

EJBCA Token Certificate Enrollment

Welcome to keystore enrollment.

If you want to, you can manually install the CA certificate(s) in your browser, otherwise this will be done automatically when the certificate is retrieved.

Install CA certificates:
[Certificate chain](#)

Please choose a key length, then click OK to fetch your certificate.

Options
Leave values as default if unsure.

Key length: 1024 bits

Certificate profile: ENDUSER

图 18-35 选择密钥长度

对于客户端产生的 PKCS#10 格式的证书请求，可以通过管理界面中左侧导航栏“Create Certificate from CSR”功能，把 P10 证书请求粘贴到编辑框中，从而实现证书签发，如图 18-36 所示。



A PEM-formatted request is a BASE64 encoded certificate request starting with
-----BEGIN CERTIFICATE REQUEST-----
and ending with
-----END CERTIFICATE REQUEST-----

Enroll

Username

Enrollment code

Request file 未选择文件
or pasted request

Result type: PEM - certificate only

图 18-36 PKCS#10 格式的证书请求

18.2.4 下载 CRL

在管理界面中单击左侧导航栏“Fetch CA CRLs”，进入 CRL 下载页面，如图 18-37 所示。

选择左侧链接“DER format”（完整 CRL，不是 Delta CRL），下载完整 CRL 为 ManagementCA.crl 文件。双击该文件可查看其中的详细内容，见图 18-38。可以看到，其中作废的证书列表为空。

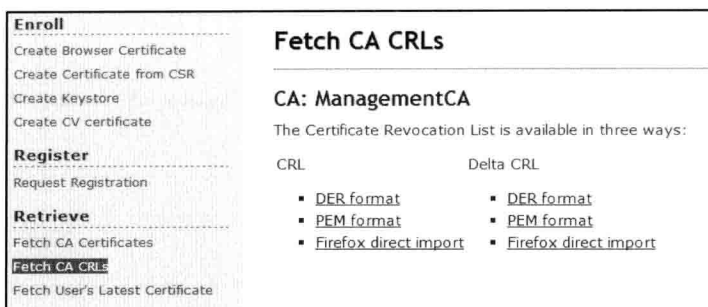


图 18-37 获取 CRL 界面

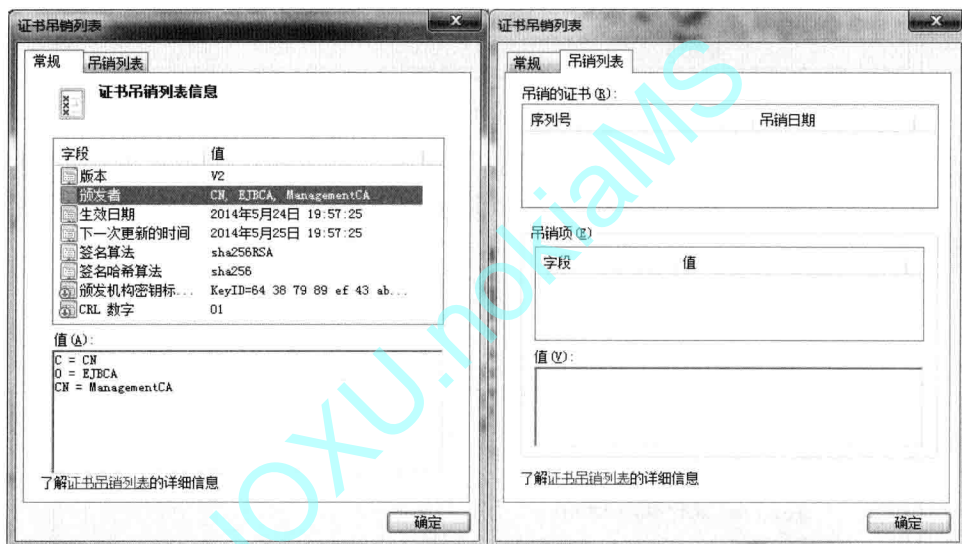


图 18-38 下载的 CRL 文件内容

为了展示非空 CRL，作废刚才产生的 ejbcauser-1 证书，在管理界面中单击左侧导航栏“Search End Entities”，出现查询界面，如图 18-39 所示。

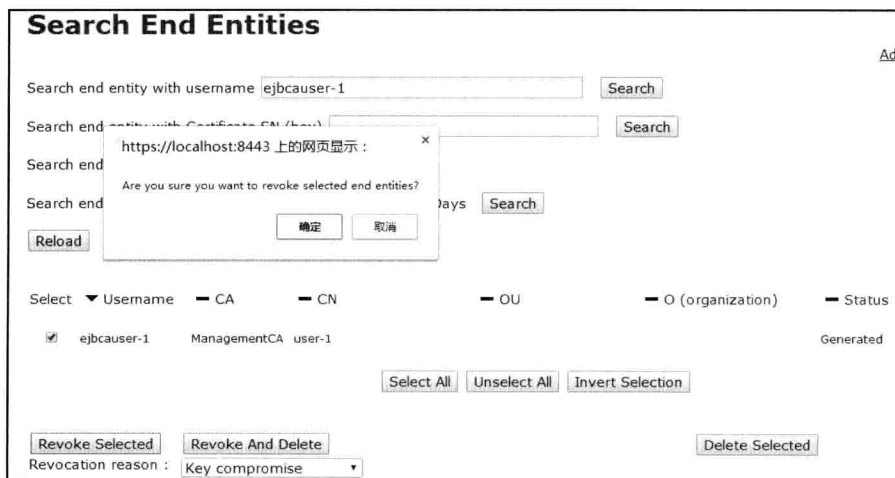


图 18-39 作废用户证书

在 Search end entity with username 中输入“ejbcauser-1”后，单击“Search”按钮进行查询。页面下边显示查询结果列表，勾选 ejbcauser-1 条目，在作废原因中选择“Key compromise”，单击“Revoke Selected”按钮，完成证书作废。

作废用户证书后，需要主动触发产生 CRL 文件。在管理界面中单击左侧导航栏“CA Structure & CRL”，出现证书作废页面，如图 18-40 所示。单击“Create CRL”按钮，完成 CRL 生成。

再次下载 CRL 后，可以看到有一条被作废的用户证书（ejbcauser-1 用户证书），如图 18-41 所示。

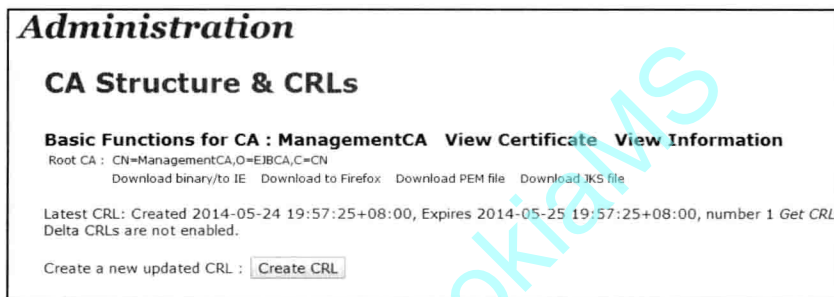


图 18-40 产生 CRL

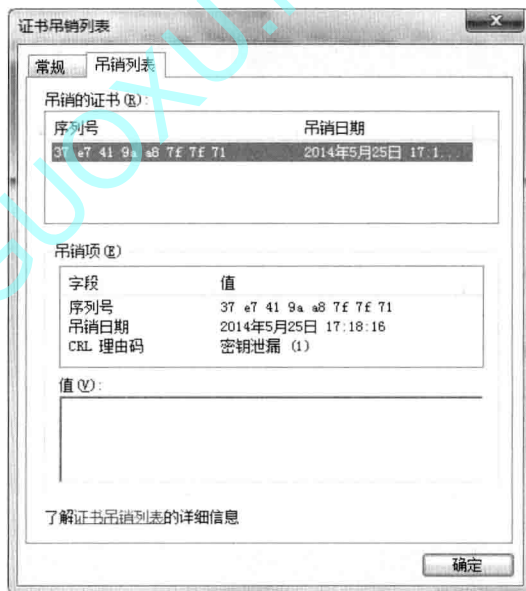


图 18-41 包含 ejbcauser-1 吊销证书的 CRL

除了手动触发生成 CRL 外，EJBCA 同时支持定时产生 CRL，即在某个设定时间产生 CRL 文件。

第五部分

PKI 之应用：使用网络身份证