CryptoWorks21

FUNDAMENTALS OF NETWORK SECURITY

PRACTICAL — X.509 CERTIFICATES AND S/MIME SECURE EMAIL

In this exercise, you will learn how to setup an X.509 certificate authority and send secure e-mail using S/MIME. You will make use of the XCA certificate authority software.

Step 0: Install XCA

You will make use of the XCA certificate authority software, which is available for Windows, Mac, and Linux. You can download it from http://sourceforge.net/projects/xca/. Once you have installed it, proceed with the steps below.

Step 1: Setup root CA

First we will put on our "Certificate Authority hat" and setup the CA.

1. Open up the XCA application.
2. Create a new database: File -> New Database.
3. Create a new private key. Name your private key "My CA private key". You should use an RSA key of at least 2048 bits.
4. Next you need to generate a new certificate for this key: Certificates -> New certificate.
5. You want to create a self-signed certificate, using the "CA" template.
6. On the "Subject" tab, fill in all of the fields of the distinguished name with some dummy values.
7. On the "Extensions" tab, make sure the "Type" is set to "Certification authority".
8. Click "OK".
9. The root certificate will be created, and you can double click on it to view its properties.

Step 2: Generate a user's private key and certificate signing request

Now we will put on the "user hat", playing the role of a user who wants to get a certificate for email signing. Normally these would be done on separate computers, but we'll do it all on the same computer for ease.

1. On the "Private Keys" tab, create a new private key called "My email private key".
2. On the "Certificate signing requests" tab, click the "New request" button.
3. On the "Subject" tab, fill in the Distinguished name with dummy values for the user, but be sure to fill in the email address you want to use.
4. Make sure the "Private key" drop down is for "My email key".
5. On the "Key usage" tab, select "Digital signature", "Non repudiation", "Key encipherment", "Data encipherment", and "Email protection".
6. Click "OK".
7. The certificate request will be created, and you can double click on it to view its properties.

Step 3: Sign the user's certificate signing request

Now we will switch back to our "certificate authority hat". Imagine the certificate authority has received the certificate signing request from the user. The CA will now generate a certificate for that user.

1. From the "Certificates" tab, click "New certificate".
2. Click "Sign this certificate signing request" and select the request your user just created.
3. Click "Use this certificate for signing", and select the CA certificate you created in Step 1.
4. Click on "Show request" and check the values supplied by the user to make sure you approve the information they entered. In particular, you should not sign any certificates that themselves ask to be a certificate authority, as you would be allowing the user to generate other certificates.
5. Click "OK". Your certificate will appear in the list of certificates. You can double click on it to view its properties.
6. Export your key and certificate as "PKCS #12 with certificate chain". Remember where you saved the file.

Step 4: Send a signed email

First you need to set up an email account in a local mail program. The following instructions are for setting up an account in Mozilla Thunderbird using the IMAP protocol. Other desktop mail clients, such as Microsoft Outlook or Apple Mail, also support S/MIME. But most webmail sites do not support S/MIME at present.

To set up a Gmail account:

1. Log in to Gmail
    a. Go to Gear in top right, then click "Mail Settings".
    b. Click on "Forwarding and POP/IMAP".
    c. Click "Enable IMAP" and "Save Changes".
2. In Thunderbird:
    a. Enter your name, Gmail address, and Gmail password.
    b. Select "IMAP" then "Create Account".

To set up a University of Waterloo IMAP account:

1. Set up a new account in your mail program using the settings at the following URL:

    https://uwaterloo.ca/information-systems-technology/services/student-email/mailservices/set-up

Your inbox should now be available through Thunderbird. It should be possible to send yourself email. You might want to give this a try to make sure it works.

Now you need to install that certificate in Thunderbird:

1. Go to Edit->Preferences->Advanced->Certificates->View Certificates.

2. Under Your Certificates, click Import.
3. Import the .p12 you just saved; use the same password you used in the export function.
4. You may need edit the trust of the CA you just added:
    a. Preferences > Advanced > Certificates > Manage Certificates > Authorities > [Select added CA] > Edit Trust > "This certificate can identify mail users."

To install the certificate in Apple Mail on Mac OS X:

1. Open the application “Keychain Access”.
2. Go to File->Import Items.
3. Import the .p12 you just saved; use the same password you used in the export function.
4. If Apple Mail is set up with an account that has the same email address as in the certificate, you will see signing and encryption icons appear in the mail composition window.

Try sending yourself a signed email, an encrypted email, and a signed and encrypted email.

TO SUBMIT

1. Send me a signed email at stebilad@mcmaster.ca.
2. If I receive your signed email, do I really have any assurance that it’s coming from you? Why or why not?
3. Why can’t you send me an encrypted email?