BBN Rule Editor User Guide

1 Introduction

The Rule Editor is a Java program that provides a GUI to allow a user to create rules for certificates and CRLs issued by CAs. For this release of the Rule Editor, the rules must follow the profile for X.509 resource certificates (draft-ietf-sidr-res-certs-02.txt). The certificate and rule files used by the Rule Editor are in ASN.1 syntax. Each file can store only one set of rules or one certificate. The Rule Editor can read both BER and DER ASN.1 encoded files and produces DER ASN.1 encoded files.

As illustrated in Figure 1, the Rule Editor should be executed on a workstation separate from the CA workstation, for security reasons. A CA staff member begins by loading into the Rule Editor the certificate of the CA for which the rules are to be generated. He then creates one rule file for CA certificates and one for CRLs (and optionally, one for end entity certificates). These rule files are imported into the Rule Engine, operating on a CA workstation. The generated rules are used to check whether certificates or CRLs that are to be signed by a CA meet the syntactic requirements established by the CA. Before being signed, each certificate or CRL is passed into the Rule Engine along with the appropriate rule file. The Rule Engine then determines if the offered certificate or CRL meets the requirements as expressed in the rule file. Figure 1 below illustrates the relationship between the Rule Editor, Rule Engine, and certificate or CRL processing by a CA.

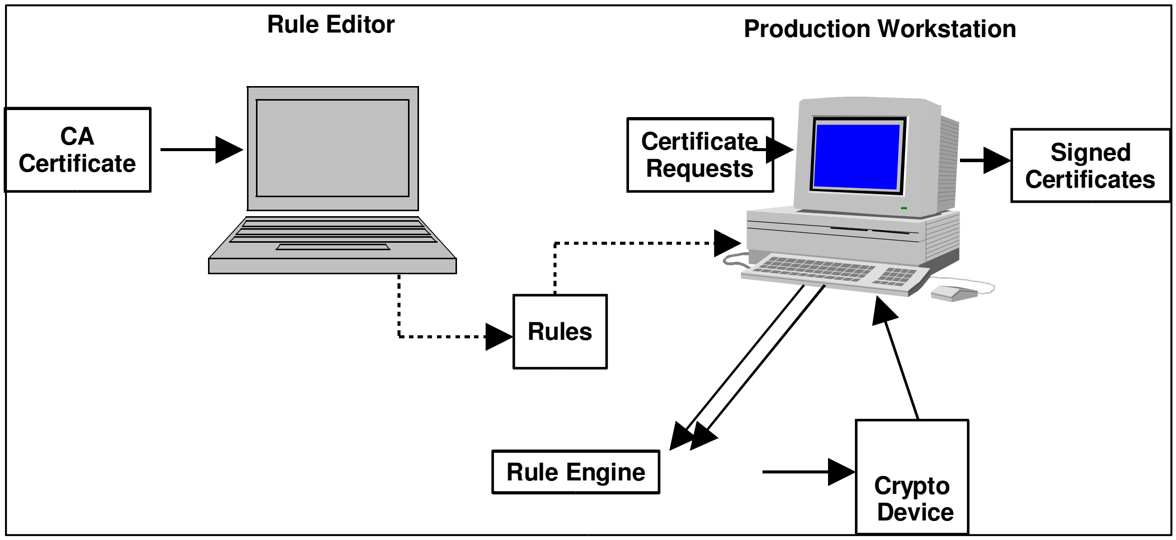


Figure 1. System Overview

2 Compiling the Rule Editor

There is a Makefile in the src directory. Type “make” at a command line in the src directory to compile the Java code in each of the subdirectories. The resulting class files are put into the lib directory.

3 Starting the Rule Editor

Open a command window, enter the lib directory, and type “java RuleEditor” to start the Rule Editor. The user is prompted to supply a CA certificate. A file browser window opens to allow the user to search for a file containing the desired CA certificate. Alternatively, the user may type “java RuleEditor myCAFilename” where the relative path name to the CA certificate file is myCAFilename. The Rule Editor imports this CA file and extracts relevant values to be used in constructing the rules. (If there are any invalid IP Address Blocks in this CA certificate, an error window appears listing them. In addition, the program lists in the command window additional information identifying the error, e.g. “V4: 0 2 6” means that entries 0, 2 and 6 in the V4 section have errors.)

If there are no errors in the supplied CA certificate, the Rule Editor Window then appears. All rules created will be based on this CA certificate until a new CA certificate file is opened, as described in Section 9.

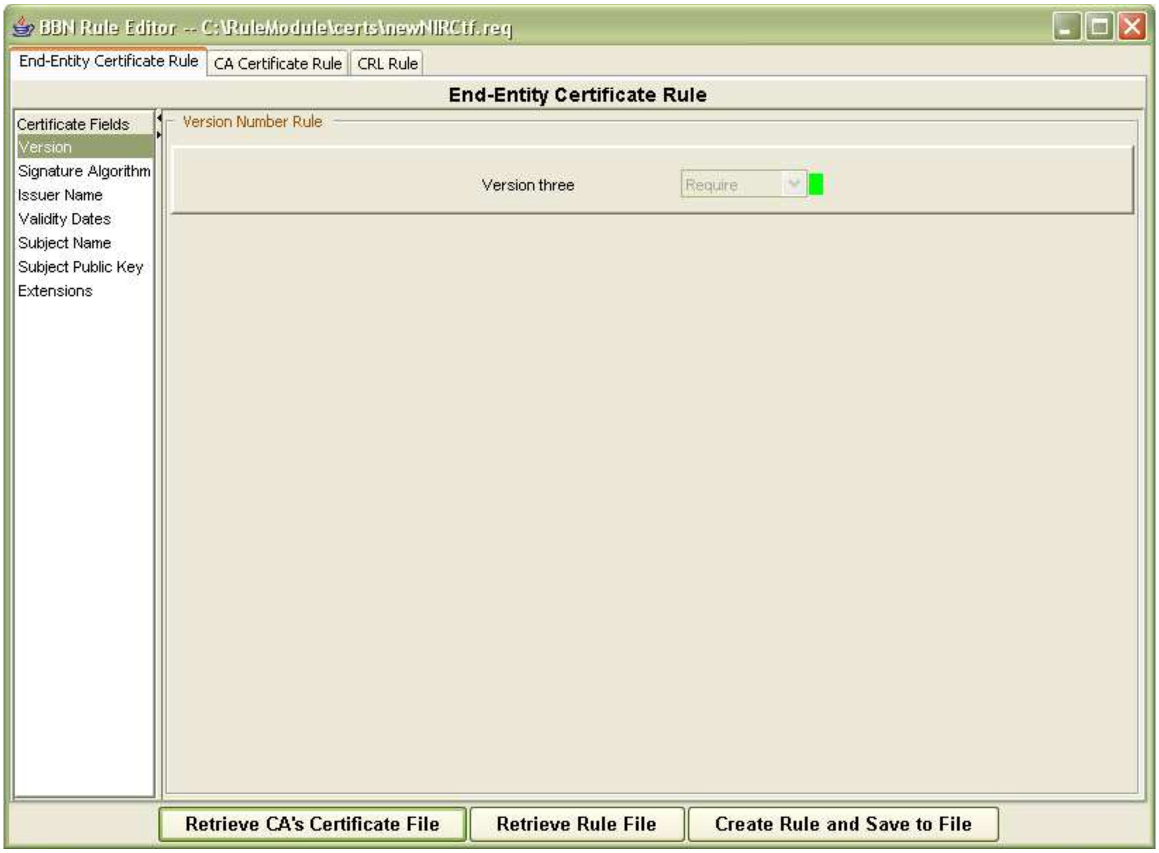
The “examples” directory contains sample certificates, CRLs, and rules. Filenames contain “Ctf”, “CRL”, or "rule" in the filename to indicate if the file contains a CA certificate, a CRL, or a rule set, respectively. A filename may have more than one of these strings. For example, the filename “NIRCRLrules” indicates a set of rules for generating CRLs. Additionally, filenames with a “.txt” extension are a textual representation of the corresponding ASN.1 (binary) file. The text file corresponding to “NIRCRLrules” is “NIRCRLrules.txt”. These “.txt” files can be opened in any text editor for inspection, but cannot be re-imported into the RuleEditor. Filenames containing “Bad” in the name, such as “NIRBad1CRL” which contains a bad CRL, are erroneous files. Certificates are often created manually, resulting in many potential errors. These errors are most commonly found in the IP Address Block and Autonomous System Identifier extensions as these extensions can be quite cumbersome to create. The Rule Editor will not open erroneous files, but will give an error message indicating the problem that was process. Finally, files ending with “results” are text files that illustrate the Rule Engine output when the corresponding rule file and certificate (or CRL) file were passed into the Rule Engine.

4 Rule Editor Window

The Rule Editor window, shown in Figure 2, has three tabs. These are labeled “End-Entity Certificate Rule”, “CA Certificate Rule”, and “CRL Rule” and are used for creating rule sets for end entity certificates, CA certificates, and CRLs issued by the current CA, respectively. Two or three rule sets typically will be generated based on the same CA certificate. If a CA issues both end-entity certificates and CA certificates, as well as CRLs, that CA’s certificate would form the basis for three rule sets.

At the bottom of the Rule Editor Window are three buttons called “Retrieve CA’s Certificate File”, “Retrieve Rule File”, and “Create Rule and Save to File”. The use of these buttons is described in sections 7, 8, and 9.

The full path to the (current) imported CA certificate file is displayed in the title bar of the window.



Version three Require 🟩

Figure 2. Rule Editor Main Window

5 Certificate Fields

If either of the certificate tabs is selected, a list of certificate fields appears on the left side of the window. The rule pertaining to the selected field appears on the right side of the window. Many of the certificate field values are fixed per the profile for X.509 resource certificates and therefore the user can only inspect these rules, not change them. For other fields, the user is allowed to impose constraints on the field values.

5.1 Version

The version number of the certificates is fixed at 3.

5.2 Signature Algorithm

The signature algorithm is fixed at sha256WithRSAEncryption.

5.3 Issuer Name

The Issuer name is imported from the Subject field of the current CA certificate, since that CA is the issuer of all certificates for which rules are being created.

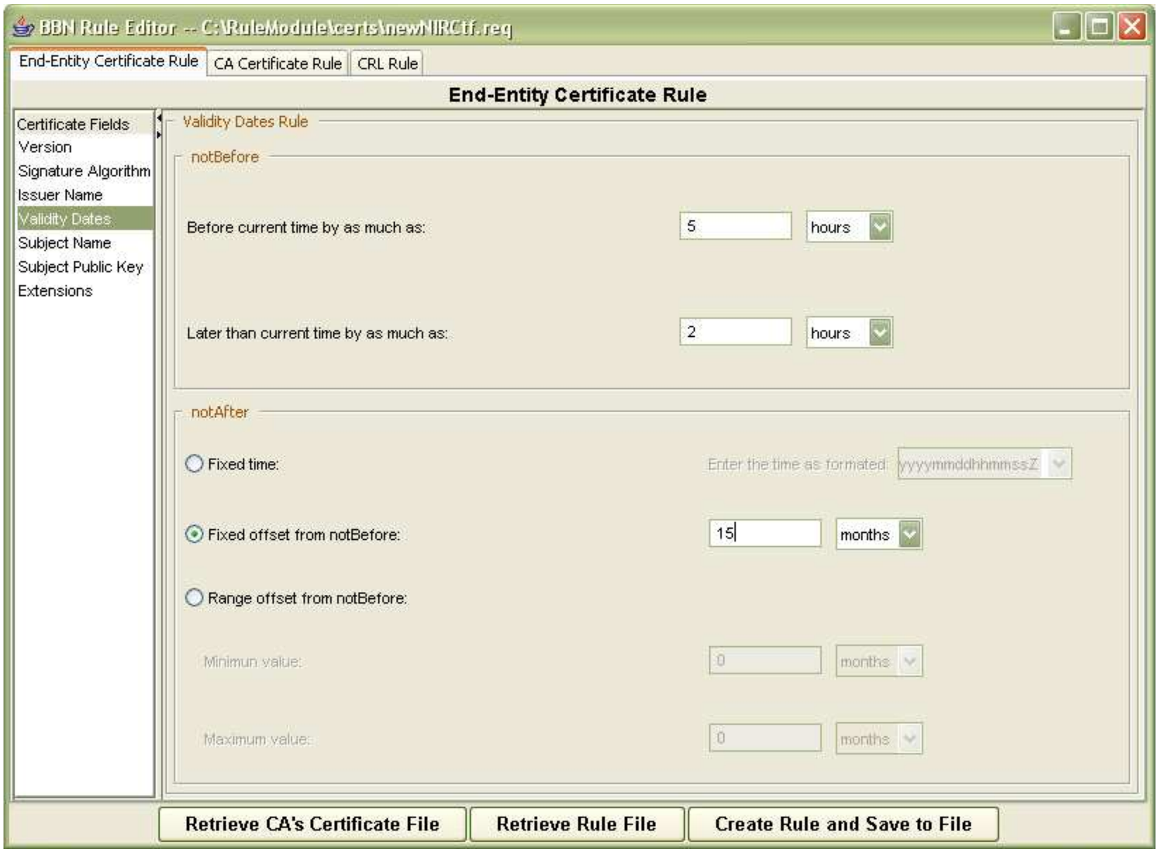
5.4 Validity Dates

Every certificate contains two dates that specify the time during which that certificate is valid. The validity dates rule allows the user to specify the window of allowable ranges for each end of the certificate validity period. In this rule the current time refers to the time that the CA signs the certificate, not the time when the rule is created.

The notBefore clause allows the user to specify a time window for the beginning of the certificate validity period.

The notAfter clause allows the user to specify allowed values for the end of the certificate validity period. This can be a fixed time, a fixed offset from the time in the notBefore clause, or a range offset from the time in the notBefore clause. As an example, for a rule to specify that all CA certificates issued by this CA should have a 15 month validity window, select the Fixed Offset radio button and enter 15 months to the right as shown in Figure 3. As another example, to specify that all CA certificates issued by this CA should be valid for anywhere between 15 and 18 months, choose the Range Offset radio button and enter 15 months for the first value and 18 months for the second value.

If a fixed date is entered, it is specified in a format :yyyymmddhhmmss. This indicates 4 digits for the year, and 2 each for the month, day, hours, minutes, and seconds. Each listed digit must be represented in order for the time to be accurately understood. Additionally, the time must be expressed as Greenwich Mean Time (as indicated by the use of the “Z” suffix).



End-Entity Certificate Rule

Validity Dates Rule

notBefore

Before current time by as much as: 5 hours

Later than current time by as much as: 2 hours

notAfter

○ Fixed time: Enter the time as formated: yyyymmddhhmmssZ

● Fixed offset from notBefore: 15 months

○ Range offset from notBefore:

Minimun value: 0 months

Maximum value: 0 months

Figure 3. Validity Dates Rule Window

5.5 Subject Name

The Subject Name rule allows the user to impose restrictions on the subject names of certificates issued by this CA. There is a list of four different types of distinguished name attributes (Country Name, Organization Name, Organizational Unit Name, and Common Name) that can be employed to create a Subject Name. Each type has a corresponding drop down box and each of the drop down boxes contains the possible values of Allow, Prohibit, and Require. “Allow” means that the attribute can optionally be present in the certificate, “Prohibit” means that the attribute cannot appear in the certificate, and “Require” means that the attribute must appear in the certificate.

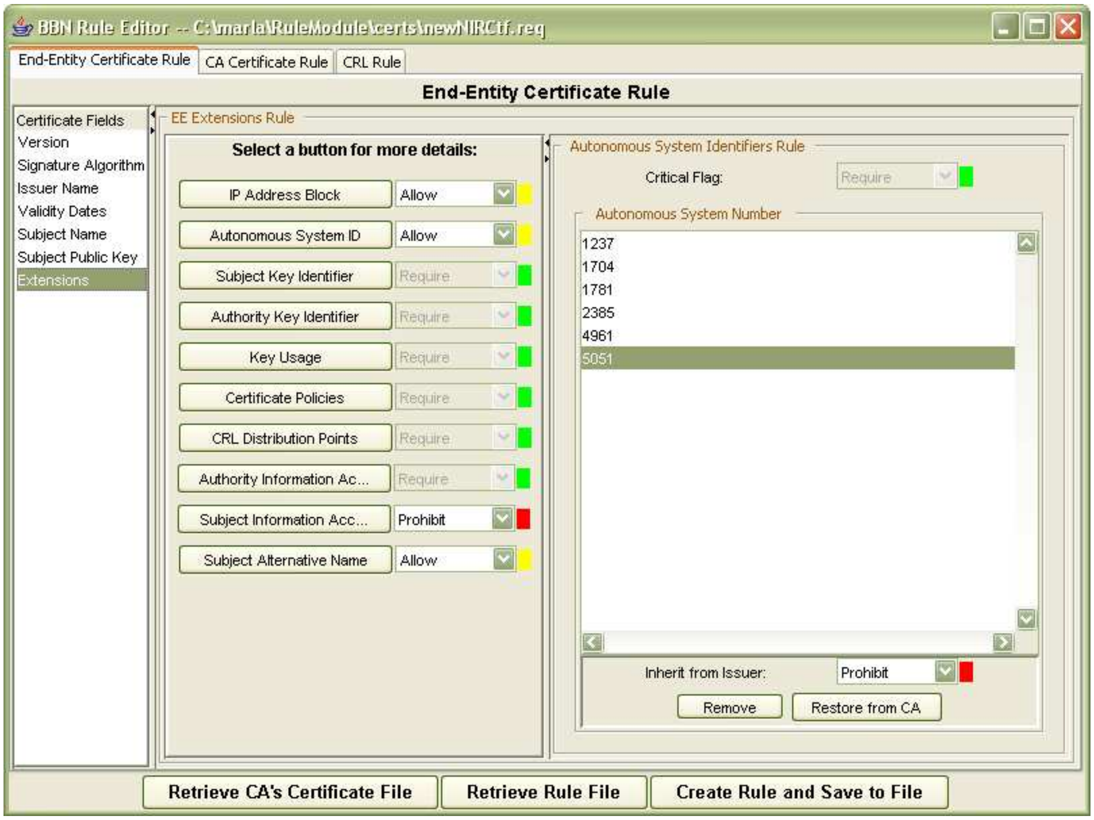
There is an optional text field to the right of each drop down box. This text box allows the user to impose restrictions on the allowable values for a particular field. For example, to specify that the Organizational Unit must be “Widget Dept.” for all end entity certificates issued by this CA, type “Widget Dept.” in the text field to the right. The drop down box can be set to either “Allow” or “Require.” Setting the drop down to “Allow” would indicate that field could be absent from the certificate, but if present must be “Widget Dept”. If the drop down is set to ”Prohibit,” the text field is cleared.

5.6 Subject Public Key

The subject public key algorithm is fixed at RSA (rsadsi-rsaEncryption), but the key size can be changed by the user.

5.7 Certificate Extensions

Selecting "Extensions" from the list at the left causes the right part of the window to break into two sections as seen in Figure 4. On the left is a list of buttons with a drop down box next to each. The buttons represent the list of extensions that are allowed to be in resource certificates per the profile for X.509 resource certificates. Clicking on a button changes the right side to display contents pertaining to the selected extension.


BBN Rule Editor -- C:\marla\RuleModule\certs\newNIRCtf.req
End-Entity Certificate Rule
CA Certificate Rule
CRL Rule
End-Entity Certificate Rule
Certificate Fields
Version
Signature Algorithm
Issuer Name
Validity Dates
Subject Name
Subject Public Key
Extensions
EE Extensions Rule
Select a button for more details:
Autonomous System Identifiers Rule
Autonomous System Number
Remove
Restore from CA
Retrieve CA's Certificate File
Retrieve Rule File
Create Rule and Save to File

IP Address Block	Allow	🟨
Autonomous System ID	Allow	🟨
Subject Key Identifier	Require	🟩
Authority Key Identifier	Require	🟩
Key Usage	Require	🟩
Certificate Policies	Require	🟩
CRL Distribution Points	Require	🟩
Authority Information Ac...	Require	🟩
Subject Information Acc...	Prohibit	🟥
Subject Alternative Name	Allow	🟨

Critical Flag: Require 🟩

1237
1704
1781
2385
4961
5051

Inherit from Issuer: Prohibit 🟥

Figure 4. Certificate Extensions Window

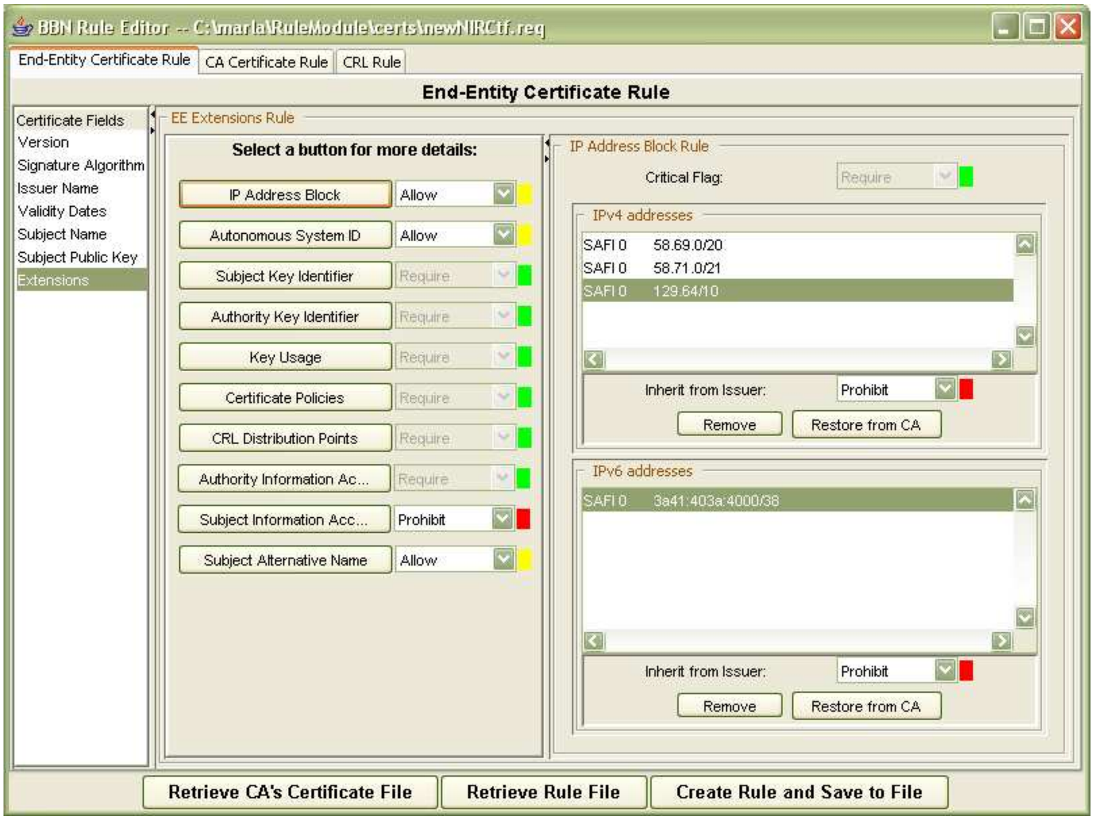
The drop down box next to each button determines if that extension is allowed, prohibited, or required to be in the certificate. A drop down box is disabled if that extension is required per the profile for X.509 PKIX resource certificates. If the drop down box is set to "Prohibit," then the right side of the window simply states that inclusion of the extension has been prohibited instead of showing contents pertaining to the extension.

Resource certificates must contain either an IP Address Block or an Autonomous System ID extension (or both). Both extensions start as being set to "Allow". If the user sets one to "Prohibit", the other will automatically be switched to "Require" and the drop down box will be disabled until the one that was prohibited is changed to either "Allow" or "Require."

Upon opening a CA certificate the Rule Editor performs a check to ensure that at least one of these extensions is present. If neither is there, then the Rule Editor indicates an error and asks the user to exit the Rule Editor or choose another CA certificate.

5.7.1 IP Address Blocks

The IP address block extension view shows the list of IPV4 list of address ranges on top and a list of IPV6 address ranges on the bottom. The list of addresses is taken directly from the current CA certificate . If this extension is missing from the CA certificate then this extension is prohibited from appearing in the rules. Figure 5 illustrates this interface.



IP Address Block	Allow	🟨
Autonomous System ID	Allow	🟨
Subject Key Identifier	Require	🟩
Authority Key Identifier	Require	🟩
Key Usage	Require	🟩
Certificate Policies	Require	🟩
CRL Distribution Points	Require	🟩
Authority Information Ac...	Require	🟩
Subject Information Acc...	Prohibit	🟥
Subject Alternative Name	Allow	🟨

Critical Flag: Require 🟩

IPv4 addresses:

```
SAFI 0    58.69.0/20
SAFI 0    58.71.0/21
SAFI 0    129.64/10
```

Inherit from Issuer: Prohibit 🟥

IPv6 addresses:

```
SAFI 0    3a41:403a:4000/38
```

Inherit from Issuer: Prohibit 🟥

Figure 5. IP Address Block Extension Window

The user can remove items from either the IPV4 or IPV6 list by selecting an IP address range and pushing the remove button. This could be used to allow the user to reserve some address ranges for later use, i.e., to ensure that the removed addresses are not permitted in any certificates issued by this CA.

Clicking the “Restore from CA” button resets the list contents to that shown in the current CA certificate. This is also true of a retrieved rule set (see section 8).

The critical flag is required.

5.7.2 Autonomous System Numbers

The list of autonomous system number ranges is taken directly from the current CA certificate. If this extension is missing from the CA certificate, this extension is prohibited from appearing in the rules. Figure 4 in Section 5.7 illustrates this interface.

The user can remove items from the list by selecting a number range and clicking the "Remove" button. This allows the user to reserve some ranges for later allocation.

Clicking the "Restore from CA" button will reset the list contents to that shown in the current CA certificate. This is also true of a retrieved rule set (see section 8).

The critical flag is required.

5.7.3 Subject Key Identifier

The Subject Key Identifier rule is fixed per the profile for X.509 resource certificates. The identifier will be produced using a 160 bit sha-1 hash of the subject's public key. The critical flag is prohibited.

5.7.4 Authority Key Identifier

The Authority Key Identifier is taken directly from the CA certificate. It is the subject key identifier of the CA certificate.

The critical flag is prohibited.

5.7.5 Key Usage

The Key Usage rule is fixed per the profile for X.509 resource certificates. Only the digital signature bit is set for end entity certificates and only the CRL sign and cert sign bits are set for CA certificates.

The critical flag is required.

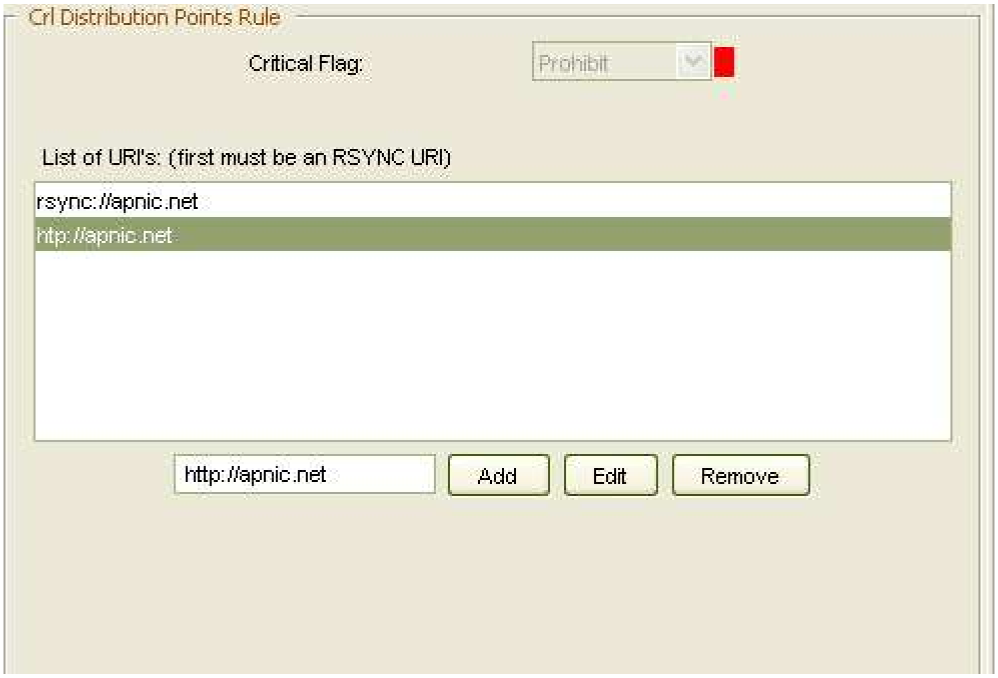
5.7.6 Certificate Policies

The certificate policy specifies the resource certificate policy, which is fixed at "1.3.6.1.5.5.7.14.2", as specified in the profile for X.509 resource certificates.

The critical flag is required.

5.7.7 CRL Distribution Points, Authority Information Access, Subject Information Access

The user interface for these three extensions is identical. For each the contents must be a list of one or more URI locations. The first URI in the list must begin with "rsync://", and there must be only one such entry.



Crl Distribution Points Rule

Critical Flag: Prohibit

List of URI's: (first must be an RSYNC URI)

rsync://apnic.net
htp://apnic.net

http://apnic.net

Figure 6. CRLDP URI List Window

An entry is added by typing the desired URI into the text field to the left of the three buttons, and clicking the "add" button. To edit an entry previously added, first select the entry with the mouse. The entry appears in the text field. Simply edit the contents and then click the "Edit" button to replace the highlighted entry with the contents of the text field. Figure 6 shows this interface with two URIs entered. The second has a misspelling of "http" so the entry was selected and then edited in the text field. The user can now push the "Edit" button to replace the selected value with the corrected value.

5.7.7.1 CRL Distribution Points

The CRL Distribution Points extension specifies the location where the CRL(s) associated with the issuer will be stored.

The critical flag is prohibited.

5.7.7.2 Authority Information Access

The Authority Information Access field specifies the name of a file containing the certificate of the issuer of the current CA's certificate.

The critical flag is prohibited.

5.7.7.3 Subject Information Access

The Subject Information Access field specifies the name of a directory containing files related to the subject of the certificate in which this extension appears, e.g., certificates signed by the currently active CA.

The critical flag is prohibited.

5.7.8 Subject Alternative Name

The subject alternative name is an optional extension. If this extension is allowed or required the interface shows four possible alternative name types. The user should set the drop down list for each to specify if that type of name is allowed, prohibited, or required to be in certificates issued. Note that at least one of the four must be allowed or required if the extension is allowed or required, so that if three types are set to “Allow” the remaining type will be automatically set to ”Require.” (If none are to be allowed, set the extension drop down box to ”Prohibit.”)

The critical flag is prohibited.

6 CRL Fields

6.1 Version

The version number of the CRLs is fixed at 2.

6.2 Signature Algorithm

The signature algorithm is fixed at sha256WithRSAEncryption.

6.3 Issuer Name

The Issuer Name is taken from the Subject field of the current CA certificate since that CA will be the issuer of all CRLs for which rules are being created.

6.4 This Update

The rule for this field allows the user to specify a time window around the time of signing the CRL. In this rule the current time refers to the time that the CA signs the CRL, not the time when the rule is created.

6.5 Next Update

The rule for this field allows the user to specify a time window for when the next CRL will be issued.

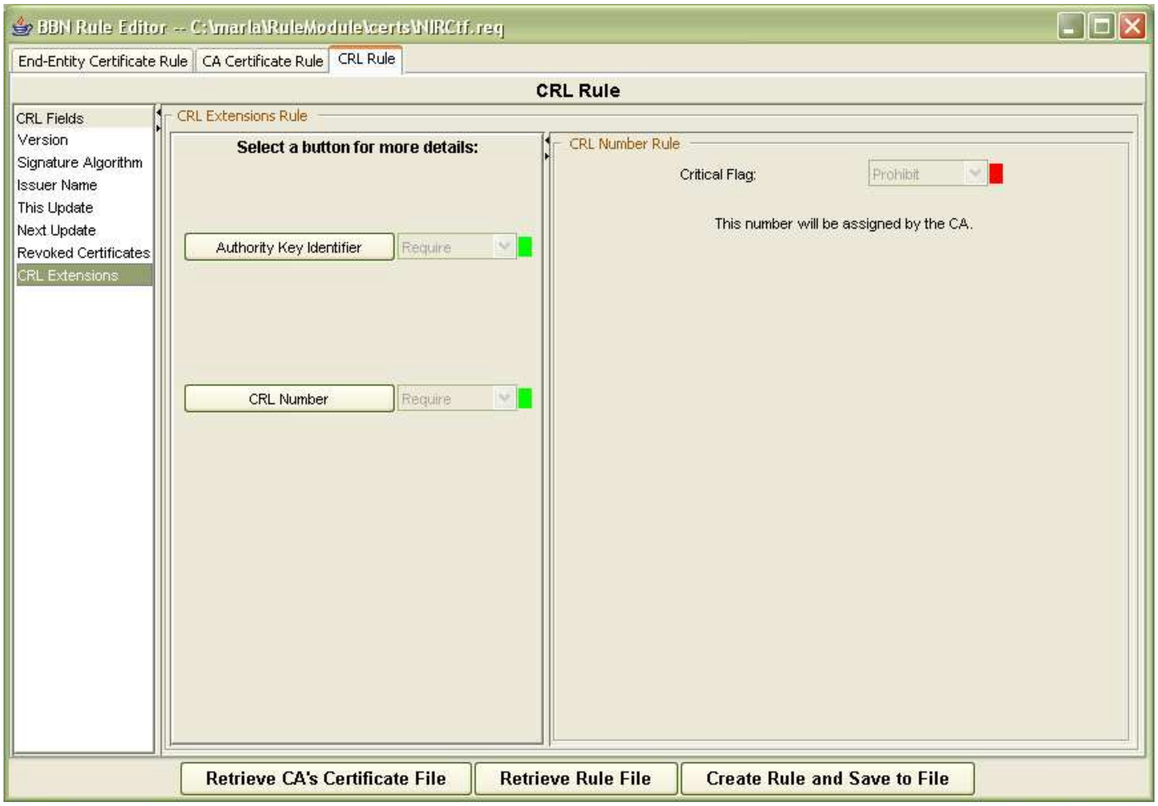
The rule may contain a fixed time, a fixed offset from the thisUpdateTime, or a range offset from thisUpdateTime. As an example, to specify that the next CRL will be issued every month, select the Fixed Offset radio button and enter 1 month to the right. As another example, to specify that the next CRL will be issued between 2 and 4 weeks after the current CRL, choose the range offset radio button and enter 2 weeks for the first value and 4 weeks for the second value.

6.6 Revoked Certificates

Revoked Certificates is a list of certificate number and revocation date pairs. Both values are required for each list entry. No rules can be specified for this portion of the CRL.

6.7 CRL Extensions

Selecting “CRL Extensions” from the list at the left causes the right part of the window to break into two sections as seen in Figure 7. On the left is a list of buttons with a drop down box next to each. The buttons represent the list of extensions that are allowed to be in CRLs per the profile for X.509 resource certificates. Clicking a button changes the right side to display contents pertaining to the selected extension.



Authority Key Identifier: Require 🟩

CRL Number: Require 🟩

Critical Flag: Prohibit 🟥

This number will be assigned by the CA.

Figure 7. CRL Extensions Window

6.7.1 Authority Key Identifier

The Authority Key Identifier must be present and is taken directly from the current CA certificate. It is the subject key identifier of the CA certificate.

The critical flag is prohibited.

6.7.2 CRL Number

The CRL number extension must be present and will be assigned by the CA. No rules can be specified.

The critical flag is prohibited.

7 Saving a Rule Set

Click the "Create Rule and Save to File" button to save the current set of rules to a file. If there are any errors in the rules, a dialog box will pop up to prompt you to fix them before saving. If there are no errors, then a browser dialog box will open. Find the desired directory, type in a file name, and click the save button. If there are errors, the Rule Editor will show a dialog box indicating where they are. These errors must be fixed before the rule set could be saved.

8 Editing an Existing Rule Set

Pushing the "Retrieve Rule File" button will open a file browsing window to select the desired rule file. Once a rule file is opened, the appropriate tab will be selected based on the type of rule set opened (i.e., End Entity, CA, or CRL rule), and the rule fields will be populated from the rules in the file. If the contents of the rule file conflict with the current CA certificate, an error pop up box appears indicating the error and the rule file will not be made available for editing. The rule fields will revert to values based on the contents of the current CA certificate.

9 Changing to Another CA Certificate

Clicking the "Retrieve CA's Certificate File" button opens a file browsing window to select the desired CA Certificate file. Once the file is opened, the rule fields will be either reset or populated from the certificate as appropriate. If there are any errors in the certificate or certificate extensions, an error box will pop up prompting the user either to either pick another certificate or to exit the Rule Editor. For example, if the CA certificate is missing both the IP Address Block and Autonomous System number extensions, or if there are overlaps in the ranges in the IP Address Block extension, or the ASN.1 does not parse properly, then the certificate is invalid and cannot be opened.