**Section 5: Cryptogen tool**

**Cryptogen Tool**

**Cryptogen Binary:**

At the end of this lecture, you should be able to

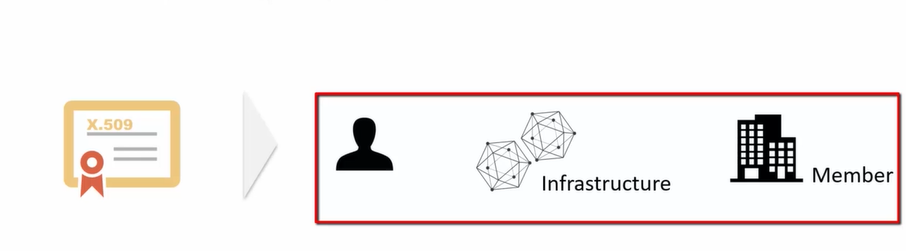
1. explain the usage of the crypto tool and
2. you should be able to generate some sample crypto material using the crypto tool.

The intent of this lecture is not to describe the configuration file that is used by the crypto gen tool.

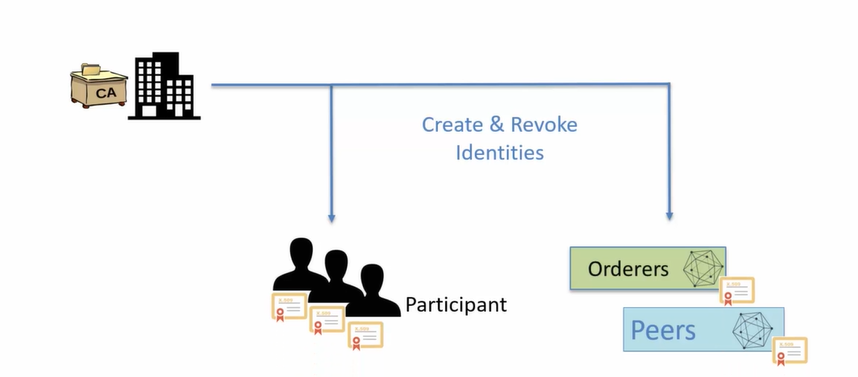
It is just to show you the various options and commands available on the crypto gen utility.

**let's recap how Permissioning is implemented on Hyperledger Fabric.**

* Hyperledger Fabric uses public key infrastructure for Permissioning certificates are issued to all the identities within the network.
* Now identities refer to not just the participants. It also refers to the infrastructure components such **as Orderers**, such as **peers**
* identities are also issued to the members or organizations that are part of the network.
* In other words, a certificate is issued to each of these identity types.



* The certificates are managed by the certification authorities, so each of the participants and the network components such as orderers and peers are issued a certificate by the certification authority.

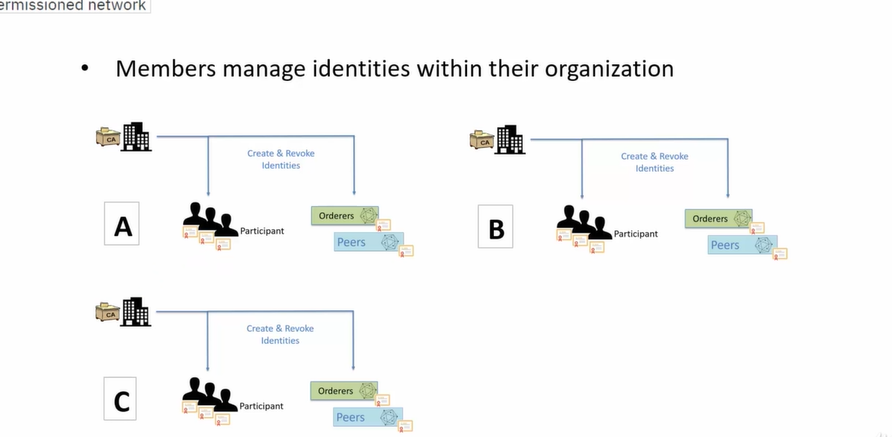


* Now, one important thing to understand here is that the identity management is not centralized. In other words, there is no single entity that is responsible for issuing the certificates.

Each member organization manages the identities within their organization.

So if a network has, let's say, three members, member A, member, B, member C,

each of these members will have their own separate certification authority, which will manage the certificates issued to the participants as well as to the network components such as orders and peers.



**Cryptogen Tool:**

crypto tool is a command line utility for generating the crypto material.

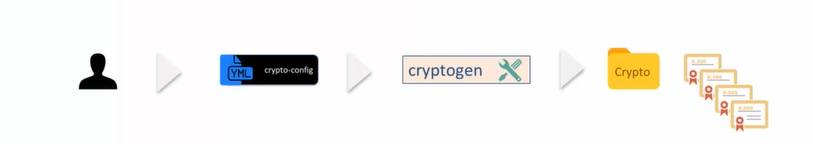
Crypto material refers to the certificate and the Keystore.

The crypto material generated by the crypto tool is typically used for setting up the test environments.

It requires the developer to provide the configuration information in Yaml format.

**At a high level The flow looks like this:**

* As a developer you would put together the crypto config . Yaml file which will have all the configuration information around the participants organization and the infrastructure components such as orders and peers.
* You would then launch the crypto gen tool, provide the crypto config yaml file as input to the crypto gen tool.
* The crypto gen tool will then generate all the crypto material in a local folder.
* So you would see all the certificates and the key stores generated for the identities defined in the crypto config yaml file.



The important point to note about crypto gen tool is that it is not meant to be used in production because real identities are issued by certification authorities managed at the organization or the member level.

Crypto gen tool is a command line tool.

In other words, you need to execute the crypto gen binary on the command shell or the command prompt.

In Windows.

It can be the PowerShell or the command shell on the Unix and Mac OS, it can be a terminal window.

The general format of the command is crypto gen command.

Then you can provide some flags and the arguments for that flag.

With crypto gen help you can get the help on all the commands which are available for crypto gen to

get help on specific command, you can use crypto gen command name, dash dash help crypto gen version

can be used to check the version of the crypto binary and crypto gen show template will show you the

template for the crypto gen configuration file.

This is the Yaml format that I was referring to.

You can save the sample template in a file and then use it for creating your own environment specific

configuration.

Let's see these commands in action.

Let's start with the Help command.

The Help command shows all the commands that are available on the crypto gen binary.

Earlier I mentioned that you can get help on specific command by using the command name, let's say

show template dash, dash, help.

So this will give you the help on a specific command, which in this case is show template.

In fact, there is another way of getting help for a command, and that is to use crypto gen help command

name in this case show template.

It is the same as the previous command to get the version of the crypto gen binary.

Simply use the command crypto gen version.

So here, as you can see I'm using version 1.1.0 of the crypto gen.

Let's try out the command crypto gen show template.

This will dump the sample configuration.

For the crypto tool on the terminal.

Obviously it's not very useful just by dumping it on the terminal.

You can in fact save this template by piping the output to a file.

So here I'm simply piping the output to a file and as you can see, I have a new file created here temp

dot yaml and if I cat it it's the contents so I can go ahead and edit this file to my needs.

You can execute the command crypto gen generate to generate a sample crypto material folder and the

sample crypto material is generated under a folder by the name crypto dash config.

The configuration used for generating this crypto material is the same configuration that is generated

by way of the command crypto gen show template.

So there are two organizations and one order that is predefined in this sample template.

Now this command is not very useful.

There are two flags that you can use with this command.

The first flag is the dash dash config flag that allows you to provide the full path to a config file

and you can also define the path to the output folder.

So instead of using the default crypto dash config as the folder name, you can provide a full folder

path that will be used by the command for generating the crypto material To demonstrate the use of the

generate command.

I will first generate the sample config pipe the output to crypto dash config dot yaml.

This has generated the crypto dash config.yaml.

Next, I'm going to run the crypto gen generate command and I'll specify this yaml file as the input

using the dash dash config and then providing it the full path to the configuration yaml file.

Now I can provide the output flag to generate a different folder name, but in this demo I'll keep the

default folder name.

So once this command has executed you will see it has generated the folder crypto dash config and this

crypto dash config folder has all of the crypto material for the organizations which are part of the

configuration file.

Since this is a sample configuration file, you will find that under the pier org there are these two

organizations which are part of the sample configuration.

Let's summarize in this lecture you learned about crypto gen tool.

Crypto Gen Tool is a command line utility for generating crypto material for testing.

You can use the command crypto gen help to get the list of commands supported by the crypto gen tool

To get help on a specific command, you can use the command crypto gen command name and help crypto

Gen Show template will show you the template that you can use for creating your own configuration file.

The user has to provide this configuration file as an input to the crypto gen Generate command to generate

the crypto material.

One important thing to keep in mind is that this tool is used for generating the crypto material for

testing.

So in other words, you will not use this tool for generating the crypto material for production.

**Cryptogen tool configuration setup**

**Test environment setup & use of cypto material**