

Privilege Escalation with Certify



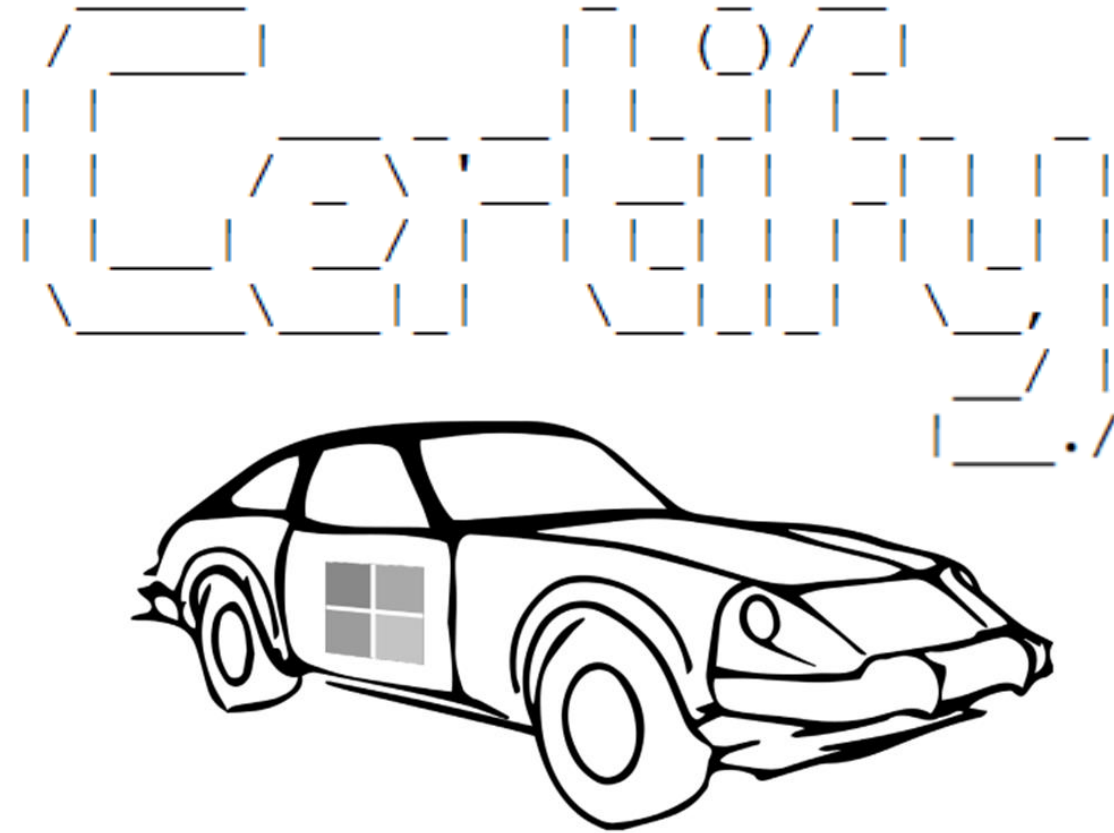
Kat Seymour

Security Staff Author

@SheSpawn13

<https://www.linkedin.com/in/kat-delorean-seymour-a846b98>



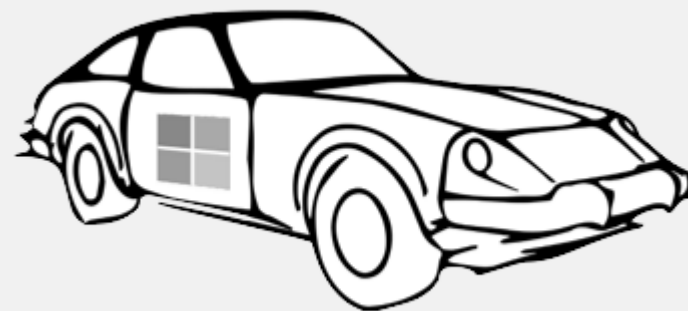


Creator: Will Schroeder & Lee Christensen

Certify is a C# tool used to enumerate and abuse misconfigured Active Directory Certificate Services (AD CS) environments.

<https://posts.specterops.io/certified-pre-owned-d95910965cd2>





Certified Pre-Owned

Abusing Active Directory Certificate Services

harmj0y & tifkin

Open-Source C# tool written to facilitate enumeration and abuse of misconfigured Active Directory Certificate Services Environments

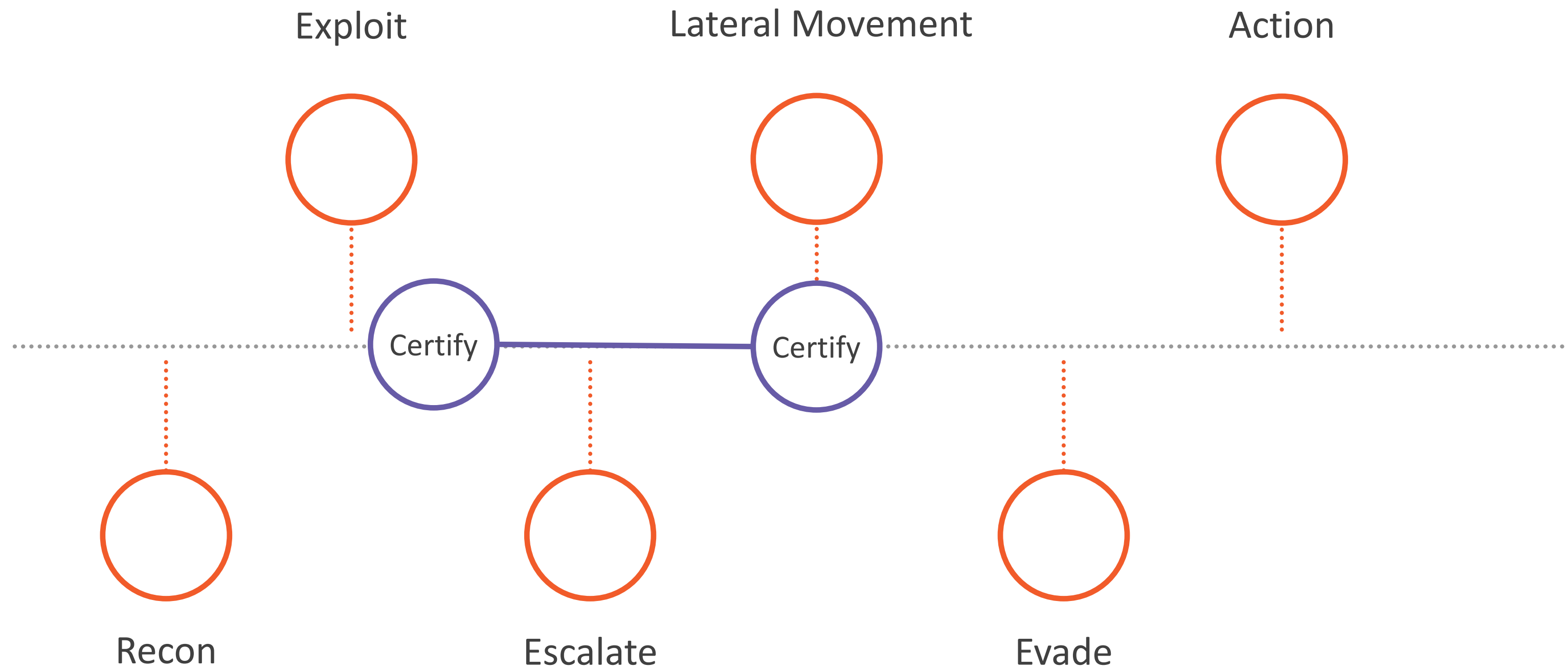
Available for download at

<https://github.com/GhostPack/Certify>

Wide-spread, difficult to detect, living off the land technique that can lead to domain escalation and machine-independent domain persistence.



Kill Chain



MITRE ATT&CK

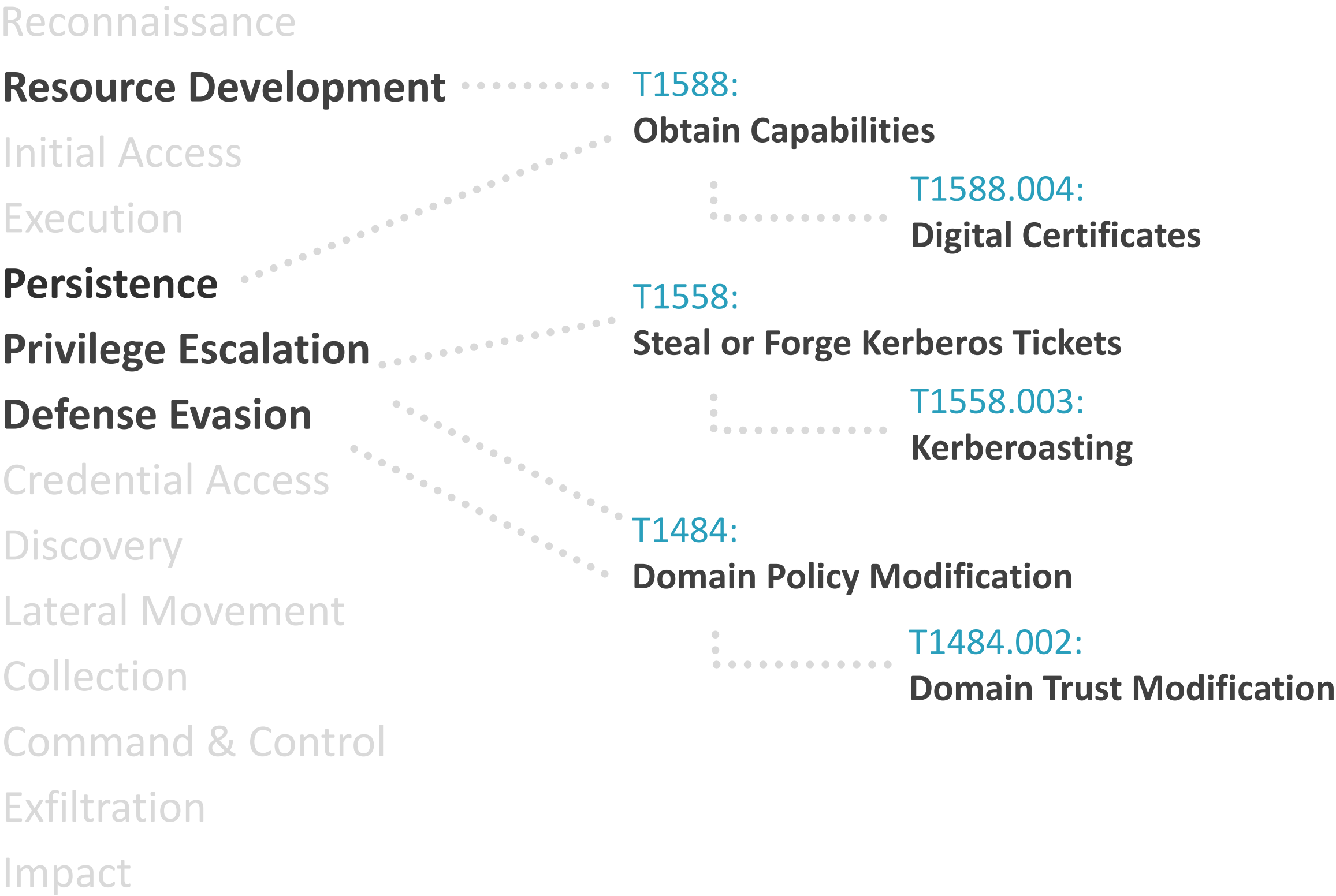
Tactics

Reconnaissance
Resource Development
Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Command & Control
Exfiltration
Impact

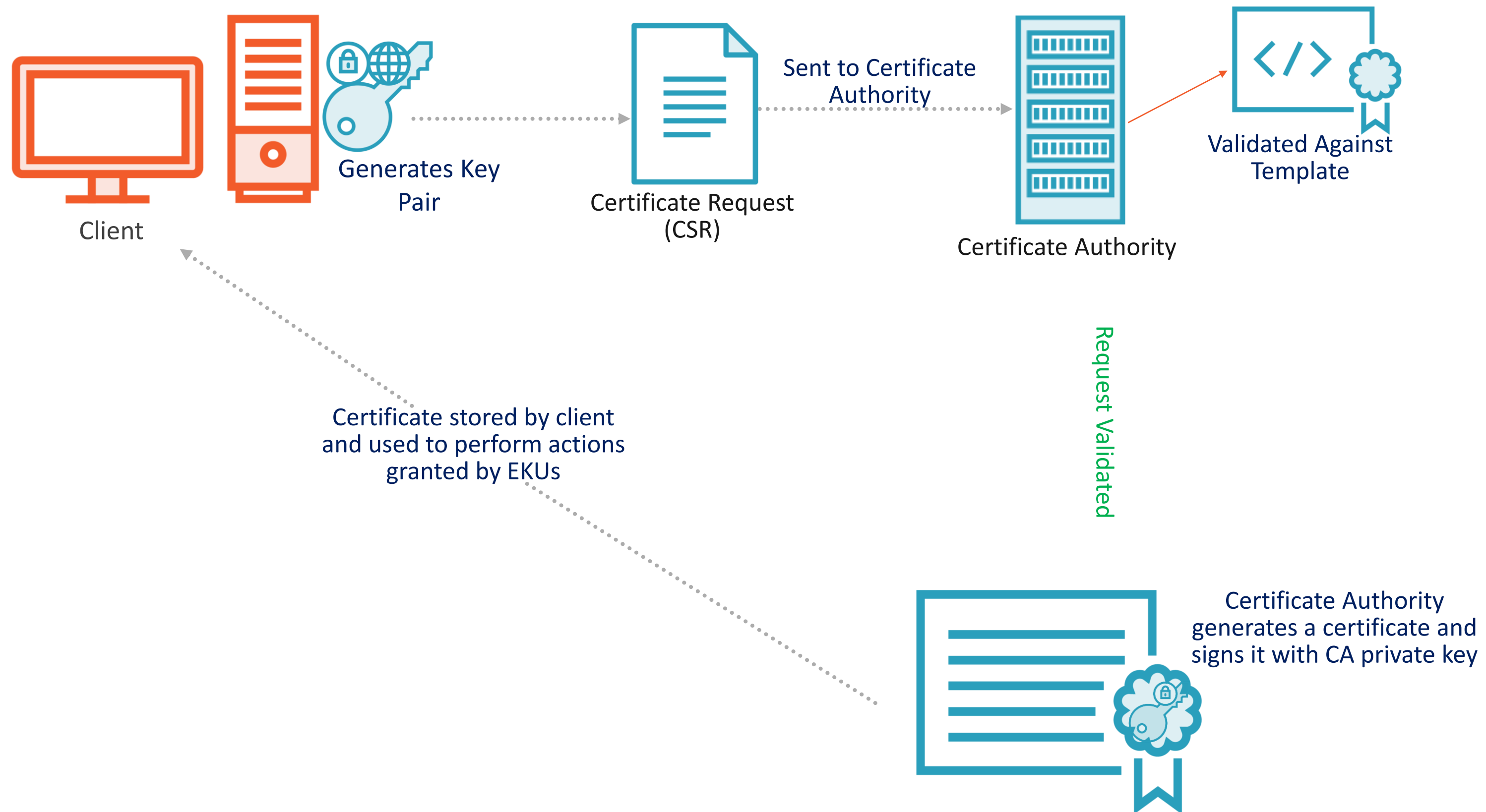


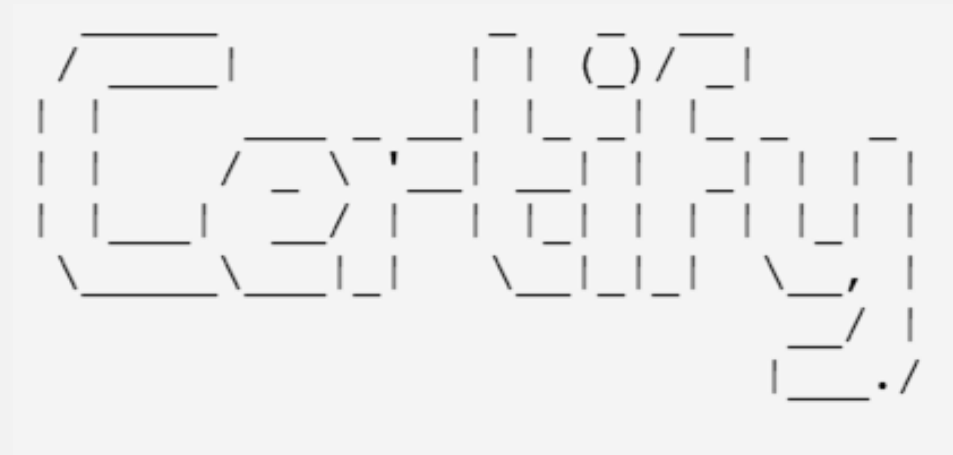
MITRE ATT&CK

Tactics



Certificate Enrollment Process





Certificate Fields

Define the parameters of the certificate

Subject



Certificate Owner

SubjectAlternativeName



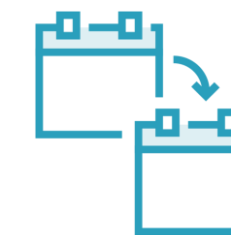
Alternate Certificate Owner

Basic Constraints



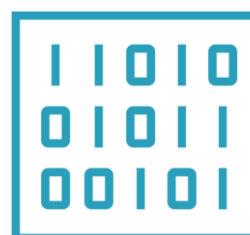
Constraints while Using

NotBefore - NotAfter



Dates Certificate is Valid

Extended Key Usages (EKU)



Define how certificate is used



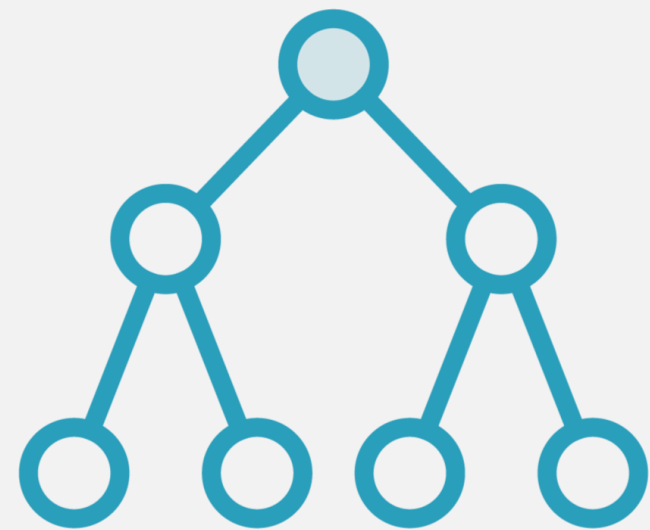
Code Signing

Encrypting File System

Client Authentication

Smart Card Logon





Lab Setup

Systems

Users

Templates

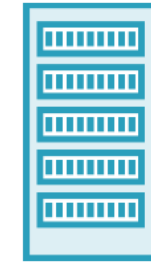
Active Directory



User System



Domain Controller



Certificate Authority



Standard User



Domain Admin



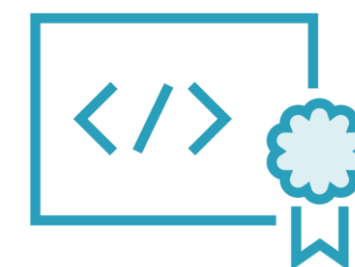
Optional User



Standard Template



SAN Vulnerable



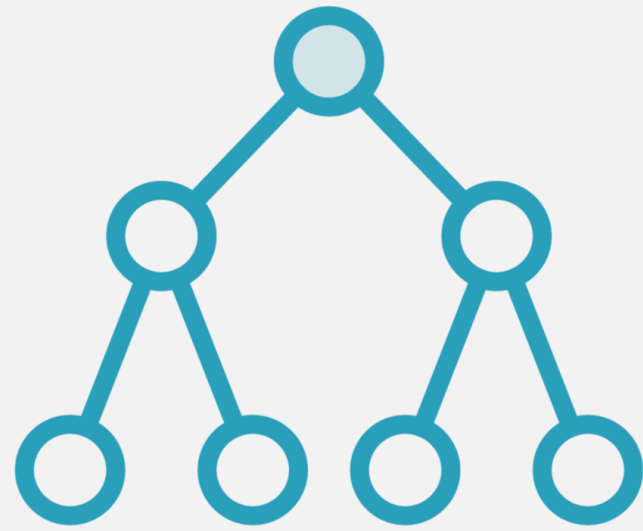
Vuln Enrollment
Agent



Enrollment Agent
Enrollee



Certificate Authority Flag



EDITF_ATTRIBUTESUBJECTALTNAME2

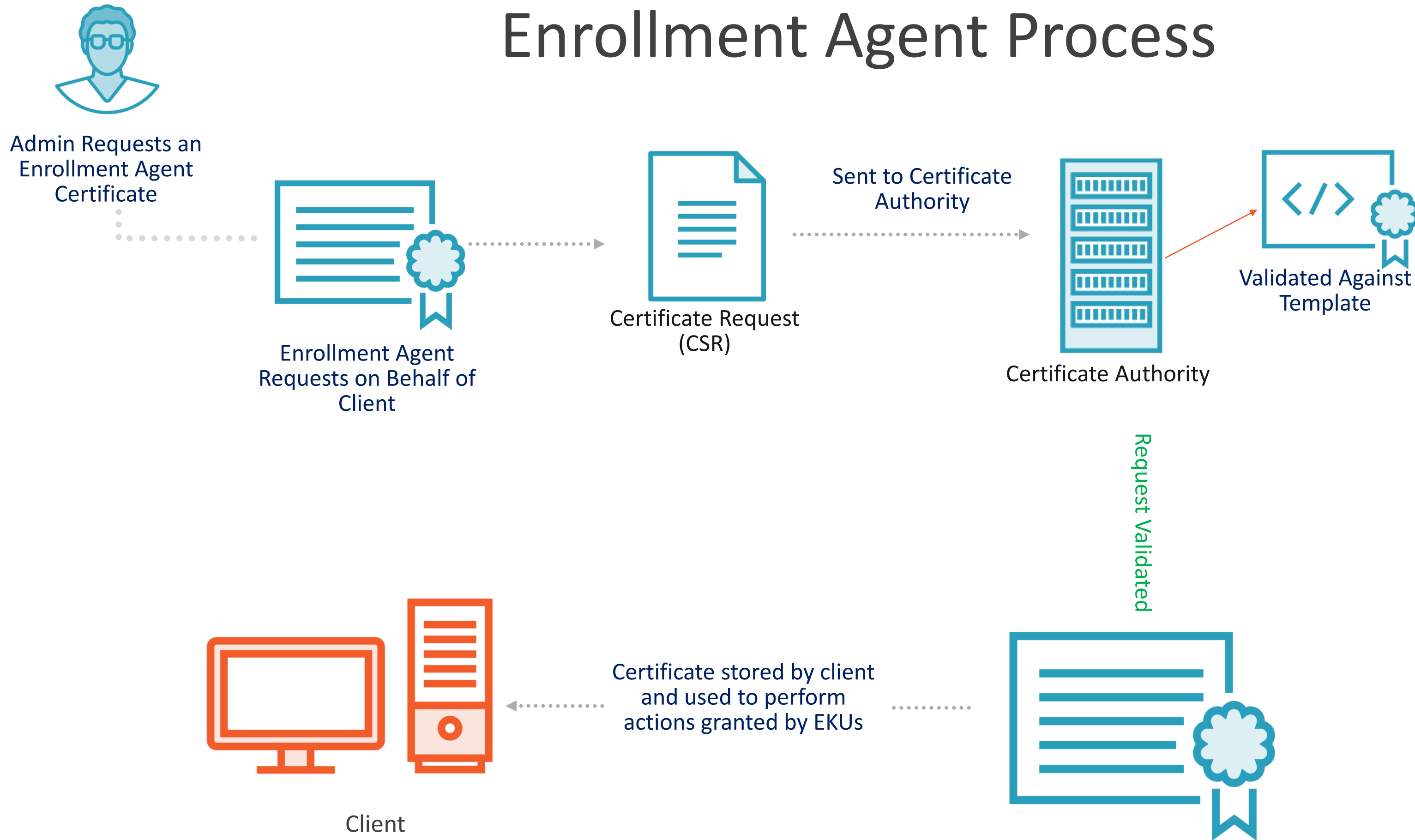
Controlling User Added Subject Alternative Names

An Active Directory® Certificate Services CA offers several methods to add subject alternative names (SANs) to a certificate:

1. **Add from known AD object attributes** – The CA can add alternative names from a defined subset of attributes when you choose to add the subject information from Active Directory®. The CA performs this addition, and the data is not specified by the user. Manipulation would require an attacker to be able to manipulate the values of attributes for a user in Active Directory®.
2. **Add as an extension in the certificate request** – If the template is configured for “supply in request”, the extensions requested will be honored by the CA if supported. The alternative names are provided by the requestor.
3. **Add as an attribute that accompanies the certificate request** – Requires the CA to allow user-specified alternative names via the **EDITF_ATTRIBUTESUBJECTALTNAME2** flag. If this flag is set on the CA, any request (including when the subject is built from Active Directory®) can have user defined values in the subject alternative name.

Allowing users to define arbitrary alternative names poses risk to the PKI if it is not implemented with proper controls. Anytime you allow a user to define SANs, implement the following additional controls:

Enrollment Agent Process



Enumeration Demo

1. Enumerate Environment with CAS
2. Enumerate Cas for enabled templates and details with Find
3. Use FIND to locate vulnerable configurations with `/enrolleeSuppliesSubject /clientauth /vulnerable` and `vulnerable /currentuser`



SubjectAlternativeName Demo

1. Use info from Find command to compromise SAN vulnerable certificate
2. Use Certify to request vulnerable certificate
3. Use certificate to generate TGT as local admin on DC with Rubeus
4. Show how to request under with /machine switch and Get System
5. Discuss how to compromise any certificate if flag set on CA



Vulnerable Enrollment Agent Demo

1. Use info from Find command to locate vulnerable enrollment agents
2. Use pkiobjects to find administrators
3. Use enrollment agent to go from standard user to domain admin with Rubeus
4. Discuss Persistence established through these methods



More Information

Certify

<https://github.com/GhostPack>

<https://posts.specterops.io/certified-pre-owned-d95910965cd2>

[https://www.specterops.io/assets/resources/Certified Pre-Owned.pdf](https://www.specterops.io/assets/resources/Certified%20Pre-Owned.pdf)

Related Information

Privilege Escalation with Rubeus -

<https://app.pluralsight.com/library/courses/privilege-escalation-rubeus/table-of-contents>

Securing AD PKI -

[https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn786426\(v=ws.11\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn786426(v=ws.11))

