Lotus. Developer Domain
The Technical Resource for Lotus software
LDD Today

Be the authority on the Domino 6 Certificate Authority

Level: Intermediate
Works with: Domino 6
Updated: 01-Oct-2002

by Amy E. Smith,
ShiuFun Poon,
and John Wray

Domino 4.6 introduced the certificate authority (CA), a trusted server-based administration tool that issues and maintains both Notes and Internet digital certificates. These certificates (similar to those issued by third-party CAs such as **VeriSign**) verify the identity of an individual, a server, or an organization, and allow them to use SSL to communicate and to use S/MIME to exchange mail. Certificates are stamped with the certifier's digital signature, which assures the recipients of the certificate that the bearer of the certificate is the entity named in the certificate. The CA consists of an application that uses the CA process server task. (For more information on the 4.6 certificate authority, see the *Iris Today* article, "**Trust yourself: Become your own Certification Authority**.")

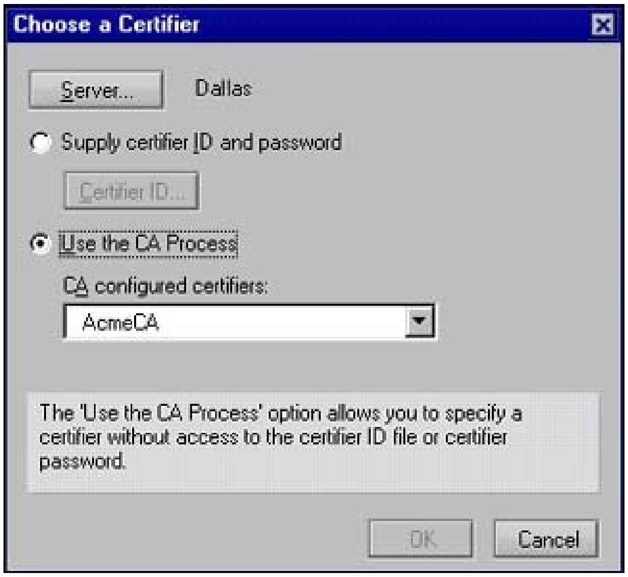
We've significantly enhanced the CA in Domino 6. For example, CA-issued Internet certificates are now compliant with security industry standards, such as X.509 v3 and PKIX. Much of the code for the Domino 6 server-based CA was developed as part of the joint IBM/Lotus/Iris **Jonah** project, a freeware implementation of the IETF's **PKIX Public Key Infrastructure** standards. The Jonah codebase takes advantage of the Domino application platform.

This article describes the CA and how we've improved it for Domino 6. We assume you're an experienced Domino administrator, and are familiar with security-related features and terminology.

The server CA process: the heart of the Domino server-based CA

Perhaps the most important change we've made to the CA in Domino 6 is the new server-based CA process task. The CA process handles requests for certificates that are placed in the Domino administration database (admin4.nsf). A Domino server can run only a single instance of the CA process, but that process can support multiple Notes and Internet certifiers. The CA process is the main reason we now refer to the Domino 6 CA as the "server-based CA."

In Domino 6, the CA process is integrated with the Notes/Domino administration process so that in all places where, in previous releases, an administrator would be required to specify a certifier ID file and password, there is now the additional option to choose a CA process certifier (in which case no password is required). The administrator simply selects the server that hosts the CA process and the particular certifier that should issue the certificate:



Dallas

○ Supply certifier ID and password

● Use the CA Process

CA configured certifiers: AcmeCA

The 'Use the CA Process' option allows you to specify a certifier without access to the certifier ID file or certifier password.

Unlike with R4.6 and R5 certifiers, certificates signed by the Domino 6 CA process are issued asynchronously. That is, a request for a certificate is placed into the administration database, but it may be some time before the CA process services the request. The delay may be only a few seconds if the request is made on the server that hosts the CA process, but it may be significantly longer if the request (and the resulting certificate) must move from one admin4.nsf replica to another. All user operations that result in certificates being issued have been enhanced to permit this asynchronous certificate process, generally by returning a provisional success message once the certificate request has been generated. The advantage of the asynchronous process is that the person requesting the certificate doesn't need to have the ability to also issue the certificate—in other words, the registration authority (RA) can be a different administrator from the person making the request. (We explain more about the new registration authority role in the next section of this article.)

For example, when registering a new user using the Domino server-based CA, you are informed that a certificate request has been created for the new user, but the user's ID file will yet not contain a signed certificate. When the CA process issues the user's certificate, the certificate will be attached to the user's Person document in the Domino Directory. When the user attempts to log in, the new certificate is downloaded to the user's ID file, completing the user registration. The user will be unable to log in before the certificate has been issued, and any attempts to do so will result in a message indicating that the user should try again later.

Aligning with PKIX standards: RAs and CRLs

To more closely align the CA with PKIX standards, Domino 6 incorporates two important new concepts: the registration authority and the certificate revocation list.

Registration authority (RA)

In Domino 6, all certificate requests—Notes and Internet—must be signed by an authorized administrator (known as a registration authority, or RA) before the Domino server-based CA will sign certificates. The RA role is defined by the PKIX standard and allows Domino administrators to delegate the user registration and certificate approval process. The most significant advantage of the Domino server-based CA is that RAs do not need to be trusted with the certifier ID to fulfill their tasks. Only the CA process itself needs access to the certifier ID file. Instead, you can grant administrators the right to act as an RA by assigning them the role when you set up a certifier. RAs are authorized to approve or deny certificate requests, and to register new users and servers. Moreover, you can have multiple RAs in an organization. For example, you could have an RA for each organizational unit.

Certificate revocation list (CRL)

Another important enhancement to the Domino 6 server-based CA is that Internet certifiers that use the CA process can create and maintain certificate revocation lists (CRLs). A CRL is a time-stamped list identifying revoked Internet certificates—for example, certificates belonging to terminated employees. The CA process issues and maintains CRLs for each Internet certifier. CRLs offer a way for Internet certificates to be rescinded or revoked if the certificate subject is no longer trusted. CRLs are published on a regular basis, according to a schedule defined when you set up the CA. You specify the duration of each CRL and the frequency with which they are published. For example, large organizations most likely have some ongoing employee turnover, and therefore need to publish CRLs more frequently than a small company with few employees.

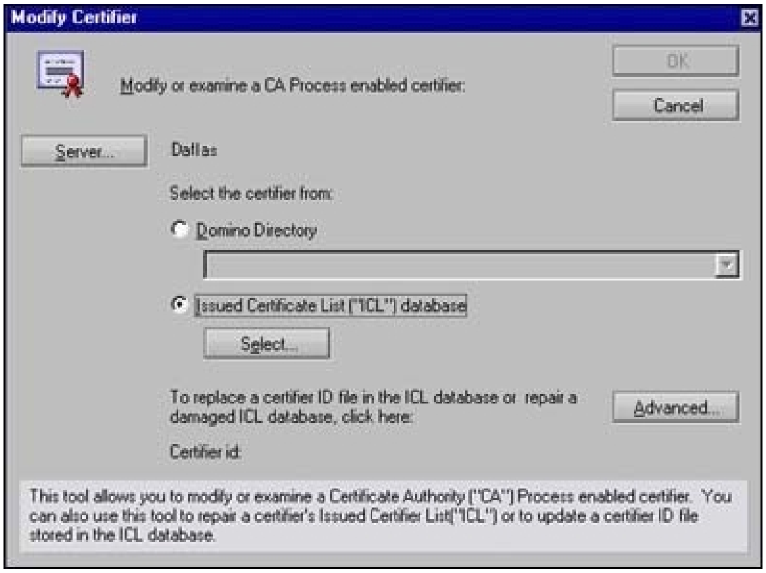
If necessary, an Internet certificate can be revoked from the certificate's Issued Certificate List (ICL) document. (See the following section.) Once a certificate has been revoked, it appears on subsequent CRLs created by the CA, until the certificate's expiration date has passed. Clients or servers wishing to check whether a given certificate has been revoked may obtain the CRL from the Domino directory (using either Domino APIs or LDAP) and verify that the certificate is not listed. Note that while CRLs are published periodically by the CA process (for Internet certifiers configured to support CRLs), the act of revoking a certificate does not cause a CRL to be published. If immediate revocation is desired—for example, the key has been compromised—you can publish an additional "nonregular" CRL that includes the revocation information once the certifier has processed the revocation request.

Even this will not guarantee immediate revocation, because CRL users may continue to use cached copies of a CRL until it expires. Thus, it is important that administrators set a reasonable schedule for publication and expiration of CRLs. By default, Domino publishes a CRL on a daily basis, and each CRL has a lifetime of two days. Decreasing these intervals allows for more immediate revocation, at the cost of increased network and directory load as CRL caches are refreshed more frequently. Also note that if certificates are frequently revoked, CRLs will grow large, which further increases system load. The best way to minimize this is to ensure that certificate lifetimes reflect the trustworthiness of the certificate owner. In other words, issue long-lived certificates only to those whom you trust, and expect to continue to trust, for the lifetime of the certificate.

The Issued Certificate List: the brains of the Domino 6 CA

When you configure a Domino 6 CA, you specify the server whose CA process will act for the certifier. This creates an Issued Certificate List database (ICL) on that server for that certifier. An ICL is unique to each certifier. It stores the certifier configuration information (for example, the list of authorized RAs) as well as details of all certificates the certifier has issued (such as certificate expiration dates). Some of the information from the ICL—namely, the list of RAs and the list of administrators permitted to change CA configuration data—is also attached to the certifier's record in the Domino Directory.

Administrators can modify certain aspects of the Internet certifier (for example, the list of RAs) either by editing the certifier document in the Domino Directory or using the Administrator client's Modify Certifier tool, which is shown in the following screen. The only procedure done directly in the ICL is Internet certificate revocation.



Modify or examine a CA Process enabled certifier:

Dallas

Select the certifier from:

○ Domino Directory

● Issued Certificate List ("ICL") database

To replace a certifier ID file in the ICL database or repair a damaged ICL database, click here:

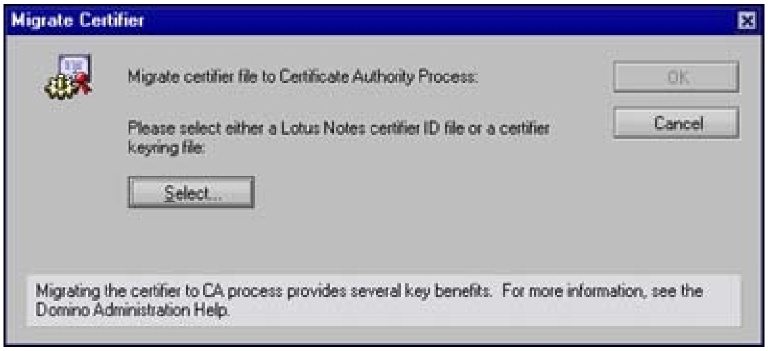
Certifier id:

This tool allows you to modify or examine a Certificate Authority ("CA") Process enabled certifier. You can also use this tool to repair a certifier's Issued Certifier List("ICL") or to update a certifier ID file stored in the ICL database.

Implementing the Domino 6 server-based CA

As domain administrator, you can choose to configure some or all of the domain certifiers as CA process-enabled certifiers. A given certifier should only be used as a Domino server-based CA or as an R5-type CA (that is, one not enabled for the server-based CA process). This is particularly important for Internet certifiers, because certificates can only be revoked if there is a record of them in the certifier's ICL database, and such records are created only for certificates issued from a Domino server-based CA.

You can migrate existing Notes certifiers to the Domino 6 CA process through the Migrate Certifier option in the Domino Administrator client. This option is shown in the following screen. New Internet certifiers can be created as CA process certifiers, or an existing R5 certifier can be migrated to the CA process. After such a migration, the original certifier ID file, or keyring, should no longer be used, to avoid gaps in the ICL certificate log.



Migrate certifier file to Certificate Authority Process:

Please select either a Lotus Notes certifier ID file or a certifier keyring file:

Migrating the certifier to CA process provides several key benefits. For more information, see the Domino Administration Help.

The Domino 6 server-based CA process is intended to be used as an alternative to the R5 Notes certifier—it provides equivalent functionality, but offers an alternate usage mode. It's also a replacement for the R5 Internet certifier, over which it provides an enhanced feature set. The CA process Internet certifier is intended for environments where it is feasible to establish a corporate set of trusted root certificates (for example, for intranet use) that clients and servers can use to communicate via SSL. The certifier can also issue certificates for use with secure email (S/MIME email).

Certificate request database
You can create a Web-accessible Certificate Request database (certreq.nsf) that browser clients can use to obtain SSL certificates for subsequent authentication to Domino or other Web servers. The certificate request database can run on any Domino server (including servers that exist in a DMZ), so long as it has a replica on a machine that has an administration database enabled.

The Certificate Requests database can also be used to issue certificates for Domino and third-party Web servers, as well as to directly create a Domino server keyring, simplifying the process of establishing SSL for Domino servers.

Web administration
Once a domain is established and an Internet certifier configured, Domino 6 can use the Internet certifier to configure SSL during server setup. This means that, after initially securing a new domain, a site can use the Web Administration database to securely register additional servers without first having to use the Administration client to configure SSL on the new server. Moreover, the use of the Domino server-based CA is required if you are using the Web Administrator to register Notes users. In this situation, the organizational Notes certifier must be enabled for the CA process.

Domino 6 server-based CA: securing safer access

As we've described, Domino 6 offers a significantly enhanced CA that now uses a server-based process to handle certificate requests and that is more closely aligned with Internet standards. The close adherence to public-key infrastructure industry standards make the option of using Domino server-based CA a viable alternative to that of third-party certifiers. We've also made it easy to migrate to Domino 6, allowing for a smooth upgrade from existing Domino R5 certifiers.

For more information on public key infrastructure (PKIX and X.509) standards:

- **Public Key Infrastructure charter page** is the best place to find information about public key infrastructure standards.
- **Internet Engineering Task Force (IETF) home page** has a fairly complete overview section that describes the IETF and its various working groups for different Internet standards.
- **PKIX profile of X.509 standard** defines the contents of a public key certificate. It describes the use of public key certificates and the way in which they're issued and contains useful references to other documents.
- **RFC 2587 Internet X.509 Public Key Infrastructure: LDAPv2 Schema** and **RFC 2559 Internet X.509 Public Key Infrastructure: Operational Protocols - LDAPv2** describe the use of an LDAP directory to store certificates and CRLs, which is how the Domino Directory is used by certificate verifiers (for example,

Internet Explorer).

ABOUT THE AUTHORS

Amy E. Smith is a principal user assistance writer for Lotus. She's primarily responsible for Domino administration documentation, particularly security. Amy is also a member of the GPD UA Web team.

ShiuFun Poon is a Software Engineer on the Domino 6 Security team. She slaves over her two "spoiled" miniature schnauzers in her spare time.

John Wray is a Senior Software Engineer on the Domino 6 Security team. He was the architect for the Jonah freeware CA project and has led the work to incorporate Jonah into Domino.