PROJECT Decipher

SHIVANGI PRASANNA KOLTHARKAR – 200495670

Information Systems Security (INSS), Georgian College

NETS1035-21F-12278: Applied Cryptography

Aaron Chow

December 9th, 2021

# DOCUMENTATION

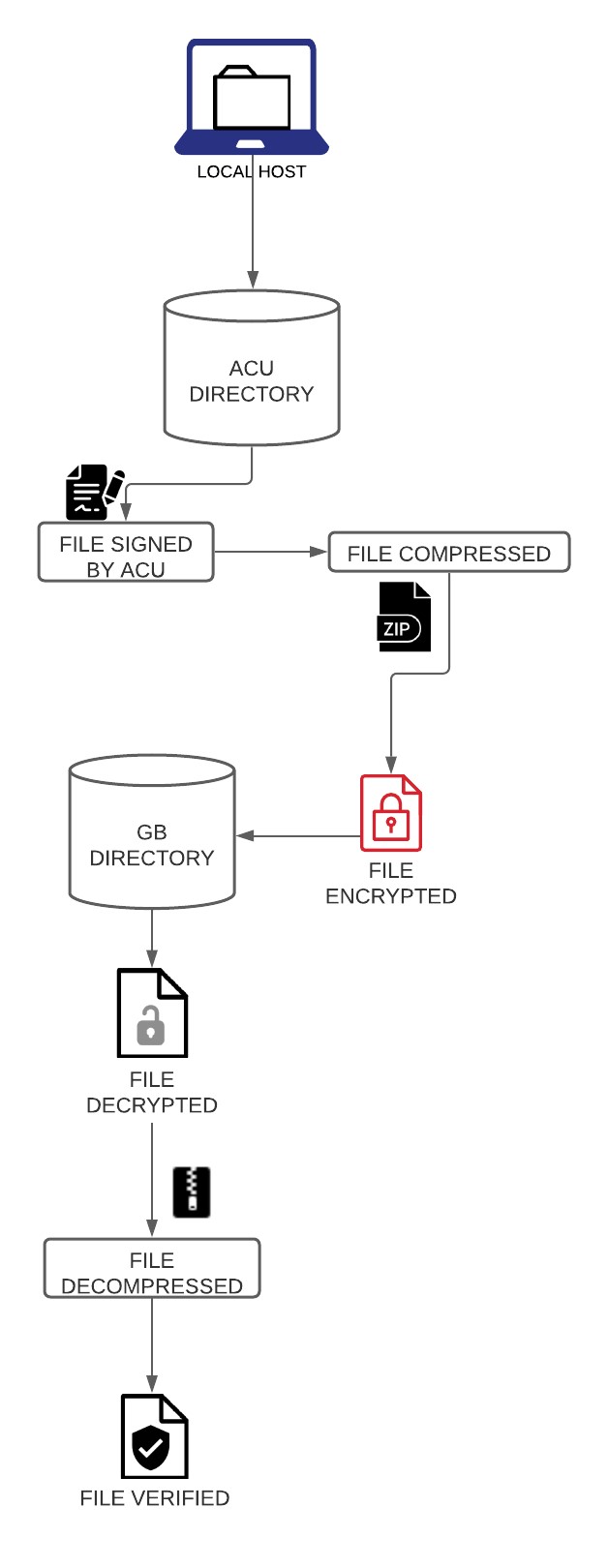
For accomplishing the project tasks a CentOS VM is created with minimal installation on VMware Workstation 16. The coding is done with Openssl and bash. For extracting some files from CentOS to the local desktop and vice versa, Windows PowerShell is used.

Here there are 3 directories created namely, ACU (Alpha Credit Union), GB (Georgian Bank) and decipher (Cryptography company).

The line of processes are:

1. Creating certificate signing request for both banks
2. Creating root certificate of my company
3. Signing the bank certificates
4. ACU signing data file
5. Compression at ACU
6. Encryption at ACU
7. Decryption at GB
8. Decompression at GB
9. Verification

DATA FLOW



Steps:

The directories of ACU, GB, decipher is made in the decipher directory.

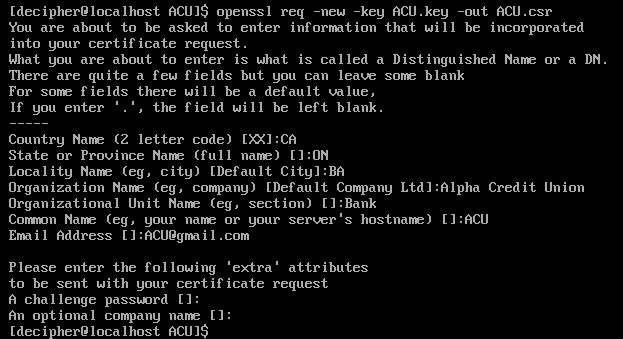


The private key for ACU is created after ending the ACU directory.



Certificate signing request (.csr) file for ACU is created with ACU key, where certificate details are entered. The entries that will be put in the certificate are Country name, State, Locality, Organization name, Organization unit, Common name, Email ID.

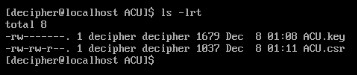
We are not entering any password here.



The csr file is copied to the decipher directory which is the cryptography company’s for further use.



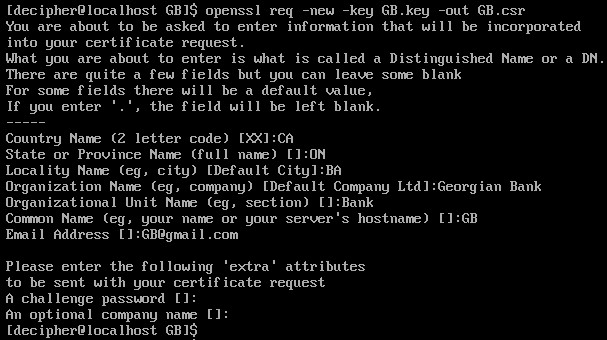
The files present in the ACU directory are the ACU private key and the csr file.



Moving into the GB directory, private key of GB is created.



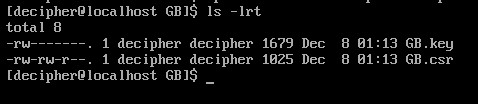
Now the certificate signing request for GB is created with GB key and the details as mentioned for ACU here the credentials of GB are put in..



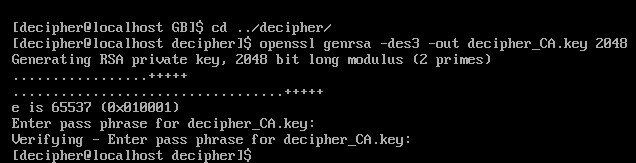
The GB csr file is copied into decipher directory



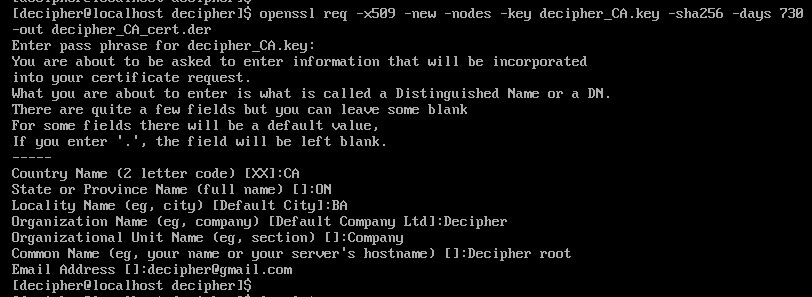
The files present in the GB directory are GB private key and GB csr file.



Moving onto the decipher directory. Private key for decipher is created with a passphrase for enhanced security as this is the root Certificate Authority.

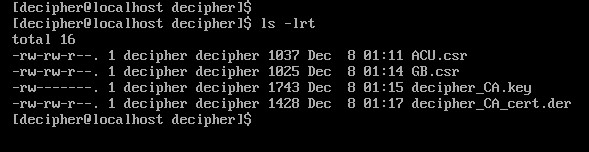


The self signed root certificate is created along with details of decipher.

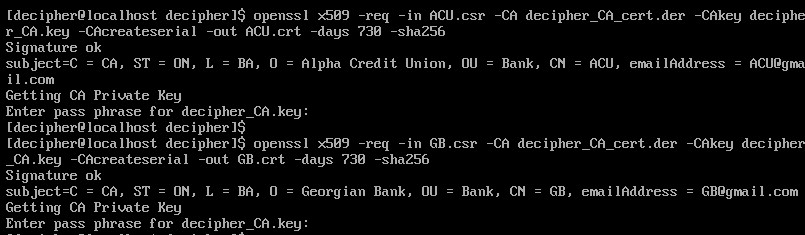


Along with the previously copied certificate signing request of the banks CA key and CA

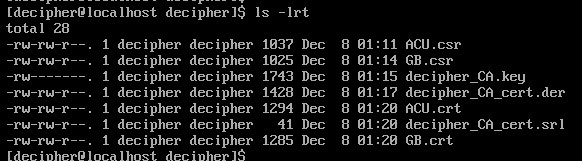
certificate is in the decipher directory.



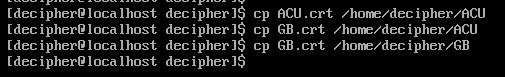
Now using the decipher certificate, ACU and GB certificates are signed. Here while reading the CA private key passphrase that was stated before is asked.



All the files that are newly added to decipher are ACU and GB certificates.

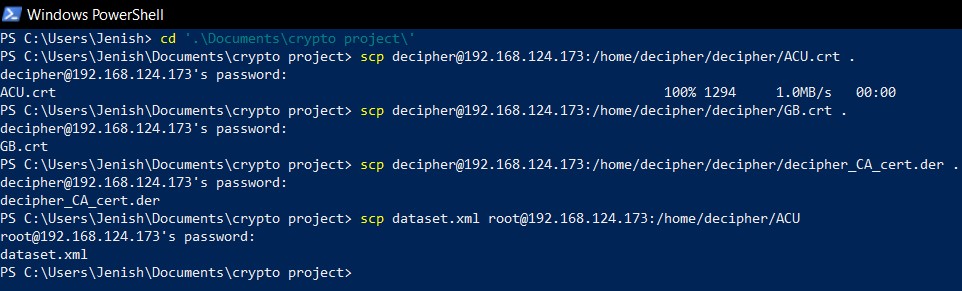


Copying the ACU certificate to ACU directory, GB certificate to ACU directory and GB directory.

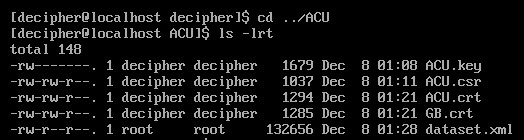


All the three certificates are created in CentOS and need to be transferred into the local computer.

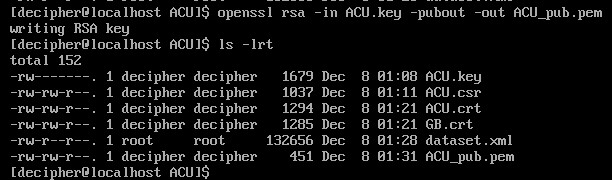
Along with this, the data file that needs to be transferred from ACU to GB needs to be uploaded to the CentOS from local computer.



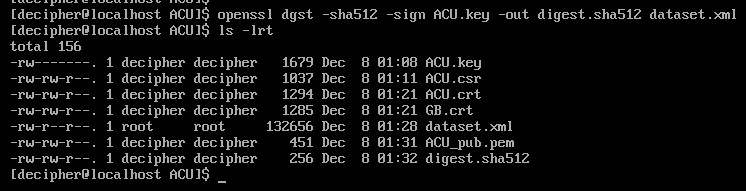
Inside the ACU directory the data file is visible.



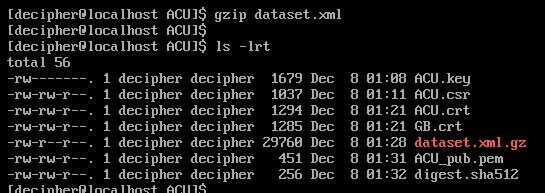
The public key of ACU is retrieved from the private key already present.



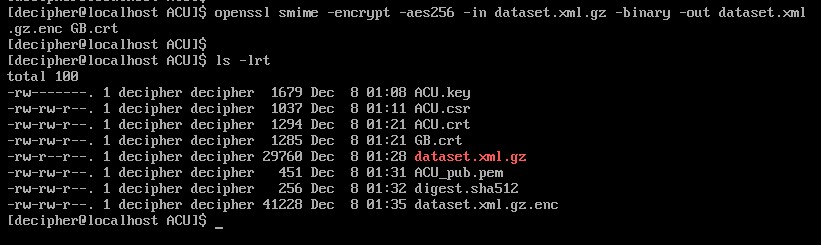
The data file is signed by ACU private key and this will be used later for verification.



Now the file is first compressed then in next step encrypted. The zipped file is highlighted in red in the directory.



The file is encrypted with GB certificate which was already sent by GB.



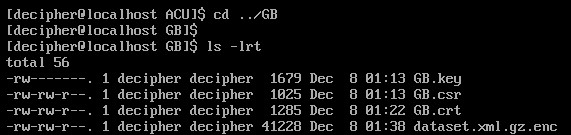
This is the encrypted data file.



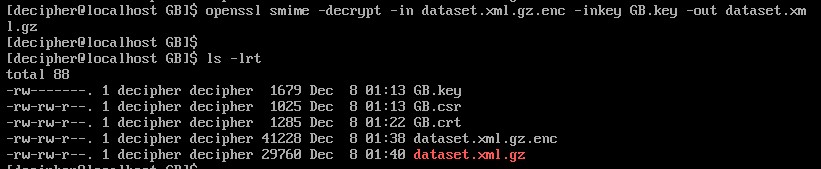
The data file is encrypted and ready to be transferred to GB.



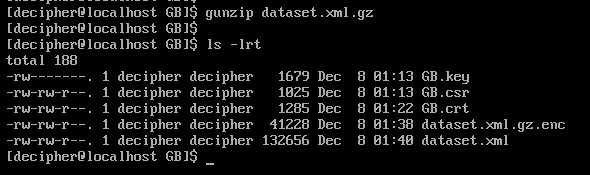
Into the GB directory, the newly arrived encrypted data file can be seen.



This encrypted file needs to be decrypted first then only decompressed. The steps are opposite of what were done in ACU.



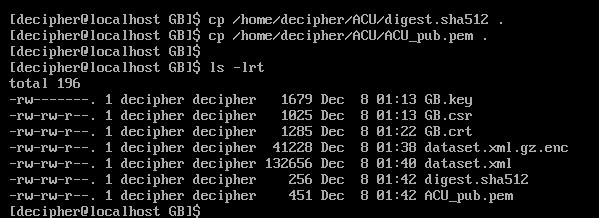
The file is decompressed and stored in the directory.



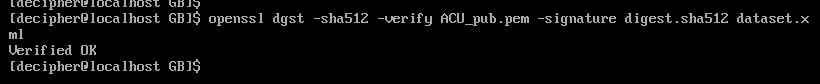
The original file is retrieved.



The signed document and the public key of ACU is transferred to GB where verification of the received document needs to be done.

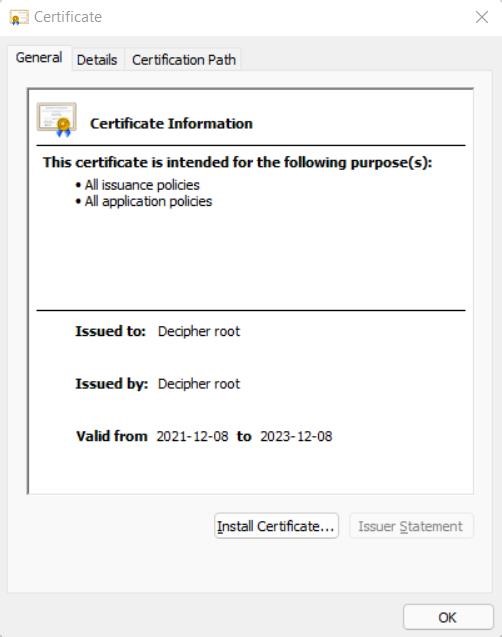


Verifying if the received signed file is the correct file sent to GB.

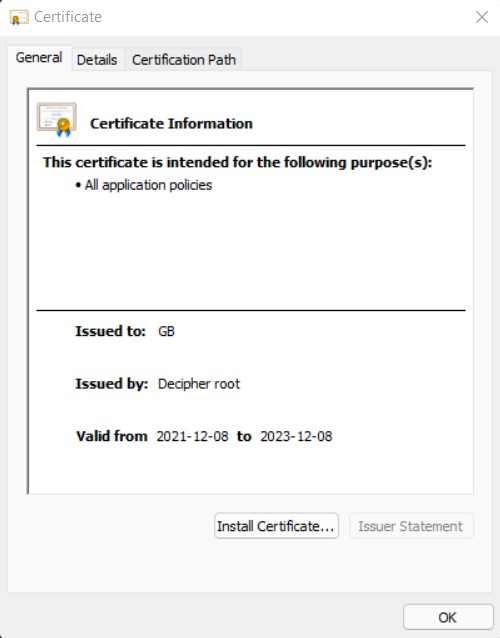


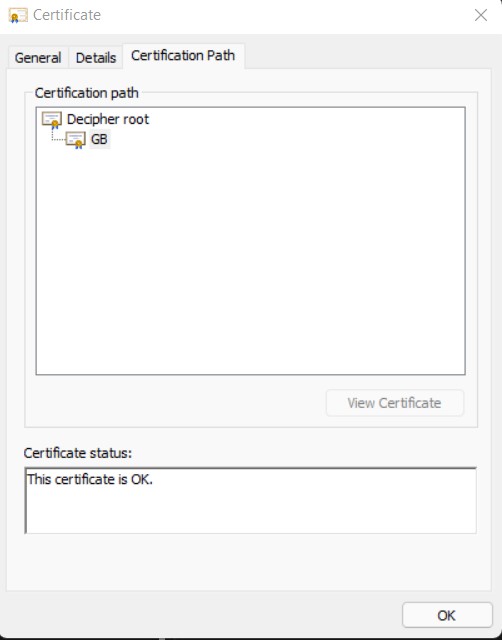
The certificates that are created for each bank and the crypto company.

ROOT CERTIFICATE



GB CERTIFICATE





ACU CERTIFICATE

