12 object, causing client to add certificates and private keys.

1.3 Supported manageable data

The PKI management object allows management servers to manage both data that has been initially added to devices through OMA DM, and data that has been added to devices through some other mechanisms (for example through the UI of the device).

1.4 Long-lasting commands

Certain management operations on the PKI management object may take a relatively long time to complete. This is because of the possible user interaction (prompting for the key store password) or lengthy command processing (for example, private key generation) involved. Behaviorally, these commands are very similar to the user interaction commands described in reference document [4] and are handled correspondingly. In particular, this means that all management operations are synchronous in nature and return a status response to the server only after the processing of the operation is really completed.

2 PKI management object nodes

This chapter describes the management nodes that constitute the PKI management object. The Device Description Framework properties (Scope, Occurrence, Access type, Format, and Value) used in the descriptions are defined in reference document [5].

All URI values in the management object are given with the root of the management tree as the starting point. As specified in reference document [5], this can be denoted by beginning each URI with “./” or “” (nothing).

2.1 List of management nodes

The list below summarizes all management nodes described later in this document.

- NokiaPKI
- NokiaPKI/Logon
- NokiaPKI/Logoff
- NokiaPKI/KeyStore
- NokiaPKI/CertStore
- NokiaPKI/General
- NokiaPKI/General/CertApplications
- NokiaPKI/Cert
- NokiaPKI/Cert/<X>
- NokiaPKI/Cert/<X>/Type
- NokiaPKI/Cert/<X>/Format
- NokiaPKI/Cert/<X>/SerialNumber
- NokiaPKI/Cert/<X>/IssuerName
- NokiaPKI/Cert/<X>/FingerprintAlg
- NokiaPKI/Cert/<X>/FingerprintValue
- NokiaPKI/Cert/<X>/ValidityBegin
- NokiaPKI/Cert/<X>/ValidityEnd
- NokiaPKI/Cert/<X>/SubjectName
- NokiaPKI/Cert/<X>/SubjectAltName
- NokiaPKI/Cert/<X>/KeyURI
- NokiaPKI/Cert/<X>/KeyID
- NokiaPKI/Cert/<X>/KeyUsage
- NokiaPKI/Cert/<X>/Deletable
- NokiaPKI/Cert/<X>/Trusted
- NokiaPKI/Cert/<X>/Applicability
- NokiaPKI/Cert/<X>/Content
- NokiaPKI/CertReq
- NokiaPKI/CertReq/<X>
- NokiaPKI/CertReq/<X>/SubjectName

- NokiaPKI/CertReq/<X>/RFC822Name
- NokiaPKI/CertReq/<X>/KeyURI
- NokiaPKI/CertReq/<X>/KeyLength
- NokiaPKI/CertReq/<X>/Content
- NokiaPKI/PrivKey
- NokiaPKI/PrivKey/<X>
- NokiaPKI/PrivKey/<X>/KeyType
- NokiaPKI/PrivKey/<X>/KeyLength
- NokiaPKI/PrivKey/<X>/KeyID
- NokiaPKI/PKCS12
- NokiaPKI/PKCS12/<X>
- NokiaPKI/PKCS12/<X>/Password
- NokiaPKI/PKCS12/<X>/Deletable
- NokiaPKI/PKCS12/<X>/Applicability
- NokiaPKI/PKCS12/<X>/Content

2.2 General

2.2.1 NokiaPKI

The `NokiaPKI` interior node is the parent of all PKI related management tree nodes. If this node can be found from a client's management tree, then the client can be assumed to support all management nodes under this parent node.

The name and version of the PKI management object described in this document is `com.nokia.devman/1.0/pki`. It is defined in the `Type` property of the `NokiaPKI` node.

Scope	Occurrence	Access type
Permanent	One	Get
Format	Value	
Node		

2.2.2 NokiaPKI/Logon

If the user key store is in use, the management operations that involve private keys require that the client asks a key store password from the client user at some point. This user interaction can be controlled through the `Logon` and `Logoff` nodes. A `Replace` command on the `Logon` node causes the client to prompt the user for the key store password, if the password has not been prompted for already. A `Replace` command on the `Logoff` node resets the client's state in such a way that the next logon or private key management operation will cause the client to prompt the user for the key store password again. The client may also automatically log off from the PKI store according to its own rules.

To ensure the user-friendliness (responsiveness) of the Logon phase, the `Replace` command on the `Logon` node should be sent to the client in its own OMA DM message.

Scope	Occurrence	Access type
Permanent	One	Replace The Replace command is used to simulate an Exec command.
Format	Value	
Null		

2.2.3 NokiaPKI/Logoff

This leaf node is a command node that can be used to cause the client to log off from the user key store. As a result, the next logon or management operation that requires private key access will cause the client to prompt the user for the key store password again.

Scope	Occurrence	Access type
Permanent	One	Replace The Replace command is used to simulate an Exec command.
Format	Value	
Null		

2.2.4 NokiaPKI/KeyStore

This leaf node is used to select the key store type. User key store is selected by default. If the device key store is set but the device does not support it, an error code is returned and the user key store is selected. The `KeyStore` value must be synchronized with the `CertStore` value. If the user key store is selected, the user certificate store must be selected. If the device key store is selected, the device certificate store must be selected.

Scope	Occurrence	Access type
Permanent	One	Replace
Format	Value	
Int	1 – user key store (default value) 2 – device key store	

2.2.5 NokiaPKI/CertStore

This leaf node is used to select the certificate store type. The user certificate store is selected by default. If the device certificate store is selected but the device does not support it, an error code is returned and the user certificate store is selected. The `KeyStore` value must be synchronized with the `CertStore` value. If the user key store is selected, the user certificate store must be selected. If the device key store is selected, the device certificate store must be selected.

Scope	Occurrence	Access type
Permanent	One	Replace

Format	Value
Int	1 – user certificate store (default value) 2 – device certificate store

2.2.6 NokiaPKI/General

This interior node is the parent of management nodes that describe general information about the PKI management object.

Scope	Occurrence	Access type
Permanent	One	Get
Format	Value	
Node		

2.2.7 NokiaPKI/General/CertApplications

This leaf node lists the possible applications for which CA certificates can be marked as applicable.

Scope	Occurrence	Access type
Dynamic	One	Get
Format	Value	
Xml	<p>A list of application name – ID pairs in XML format.</p> <p>DTD:</p> <pre><!ELEMENT CertApps (App)> <!ELEMENT App EMPTY> <!ATTLIST App id CDATA #REQUIRED> <!ATTLIST App name CDATA #IMPLIED></pre> <p>Example:</p> <pre><CertApps> <App id='268441661' name='Internet' /> <App id='270498195' name='VPN' /> ... </CertApps></pre>	

2.3 Certificates

This section describes the management tree structure and management nodes that can be used to manage certificates.

2.3.1 NokiaPKI/Cert

This interior node is the parent of all management tree nodes that are used to manage certificates.

Scope	Occurrence	Access type
Permanent	One	Get
Format	Value	
Node		

2.3.2 NokiaPKI/Cert/<X>

This interior node together with its descendant nodes represents a single certificate. A certificate should be added to and deleted from a client as a single entity. To delete a certificate from a device, the management server should simply issue a single `Delete` command on a certificate node (<X>).

Scope	Occurrence	Access type
Dynamic	ZeroOrMore	Add, Delete, Get, Replace The <code>Replace</code> command can only be used for setting the ACL of this node.
Format	Value	
Node		

2.3.3 NokiaPKI/Cert/<X>/Type

This leaf node specifies the type of the certificate.

Scope	Occurrence	Access type
Dynamic	One	Add, Get
Format	Value	
Int	1 – CA certificate 2 – user certificate	

2.3.4 NokiaPKI/Cert/<X>/Format

This leaf node specifies the format of the certificate. The value of this node is read from the certificate and is thus read-only.

Scope	Occurrence	Access type
Dynamic	One	Get
Format	Value	
Int	1 – X.509 v3 certificate (see reference document [6])	

2.3.5 NokiaPKI/Cert/<X>/SerialNumber

This leaf node specifies the serial number of the certificate in binary DER format. The value of this node is read from the certificate and is thus read-only.

Scope	Occurrence	Access type
Dynamic	One	Get
Format	Value	
Bin	The serial number of the certificate in binary DER format.	

2.3.6 NokiaPKI/Cert/<X>/IssuerName

This leaf node specifies the name of the certificate issuer in binary DER format. The value of this node is read from the certificate and is thus read-only.

Scope	Occurrence	Access type
Dynamic	One	Get
Format	Value	
Bin	The name of the certificate issuer in binary DER format.	

2.3.7 NokiaPKI/Cert/<X>/FingerprintAlg

This leaf node specifies the algorithm that has been used to calculate the fingerprint value in the `FingerprintValue` node. Note that this node is read-only.

Scope	Occurrence	Access type
Dynamic	One	Get
Format	Value	
Int	1 – MD5 2 – SHA-1	

2.3.8 NokiaPKI/Cert/<X>/FingerprintValue

This leaf node contains a fingerprint of the certificate. The value of this node is derived from the certificate and is thus read-only.

Scope	Occurrence	Access type
Dynamic	One	Get
Format	Value	
Bin	The certificate fingerprint calculated with the algorithm specified in the <code>Alg</code> sibling node, in binary format.	

2.3.9 NokiaPKI/Cert/<X>/ValidityBegin

This leaf node specifies the date and time on which the certificate validity period begins. The value of this node is read from the certificate and is thus read-only.

Scope	Occurrence	Access type
Dynamic	One	Get
Format	Value	
Chr	The date and time on which the certificate validity period begins expressed in the ISO 8601 format (CCYYMMDD'T'hhmmss'Z'). For example, "20010824T133000Z".	

2.3.10 NokiaPKI/Cert/<X>/ValidityEnd

This leaf node specifies the date and time on which the certificate validity period ends. The value of this node is read from the certificate and is thus read-only.

Scope	Occurrence	Access type
Dynamic	One	Get
Format	Value	
Chr	For applicable certificate formats, the date and time on which the certificate validity period ends expressed in the ISO 8601 format (CCYYMMDD'T'hhmmss'Z'). For example, "20010824T133000Z".	

2.3.11 NokiaPKI/Cert/<X>/SubjectName

This leaf node specifies the name of the certificate subject in binary DER format. The value of this node is read from the certificate and is thus read-only.

Scope	Occurrence	Access type
Dynamic	One	Get
Format	Value	
Bin	The name of the certificate subject in binary DER format.	

2.3.12 NokiaPKI/Cert/<X>/SubjectAltName

This leaf node specifies the subject alternative name extension of the certificate in binary DER format. The value of this node is read from the certificate and is thus read-only.

Scope	Occurrence	Access type
Dynamic	One	Get
Format	Value	
Bin	The subject alternative name extension of the certificate in binary DER format. The value can also be empty.	

2.3.13 NokiaPKI/Cert/<X>/KeyURI

This leaf node specifies the management tree URI of the private key that corresponds to the public key that the certificate contains. This node is non-empty for client certificates, the associated private key of which is present in the client. The value of this node is deduced from the certificate and is thus read-only.

Scope	Occurrence	Access type
Dynamic	One	Get
Format	Value	
Chr	The URI of the associated private key node in the management tree. The URI is given relative to the management tree root and does not use the “./” prefix, for example, “NokiaPKI/PrivKey/123”. The value is empty if the private key does not reside in the client’s PKI store.	

2.3.14 NokiaPKI/Cert/<X>/KeyID

This leaf node specifies an identifier of the public key that the certificate contains. The value of this node is deduced from the certificate and is thus read-only.

Scope	Occurrence	Access type
Dynamic	One	Get
Format	Value	
Bin	160-bit SHA-1 hash of the certificate public key (excluding the tag, length, and number of unused bits).	

2.3.15 NokiaPKI/Cert/<X>/KeyUsage

This leaf node specifies the purpose of the private key that corresponds to the certificate. The value of this node is read from the certificate and is thus read-only.

Scope	Occurrence	Access type
Dynamic	One	Get
Format	Value	
Chr	A string representation of the certificate key usage bits expressed according to the <code><bstring></code> rule specified in [7]. See reference document [6] for the possible values. The value can also be empty, if key usage information is not present in the certificate.	

2.3.16 NokiaPKI/Cert/<X>/Deletable

This leaf node tells whether the certificate is a deletable or non-deletable certificate. A non-deletable certificate is a certificate that cannot be deleted from a device’s PKI store through the UI of the device after it has been added there. However, it is possible to delete a non-deletable certificate via OMA DM.

Scope	Occurrence	Access type
Dynamic	One	Add, Get
Format	Value	
Bool	True if the certificate is deletable, false if not. If this setting is not specified for a certificate when the certificate is added to a client, the default value is true.	

2.3.17 NokiaPKI/Cert/<X>/Trusted

This leaf node specifies whether the certificate is trusted, that is, whether it can be used for authenticating servers or other types of entities.

Scope	Occurrence	Access type
Dynamic	ZeroOrOne	Add, Get, Replace
Format	Value	
Bool	True if the certificate is trusted, false if not. If this setting is not specified for a certificate when the certificate is added to a client, the default value is true.	

2.3.18 NokiaPKI/Cert/<X>/Applicability

This leaf node defines the purposes or application areas (for example, SSL/TLS, application installation, VPN) for which the certificate is marked as applicable.

Scope	Occurrence	Access type
Dynamic	ZeroOrOne	Add, Get, Replace
Format	Value	
Xml	A list of application IDs using the XML format defined in the NokiaPKI/General/CertApplications node description. If this setting is not specified for a certificate when the certificate is added to a client, the applicability list for the certificate is empty. Example: <pre><CertApps> <App id='268441661' name='Internet' /> <App id= '270498195' name='VPN' /> ... </CertApps></pre>	

2.3.19 NokiaPKI/Cert/<X>/Content

This leaf node stores the actual certificate content as a single large binary object.

Scope	Occurrence	Access type
Dynamic	One	Add, Get
Format	Value	
Bin	The certificate content in binary DER format. Note that this is not the same as base64-encoded certificate format (with or without the PEM headers).	

2.4 Certificate signing requests

This section describes the management tree structure and management nodes that can be used to manage certificate requests.

2.4.1 NokiaPKI/CertReq

This interior node is the parent of all management tree nodes that are used to manage certificate requests.

Scope	Occurrence	Access type
Permanent	One	Get
Format	Value	
Node		

2.4.2 NokiaPKI/CertReq/<X>

This interior node together with its descendant nodes represents a single certificate request. A certificate request should be created and deleted from a client as a single entity. To delete a certificate request from a device, the management server should simply issue a single `Delete` command on a certificate request node (<X>).

The addition of this node and its descendant nodes to the client causes the client to create a certificate request with the parameters specified in the descendant nodes (for example `SubjectName`). The generated certificate request can be read from the client through the `Content` node.

The creation of a certificate request requires a private key, or more precisely a public-private key pair. The public key is included in the certificate request (and eventually in the certificate) and the private key is used to sign the certificate request.

A certificate request can be created in two ways. In the first case, the associated private key already exists in the device and is identified through the `KeyURI` node. In the second case, the private key does not yet exist and is created during the certificate request creation process. In this case, the length of the private key can be specified in the `KeyLength` node. The default type of the implicitly created private key is RSA. After the certificate request creation phase, the implicitly created private key appears in the management tree like any other private key that has been configured to the client through some non-DM mechanism.

If the user key store is used, the use of a private key in the client is protected by a password. The client user is prompted for the password as a part of the certificate request creation, unless it has been asked from the user already earlier, for example, as a result of a `Replace` command on the `NokiaPKI/Logon` node (see Section 2.2.2). For usability reasons, the use of the `Logon` node is encouraged. The user is not prompted for the password, if the device key store is in use.

Scope	Occurrence	Access type
Dynamic	ZeroOrMore	Add, Delete, Get, Replace The <code>Replace</code> command can only be used for setting the ACL of this node.
Format	Value	
Node		

2.4.3 NokiaPKI/CertReq/<X>/SubjectName

This leaf node specifies the subject name to be placed on the certificate request.

Scope	Occurrence	Access type
Dynamic	One	Add
Format	Value	
Chr	A string representation of the subject distinguished name in the format specified in reference document [8]. See Table 1 for the supported attribute types.	

Attribute type	Short name	OID
commonName	CN	2.5.4.3
surname	SN	2.5.4.4
serialNumber	-	2.5.4.5
countryName	C	2.5.4.6
localityName	L	2.5.4.7
stateOrProvinceName	ST	2.5.4.8
organizationName	O	2.5.4.10
organizationalUnitName	OU	2.5.4.11
title	-	2.5.4.12
givenName	-	2.5.4.42
initials	-	2.5.4.43
generationQualifier	-	2.5.4.44
dnQualifier	-	2.5.4.46
domainComponent	DC	0.9.2342.19200300.100.1.25

Table 1: Supported attribute types in subject names

2.4.4 NokiaPKI/CertReq/<X>/RFC822Name

This leaf node specifies the `rfc822Name` subject alternative name extension to be placed on the certificate request. If this node has an empty value, no subject alternative name is placed on the certificate request.

Scope	Occurrence	Access type
Dynamic	One	Add
Format	Value	
Chr	An "addr-spec" as defined in [9]. An <code>addr-spec</code> has the form "local-part@domain".	

2.4.5 NokiaPKI/CertReq/<X>/KeyURI

This leaf node specifies the management tree URI of the private key that is associated with this certificate request. During a certificate request creation process, if this node value is specified, the referenced private key (actually a public-private key pair) is used to create the certificate request. In this case, the referenced key pair must be present in the client in order for the certificate request generation to succeed.

Scope	Occurrence	Access type
Dynamic	One	Add
Format	Value	
Chr	The URI of the associated private key node in the management tree. The URI is given relative to the management tree root and does not use the “./” prefix. For example, “NokiaPKI/PrivKey/123”.	

2.4.6 NokiaPKI/CertReq/<X>/KeyLength

This node is used only in the certificate request creation phase and only if the `KeyURI` node value is empty (that is, when there is no reference to an existing private key).

In such a case, this leaf node specifies the length of an RSA private key that is created as a part of the certificate request creation process. If this node is missing, the default key length of 1024 bits is used.

Scope	Occurrence	Access type
Dynamic	One	Add
Format	Value	
Int		

2.4.7 NokiaPKI/CertReq/<X>/Content

This leaf node contains the actual certificate request content. Note that this node is meant only for the fetching of certificate request content from a client (certificate requests are always created in the client).

Scope	Occurrence	Access type
Dynamic	One	Get
Format	Value	
Bin	Certificate request content as a PKCS #10 (see reference document [1]) package in binary DER format.	

2.5 Private keys

This section describes the management tree structure and management nodes that can be used to manage private keys or key pairs.

Accessing and using private keys in the client is protected by a password, if the user key store is in use. The client user is prompted for the password as a part of the private key related management operations, unless the user has been prompted for it already earlier, for example as a result of a `Replace` command on the `NokiaPKI/Logon` node (see Section 2.2.2). For usability reasons, the use of the `Logon` node is encouraged. The user is not prompted for the password, if the device key store is in use.

2.5.1 NokiaPKI/PrivKey

This interior node is the parent of all management tree nodes that are used to manage private keys.

Scope	Occurrence	Access type
Permanent	One	Get
Format	Value	
Node		

2.5.2 NokiaPKI/PrivKey/<X>

This interior node together with its descendant nodes represents a single private key. The node can be used to delete a private key from a client. To delete a private key from a device, the management server should simply issue a single `Delete` command on a private key node (<X>).

Scope	Occurrence	Access type
Dynamic	ZeroOrMore	Delete, Get, Replace The <code>Replace</code> command can only be used for setting the ACL of this node.
Format	Value	
Node		

2.5.3 NokiaPKI/PrivKey/<X>/KeyType

This leaf node specifies the type of the private key.

Scope	Occurrence	Access type
Dynamic	One	Get
Format	Value	
Int	1 – RSA 2 – DSA	

2.5.4 NokiaPKI/PrivKey/<X>/KeyLength

This leaf node specifies the length of the private key.

Scope	Occurrence	Access type
Dynamic	One	Get
Format	Value	
Int		

2.5.5 NokiaPKI/PrivKey/<X>/KeyID

This leaf node contains an identifier of the private key. Note that this value is derived from the key and is thus read-only.

Scope	Occurrence	Access type
Dynamic	One	Get
Format	Value	
Chr	A 160-bit SHA-1 hash of the corresponding public key (excluding the tag, length, and number of unused bits).	

2.6 PKCS #12

This section describes the management tree structure and management nodes that can be used to manage PKCS #12 objects. A PKCS #12 object can contain the user certificate, the CA certificate, and the private key.

2.6.1 NokiaPKI/PKCS12

This interior node is the parent of all management tree nodes that are used to manage PKCS #12 objects.

Scope	Occurrence	Access type
Permanent	One	Get
Format	Value	
Node		

2.6.2 NokiaPKI/PKCS12/<X>

This interior node together with its descendant nodes represents a single PKCS #12 object. A PKCS #12 object should be added as a single entity. Deleting a PKCS #12 object as such is not possible, as it is extracted to different stores and the original PKCS #12 object is deleted after the add operation.

Scope	Occurrence	Access type
Dynamic	ZeroOrMore	Add.
Format	Value	
Node		

2.6.3 NokiaPKI/PKCS12/<X>/Password

This leaf node specifies a password that can be used to open a PKCS #12 object. If this node is not present in the DM tree or if the value is empty, the user is prompted to get the password.

Scope	Occurrence	Access type
Dynamic	ZeroOrOne	Add
Format	Value	
Chr	A sequence of 0 to 32 ASCII characters. Leading or trailing white space, tabs, newlines and other control characters are not allowed.	

2.6.4 NokiaPKI/PKCS12/<X>/Deletable

This leaf node tells whether the certificates inside a PKCS #12 object are deletable or non-deletable. A non-deletable certificate is a certificate that cannot be deleted from a device's PKI store via the UI of the device after it has been added there. However, it is possible to delete a non-deletable certificate via OMA DM.

Scope	Occurrence	Access type
Dynamic	ZeroOrOne	Add
Format	Value	
Bool	True if the certificate is deletable, false if not. If this setting is not specified for a PKCS #12 object when it is added to a client, the default value is true.	

2.6.5 NokiaPKI/PKCS12/<X>/Applicability

This leaf node defines the purposes or application areas (for example, SSL/TLS, application installation, VPN) for which the certificate inside the PKCS #12 object is marked as applicable.

Scope	Occurrence	Access type
Dynamic	ZeroOrOne	Add
Format	Value	
Xml	<p>A list of application IDs using the XML format defined in the NokiaPKI/General/CertApplications node description. If this setting is not specified for a certificate when the certificate is added to a client, the applicability list for the certificate is empty.</p> <p>Example:</p> <pre><CertApps> <App id='268441661' name='Internet' /> <App id= '270498195' name='VPN' /> ... </CertApps></pre>	

2.6.6 NokiaPKI/PKCS12/<X>/Content

This leaf node stores the actual PKCS #12 object content as a single large binary object.

Scope	Occurrence	Access type
Dynamic	One	Add
Format	Value	
Bin	PKCS #12 object in binary format.	

3 Management object usage

This chapter describes how management servers should use the PKI management object to perform different management operations.

3.1 General

Management operation	Implementation
Find out the version of the PKI management object that the client supports	Get command on the <code>NokiaPKI</code> node's <code>Type</code> property. GET <code>./NokiaPKI?Type</code>
Logon to the PKI store	Replace command on the <code>Logon</code> node. REPLACE <code>./NokiaPKI/Logon=""</code> To ensure the user-friendliness (responsiveness) of the Logon phase, the Replace command on the Logon node should be sent to the client in its own OMA DM message.
Logoff from the PKI store	Replace command on the <code>Logoff</code> node. REPLACE <code>./NokiaPKI/Logoff=""</code>
KeyStore	Replace command on the <code>KeyStore</code> node For example, // select device key store to be used REPLACE <code>./NokiaPKI/KeyStore="2"</code> The right key store has to be selected before the keys are accessed. Key stores are differentiated by unique identifiers.
CertStore	Replace command on the <code>CertStore</code> node For example, // select device certificate store to be used REPLACE <code>./NokiaPKI/CertStore="2"</code> The right certificate store has to be selected before the certificates are accessed. Certificate stores are differentiated by unique identifiers.
CertApplications	Get command on the <code>CertApplications</code> node GET <code>./NokiaPKI/General/CertApplications</code>

3.2 Certificate management (Cert node)

Management operation	Implementation
List certificates	Certificate listing is done by issuing multiple Get commands under the <code>NokiaPKI/Cert</code> node in multiple OMA DM request messages: // First OMA DM request message: GET <code>./NokiaPKI/Cert</code> // Second OMA DM request message // (100 and 101 are dynamic // node names returned by the first // OMA DM request message: GET <code>./NokiaPKI/Cert/100/SubjectName</code>

	<pre>GET ./NokiaPKI/Cert/100/SerialNumber GET ./NokiaPKI/Cert/101/SubjectName GET ./NokiaPKI/Cert/101/SerialNumber ...</pre>
Add certificate	<p>Add commands for a certificate node 102:</p> <pre>ADD ./NokiaPKI/Cert/102="" ADD ./NokiaPKI/Cert/102/Type="1" ... ADD ./NokiaPKI/Cert/102/Applicability="<CertApps><App id='270498195' name='VPN'/></CertApps>" ... ADD ./NokiaPKI/Cert/102/Content="<data>"</pre> <p>In the example above, '<data>' denotes the certificate content in binary DER format.</p> <p>Most of the leaf nodes in the new certificate node are derived from the respective certificate by the client, and are thus read-only.</p>
Update certificate	<p>Add, Delete and Replace commands on a certificate node</p> <pre>REPLACE ./NokiaPKI/Cert/Applicability="<CertApps><App id='270498195' name='VPN'/></CertApps>"</pre>
Delete certificate	<p>Delete command on a certificate node 102</p> <pre>DELETE ./NokiaPKI/Cert/102</pre>
Get actual certificate content	<p>Get command on a certificate node 102 content</p> <pre>GET ./NokiaPKI/Cert/102/Content</pre>

3.3 Certificate request management (CertReq node)

Management operation	Implementation
List certificate requests	<p>Certificate request listing is done by issuing multiple Get commands under the <code>NokiaPKI/CertReq</code> node in multiple OMA DM request messages:</p> <pre>// First OMA DM request message: GET ./NokiaPKI/CertReq // Second OMA DM request message // (100 and 101 are dynamic // node names returned by the first // OMA DM request message: GET ./NokiaPKI/CertReq/100/Content GET ./NokiaPKI/CertReq/101/Content ...</pre>
Create certificate request	<p>Add commands for certificate request node 102</p> <p>Option 1 (implicit private key generation):</p> <pre>ADD ./NokiaPKI/CertReq/102="" ADD ./NokiaPKI/CertReq/102/SubjectName="CN=name, OU=Organization, O=company, L=Helsinki, C=FI" ...</pre>

	<pre>ADD ./NokiaPKI/CertReq/102/KeyLength="2048"</pre> <p>Option 2 (private key already exists):</p> <pre>ADD ./NokiaPKI/CertReq/102="" ADD ./NokiaPKI/CertReq/102/SubjectName="CN=name, OU=Organization, O=company, L=Helsinki, C=FI" ... ADD ./NokiaPKI/CertReq/102/KeyURI="NokiaPKI/PrivKey/100"</pre> <p>The creation of a certificate request in the client involves the use of a private key, which in clients is protected by a password if the user key store is in use. The client user is prompted for the password as a part of the certificate request creation, unless it has been asked from the user already earlier, for example, as a result of a <code>Replace</code> command on the <code>NokiaPKI/Logon</code> node (see Section 2.2.2). For usability reasons, the use of the <code>Logon</code> node is encouraged.</p>
Delete certificate request	<p>Delete command on a certificate request node 102</p> <pre>DELETE ./NokiaPKI/CertReq/102</pre>
Get actual certificate request data	<p>Get command on a certificate request content node 102</p> <pre>GET ./NokiaPKI/CertReq/102/Content</pre>

3.4 Private key management (PrivKey node)

Accessing or using private keys in clients is protected by a password, if the user key store is used. The client user is prompted for the password as a part of the below management operations, unless the user has been prompted for it already earlier, for example, as a result of a `Replace` command on the `NokiaPKI/Logon` node (see Section 2.2.2). For usability reasons, the use of the `Logon` node is encouraged. The user is not prompted for the password, if the device key store is in use.

Management operation	Implementation
List private keys	<p>The private key listing is done by issuing multiple <code>Get</code> commands under the <code>NokiaPKI/PrivKey</code> node in multiple OMA DM request messages:</p> <pre>// First OMA DM request message: GET ./NokiaPKI/PrivKey // Second OMA DM request message // (100, 101 and 102 are dynamic // node names returned by the first // OMA DM request message: GET ./NokiaPKI/PrivKey/100 GET ./NokiaPKI/PrivKey/101 ...</pre>
Delete private key	<p>Delete command on a private key node 101</p> <pre>DELETE ./NokiaPKI/PrivKey/101</pre>

3.5 PKCS #12 management (PKCS12 node)

Accessing or using a PKCS #12 object in clients is protected by a password. The client user is prompted for the password as a part of the management operations, unless it has been provided by the Password node. For usability reasons, the use of the Password node is encouraged.

Management operation	Implementation
Add PKCS #12 object	<p>Add commands for PKCS12 node 123. In this case, the PKCS #12 object is delivered to the client.</p> <p>For example:</p> <pre>ADD ./NokiaPKI/PKCS12/123="" ADD ./NokiaPKI/PKCS12/123/Password="password" ... ADD ./NokiaPKI/PKCS12/123/Content="<data>"</pre> <p>In the example above, '<data>' denotes binary data.</p>

4 Terms and abbreviations

Term or abbreviation	Meaning
ACL	Access Control List
CA	Certificate Authority
Client	A mobile device running the Nokia Mobile VPN Client software with OMA DM client support.
DDF	Device Description File
DER	Distinguished Encoding Rules
DM	Device Management
DSA	Digital Signature Algorithm
DTD	Document Type Definition
Management server	An OMA DM server
OMA	Open Mobile Alliance
PKCS	Public-Key Cryptography Standards
PKCS#12	Personal Information Exchange Syntax Standard. For more information, see [1].
PKI	Public Key Infrastructure
PKI object	A certificate, a private key, a certificate request, or a PKCS#12 object
PKI store	A client-side centralized storage for PKI objects
RSA	An algorithm for public-key cryptography
SSL	Secure Sockets Layer
TLS	Transport Layer Security
URI	Uniform Resource Identifier
User certificate	User certificate is used to authenticate a user. If a user certificate is stored to device store, it means that in practice only the device is authenticated.
VPN	Virtual Private Network
XML	Extensible Markup Language

5 References

- [1] Public-Key Cryptography Standards (PKCS) (<http://www.rsasecurity.com/rsalabs/node.asp?id=2124>)
- [2] Enabler Release Definition for OMA Device Management (based on SyncML DM), OMA-ERELED-SyncML_DM-V1_1_2-20031209-A.pdf (<http://www.openmobilealliance.org/>)
- [3] Nokia Mobile VPN (<http://www.nokia.com>)
- [4] SyncML Device Management Protocol, Version 1.1.2 (OMA-SyncML-DMProtocol-V1_1_2-20031203-A.pdf) (<http://www.openmobilealliance.org/>)
- [5] SyncML Device Management Tree and Description, Version 1.1.2 (OMA-SyncML-DMTND-V1_1_2-20031202-A.pdf) (<http://www.openmobilealliance.org/>)
- [6] Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (RFC 3280) (<http://www.ietf.org>)
- [7] Generic String Encoding Rules (GSER) for ASN.1 Types (RFC 3641) (<http://www.ietf.org>)
- [8] Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names (RFC 4514) (<http://www.ietf.org>)
- [9] Standard for the format of ARPA Internet text messages (RFC 822) (<http://www.ietf.org>)

6 Evaluate this resource

Please spare a moment to help us improve documentation quality and recognize the resources you find most valuable, by [rating this resource](#).