IBM Education Assistance for z/OS V2R2

Item: PKI nxm Authorization
Element/Component: PKI Services

Material current as of May 2015

Agenda

- Trademarks
- Presentation Objectives
- Overview
- Usage & Invocation
- Migration & Coexistence Considerations
- Presentation Summary
- Appendix

Trademarks

- See url http://www.ibm.com/legal/copytrade.shtml for a list of trademarks.

Presentation Objectives

- Digital certificates usage has been growing
- Continuous enhancements to fulfill customer requirements
- Components on certificate support:
  - PKI Services
- At the end of this presentation, you should have an understanding of the support from PKI Services for nxm authorization.

Overview

- Problem Statement / Need Addressed
  - Currently PKI Services supports both automatic approval mode and administrator approval mode
  - In the administrator approval mode, only one administrator is required to approve the requests
  - Some government agency requires all PKI products to have an NxM authentication factor
    - For example, two PKI administrators have to validate a request before issuing the certificate

Overview

- Solution
  - In this release, PKI Services will enhance the administrator approval mode to support multiple number of approvers
  - A configuration option with be provided in the CGI templates file and JSP templates xml file to set the number of administrators required to approve a certificate request
  - The option will be provided on a per template basis
  - A change of the configured number of approvers will not affect the existing certificate requests, only the new requests

Overview

All ☑	Requestor	Certificate Request Information	Status	Processed by	Modified time
☑	Paul	**Trans ID:** 1kM7z6No36sc2AYS++++++++ **Template:** 5-Year PKI SSL Server Certificate **Subject:** CN=test1,OU=Class 1 Internet Certificate CA,O=The Firm **Creation date:** 2013/01/30 **Approvals required:** 3	Approved	adminX (Approved)	2013/01/30 08:23:44
				adminY (Approved)	2013/02/01 23:59:45
				adminZ (Approved)	2013/02/01 23:59:45
☑	Vicky	**Trans ID:** 1kM7z6No36sc2AYS++++++++ **Template:** 5-Year PKI SSL Server Certificate **Subject:** CN=test1,OU=Class 1 Internet Certificate CA,O=The Firm **Creation date:** 2013/01/30 **Approvals required:** 3	Pending Approval	adminX (Approved)	2013/01/30 08:23:44
☑	Sudha	**Trans ID:** 1kJ8z9Mx48sc2KBB++++++++ **Template:** 1-Year PKI Generated Key Certificate **Subject:** CN=test1,OU=Class 1 Internet Certificate CA,O=The Firm **Creation date:** 2013/01/30 **Approvals required:** 4	Pending Approval	adminX (Approved)	2013/02/01 23:23:45
				adminY (Approved)	2013/02/01 23:59:45
☑	Tony	**Trans ID:** 1hK7z9Mx48sc2ECC++++++++ **Template:** 1-Year PKI Generated Key Certificate **Subject:** CN=test1,OU=Class 1 Internet Certificate CA,O=The Firm **Creation date:** 2013/01/31 **Approvals required:** 4	Rejected	adminX (Approved with Modification)	2013/02/01 12:13:41
				adminY (Rejected)	2013/02/01 14:11:23
☑	Bob	**Trans ID:** 1kB9z7MxuCQ/2SHV++++++++ **Template:** 1-Year PKI SSL Browser Certificate **Subject:** CN=test2,OU=Class 1 Internet Certificate CA,O=The Firm **Creation date:** 2013/01/30 **Approvals required:** 1	Pending Approval		

Overview

Single Request

Requestor:	Paul	**Created:**	2013/02/07
Status:	Approved	**Modified:**	2013/02/09
Transaction Id:	1kFkLK/Yij6+2SHV++++++++	**Passphrase:**	a
Template:	5-Year PKI SSL Server Certificate		
Approvals required:	3		
Approval history:	adminX approved on 2013/02/09 10:20:00 (key size acceptable)		
	adminY approved on 2013/02/09 12:10:12		
	adminZ approved on 2013/02/09 15:20:23 (the last year to allow 2048 key)		

Subject:	CN=aug30a,OU=Class 1 Internet Certificate CA,O=The Firm
Issuer:	OU=Master CA,O=IBM,C=US
Validity:	2013/02/07 00:00:00 - 2014/02/06 23:59:59
Usage:	handshake(digitalSignature, keyEncipherment)
Key type and key size:	RSA-2048
Signature algorithm:	sha-256WithRSAEncryption
Fingerprints:	
SHA1:	4E:28:4B:A3:E9:47:05:32:67:54:5B:50:7A:47:6B:4A:65:38:BA:E7
MD5:	5B:0E:BF:53:D5:A3:02:20:BF:68:E8:8C:CC:04:A4:AC
SHA256:	5D:25:B2:B5:87:11:8D:C2:F8:B3:C6:AD:51:32:35:A4:72:99:71:F0:B4:C8:9D:51:4D:1E:49:12:3D:FB:7F:35
SHA512:	B4:14:E8:4D:A1:2D:14:9C:B8:F0:DA:C6:E6:46:F5:55:88:EB:E9:82:35:FD:AF:33:46:1E:8F:B6:52:D4:B4:B5:E6:41:99:93:CB:42:76:3F:3A:B4:CF:A8:13:52:66:40:F7:39:82:20:69:AD:D7:E7:8A:B0:28:0C:19:97:17:06

Overview

- Benefit / Value
  - With nxm support, the PKI Services run by the customer may be certified as a standard Certificate Authority as required by some countries

Usage & Invocation

- Update the template section in pkiserv.tmpl or pkitmpl.xml
- Example 1 – request for SSL server certificate requires 3 administrator to approve

pkiserv.tmpl

```
<TEMPLATE NAME=5-Year PKI SSL Server
Certificate>
....
<ADMINAPPROVE>
<ADMINNUM=3>
 %%CommonName (Optional)%%
 %%OrgUnit (Optional)%%
 ...
</ADMINAPPROVE>
....
</TEMPLATE>
```

pkitmpl.xml

```
<tns:certreq_template nickname="5YSSSL">
  <tns:certname>5-Year PKI SSL Server
Certificate</tns:certname>

…
<tns:AdminNum>3</tns:AdminNum>
…
</tns:certreq_template>
```

Usage & Invocation

- Example 2 – request for SCEP certificate requires 2 administrator to approve

pkiserv.tmpl

```
<TEMPLATE NAME=5-Year SCEP
Certificate - Preregistration>

....
<PREREGISTER>
<ADMINNUM=2>
AuthenticatedClient=AutoApprove
SemiauthenticatedClient=AdminApprove
UnauthenticatedClient=Reject
SubsequentRequest=AutoApprove
RenewalRequest=AutoApprove
</PREREGISTER>
</TEMPLATE>
```

pkitmpl.xml

```
<tns:certreq_template
nickname="5YSCEPP">
  <tns:certname>5-Year SCEP Certificate
– Preregistration</tns:certname>
…
 <tns:AdminNum>2</tns:AdminNum>

…
</tns:certreq_template>
```

Migration & Coexistence Considerations

- Toleration APAR OA44392 if you run PKI V2R2 to create requests with multiple approvers and then fall back to previous releases.

Presentation Summary

- At the end of this presentation, you should now have an understanding of the PKI Services nxm authorization support.

Appendix

- Publication references
  - Cryptographic Services PKI Services Guide and Reference (*SA22-7693*)