SSL client authentication: It's a matter of trust

Joann Spera

March 02, 1998

This article introduces client authentication with SSL (Secure Sockets Layer, a security protocol), discusses its benefits and explains how to set up SSL client authentication on a Domino 4.6 or 4.6.1 server.

[Editor's note: This article explains how to set up SSL client authentication for both Domino 4.6 and 4.6.1.]

The latest industry buzzword in security on the Internet is SSL. But what does SSL really have to offer?

Secure Sockets Layer (SSL) is a security protocol that:

- Encrypts information sent over the network.
- Validates that a message sent to a recipient arrived without tampering.
- Authenticates the server identity to prevent server spoofing.
- With SSL 3.0, authenticates the client identity.

For an introduction to these SSL concepts, see Hugo Curbelo and Russell Lipton's article, "SSL: it's not just for commerce anymore." In addition, check out the Lotus Internet Security Zone and Netscape's SSL information.

The focus of this article is on the last item, client authentication. The article will give a brief introduction to client authentication with SSL, detail the benefits of using client authentication, explain when you might not need client authentication, and outline the steps involved with setting up client authentication on your server.

What is client authentication?

Client authentication is a nifty feature that lets you authenticate users who are accessing the server by exchanging a client certificate -- this means no more "Anonymous" entries appearing in the User Activity log of a database when accessed by an Internet user. And, the client certificate is vouched for by either an external Certification Authority (CA), such as VeriSign, or by you as an internal CA, so you can be assured that the person represented by the certificate is the person you expect. If you are not familiar with CAs or trusted roots, read the article, "Trust Yourself: Become Your Own Certification Authority."
With the release of 4.6.1, using client authentication just got a whole lot easier than before. You can now use the Certificate Authority application in Notes to issue both client and server certificates. You cannot issue client certificates using Release 4.6; however, you can obtain the client certificate from an external CA and use the client certificate to authenticate users accessing a Domino server.

**Things to know about client authentication**

Client authentication requires a client certificate in x.509 format from a CA. The x.509 format is an industry-standard format for SSL certificates. In 4.6.1, Notes creates client certificates using this format. Using a standard format ensures that Domino and other applications can exchange certificates easily.

The certificate contains information about the user, in addition to a unique private-public key pair. For Netscape users, the client certificate is stored in the certificate database on the server machine. For Microsoft Internet Explorer users, the client certificate is stored in the registry. In order to verify the user, the Public Address Book on the server that the client accesses must also contain the user's public key.

Client authentication occurs when the server requests the client certificate during the SSL handshake over the network. One thing to keep in mind is that the server controls whether client authentication occurs; a client cannot ask to be authenticated.

Like a server certificate, a client certificate can be issued with different classes. The classes indicate the amount of investigation, typically out-of-bandwidth procedures (such as, face-to-face contact with the client), used to determine the identity of the person requesting the certificate. Classes are important when your users receive certificates from external CAs, since you want to make sure that the CA took the utmost precautions when issuing the certificate. Classes of certificates are of lesser importance when they are issued by an internal CA, since typically you will use already established processes to ensure user identity.

If you are familiar with Notes IDs, then you will quickly see the similarities between the Notes ID and client certificate designs. Here are some similarities:

- A Notes ID is a unique identifier for a user and contains the person's public and private key pair. The public key also exists in the Public Address Book in that user's Person document. Like the Notes ID, a client certificate has both a public and private key, and the public key exists in the Public Address Book.
- When you want to communicate with organizations other than the one that is stamped on your Notes ID, you request a cross certificate and merge that into your Notes ID. With client certificates, you merge the other organization's CA certificate as a trusted root into your client certificate.

There are also some major differences between Notes IDs and client certificates:
• Notes IDs are stored in a binary file on your hard drive. Client certificates are stored in your browser. Because of this, you cannot move your client certificate from one computer to another.
• This should be no surprise, but it's worth mentioning: you cannot use your client certificate for Notes RPC transactions, for example, replication.

**Client certificates: the internals**

You can think of a client certificate as follows:

**Figure 1. Client certificate diagram**

- The certificate information section contains information about the SSL version number, the serial number for the certificate, and other information that identifies this certificate.
- The CA name is the name of the CA that issued the client certificate.
- The validity period is the date on which the certificate was issued and the date it will expire.
- The client name is the name you specify when you request a certificate. This is a hierarchical name, for example, Joann Spera/Acme/Lotus/US. If you already registered using Notes, the client name is the common name that appears in the Person document.
- The public and private key pairs are generated when you send your request to the CA and are used for client identification and encryption over the network. You can select the size of your public and private keys; however, you cannot make this choice if you are creating an international key pair -- 512 bits is your only choice. The key pair size indicates the strength of the security. The larger the size used when generating the key pairs, the stronger the security.
  Do not confuse the key pair size with the negotiated session key. The key pair is the public and private key combination that uniquely identifies the client. The negotiated session key is the encryption key created when initiating an SSL session between the server and client. If you are using software licensed in North America, you can use up to 128 bits for the session key. Release 4.6.1 also allows 128-bit encryption for communication to international sites if the site uses the VeriSign Global ID.
- Depending on the version of the x.509 certificate you are using, your certificate may contain additional information and extensions.
- The digital signature of the CA is added to the client certificate when you merge the CA as a trusted root. You could have many digital signatures attached to a single certificate, depending on the number of trusted roots you merged.
Client authentication: the big win

As mentioned previously, you can use client authentication to identify and control access for users who are accessing the server. This is a simple concept that has exciting opportunities.

You can set up specific access to a database based on the user name instead of setting up access for all Anonymous users. For example, if you want Alan Jones to have Editor access to a database and all other Internet users to have Reader access, you could add Alan's name to the ACL with Editor access and add an Anonymous entry to the ACL with Reader access. Without client authentication, all anonymous users can only have the same level of access to the database. Client authentication takes away this restriction and allows you to specify access on an individual basis.

Another way to use client authentication is to set up a profile document that performs a calculation based on the user name. For example, when a specific user opens a database, use the settings for the user stored in the profile document to change the display of the database.

Identifying users not only works in the database ACL, profile documents, and formulas, but also the design access lists such as view, form, and reader fields.

All this bundled with message integrity, server authentication, and network encryption makes for a pretty strong case for using client authentication.

You might be wondering whether you could use SSL server authentication with Domino basic password authentication to perform the same function as SSL client authentication. If you are not familiar with Domino basic password authentication, it is a security mechanism that requires the user to enter a name and password when accessing the server. If you have SSL server authentication enabled, the name and password is also encrypted using SSL when sent over the network.

Client authentication differs from server authentication with Domino basic password authentication in significant ways. Here's how they compare:
SSL client authentication: It’s a matter of trust

Figure 2. Comparison table of client and server authentication

<table>
<thead>
<tr>
<th></th>
<th>SSL client authentication</th>
<th>SSL server authentication with basic password authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requires the user to enter a name and password</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Encrypts transactions over the network, identifies the server, and validates messages sent</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Validates user identity</td>
<td>Yes</td>
<td>Not validated by a third party – only as trusted as the physical security imposed on the name and password</td>
</tr>
<tr>
<td>Portable to other computers</td>
<td>No–browser software contains the certificate</td>
<td>Yes–user can enter the name and password on any machine</td>
</tr>
<tr>
<td>Name and password encrypted over the network to prevent eavesdropping</td>
<td>n/a</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Depending on your organization, you might benefit from some of the client authentication's seeming lack of functionality. For example, if your users continually forget or lose their passwords, the fact that they do not have to enter a name and password might be beneficial. In addition, by not allowing the client certificate to move to another computer, you might further secure data since a hacker must have explicit access to the computer to impersonate a user.

When you might not need client authentication

Client authentication may not be the security solution for everyone. Before you commit to using client authentication at your organization, here are some things to think about:

- Do you need to gather information on users accessing your server or control access to databases based on the user identity? If not, don't bother with client authentication. If you set up server authentication, the data transmitted is still secured and the server identity is validated for the user.
- Both you and your users accessing the server must perform steps to set up client authentication. If you have a Web site that you want users to access easily and the bullet above doesn't apply, then you probably do not want client authentication. Users might get discouraged and leave your site if you require them to get a client certificate before accessing it.
- If it is a requirement at your organization that clients must use multiple computers and you do not want to set up client authentication for the user on each computer, then use SSL server authentication with Domino basic password authentication instead. This lets the user identify themselves without requiring that they use the same computer each time they access the server.

Internal vs. external CA client certificates

If you are using Release 4.6, your choice is an easy one: you must obtain a client certificate from an external CA because the Release 4.6 Certificate Authority application does not allow you to create client certificates.
If you are using Release 4.6.1, you have the choice of obtaining a client certificate from either an internal or external CA. Keep in mind that even if you set up your servers using an internal CA, you can still obtain client certificates from an external CA and use them with these servers. Domino adheres to the x.509 standard, which lets certificates from an internal and external CA work seamlessly together.

In most instances, if you have an internal CA already set up at your organization, then you will want to issue client certificates using the internal CA. External CA's charge a fee for new certificates and yearly renewals, so to avoid these costs, use the internal CA. And, with the new, streamlined Certificate Authority application in 4.6.1, setting yourself up as a Certification Authority and picking up and requesting client certificates is a snap.

Even if your users obtain certificates from an external CA, you and your users will still need to use the Certificate Authority application to set up client authentication. The CA uses the application to add the client public key to the Public Address Book. Clients use the application to merge the server CA's certificate into their client certificates, if the server's certificate was issued from an internal CA.

**Client authentication: the steps**

Setting up client authentication involves both the client and the CA. The steps below show you an overview of how to set up client authentication on both Domino 4.6 and 4.6.1. You can then go to the sidebar articles to see the steps in detail. Notice that some of the steps are the same regardless of whether you are setting up client authentication for 4.6 or 4.6.1.

**Note:** Before getting started, make sure you have already set up the server as a Certification Authority server. (For information on how to set up your server as a CA, see the article, "Trust Yourself: Become Your Own Certification Authority.")

## Setting up client authentication for Domino 4.6.1: Overview

Here's an overview of the steps involved for setting up SSL client authentication for Domino 4.6.1.

1. Add a Person document to the Public Address Book. The CA needs to add a Person document to the Public Address Book for the user if they don't already have one. Notes stores the client public key in the Person document.
2. Request the client certificate. The client fills out a request for the certificate by accessing the Certificate Authority application using a browser.
3. Merge the server's CA certificate as a trusted root. Clients must have the trusted root certificate for the servers that they want to access.
4. Approve the request and add the public key to the Person document in the Public Address Book. The CA uses the Certificate Authority application to approve the client certificate request sent to them in step 2 above. The CA then adds the client's public key to the Person document.
5. Merge the approved certificate. After the CA approves the certificate, the client merges the certificate into the browser software.
6. Configure the Server document for client authentication. The CA must enable SSL and client authentication on the server so Domino requests the client certificate during the SSL handshake.

For more details on these steps, see the sidebar article, "Setting up client authentication for Domino 4.6.1."

**Setting up client authentication for Domino 4.6: Overview**

Here’s an overview of the steps involved for setting up SSL client authentication for Domino 4.6.

1. Add a Person document to the Public Address Book. The CA needs to add a Person document to the Public Address Book for the user if they don't already have one. Notes stores the client public key in the Person document.
2. Request the client certificate. Since Release 4.6 does not let you issue client certificates from the Certificate Authority application, the client requests the certificate from the external CA's Web site. After obtaining the certificate, the client submits a request to add the public key to the Person document in the Public Address Book.
3. Merge the server's CA certificate as a trusted root. The client must have the trusted root certificate for the servers that they want to access.
4. Add the public key to the Public Address Book. The CA approves the request sent by the client in step 2 to add the public key to the Public Address Book.
5. Configure the Server document for client authentication. The CA must enable SSL and client authentication on the server so Domino requests the client certificate during the SSL handshake.

For more details on these steps, see the sidebar article, "Setting up client authentication for Domino 4.6."

**Testing your setup**

Try the following to make sure you set up client authentication properly:

- Change the ACL for a database on the server and give Anonymous users no access and give Reader access to a client to whom you issued a certificate.
- From the client's computer using a browser, enter https://name_of_server/database_name

If you are not prompted for a name and password and you can get into the database, then client authentication is working. You can look at the User activity log in Database properties and make sure the client name appears.

**Bonus exercise**

In 4.6.1, you can set up your system so Domino searches multiple Public Address Books when users access the server. With this feature, you can include several Public Address Books on a server -- for example, one for Notes users, Internet users, and both Notes and Internet users -- and Domino automatically searches the address books until it finds the user's certificate.
You must know about the Directory Assistance feature before attempting this task.

1. Set up directory assistance
2. Open the Master Address Book.
3. Open the Directory Assistance document for each domain you want to search for client certificates.
4. In the naming rules section, choose Yes in the Trusted field for those naming hierarchies that you want to search when adding a new client certificate or when clients authenticate with the server.
5. Save the Directory Assistance document.
Related topics

- Setting up client authentication for Domino 4.6.1
- Setting up client authentication for Domino 4.6
- SSL: it's not just for commerce anymore
- Trust Yourself: Become Your Own Certification Authority
- Lotus Internet Security Zone
- Netscape's SSL information