**Ahmed Almass,** **Ramaz Dhothar,** **Madusha Samarajeewa****,** **Divyadeep Parmar**

**Group Activity: Cryptography**

**Part 1**

You have been tasked with obtaining an extended validation SSL digital certificate for an online shopping portal.

**1. Research and choose an issuing CA (Certificate or Certification Authority). Explain why you chose the specific CA.**

GlobalSign ExtendedSSL, because it verifies, the rights to use domain, extended company vetting including confirming the legal, operational and physical existence.

**2. Describe the process and requirements for obtaining a digital certificate.**

* Identify which Client Digital Certificate best suits your requirements.
* Create a GlobalSign Certificate Center (GCC) account and complete the application to order and purchase the certificate OR if you already have a GCC account place the new order in your account.
* Receive the approval email and accept the application.
* Wait for the vetting process to be completed by GlobalSign (varies depending on the type of certificate you purchased).
* Pick up your Client Digital Certificate using your pickup password. Remember this cannot be reset if forgotten so make sure to take note of it during the application process.
* Download the Client Digital Certificate. Instructions to do this can be searched for in the search bar above.
* Install the Client Digital Certificate by following the instructions specific to your operating system, browser, and/or email client. Specific instructions can be searched for in the search bar above.
* Your certificate is now ready for use.

**3. Who in the organization should be tasked with installing the certificate and why?**

The owner because to confirm who owns the company and if anything goes wrong he is at fault.

**Part 2**

On Thursday January 3, 2013, Microsoft issued the following Security Advisory (2798897):

“Fraudulent Digital Certificates Could Allow Spoofing

“Microsoft is aware of active attacks using one fraudulent digital certificate issued by TURKTRUST Inc., which is a CA present in the Trusted Root Certification Authorities Store. This fraudulent certificate could be used to spoof content, perform phishing attacks, or perform man-in-the-middle attacks. This issue affects all supported releases of Microsoft Windows.

“TURKTRUST Inc. incorrectly created two subsidiary CAs (\*.EGO.GOV.TR and e-islem.kktcmerkezbankasi.org). The \*.EGO.GOV.TR subsidiary CA was then used to issue a fraudulent digital certificate to \*.google.com. This fraudulent certificate could be used to spoof content, perform phishing attacks, or perform man-in-the-middle attacks against several Google web properties.

“To help protect customers from the fraudulent use of this digital certificate, Microsoft is updating the Certificate Trust List (CTL) and is providing an update for all supported releases of Microsoft Windows that removes the trust of certificates that are causing this issue.

For systems using the automatic updater of revoked certificates (see Microsoft Knowledge Base Article 2677070 for details), including Windows 8, Windows RT, Windows Server 2012, and devices running Windows Phone 8, no action is needed as these systems will be automatically protected.

For Windows XP and Windows Server 2003 customers or customers who choose not to install the automatic updater of revoked certificates, Microsoft recommends that the 2798897 update be applied immediately using update management software, by checking for updates using the Microsoft Update service, or by downloading and applying the update manually.”

**1. Who is TURKTRUST?**

* is a CA present in the Trusted Root Certification Authorities Store.

**2. Explain what happened and why this is a potentially dangerous situation.**

* This fraudulent certificate could be used to spoof content, perform phishing attacks, or perform man-in-the-middle attacks

**3. Research this event. Did any other organizations issue advisories?**

The fake certificates were issued by intermediate certificate authority CNNIC which is owned by MCS Holdings, said Google engineer Adam Langley.