# TTP Detail – T1587.003

## TTP Information

Name: Digital Certificates

Description: Adversaries may create self-signed SSL/TLS certificates that can be used during targeting. SSL/TLS certificates are designed to instill trust. They 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 with its owner. In the case of self-signing, digital certificates will lack the element of trust associated with the signature of a third-party certificate authority (CA).

Adversaries may create self-signed 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 even enabling [Adversary-in-the-Middle](https://attack.mitre.org/techniques/T1557) if added to the root of trust (i.e. [Install Root Certificate](https://attack.mitre.org/techniques/T1553/004)).

After creating a digital certificate, an adversary may then install that certificate (see [Install Digital Certificate](https://attack.mitre.org/techniques/T1608/003)) on infrastructure under their control.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

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

## APTs (Intrusion Sets)

* APT29
* PROMETHIUM