ALGONQUIN COLLEGE

CST8805 Applied Cryptography

Final Project

Submitted by Group 3 – Shubham Chawla, Sachin Mahajan, Gonca Ayca Karasu, Manav Modi

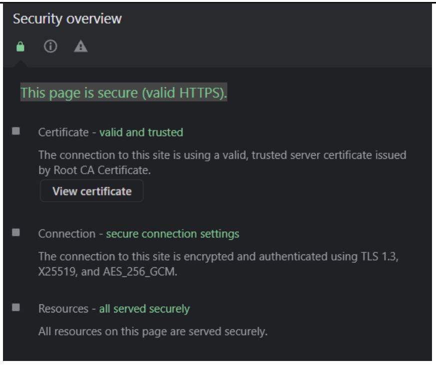
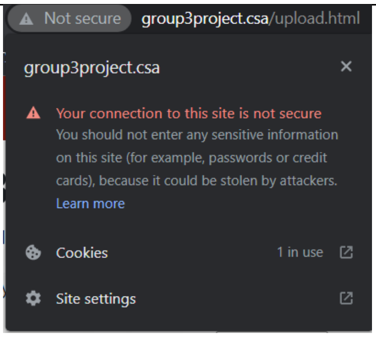
Submitted to Prof. Yvan Perron

PKI – Windows 10 VM

Bank Web Server – Cent OS VM

Client – Windows 11 (Local Machine)

Test Plan

No.	Test Case	Test Solution	Expected Output	Success
1.	**Document Transition** 1. Over HTTPS with the client browser having fully authenticated the Bank's web server against a trusted root CA 2. Uses asymmetric encryption for symmetric key negotiation that implements forward secrecy 3. Uses approved NIST algorithm and key sizes **4.** Web browser MUST report/display that the connection to the web server is SECURE!	**Navigate to** **https://www.group3project.csaupload.html** **Open Developer Tools > Security** Check Security Parameters	 Security overview This page is secure (valid HTTPS). Certificate - valid and trusted The connection to this site is using a valid, trusted server certificate issued by Root CA Certificate. Connection - secure connection settings The connection to this site is encrypted and authenticated using TLS 1.3, X25519, and AES_256_GCM. Resources - all served securely All resources on this page are served securely. • **TLS 1.3** • **X25519 -** elliptic curve Diffie-Hellman key exchange using Curve25519 – **forward secrecy** • **RSA** used for signatures – authentication function • **AES algorithm – 256 bits** key with **GCM** mode of operation ensuring **confidentiality** and **integrity**	**Yes**
2.	**Test with client that does not use NIST approved algorithms**	**Navigate to** **http://www.group3project.csa/upload.html**	 group3project.csa/upload.html group3project.csa Your connection to this site is not secure You should not enter any sensitive information on this site (for example, passwords or credit cards), because it could be stolen by attackers. Cookies 1 in use **Connection is rejected**	**Yes**
3.	**Verifying Document Signature**	**openssl dgst -sha256 -verify $target_filePubKey -signature $target_fileSig $target_file**	**Verified OK**	**Yes**
4.	**Verifying Document Signer Certificate Issued by Trusted Root**	**openssl verify -verbose -trusted CARootCert.cer $target_fileX509**	**User1-Project.cer: OK**	

5.	**Verifying valid certificate against local CRL**	**openssl verify -verbose -crl_check -CRLfile CAProject.crl.pem -trusted CARootCert.cer $target_fileX509**	**User1-Project.cer: OK**	
6.	**Verifying revoked certificate against local CRL**		**certificate revoked** **verification failed**	
7.	**Verifying expired certificate against local CRL**		**certificate has expired** **verification failed**	
8.	**Verifying certificate issued by untrusted CA against local CRL**		**unable to get local issuer certificate** **verification failed**	
9.	**Downloading CRL from distribution Point**	**Navigate to https://www.group3project.csa/CAProject.crl**	**File downloaded successfully**	**Yes**
10.	**Certificate Validation against the CRL distribution Point via local terminal**	**openssl verify -verbose -crl_check -crl_download -trusted CARootCert.cer $target_fileX509**	**Works in all cases**	**Yes**
11.	**Verifying failed document signature**	**openssl dgst -sha256 -verify $target_filePubKey -signature $target_fileSig $target_file**	**Verification failed**	**Yes**