# TTP Detail – T1608.003

## TTP Information

Name: Install Digital Certificate

Description: Adversaries may install SSL/TLS certificates that can be used during targeting. SSL/TLS certificates are files that can be installed on servers to enable secure communications between systems. Digital certificates include information about the key, information about its owner's identity, and the digital signature of an entity that has verified the certificate's contents are correct. If the signature is valid, and the person examining the certificate trusts the signer, then they know they can use that key to communicate securely with its owner. Certificates can be uploaded to a server, then the server can be configured to use the certificate to enable encrypted communication with it.(Citation: DigiCert Install SSL Cert)

Adversaries may install SSL/TLS certificates that can be used to further their operations, such as encrypting C2 traffic (ex: [Asymmetric Cryptography](https://attack.mitre.org/techniques/T1573/002) with [Web Protocols](https://attack.mitre.org/techniques/T1071/001)) or lending credibility to a credential harvesting site. Installation of digital certificates may take place for a number of server types, including web servers and email servers.

Adversaries can obtain digital certificates (see [Digital Certificates](https://attack.mitre.org/techniques/T1588/004)) or create self-signed certificates (see [Digital Certificates](https://attack.mitre.org/techniques/T1587/003)). Digital certificates can then be installed on adversary controlled infrastructure that may have been acquired ([Acquire Infrastructure](https://attack.mitre.org/techniques/T1583)) or previously compromised ([Compromise Infrastructure](https://attack.mitre.org/techniques/T1584)).

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: resource-development

## APTs (Intrusion Sets)

* Sea Turtle