1 Introduction

You are to implement identity Certificate Authorities (CA). There are three types processes: clients, CA servers, Group servers.

Certificates are of two types.

identity certificates binds a user to a given public key and is “signed” by a CA. It contains fields for the user name, public key, CA name, and signature.

delegation certificates state that a CA $c_0$ says that CA $c_1$ can also issue certificates as if they were signed by $c_0$. These certificates provide $c_0$ and $c_1$’s ids, FQDN, and port; they are signed by $c_0$. (Note that delegated CAs can also delegate).

Normally, signatures are created cryptographically to prevent forgery, and are a combination of signer and the contents of the certificate. However, for the purposes of this project we will use a constant signature per entity, whether the entity is a CA or a user.

Certificates also have validity to and from dates during which the certificate is valid.

The configuration files are as follows:

- Client: contains a set of top level CAs, specifying for each CA the CA id, FQDN, port, and signature.

- CA server: id, port.

- Group server: secret, port.

The code must not depend on the types of hosts used for servers or clients.

Dynamics Here is the sequence of what must happen:

- A user presents a user name and public key to a client process.

- The client process request the user’s identity certificate from the group server.
• The client verifies that there is a certificate chain from its top level CAs to the user certificate. All but the last of the certificates on the certificate chain are delegation certificates and are obtained starting at the top level server. The client should not refetch certificates it has fetched in the past.

• The client verifies that none of the certificates in this chain are not current (date checks).

• The client verifies that none of the certificates are revoked.

The interface to the CA servers allows are:

• Add a delegate certificate.

• Delete a delegate certificate.

• Revoke a certificate.

• Return all delegate certificates signed by that CA.

• Revocation status of certificates signed by that CA.

The first three of these requests must contain the CA’s signature.

The interface to the Group servers:

• Add a certificate.

• Delete a certificate.

• Get certificate for username.

The first two of these require the group servers secret to be provided.

2 Grading Criteria

• Code quality (20 pts)

• Documentation (20 pts)

• Testing (20 pts)

• Correctness (40 pts)