Secure Email between Lotus Notes and the Outside World

By Chuck Connell, www.chc-3.com

In 2001 I wrote an article about Notes and S/MIME email security. That article provides a general introduction to the principles of email encryption and signatures, explains how the S/MIME protocol works, and gives some details about using S/MIME with Domino and Notes. The article has remained popular during the past 10 years, and most of the information in it still applies. But the article suffers from two problems.

- It glosses over some of the nitty-gritty details about setting up S/MIME for Notes users and non-Notes outside recipients.
- It is a bit dated, since it refers to R6 of Notes/Domino, which is two major versions old.

With this new article, I revisit the same topics but provide more detailed, current instructions. The general goal is the same: To send and receive secure (signed and/or encrypted) email between Notes users and non-Notes outside users. Since it is the most common, I assume that the outside user is on the Windows operating system and is using Outlook as their email program.

The instructions below may appear daunting, but nearly all of the steps are one-time-only during the setup phase. Sending and receiving secure email is very simple once the setup is done.

Add the Certificate Authority task to the Domino server.

1. Using Windows Explorer (or similar) on the Domino server, go to the Domino program directory.
2. Edit notes.ini. Add ",CA" to the ServerTasks line.
3. Restart Domino.

Create an Internet root certifier.

1. A Domino admin person logs on to Domino Administrator
2. Go to Configuration / Registration / Internet Certifier.
3. Choose "I want to use the CA process".
4. Select the server = <your main server>.
5. Press the button "Create Certifier Name". Enter a Common Name (required) such as Acme-Corp-Email, and other fields if you want.
6. Set the filename for the ICL database to something like ICL_Acme-Corp-Email.nsf.
7. Set Encrypt Certifier ID With = Server ID.
8. Set Require Password to Activate = NO.
9. If possible, add at least one other person (in addition to yourself) as an administrator, both CAA and RA.
10. Go to the MISC tab.

11. Press “Create a local copy of the certifier ID”.
12. Press “Set ID file”. Give the ID file a logical name such as Acme-Corp-Email.id. Choose a good password and write it down somewhere.
13. Go back to the BASICS tab. Press OK to create the certifier.
14. Wait 30 minutes or so, to be sure the AdminP process has created the certifier.
15. Go to the Domino console and type TELL CA STAT. You should see the new certifier with state “Active=Yes”.
16. You can speed up the certifier creation by typing the following commands at the Domino console: TELL ADMINP PROCESS ALL, then TELL CA REFRESH, then TELL CA STAT.

Create and install the Notes email certificates. These steps are one time only for each Notes user…

1. One of the people authorized to create Internet certificates logs on to Domino Administrator
2. Go to People & Groups / People, select users who will be sending/receiving encrypted email, then pull down Actions / Add Internet Cert To Selected People.
3. Make sure the server is set to your main server, and CA Process = Acme-Corp-Email.
4. Wait about 30 minutes, to make sure the certificates are created and installed in each user’s Person record.
5. Verify the certificates are ready to go. Open each Person record / Certificates / Internet Certificates / Internet Certificate = present / Issuer = Acme-Corp-Email.
6. Wait another 30 minutes or so, to allow the certificates to be installed into each person’s Notes ID file. The users should exit and restart their Notes client software a couple times, to force their IDs to receive the new certificates.
7. Each user should check that they have the new certificates. File / Security / User Security / Your Identity / Your Certificates / Your Internet Certificates / Issued By = Acme-Corp-Email.

Outside person purchases a Verisign Digital ID. These steps are one time only for each outside person…

1. Go to http://www.verisign.com/authentication/digital-id/index.html and follow the instructions there. The price is $20 per year.
2. This digital ID is useful for secure email with anyone, so is not limited to just email with your Notes organization.

Notes user sends public key to outside person. These steps are one time only for each pair of email correspondents.

1. Notes user calls outside person on the phone and says, “I am about to send you my email key. When you get that email, you can trust that it is from me.”
2. Notes user sends signed email to outside person. Delivery Options = Sign.
3. Outside person receives the signed email. When he/she sees a question about whether to trust the signer, they say YES.
4. Outside user adds Notes person to their contact list. This is usually done by opening the email, right-clicking on the name, and choosing “Add to Contacts”.
5. Outside user checks that the email key has been accepted. Open the contact list, open the contact information for the Notes person, click on Certificates, then properties. It should say Issued By = Acme-Corp-Email.

Outside person sends public key to Notes user. These steps are one time only for each pair of email correspondents.

1. Outside person exports his/her Internet certificate. In Windows, Start / Control Panel / Internet / Content / Certificates / your name / Export / no private key / DER encoded CER.
2. Outside person calls Notes user on the phone and says, "I am about to send you my email key. When you get that email, you can trust that it is from me."
3. Outside person sends certificate to Notes user as a signed email. Outside person creates an email with the .CER file as an attachment, and signs the mail. In Outlook, this is found under Options / red seal.
4. Notes user receives the signed email. When he/she sees a question about whether to issue a cross-certificate, they say YES.
5. Notes user adds outside person to their contact list. Right click on the message / Add Sender to Contacts / Include X.509 Certificates = Yes.
6. Notes user checks that the email key has been accepted. Open the local address book (names.nsf), then open the contact information for the outside person. Go to Certificates. Check that Certificate=Present and Issuer=VerisignClass1.
7. If the certificate is not present, detach the .CER file from the incoming mail and perform a manual import. Open the Notes contact again and choose Actions / Certificates / Import Internet Certificate / File Type = CER / select file / Open.

Notes user sends signed and encrypted email to outside person, and Outside person verifies it.

1. Notes Delivery Options = Sign + Encrypt.
2. Outside person may be asked permission to use their private key (needed to decrypted the message). Click YES or GRANT.
3. Outside person sees indication that the mail is signed and encrypted. In Outlook, these are a small red "seal" icon and a small blue lock. Clicking on these icons will verify who sent the message and who it was encrypted for.

Outside person sends signed and encrypted email to Notes user, and Notes user verifies it.

1. In Outlook, this is found under Options / blue lock + red seal.
2. Notes user sees indication that the mail is signed and encrypted. This is found near the lower-right of the screen. There is a small red pen if the mail is signed, and a black lock if it is encrypted, and both if the mail is signed + encrypted.

Chuck Connell is president of CHC-3 Consulting, which helps organizations with all aspects of Lotus products – Domino, Notes, Sametime, LotusLive and others.