

Comware V7 PKI NETCONF XML API Data Reference

Copyright © 2013 Hangzhou H3C Technologies Co., Ltd. All rights reserved.
No part of this manual may be reproduced or transmitted in any form or by any means
without prior written consent of Hangzhou H3C Technologies Co., Ltd.
The information in this document is subject to change without notice.

The H3C logo is displayed in a bold, red, sans-serif font. It consists of the letters 'H3C' where the '3' is slightly smaller and positioned between the 'H' and 'C'.

Contents

PKI.....	1
PKI/Domains.....	1
XML structure	1
Table description.....	1
Columns	1
PKI/DomainPubkeys	2
XML structure	2
Table description.....	3
Columns	3
PKI/Entities	3
XML structure	3
Table description.....	4
Columns	4
PKI/CertAccessPolicies.....	5
XML structure	5
Table description.....	5
Columns	6
PKI/CertAccessRules.....	6
XML structure	6
Table description.....	6
Columns	6
PKI/CertAttributeGroups	7
XML structure	7
Table description.....	7
Columns	7
PKI/CertAttributes	8
XML structure	8
Table description.....	8
Columns	8
PKI/StoragePath	9
XML structure	9
Table description.....	9
Columns	10
PKI/DomainCACerts	10
XML structure	10
Table description.....	10
Columns	11
PKI/DomainLocalCerts	11
XML structure	11
Table description.....	12
Columns	12
PKI/CertificateRequests	13
XML structure	13
Table description.....	13
Columns	14
PKI/ImportCertStatus	14
XML structure	14
Table description.....	15
Columns	15

PKI/AuthorityAlgs	17
XML structure	17
Table description	17
Columns	17
PKI/PKICapabilities	18
XML structure	18
Table description	18
Columns	19

PKI

PKI/Domains

This table is used to get information of PKI domain

XML structure

```
<PKI>
  <Domains>
    <Domain>
      <Name></Name>
      <Entity></Entity>
      <CRLCheck></CRLCheck>
      <Usage>
        <IKE></IKE>
        <SSLServer></SSLServer>
        <SSLClient></SSLClient>
      </Usage>
    </Domain>
  </Domains>
</PKI>
```

Table description

Item	Description
Feature name	PKI
Table name	Domains
Table type	Multi-instance table
Row name	Domain
Restrictions	None

Columns

Column name	Column description	Column type	Data type and restrictions	Remarks
Name	PKI domain name	Index	String. Length: 1 to 31 characters. Case insensitive.	Can't include: "~", "*", "\", " ", ":", ";", "<", ">", " ", "\n", "/"
Entity	Reference a PKI entity for the	N/A	String.	N/A

Column name	Column description	Column type	Data type and restrictions	Remarks
	PKI domain		Length: 1 to 31 characters. Case insensitive.	
CRLCheck	If check whether the certificate has been revoked by CRL	N/A	Boolean: true—Enable. false—Disable. Default value is false.	N/A
Usage	Certificate usage for requesting certificate	Data structure	Members include: - IKE - SSLServer - SSLClient.	Can include one or more certificate usage at the same time.
IKE	Use certificate as the IKE	N/A	Boolean: true—Enable. false—Disable.	N/A
SSLServer	Use certificate as the SSL server certificates	N/A	Boolean: true—Enable. false—Disable.	N/A
SSLClient	Use certificate as the SSL client certificates	N/A	Boolean: true—Enable. false—Disable.	N/A

PKI/DomainPubkeys

This table is used to get the asymmetric keys of PKI domain.

XML structure

```

<PKI>
  <DomainPubkeys>
    <Pubkey>
      <Domain></Domain>
      <Type></Type>
      <Purpose></Purpose>
      <Name></Name>
      <Length></Length>
    </Pubkey>
  </DomainPubkeys>
</PKI>

```

Table description

Item	Description
Feature name	PKI
Table name	DomainPubkeys
Table type	Multi-instance table
Row name	Pubkey
Restrictions	None

Columns

Column name	Column description	Column type	Data type and restrictions	Remarks
Domain	PKI domain name	Index	String. Length: 1 to 31 characters. Case insensitive.	Can't include: "~", "*", "\", " ", ":", ":", "<", ">", " ", " ", " /".
Type	Type of algorithm	Index	Enumeration: 1—RSA. 2—DSA. 3—ECDSA.	See table PKI/AuthorityAlgs for supported encryption algorithm.
Purpose	Key purpose	Index	Enumeration: 1—General 2—Signature 3—Encryption	ECDSA key and DSA key can be used for signature purpose, while RSA key can be used for all purpose.
Name	Key name	N/A	String. Length: 1 to 64 characters Case insensitive.	Only contain letters, number and ".".
Length	Length of public key	N/A	Unsigned integer.	See table PKI/AuthorityAlgs for supported length.

PKI/Entities

This table is used to get the PKI entities.

XML structure

```
<PKI>
  <Entities>
    <Entity>
      <EntityName></EntityName>
```

```

<CommonName></CommonName>
<Country></Country>
<State></State>
<Locality></Locality>
<Organization></Organization>
<OrganizationUnit></OrganizationUnit>
<FQDN></FQDN>
<IP>
  <Ipv4Address></Ipv4Address>
  <IfIndex></IfIndex>
</IP>
</Entity>
</Entities>
</PKI>

```

Table description

Item	Description
Feature name	PKI
Table name	Entities
Table type	Multi-instance table
Row name	Entity
Restrictions	None

Columns

Column name	Column description	Column type	Data type and restrictions	Remarks
EntityName	PKI entity name	Index	String. Length: 1 to 31 characters. Case insensitive.	N/A
CommonName	The common name	N/A	Text. Length: 1 to 63 characters. Case sensitive.	Comma can not be contained.
Country	The country code	N/A	Text. Length: 2 to 2 characters.	Country code is described in ISO 3166-1
State	The state name	N/A	Text. Length: 1 to 63 characters. Case sensitive.	Comma can not be contained.
Locality	The locality name	N/A	Text. Length: 1 to 63 characters. Case sensitive.	Comma can not be contained.
Organization	The	N/A	Text.	Comma can not be

Column name	Column description	Column type	Data type and restrictions	Remarks
n	organization name		Length: 1 to 63 characters. Case sensitive.	contained.
OrganizationUnit	The unit name	N/A	Text. Length: 1 to 63 characters. Case sensitive.	Comma can not be contained.
FQDN	The FQDN name	N/A	String. Length: 1 to 255 characters Case sensitive.	N/A
IP	The IP address	Data structure	Members include: - Ipv4Address. - IfIndex..	Either Ipv4Address or IfIndex can be specified.
Ipv4Address	Ipv4 address	N/A	Ipv4Address	N/A
IfIndex	The index of interface	N/A	Unsigned integer.	Get the primary Ipv4 address of the interface.

PKI/CertAccessPolicies

This table is used to get the certificate access control policies.

XML structure

```
<PKI>
  <CertAccessPolicies>
    <Policy>
      <Name></Name>
    </Policy>
  </CertAccessPolicies>
</PKI>
```

Table description

Item	Description
Feature name	PKI
Table name	CertAccessPolicies
Table type	Multi-instance table
Row name	Policy
Restrictions	None

Columns

Column name	Column description	Column type	Data type and restrictions	Remarks
Name	The name of certificate access control policy	Index	String. Length: 1 to 31 characters. Case insensitive.	N/A

PKI/CertAccessRules

This table is used to get the rules of the certificate access control policy.

XML structure

```
<PKI>
  <CertAccessRules>
    <Rule>
      <Policy></Policy>
      <RuleID></RuleID>
      <Action></Action>
      <AttributeGroup></AttributeGroup>
    </Rule>
  </CertAccessRules>
</PKI>
```

Table description

Item	Description
Feature name	PKI
Table name	CertAccessRules
Table type	Multi-instance table
Row name	Rule
Restrictions	None

Columns

Column name	Column description	Column type	Data type and restrictions	Remarks
Policy	The name of certificate access control policy	Index	String. Length: 1 to 31 characters. Case insensitive.	N/A

Column name	Column description	Column type	Data type and restrictions	Remarks
RuleID	Index of the rule in the access control policy.	Index	Unsigned integer. Value range: 1 to 16	The smaller the RuleID is, the higher the priority is.
Action	How to operate the certificate that match the rule	N/A	Enumeration: • 1—Permit • 2—Deny	N/A
AttributeGroup	The name of certificate attribute group	N/A	String. Length: 1 to 31 characters. Case insensitive.	N/A

PKI/CertAttributeGroups

This table is used to get the certificate attribute groups.

XML structure

```

<PKI>
  <CertAttributeGroups>
    <Group>
      <Name></Name>
    </Group>
  </CertAttributeGroups>
</PKI>

```

Table description

Item	Description
Feature name	PKI
Table name	CertAttributeGroups
Table type	Multi-instance table
Row name	Group
Restrictions	None

Columns

Column name	Column description	Column type	Data type and restrictions	Remarks
Name	The name of certificate	Index	String. Length: 1 to 31 characters.	N/A

Column name	Column description	Column type	Data type and restrictions	Remarks
	attribute group		Case insensitive.	

PKI/CertAttributes

This table is used to get the attributes of the certificate attribute groups.

XML structure

```

<PKI>
  <CertAttributes>
    <Attribute>
      <Group></Group>
      <AttributeID></AttributeID>
      <Object></Object>
      <Item></Item>
      <Operator></Operator>
      <Value></Value>
    </Attribute>
  </CertAttributes>
</PKI>

```

Table description

Item	Description
Feature name	PKI
Table name	CertAttributes
Table type	Multi-instance table
Row name	Attribute
Restrictions	None

Columns

Column name	Column description	Column type	Data type and restrictions	Remarks
Group	The name of certificate attribute group	Index	String. Length: 1 to 31 characters. Case insensitive.	N/A
AttributeID	Index of the attribute in the certificate attribute group	Index	Unsigned integer. Value range:1 to 16	The smaller the AttributeID is, the higher the priority is.

Column name	Column description	Column type	Data type and restrictions	Remarks
Object	The object which to be matched	N/A	Enumeration: 1—alt-subject-name 2—issuer-name 3—subject-name	N/A
Item	The item in the object	N/A	Enumeration: 1—DN 2—FQDN 3—IpAddress	It's can be each value when the object is subject-name or issuer-name, but only can be FQDN o IpAddress when the object is alt-subject-name.
Operator	How to operate the item	N/A	Enumeration: 1—contain 2—equal 3—not contain 4—not equal	N/A
Value	The value that be used to match with item.	N/A	String. Length: 1 to 255 characters. Case insensitive.	N/A

PKI/StoragePath

This table is used to get the PKI storage path.

XML structure

```
<PKI>
  <StoragePath>
    <StorageCertPath></StorageCertPath>
    <StorageCRLPath></StorageCRLPath>
  </StoragePath>
</PKI>
```

Table description

Item	Description
Feature name	PKI
Table name	StoragePath
Table type	Single-instance table
Row name	None

Restrictions	None
--------------	------

Columns

Column name	Column description	Column type	Data type and restrictions	Remarks
StorageCertPath	The PKI certificate storage path	N/A	String. Case sensitive.	The path can't begin with "/" or "../"
StorageCRLPath	The PKI CRL storage path	N/A	String. Case sensitive.	The path can't begin with "/" or "../"

PKI/DomainCACerts

This table is used to get the CA certificates of the PKI domain

XML structure

```
<PKI>
  <DomainCACerts>
    <Cert>
      <Domain></Domain>
      <SerialNumber></SerialNumber>
      <Issuer></Issuer>
      <Subject></Subject>
      <Validity>
        <NotBefore></NotBefore>
        <NotAfter></NotAfter>
      </Validity>
      <IsLowestCA></IsLowestCA>
      <DetailInfoText></DetailInfoText>
    </Cert>
  </DomainCACerts>
</PKI>
```

Table description

Item	Description
Feature name	PKI
Table name	DomainCACerts
Table type	Multi-instance table
Row name	Cert

Columns

Item	Description
Feature name	PKI
Table name	DomainLocalCerts
Table type	Multi-instance table
Row name	Cert
Restrictions	None

Column name	Column description	Column type	Data type and restrictions	Remarks
Domain	The PKI domain name	Index	String. Length: 1 to 31 characters. Case insensitive.	Can't include: "~ " * " \ " , ; : . , < " , > " , _ , - , / " .
KeyUsage	The key usage of the certificate	Index	Enumeration: • 1—General. • 2—Signature. • 3—Encryption.	There is only one special usage certificate in one domain, and general usage certificate can't appear with signature/encrypt on certificate at the same time.
SerialNumber	The serial number of the certificate	N/A	String.	N/A
Issuer	The issuer name	N/A	String	N/A

Column name	Column description	Column type	Data type and restrictions	Remarks
Subject	The Subject name	N/A	String	N/A
Validity	The validity date of the certificate	Data structure	Members include: - NotBefore. - NotAfter.	N/A
NotBefore	The begin time of the validity	N/A	DateTime	N/A
NotAfter	The end time of the validity	N/A	DateTime	N/A
DetailInfoText	The text of the local certificate or the certificate chain	N/A	String	N/A

PKI/CertificateRequests

This table is used to get the certificate requests for the domain

XML structure

```

<PKI>
  <CertificateRequests>
    <Request>
      <Domain></Domain>
      <Password></Password>
      <Value></Value>
    </Request>
  </CertificateRequests>
</PKI>

```

Table description

Item	Description
Feature name	PKI
Table name	CertificateRequests
Table type	Multi-instance table
Row name	Request
Restrictions	None

Columns

Column name	Column description	Column type	Data type and restrictions	Remarks
Domain	The PKI domain name	Index	String. Length: 1 to 31 characters. Case insensitive.	Can't include: "~", "*", "\", " ", " ", "<", ">", ":", ";", "/", "."
Password	The challenge word which is needed when revoke the certificate	N/A	String. Length: 1 to 31 characters. Case sensitive.	N/A
Value	The certificate request value	N/A	String	N/A

批注 [z01]: Password 不做为索引列，且 tree.xml 里面设置 not return to user，并且添加 filter_mor

PKI/ImportCertStatus

This table is used to get the status when import certificate to a domain

XML structure

```
<PKI>
  <ImportCertStatus>
    <Status>
      <Domain></Domain>
      <CertificateType></CertificateType>
      <FilePath></FilePath>
      <Password></Password>
      <NewPubKeyName></NewPubKeyName>
      <IsNewPubKeyExist></IsNewPubKeyExist>
      <IsPubKeyConfiged></IsPubKeyConfiged>
      <IsCorrectFormat></IsCorrectFormat>
      <IsNoCA></IsNoCA>
      <IsKeyPairExist></IsKeyPairExist>
      <IsKeyPairMatched></IsKeyPairMatched>
      <CertFingerprint></CertFingerprint>
      <DomainFingerprint></DomainFingerprint>
      <IsFingerprintMatched></IsFingerprintMatched>
      <NeedReplaceCACert></NeedReplaceCACert>
      <NeedReplaceLocalCert></NeedReplaceLocalCert>
      <NeedReplaceKeyPair></NeedReplaceKeyPair>
      <CertVerifyErrStr></CertVerifyErrStr>
    </Status>
  </ImportCertStatus>
</PKI>
```

Table description

Item	Description
Feature name	PKI
Table name	ImportCertStatus
Table type	Multi-instance table
Row name	Status
Restrictions	None

Columns

Column name	Column description	Column type	Data type and restrictions	Remarks
Domain	The PKI domain name	Index	String. Length: 1 to 31 characters. Case insensitive.	Can't include: "~", " ", "*", "\\", " ", ":", ";", "<", ">", ",", "-", "/", ".".
CertificateType	The type of certificate	Index	Enumeration: • 1 —CA • 2 —Local.	N/A
FilePath	The path of the file contain certificate	Index	String	The file must be existed in the device
Password	Password which will be used to encrypt the file when the certificate contains private key.	N/A	String Case sensitive.	The password is required as follow: • The file format is PKCS#12 and the certificate type is local • The file format is PEM, and there is local certificate and private key in the file.
NewPublicKeyName	The name of new public key.	N/A	String. Length: 1 to 64 characters. Case insensitive.	Only contain letters, number and "-". If the name is empty and there is no key name in the domain, it will use the domain name as the key name.
IsNewPublicKeyExist	If the new public key is	N/A	Boolean: • true —Yes.	N/A

批注 [z02]: Password 不做为索引列，且 tree.xml 里面设置 not return to user，并且添加 filter_mor

批注 [z03]: 不做为索引列, 且 tree.xml 里面添加 filter mor

Column name	Column description	Column type	Data type and restrictions	Remarks
	existed		• false—No.	
IsPubKeyConfigured	If there is public key configure in the domain	N/A	Boolean: • true—Yes. • false—No.	N/A
IsCorrectFormat	If the file format is correct	N/A	Boolean: • true—Yes. • false—No.	Error information
IsNoCA	If there is no any CA certificate when import	N/A	Boolean: • true—Yes. • false—No.	Error information
IsKeyPairExisted	If the key pair is existed	N/A	Boolean: • true—Yes. • false—No.	If there isn't key pair in both file and device, the value is false, otherwise it is true Error information
IsKeyPairMatched	If the key pair is matched with the certificate	N/A	Boolean: • true—Yes. • false—No.	Error information
CertFingerprint	The fingerprint of the root certificate	N/A	String. Length: 1 to 127 characters.	The column is appended only when there is new root certificate be imported to device Confirm information
DomainFingerprint	The fingerprint configured in the PKI domain	N/A	String. Length: 1 to 127 characters.	The column is appended only when the PKI domain configured the root fingerprint
IsFingerprintMatched	If the root fingerprint is matched	N/A	Boolean: • true—Yes. • false—No.	Error information
NeedReplaceCACert	If the ca certificate need to be replaced	N/A	Boolean: • true—Yes. • false—No.	Confirm information
NeedReplaceLocalCert	If the local certificate need to be replaced	N/A	Boolean: • true—Yes. • false—No.	Confirm information
NeedReplaceKeyPair	If the key pair need to be replaced	N/A	Boolean: • true—Yes. • false—No.	Confirm information
CertVerifyErr	The result of the	N/A	String.	The column is

Column name	Column description	Column type	Data type and restrictions	Remarks
Str	validate when import		Length: 1 to 255 characters.	appended only when it is failed to verify the certificate

PKI/AuthorityAlgs

This table is used to get the authority algorithm

XML structure

```

<PKI>
  <AuthorityAlgs>
    <Alg>
      <AlgID></AlgID>
      <AlgName></AlgName>
      <MinLength></MinLength>
      <MaxLength></MaxLength>
      <DefaultLength></DefaultLength>
    </Alg>
  </AuthorityAlgs>
</PKI>

```

Table description

Item	Description
Feature name	PKI
Table name	AuthorityAlgs
Table type	Multi-instance table
Row name	Alg
Restrictions	None

Columns

Column name	Column description	Column type	Data type and restrictions	Remarks
AlgID	Identity of algorithm	Index	Unsigned integer. Value range: 1 to 2^32-1.	
AlgName	Name of algorithm	N/A	String. Length: 1 to 255 characters	The name of supported algorithm

Column name	Column description	Column type	Data type and restrictions	Remarks
Case insensitive.				
MinLength	Minimal length of supported algorithm	N/A	Unsigned integer.	N/A
MaxLength	Maximal length of supported algorithm	N/A	Unsigned integer.	N/A
DefaultLength	Default length of supported algorithm	N/A	Unsigned integer.	N/A

PKI/PKICapabilities

This table is used to get the PKI capabilities

XML structure

```

<PKI>
  <PKICapabilities>
    <PKICapability>
      <EncAlgID></EncAlgID>
      <Name></Name>
    </PKICapability>
  </PKICapabilities>
</PKI>

```

Table description

Item	Description
Feature name	PKI
Table name	PKICapabilities
Table type	Multi-instance table
Row name	PKICapability
Restrictions	None

Columns

Column name	Column description	Column type	Data type and restrictions	Remarks
EncAlglD	Identity of encryption algorithm	Index	Unsigned integer. Value range: 1 to $2^{32}-1$.	N/A
Name	Name of encryption algorithm	N/A	String. Length: 1 to 255 characters. Case insensitive.	The name of supported encryption algorithm