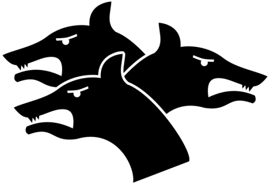


Fixing a Kerberos vulnerability with the bare necessities

Bronze-Bit exploit mitigation on old FreeIPA releases

Julien Rische

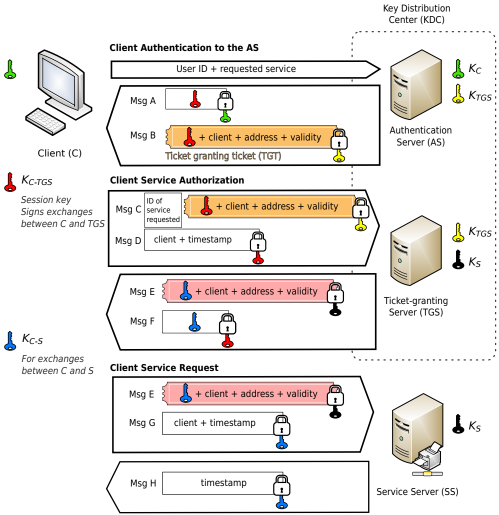
jrische@redhat.com

2024-02-04 FOSDEM

Red Hat France

About Kerberos

- Symmetric cryptography-based authentication protocol
- Created in 1988
- Early implementation of Single-Sign-On principles
- Use specific concepts
  - **Ticket**:
    Token used to authenticate a user or service against another service
  - **Key Distribution Center** (KDC):
    Server storing all the keys and providing *tickets* to authenticated clients
  - **Ticket-Granting Ticket** (TGT):
    Ticket to the *KDC*


Key Distribution Center (KDC)
Client Authentication to the AS
User ID + requested service
Msg A
Msg B
+ client + address + validity
Ticket granting ticket (TGT)
Client (C)
Authentication Server (AS)
K_C
K_{TGS}
$K_{C\text{-}TGS}$
Session key
Signs exchanges between C and TGS
Client Service Authorization
Msg C
ID of service requested
+ client + address + validity
Msg D
client + timestamp
K_{TGS}
K_S
Ticket-granting Server (TGS)
Msg E
+ client + address + validity
Msg F
$K_{C\text{-}S}$
For exchanges between C and S
Client Service Request
Msg E
+ client + address + validity
Msg G
client + timestamp
Msg H
timestamp
K_S
Service Server (SS)

Kerberos protocol by *Jeran Renz* under CC BY-SA 4.0

The MS-SFU Kerberos extension

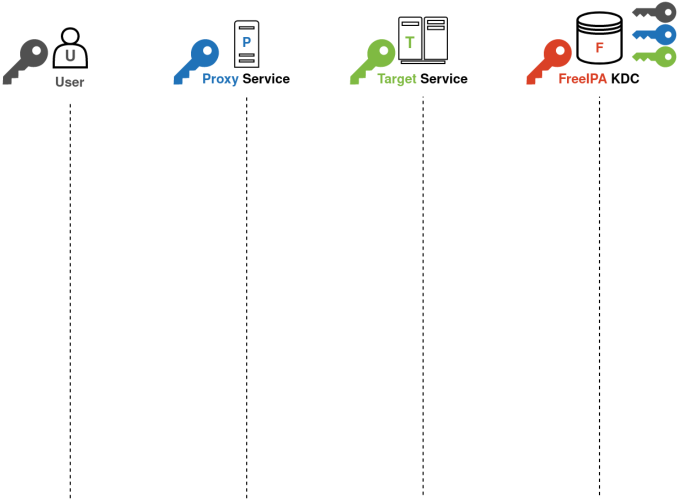
MS-SFU: Motivations

- Need to allow frontend **services to impersonate users**
  - Frontend: web service, . . .
  - Backend: SQL database, distributed storage system, . . .
- Historical solution: **TGT forwarding** (aka. *unconstrained delegation*)
  - Allow frontend service to access ANY service as the user
  - Bad solution from security perspective, more **granularity** required
- Microsoft implemented an extension called **MS-SFU**
  - Introducing 2 new mechanisms

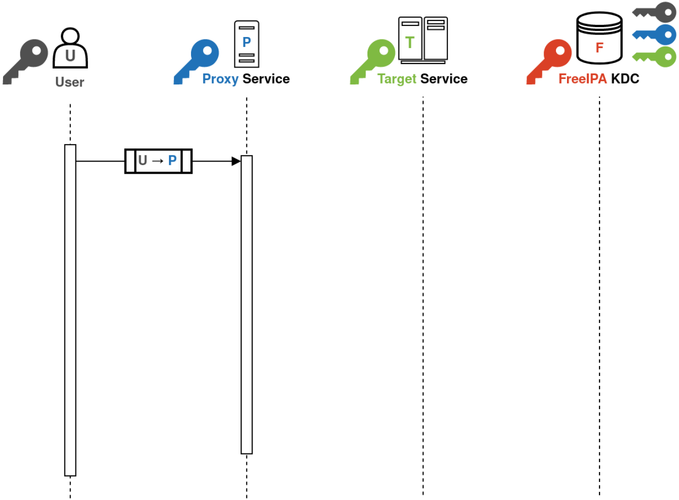
Constrained Delegation (S4U2Proxy)

- Allow a **proxy** service to impersonate a **user** against a specific **target** service
- Configure service **delegation rules**
  - `ipa servicedelegation` commands
  - Specific administration permissions required to configure such rules
- At the condition of providing an **evicence ticket** to the **KDC**
  - Ticket for user-to-proxy service
  - With `forwarable` ticket flag set

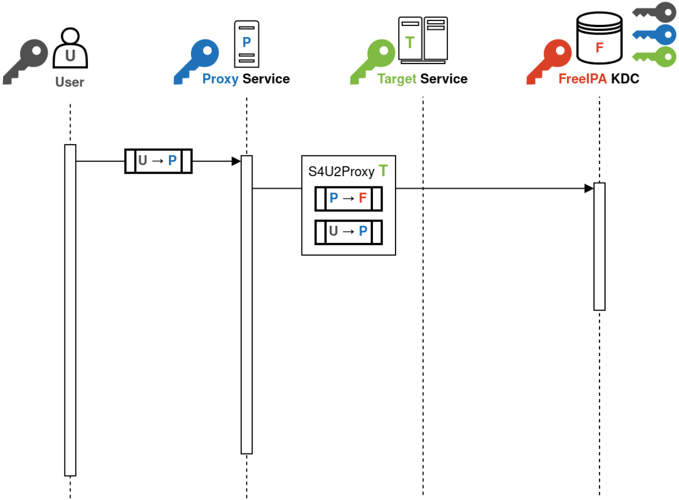
Constrained Delegation (S4U2Proxy)



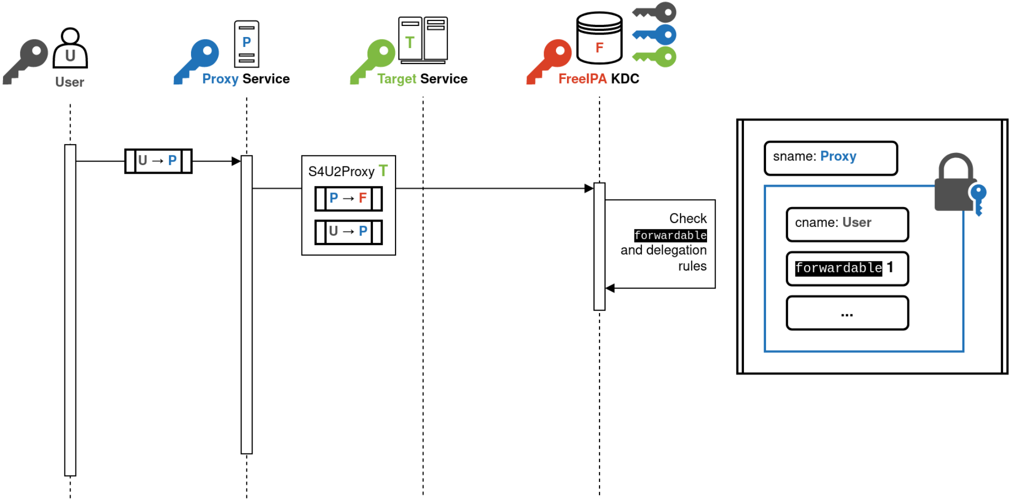
Constrained Delegation (S4U2Proxy)



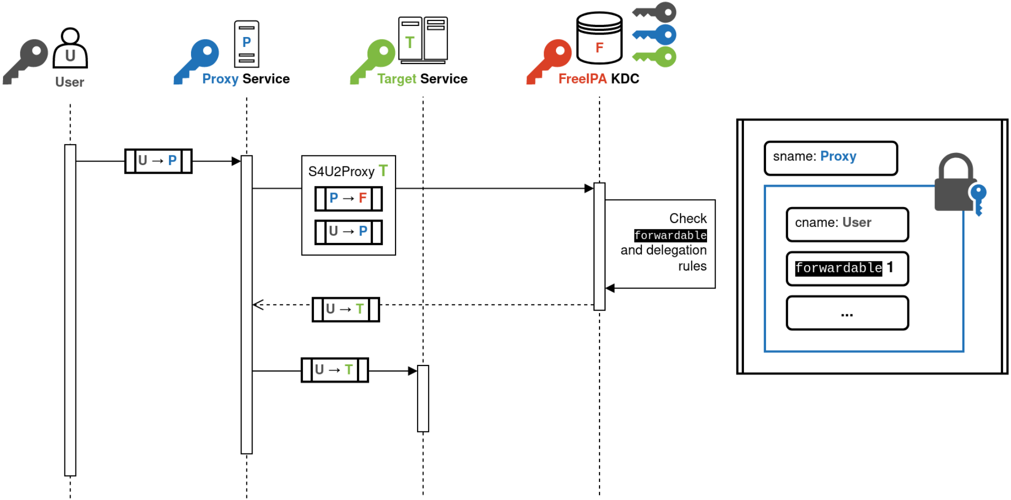
Constrained Delegation (S4U2Proxy)



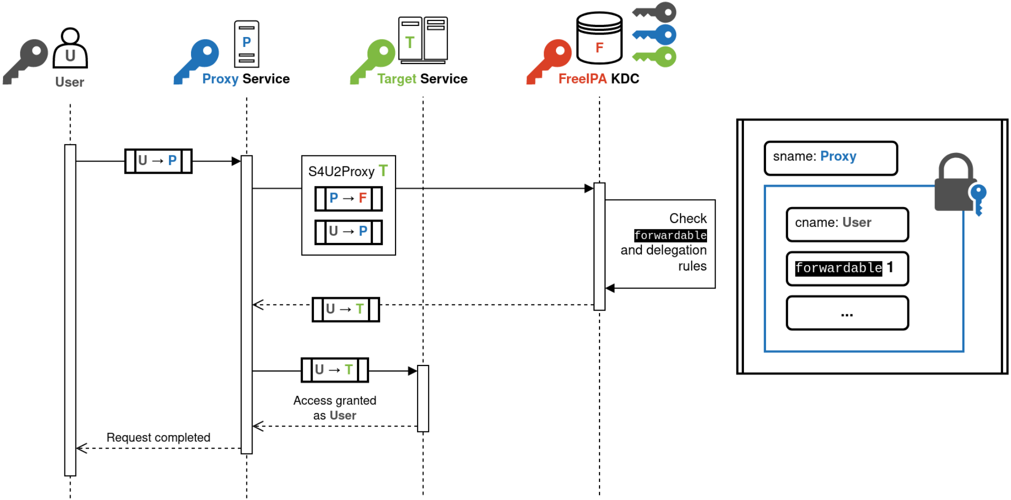
Constrained Delegation (S4U2Proxy)



Constrained Delegation (S4U2Proxy)



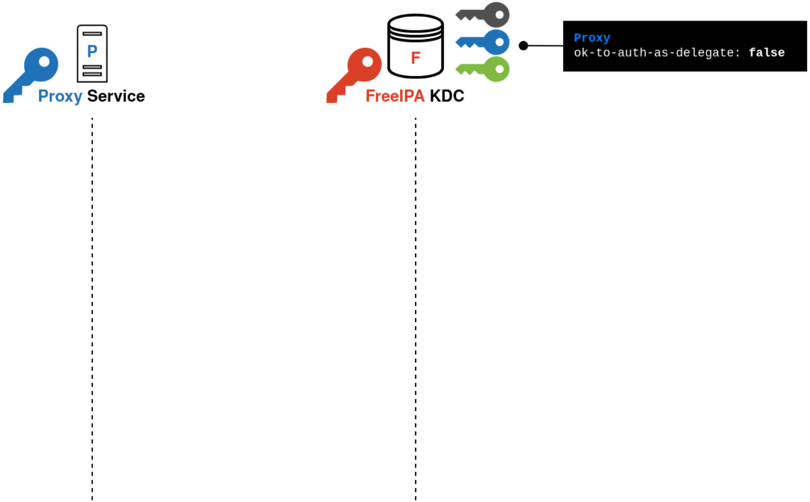
Constrained Delegation (S4U2Proxy)



Protocol Transition (S4U2Self)

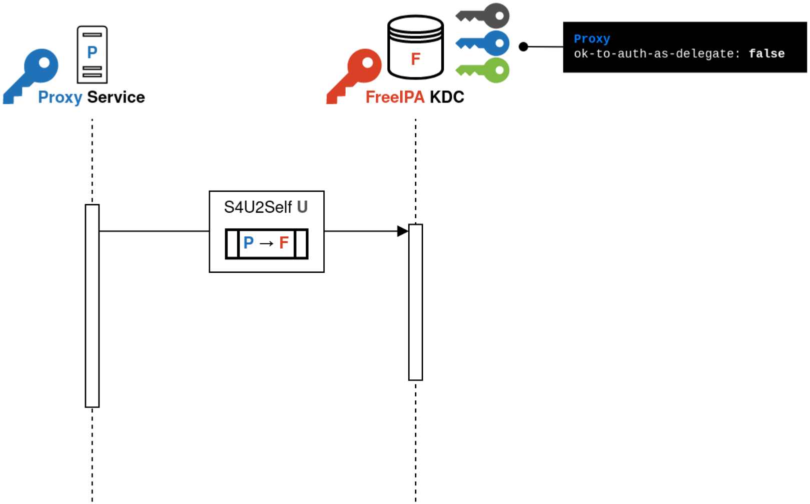
- Mean to:
  - Integrate services relying different authentication methods for users requests into the Kerberos authentication system
    - OIDC, SASL, ...
  - Obtain encrypted user authorization information
    - Use Kerberos as group membership provider
- Allow **any service with a valid TGT** to request a ticket from **any user to the service itself**
- Resulting ticket has `forwardable` flag set only if:
  - FreeIPA: principal configured with `ok-to-auth-as-delegate` privilege
  - AD: account configured with `TrustedToAuthForDelegation` privilege

Protocol Transition (S4U2Self)



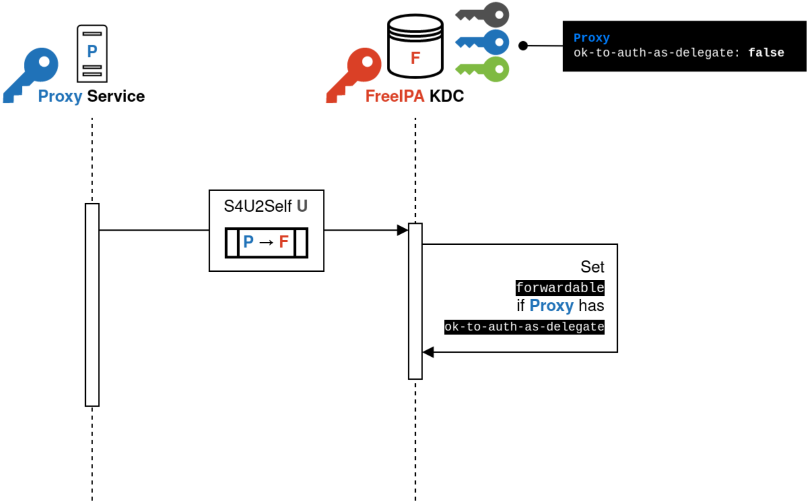
```
Proxy
ok-to-auth-as-delegate: false
```

Protocol Transition (S4U2Self)



```
Proxy
ok-to-auth-as-delegate: false
```

Protocol Transition (S4U2Self)

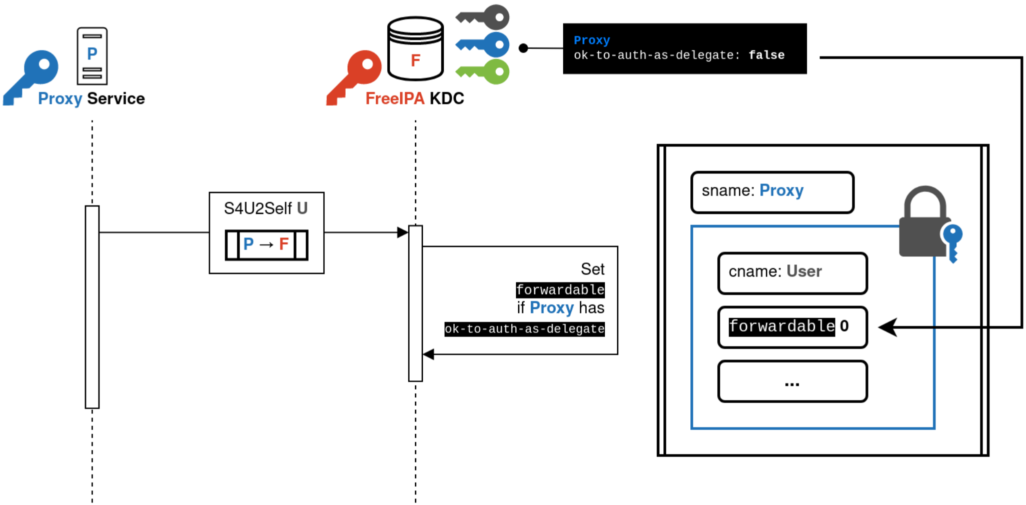


```
Proxy
ok-to-auth-as-delegate: false
```

S4U2Self **U**

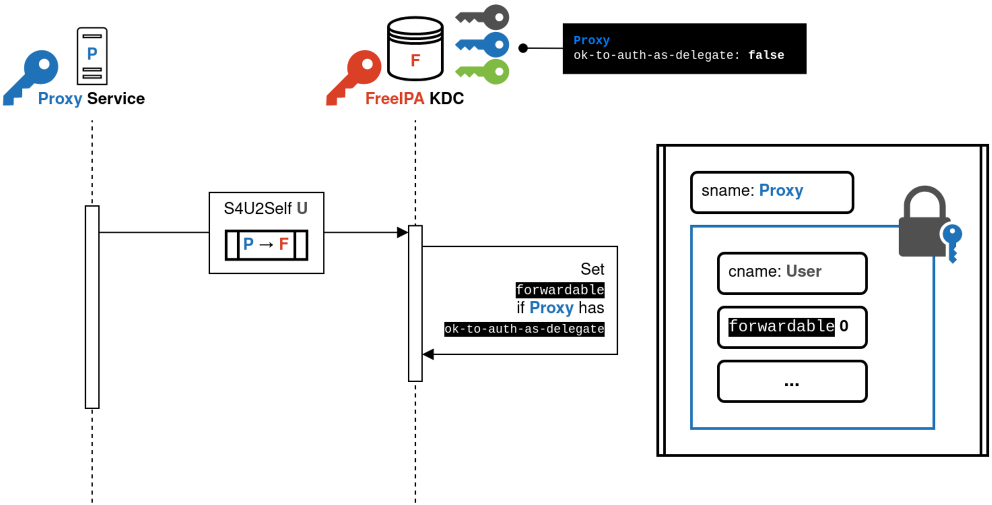
Set `forwardable` if **Proxy** has `ok-to-auth-as-delegate`

Protocol Transition (S4U2Self)



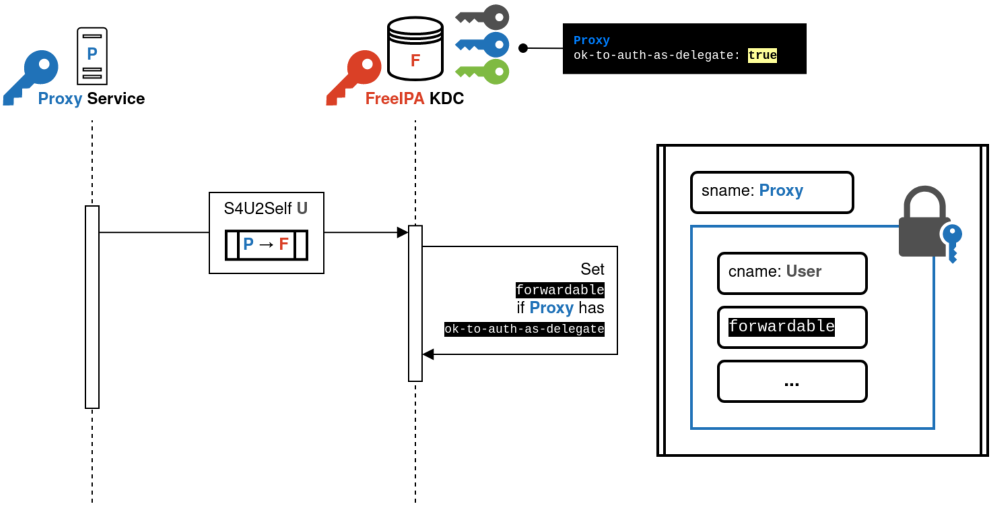
```
Proxy
ok-to-auth-as-delegate: false
```

Protocol Transition (S4U2Self)



```
Proxy
ok-to-auth-as-delegate: false
```

Protocol Transition (S4U2Self)



P

Proxy Service

F

FreeIPA KDC

```
Proxy
ok-to-auth-as-delegate: true
```

S4U2Self U

P → F

Set `forwardable` if Proxy has `ok-to-auth-as-delegate`

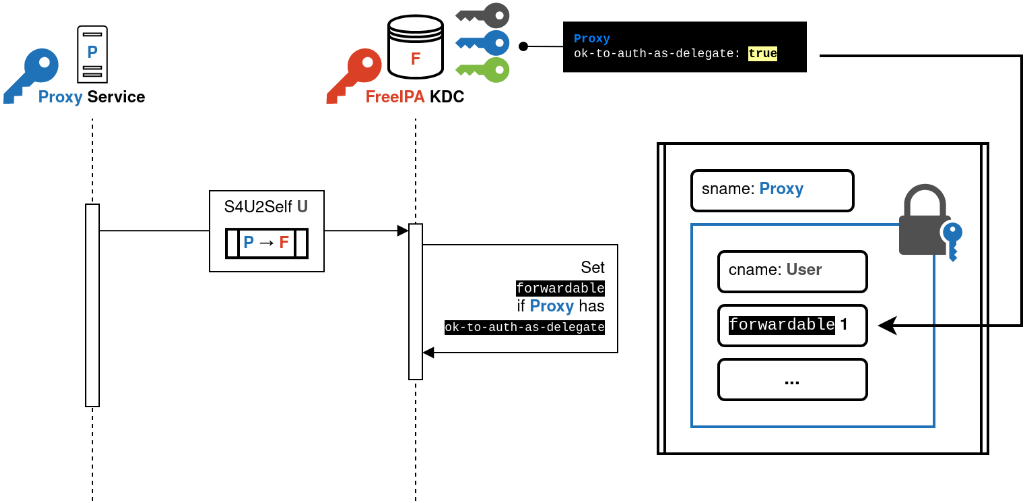
sname: Proxy

cname: User

`forwardable`

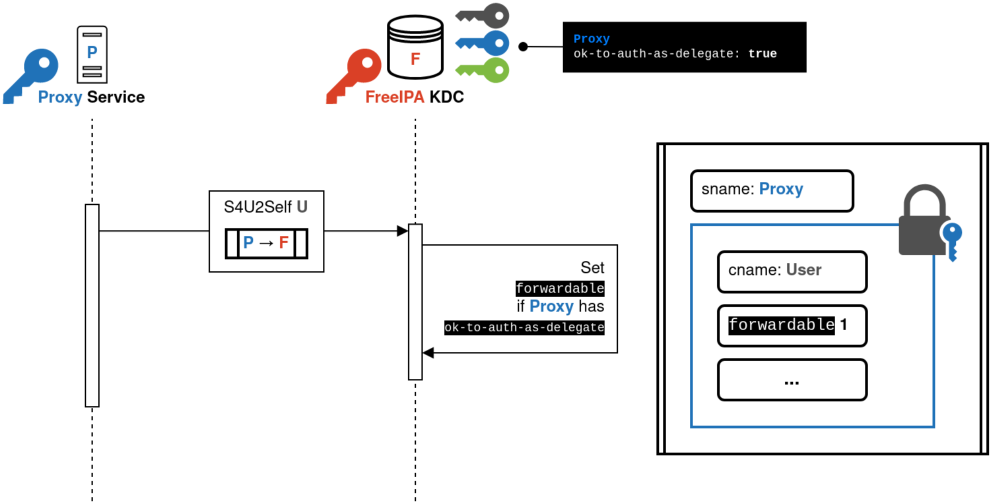
...

Protocol Transition (S4U2Self)

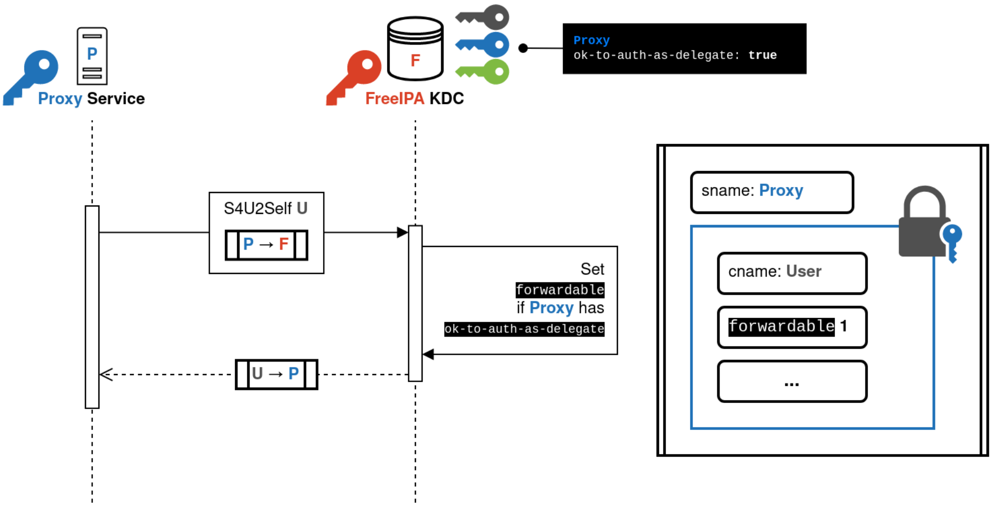


```
Proxy
ok-to-auth-as-delegate: true
```

Protocol Transition (S4U2Self)



Protocol Transition (S4U2Self)



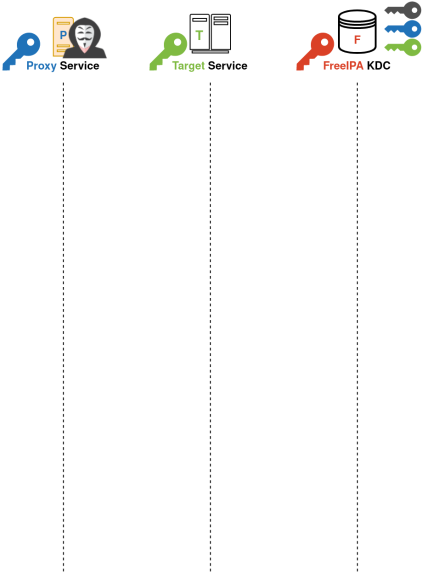
```
Proxy
ok-to-auth-as-delegate: true
```

The Bronze-Bit exploit

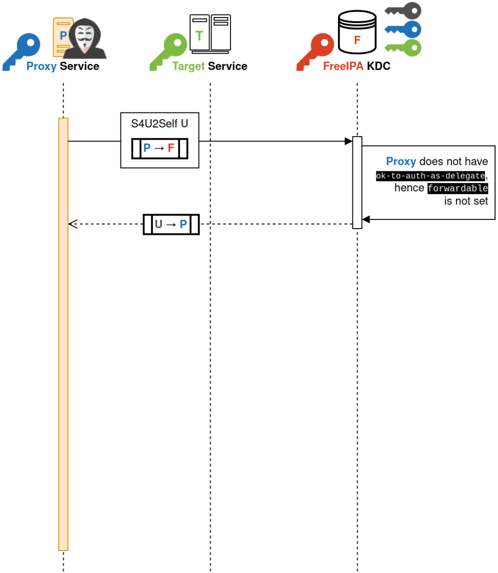
The problem with MS-SFU

- A service with the `forwardable` S4U2Self ticket permission AND a constrained delegation rule can impersonate **any user** against the **target service** of this delegation rule
  - Including users with **administration privileges** for this service
- The `forwardable` flag is encrypted using the **proxy service** key
  - But nothing keeps the service from changing the value of this flag
- If the host running the proxy service is compromised, the attacker could use proxy service's credentials to **access the target service as an admin user**

The Bronze-Bit exploit

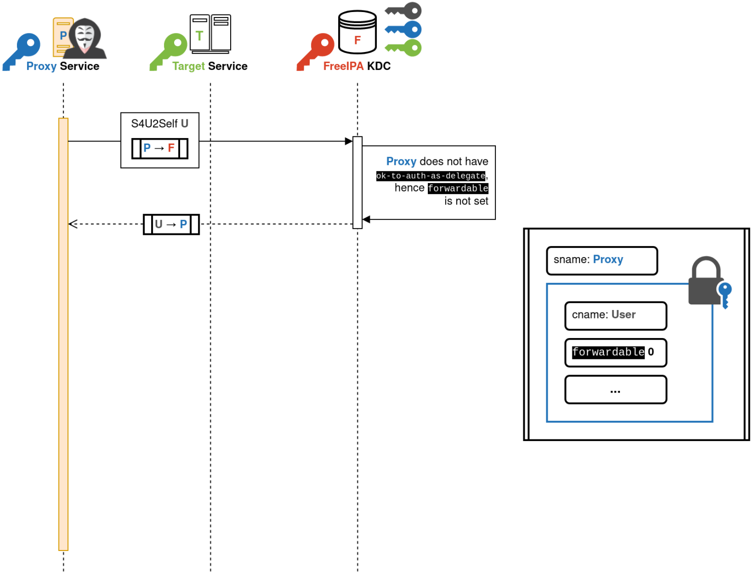


The Bronze-Bit exploit



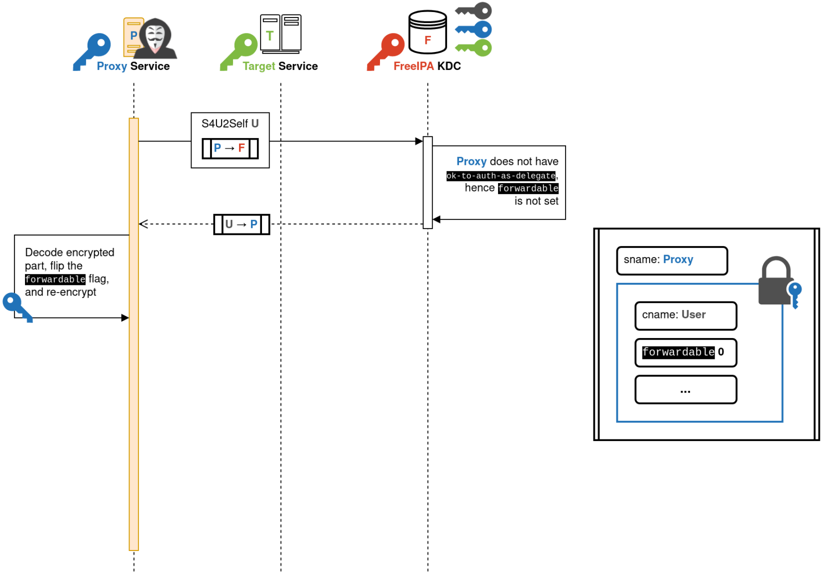
Proxy does not have `ok-to-auth-as-delegate`, hence `forwardable` is not set

The Bronze-Bit exploit



Proxy does not have `ok-to-auth-as-delegate`, hence `forwardable` is not set

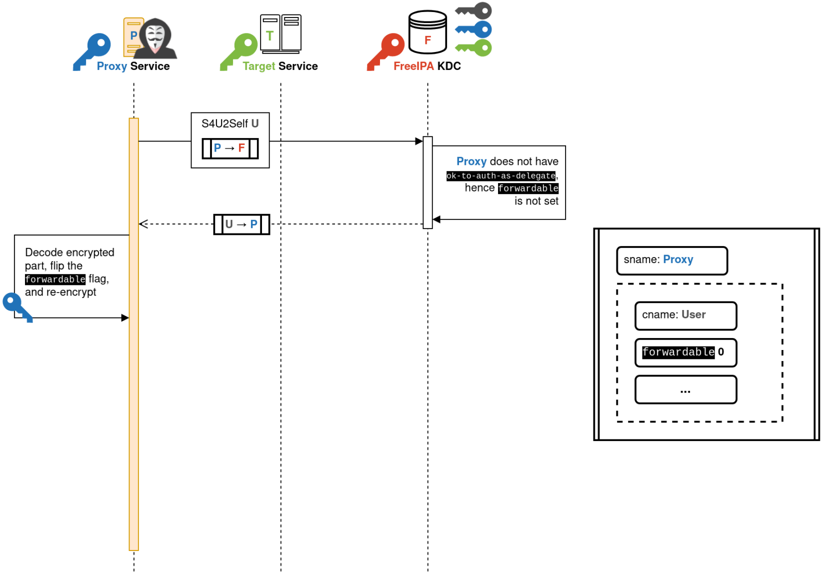
The Bronze-Bit exploit



Proxy does not have ok-to-auth-as-delegate, hence forwardable is not set

Decode encrypted part, flip the forwardable flag, and re-encrypt

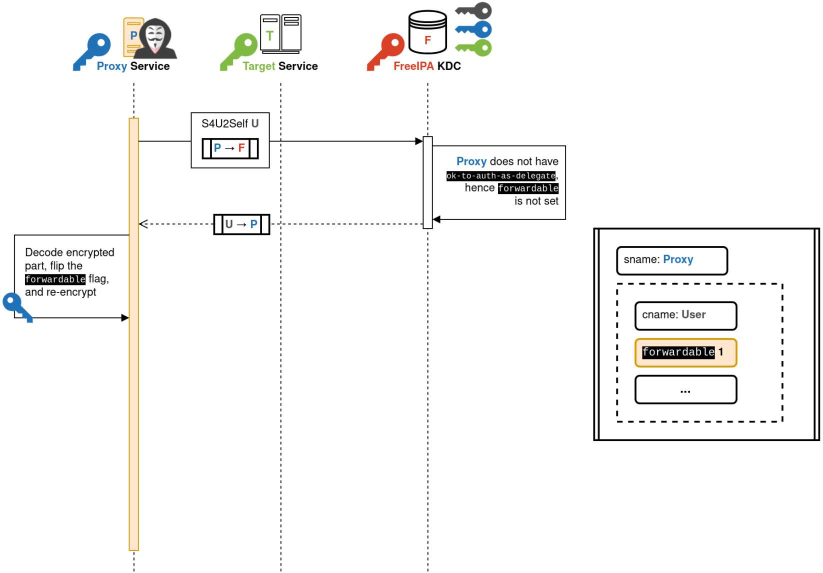
The Bronze-Bit exploit



Proxy does not have `ok-to-auth-as-delegate`, hence `forwardable` is not set

Decode encrypted part, flip the `forwardable` flag, and re-encrypt

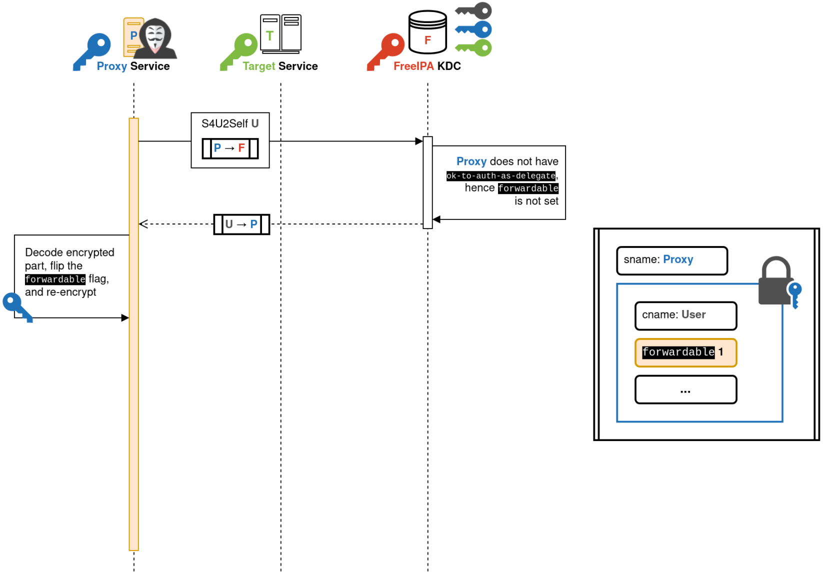
The Bronze-Bit exploit



Proxy does not have ok-to-auth-as-delegate, hence forwardable is not set

Decode encrypted part, flip the forwardable flag, and re-encrypt

The Bronze-Bit exploit



Proxy Service

Target Service

FreeIPA KDC

S4U2Self U

P → F

Proxy does not have `ok-to-auth-as-delegate`, hence `forwardable` is not set

U → P

Decode encrypted part, flip the `forwardable` flag, and re-encrypt

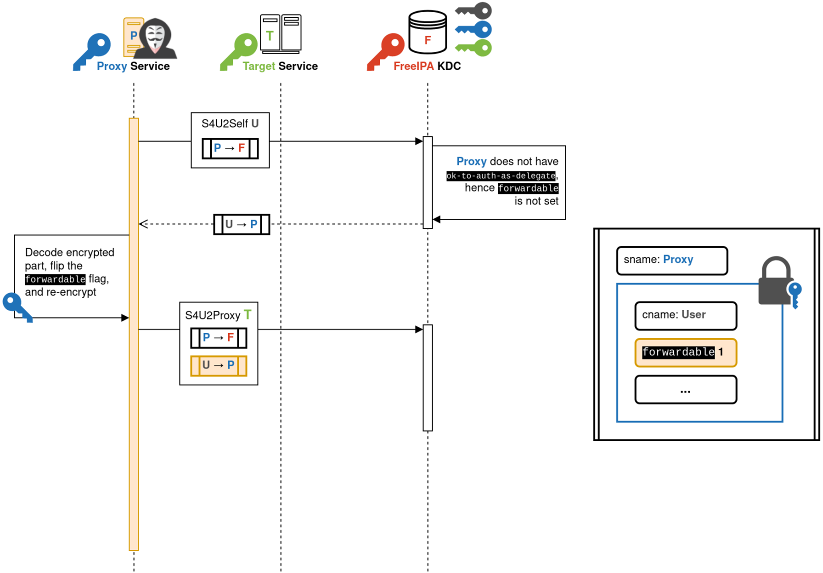
sname: Proxy

cname: User

`forwardable` 1

...

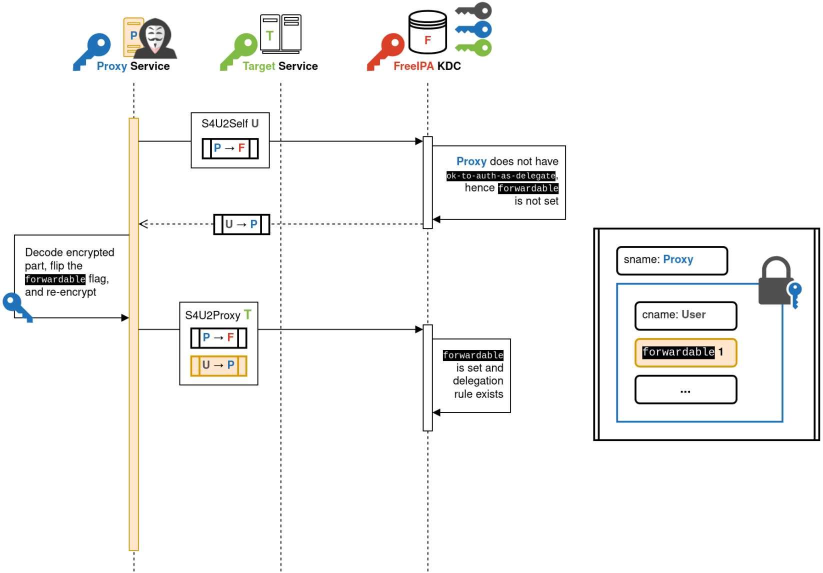
The Bronze-Bit exploit



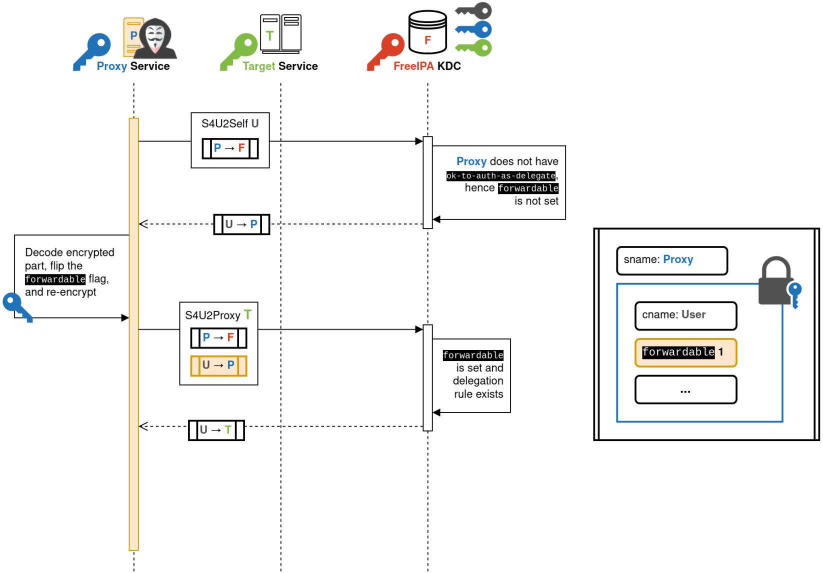
Proxy does not have ok-to-auth-as-delegate, hence forwardable is not set

Decode encrypted part, flip the forwardable flag, and re-encrypt

The Bronze-Bit exploit


Proxy Service
Target Service
FreeIPA KDC
P
T
F
S4U2Self U
P → F
Proxy does not have ok-to-auth-as-delegate, hence forwardable is not set
U → P
Decode encrypted part, flip the forwardable flag, and re-encrypt
S4U2Proxy T
P → F
U → P
forwardable is set and delegation rule exists
sname: Proxy
cname: User
forwardable 1
...

The Bronze-Bit exploit

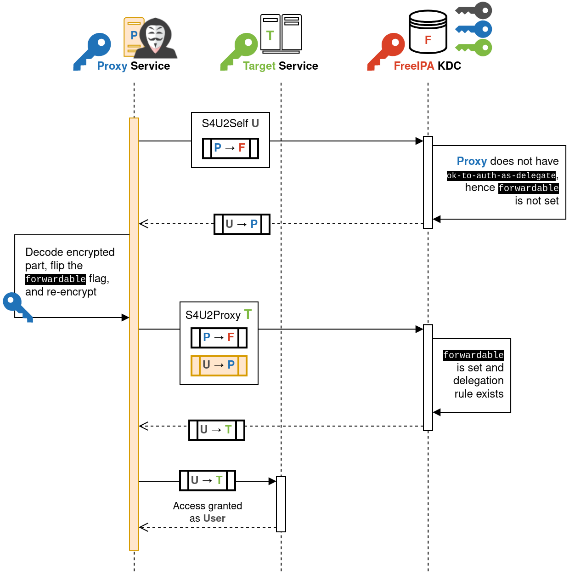


Proxy does not have ok-to-auth-as-delegate, hence forwardable is not set

Decode encrypted part, flip the forwardable flag, and re-encrypt

forwardable is set and delegation rule exists

The Bronze-Bit exploit



Proxy Service

Target Service

FreeIPA KDC

S4U2Self U

P → F

Proxy does not have `ok-to-auth-as-delegate`, hence `forwardable` is not set

U → P

Decode encrypted part, flip the `forwardable` flag, and re-encrypt

S4U2Proxy T

P → F

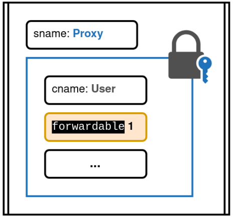
U → P

`forwardable` is set and delegation rule exists

U → T

U → T

Access granted as User



sname: Proxy

cname: User

`forwardable` 1

...

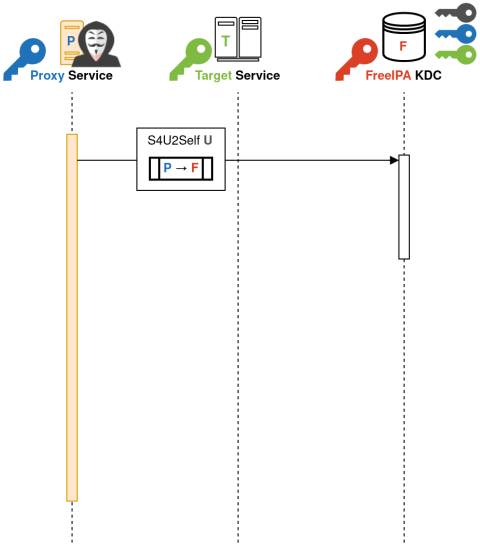
Reproducer for MIT Kerberos and FreeIPA

- All available reproducers designed for Active Directory
- None of them could work against FreeIPA, because they were missing support for:
    - `PA_S4U_X509_USER` ASN.1 sequence (for S4U2Proxy)
    - AES HMAC-SHA2 encryption types familly (from RFC8009)
- We implemented support for these 2 features in the **Impacket Python library**
    - `fortra/impacket#1684`:
      Implement Kerberos encryption types from RFC8009 (AES HMAC-SHA2 familly)
      `https://github.com/fortra/impacket/pull/1684`

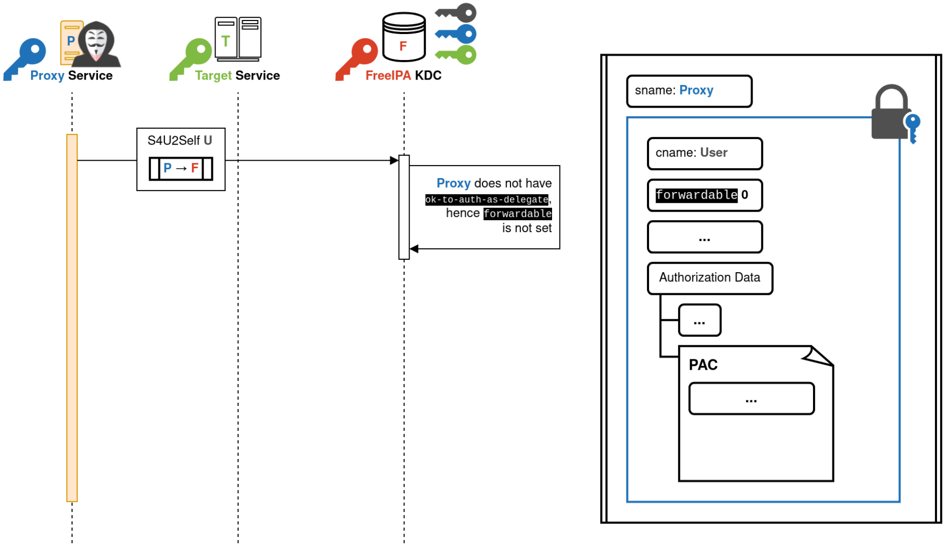
Fix: Ticket signature

- Solution designed my Microsoft
  - **Signature** actually means **keyed checksum** (RFC3961, RFC4120)
- Implemented by AD and MIT Kerberos 1.20
- Sign the encrypted part of the ticket using the **KDC key**
  - KDC able to detect any modification of ticket's encrypted part
  - `forwardable` flag protected
- MS-PAC Kerberos extension
  - Add a **Privilege Attribute Certificate** (PAC) in the ticket

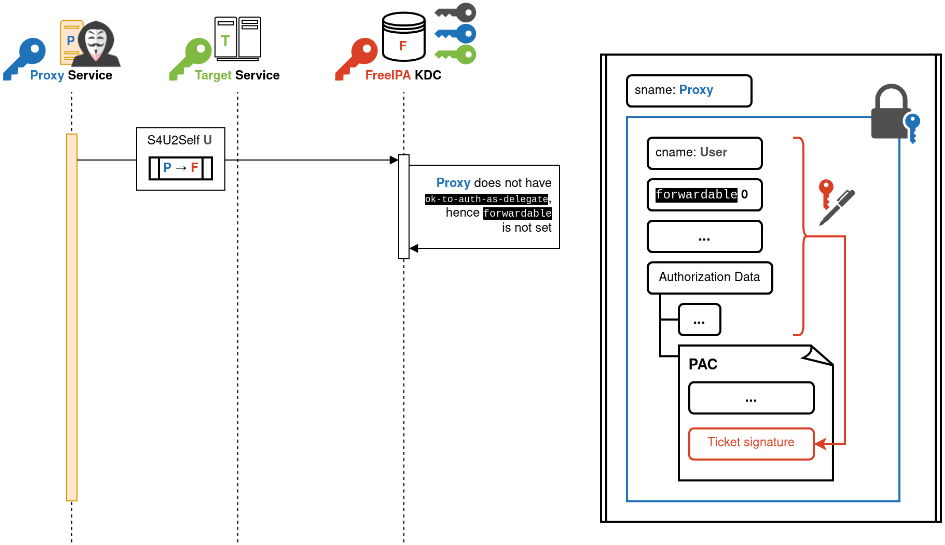
PAC ticket signature



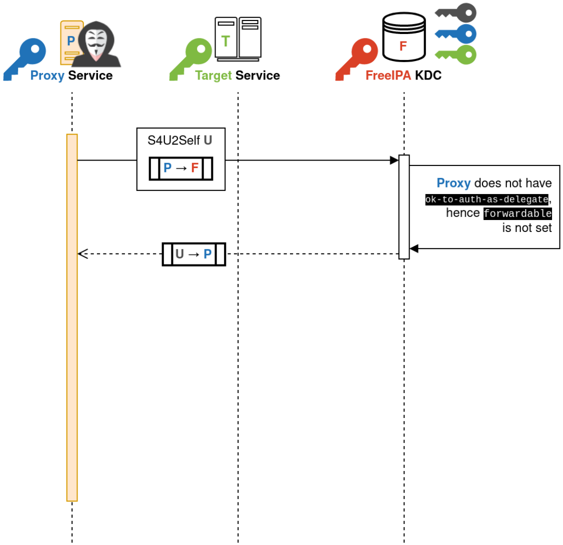
PAC ticket signature



PAC ticket signature



PAC ticket signature



Proxy Service

Target Service

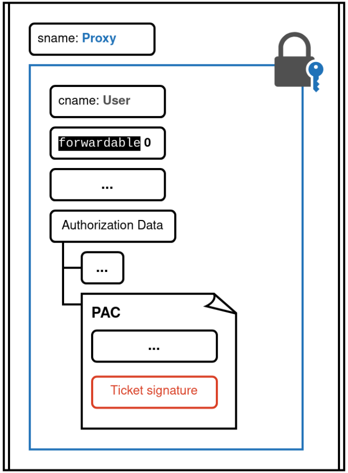
FreeIPA KDC

S4U2Self U

P → F

U → P

Proxy does not have `ok-to-auth-as-delegate`, hence `forwardable` is not set



sname: Proxy

cname: User

`forwardable` 0

...

Authorization Data

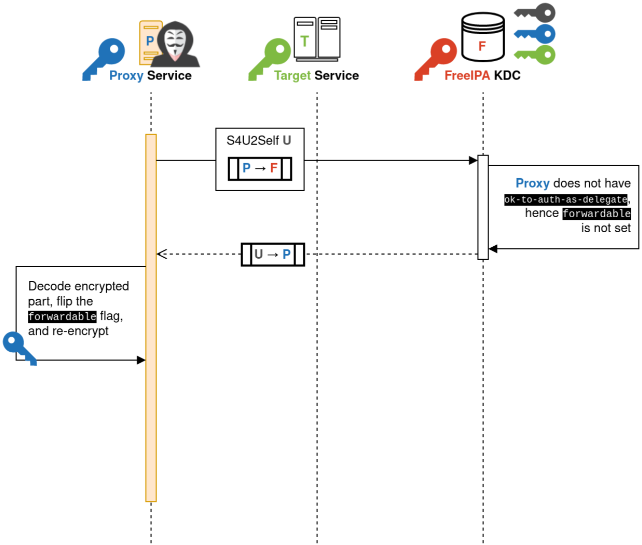
...

PAC

...

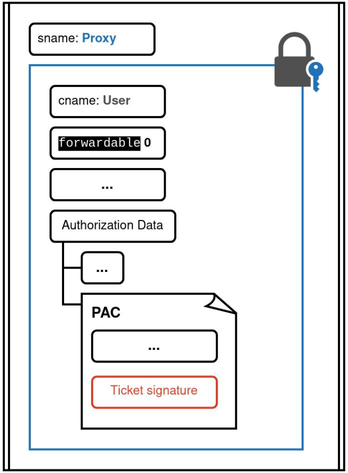
Ticket signature

PAC ticket signature

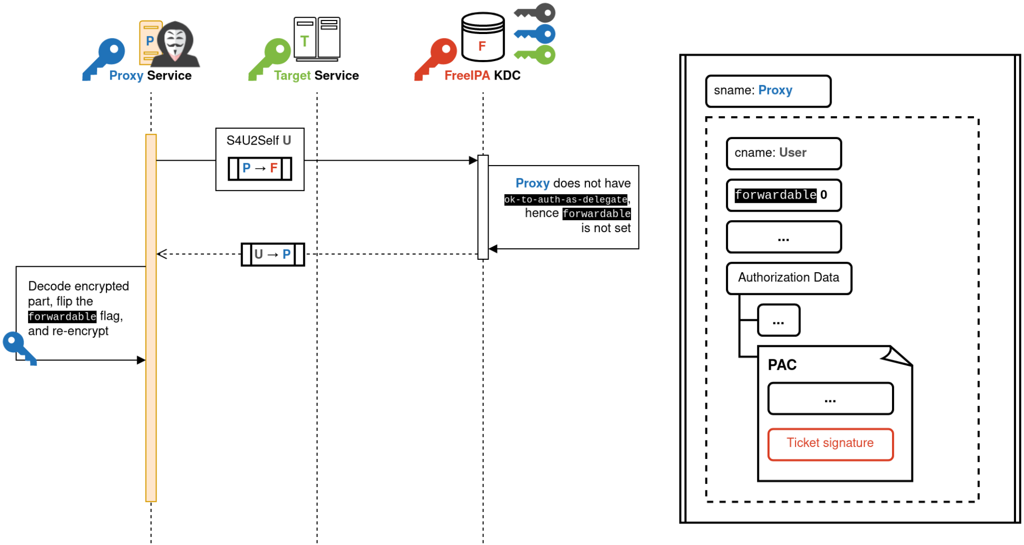


Proxy does not have `ok-to-auth-as-delegate`, hence `forwardable` is not set

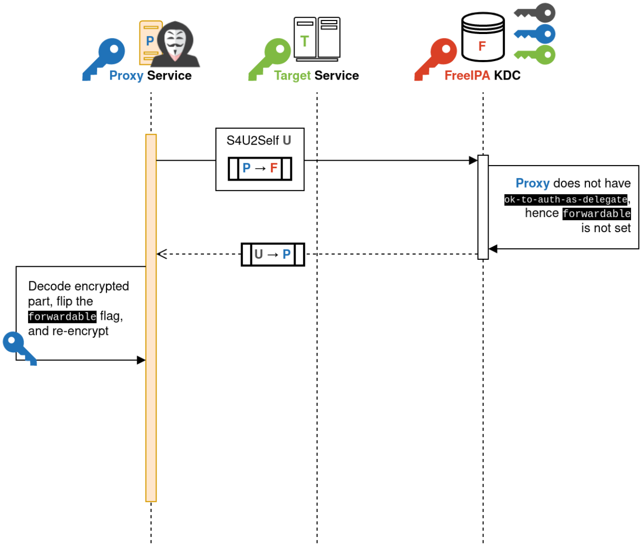
Decode encrypted part, flip the `forwardable` flag, and re-encrypt



PAC ticket signature

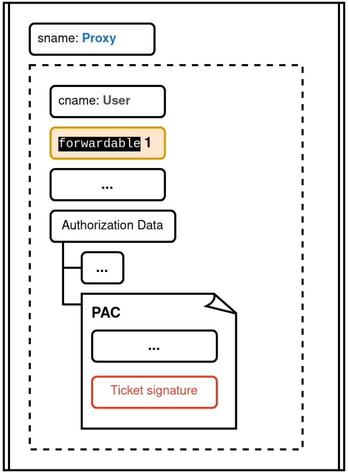


PAC ticket signature

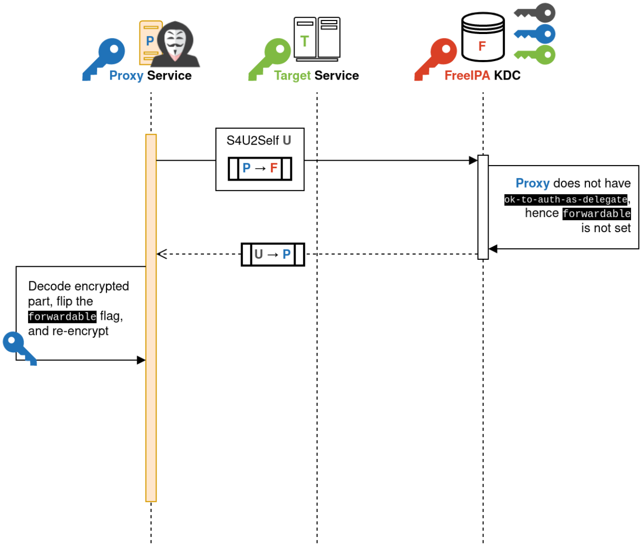


Proxy does not have ok-to-auth-as-delegate, hence forwardable is not set

Decode encrypted part, flip the forwardable flag, and re-encrypt

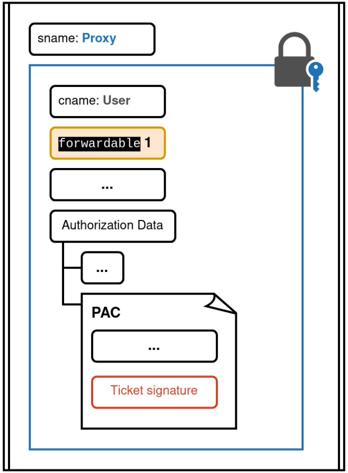


PAC ticket signature

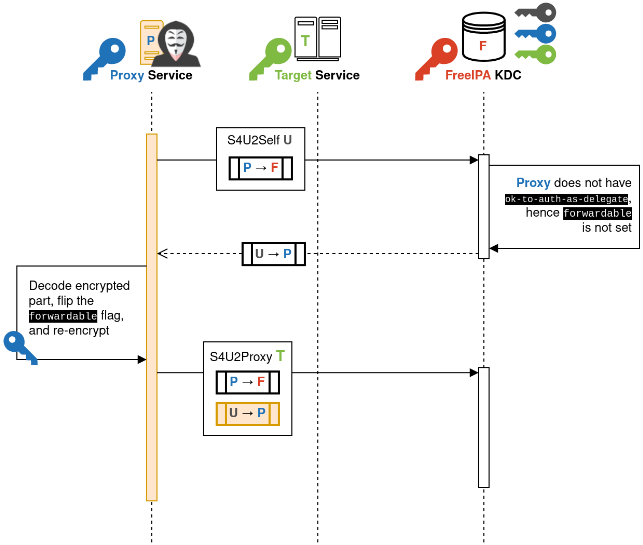


Proxy does not have ok-to-auth-as-delegate, hence forwardable is not set

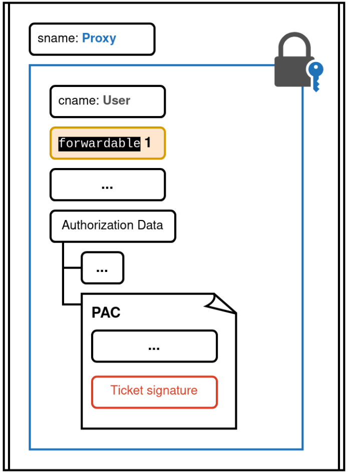
Decode encrypted part, flip the forwardable flag, and re-encrypt



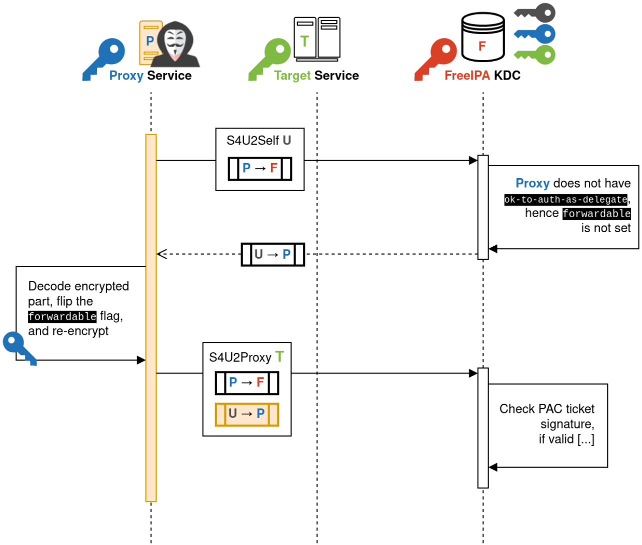
PAC ticket signature



Proxy does not have ok-to-auth-as-delegate, hence forwardable is not set



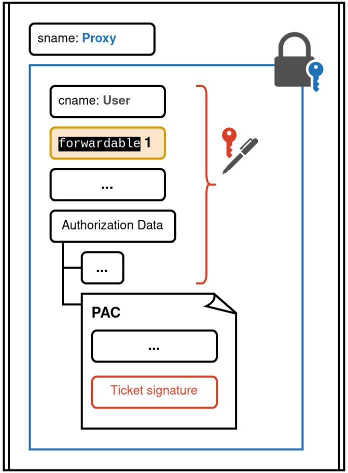
PAC ticket signature



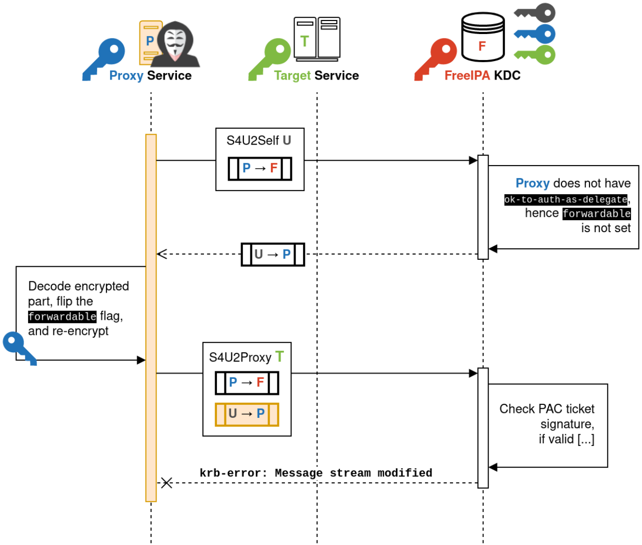
Proxy does not have `ok-to-auth-as-delegate`, hence `forwardable` is not set

Decode encrypted part, flip the `forwardable` flag, and re-encrypt

Check PAC ticket signature, if valid [...]



PAC ticket signature



Proxy Service

Target Service

FreelPA KDC

S4U2Self U

P → F

Proxy does not have `ok-to-auth-as-delegate`, hence `forwardable` is not set

U → P

Decode encrypted part, flip the `forwardable` flag, and re-encrypt

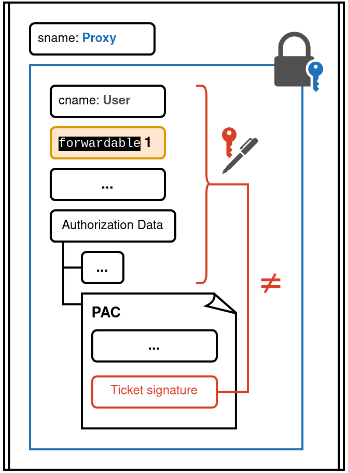
S4U2Proxy T

P → F

U → P

Check PAC ticket signature, if valid [...]

`krb-error: Message stream modified`



sname: Proxy

cname: User

`forwardable` 1

...

Authorization Data

...

PAC

...

Ticket signature

≠

Fix for CentOS 8 Stream and RHEL 8

C8S/RHEL8: Software constraints

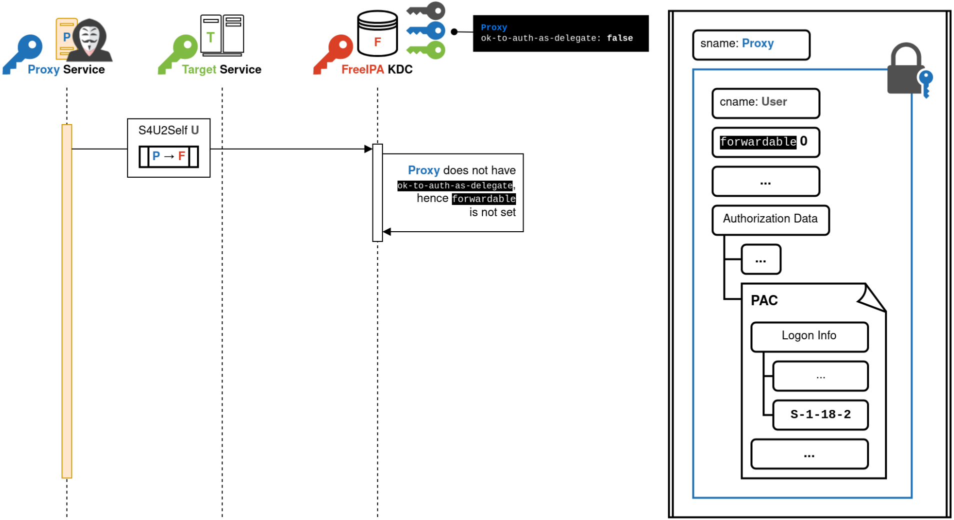
- Using MIT Kerberos 1.18
- PAC generation handled by IPA KDB plugin
- ABI compatibility within major release
  - Update to MIT krb5 1.20 impossible
- PAC ticket signature not backportable

```
krb5_error_code
(*sign_authdata)(krb5_context kcontext,              unsigned int flags,
                 krb5_const_principal client_princ,  krb5_const_principal server_princ,
                 krb5_db_entry *client,              krb5_db_entry *server,
                 krb5_db_entry *header_server,       krb5_db_entry *local_tgt,
                 krb5_keyblock *client_key,          krb5_keyblock *server_key,
                 krb5_keyblock *header_key,          krb5_keyblock *local_tgt_key,
                 krb5_keyblock *session_key,         krb5_timestamp authtime,
                 krb5_authdata **tgt_auth_data,      void *ad_info,
                 krb5_data ***auth_indicators,       krb5_authdata ***signed_auth_data);
```

Attack detection

- If the ticket cannot be protected, maybe the KDC could detect the attack
- The PAC contains **additional authorization information**
  - List of SIDs
- *Security identifier* (SID)
  - Identifiers used in the AD world
  - Unique, except for some well-known ones
- Well-known SIDs supported by FreeIPA:
  - **S-1-18-1**: *Authentication authority asserted identity*
    - Ticket obtained using normal user request
  - **S-1-18-2**: *Service asserted identity*
    - Ticket obtained using S4U2Self

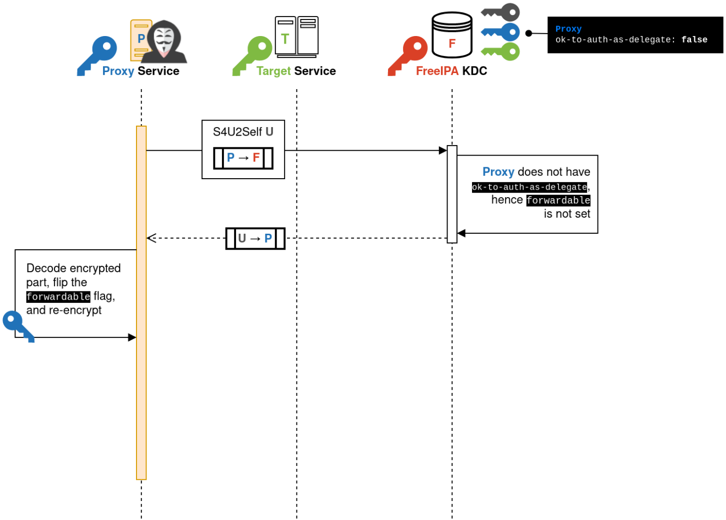
Bronze-Bit attack detection



```
Proxy
ok-to-auth-as-delegate: false
```

Proxy does not have `ok-to-auth-as-delegate`, hence `forwardable` is not set

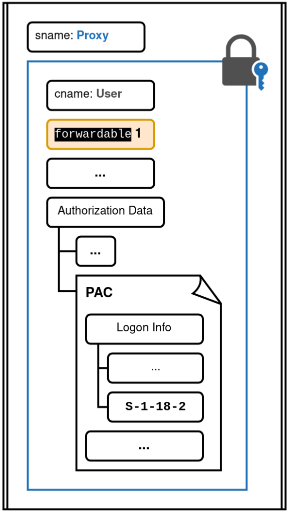
Bronze-Bit attack detection



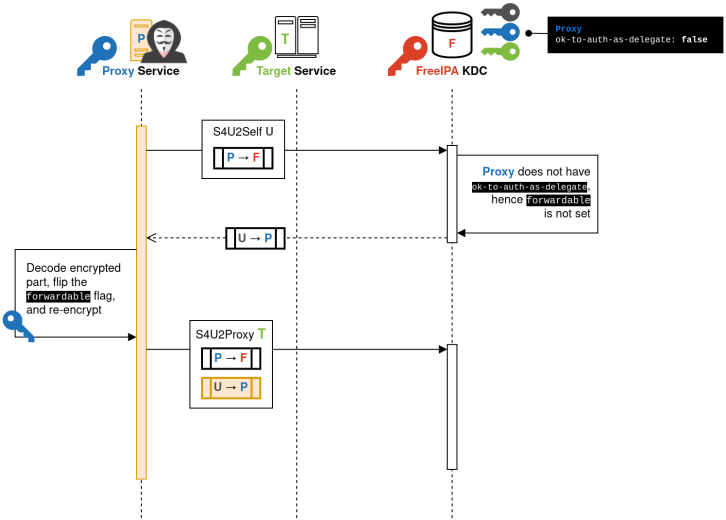
```
Proxy
ok-to-auth-as-delegate: false
```

Proxy does not have `ok-to-auth-as-delegate`, hence `forwardable` is not set

Decode encrypted part, flip the `forwardable` flag, and re-encrypt



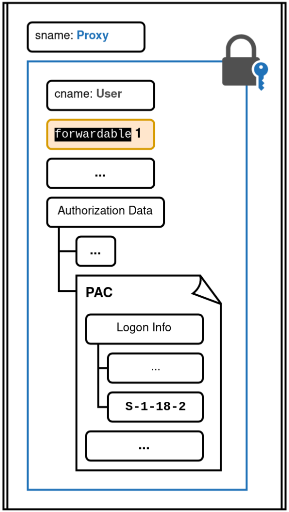
Bronze-Bit attack detection



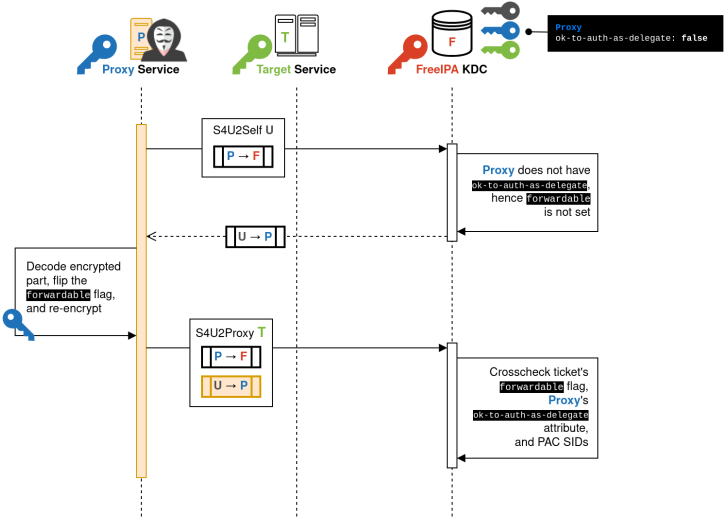
```
Proxy
ok-to-auth-as-delegate: false
```

Proxy does not have `ok-to-auth-as-delegate`, hence `forwardable` is not set

Decode encrypted part, flip the `forwardable` flag, and re-encrypt



Bronze-Bit attack detection

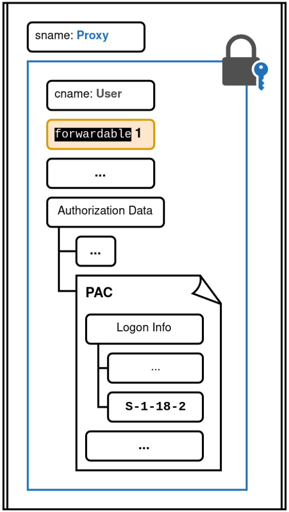


```
Proxy
ok-to-auth-as-delegate: false
```

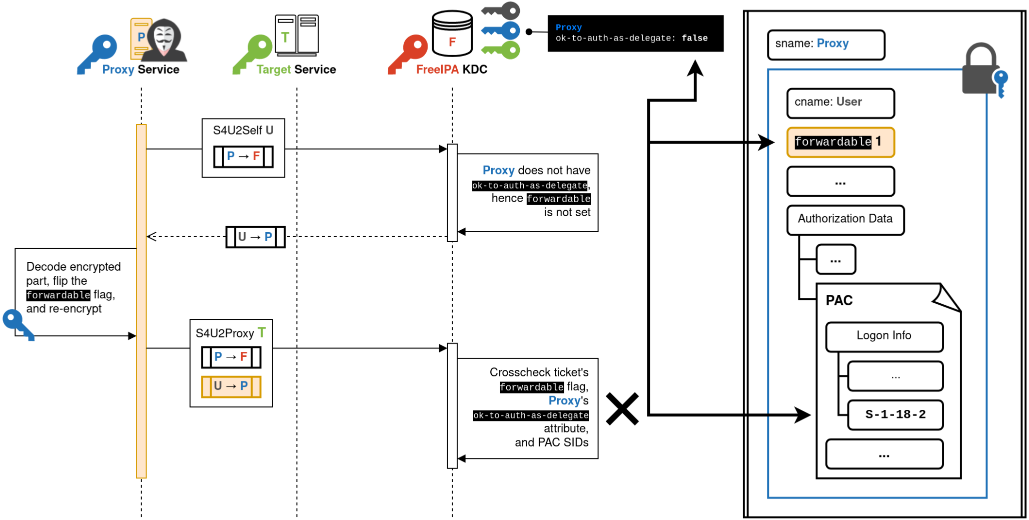
Proxy does not have `ok-to-auth-as-delegate`, hence `forwardable` is not set

Decode encrypted part, flip the `forwardable` flag, and re-encrypt

Crosscheck ticket's `forwardable` flag, Proxy's `ok-to-auth-as-delegate` attribute, and PAC SIDs



Bronze-Bit attack detection



Proxy Service

Target Service

FreeIPA KDC

```
Proxy
ok-to-auth-as-delegate: false
```

S4U2Self U

P → F

Proxy does not have ok-to-auth-as-delegate, hence forwardable is not set

U → P

Decode encrypted part, flip the forwardable flag, and re-encrypt

S4U2Proxy T

P → F

U → P

Crosscheck ticket's forwardable flag, Proxy's ok-to-auth-as-delegate attribute, and PAC SIDs

sname: Proxy

cname: User

forwardable 1

...

Authorization Data

...

PAC

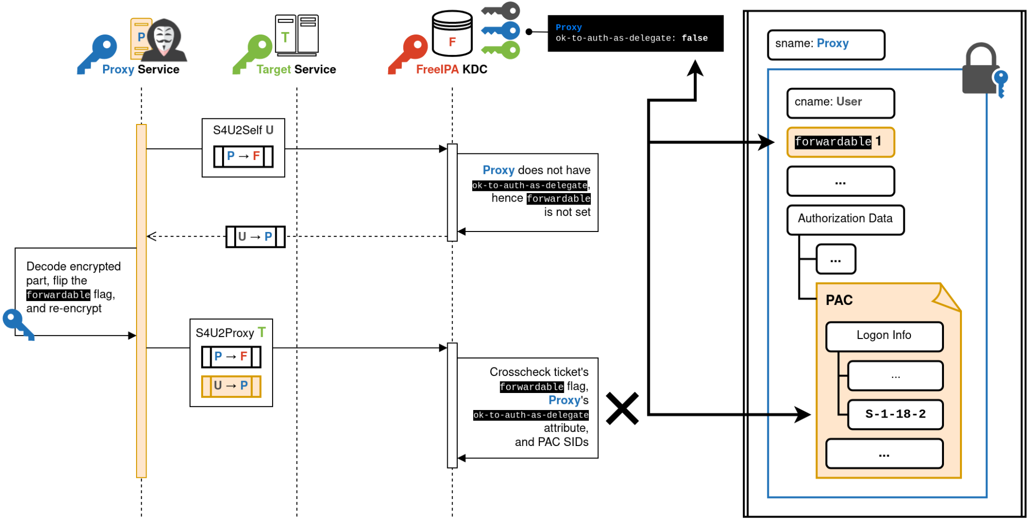
Logon Info

...

S-1-18-2

...

Bronze-Bit attack detection



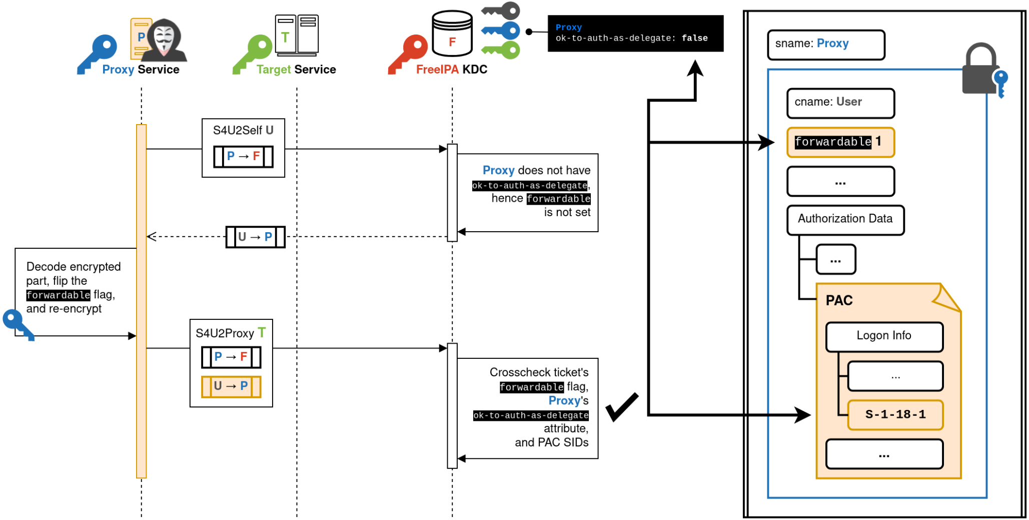
```
Proxy
ok-to-auth-as-delegate: false
```

Proxy does not have ok-to-auth-as-delegate, hence forwardable is not set

Decode encrypted part, flip the forwardable flag, and re-encrypt

Crosscheck ticket's forwardable flag, Proxy's ok-to-auth-as-delegate attribute, and PAC SIDs

Bronze-Bit attack detection



```
Proxy
ok-to-auth-as-delegate: false
```

Proxy does not have ok-to-auth-as-delegate, hence forwardable is not set

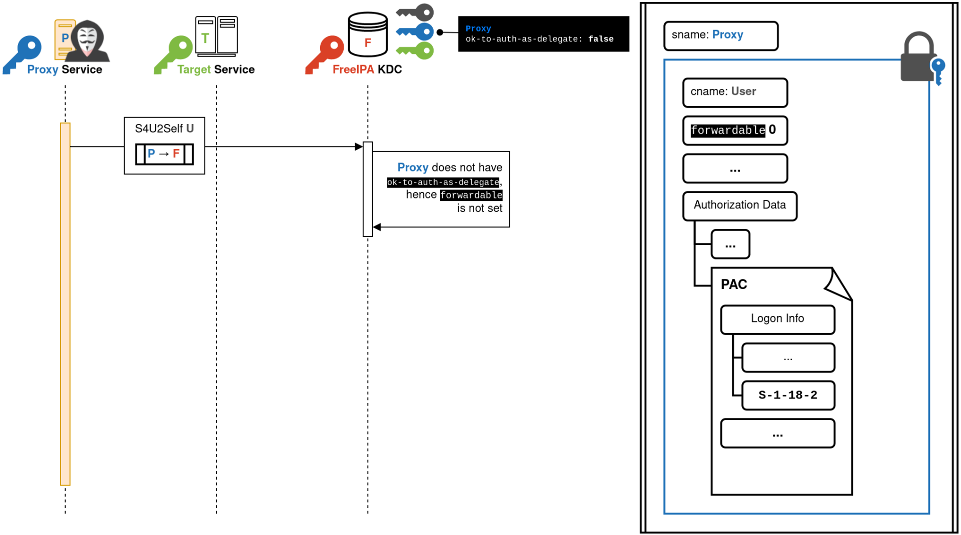
Decode encrypted part, flip the forwardable flag, and re-encrypt

Crosscheck ticket's forwardable flag, Proxy's ok-to-auth-as-delegate attribute, and PAC SIDs ✓

CVE-2022-37967

- **PAC spoofing**
  - Authorization information can be modified
- MS-PAC updated to add the **extended KDC signature**

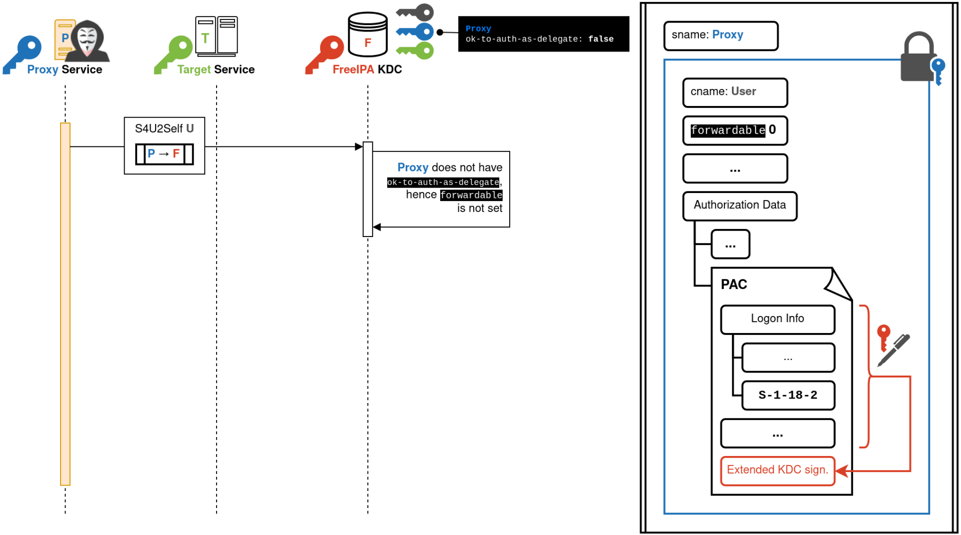
Bronze-Bit attack detection with PAC extended KDC signature



```
Proxy
ok-to-auth-as-delegate: false
```

Proxy does not have ok-to-auth-as-delegate, hence forwardable is not set

Bronze-Bit attack detection with PAC extended KDC signature



Proxy Service

Target Service

FreeIPA KDC

```
Proxy
ok-to-auth-as-delegate: false
```

S4U2Self U

P → F

Proxy does not have `ok-to-auth-as-delegate`, hence `forwardable` is not set

sname: Proxy

cname: User

`forwardable` 0

...

Authorization Data

...

PAC

Logon Info

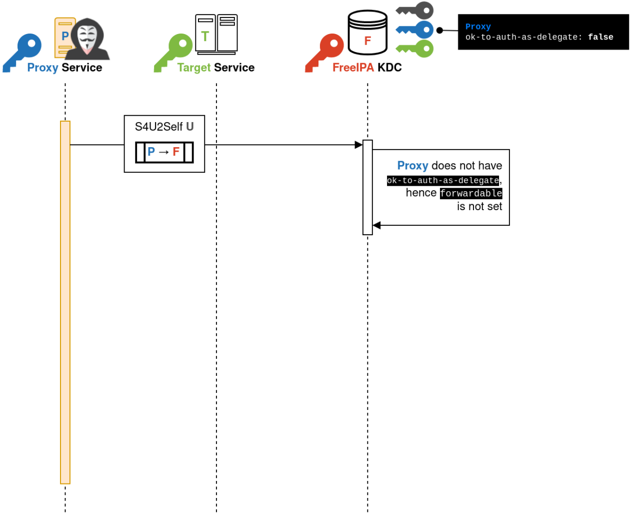
...

`S-1-18-2`

...

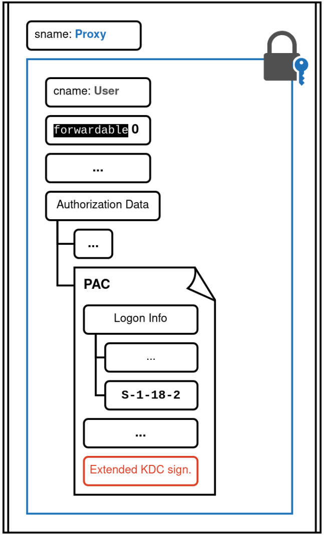
Extended KDC sign.

Bronze-Bit attack detection with PAC extended KDC signature

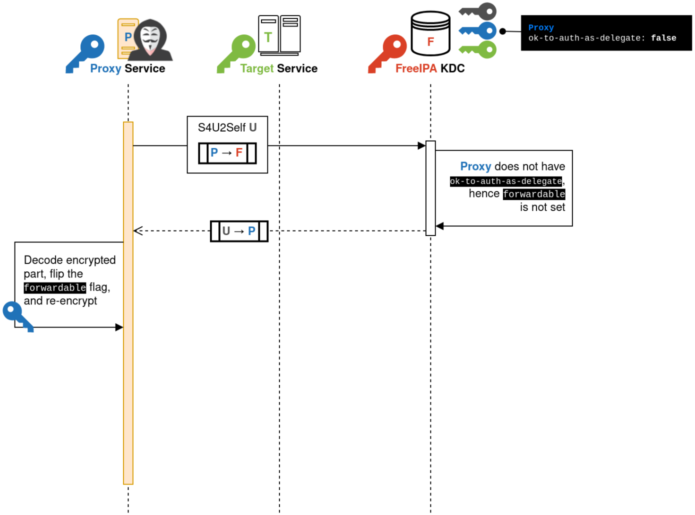


```
Proxy
ok-to-auth-as-delegate: false
```

Proxy does not have `ok-to-auth-as-delegate`, hence `forwardable` is not set



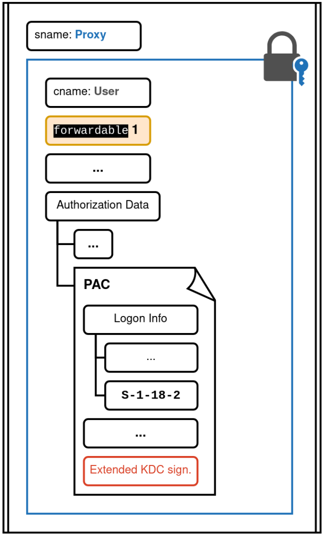
Bronze-Bit attack detection with PAC extended KDC signature



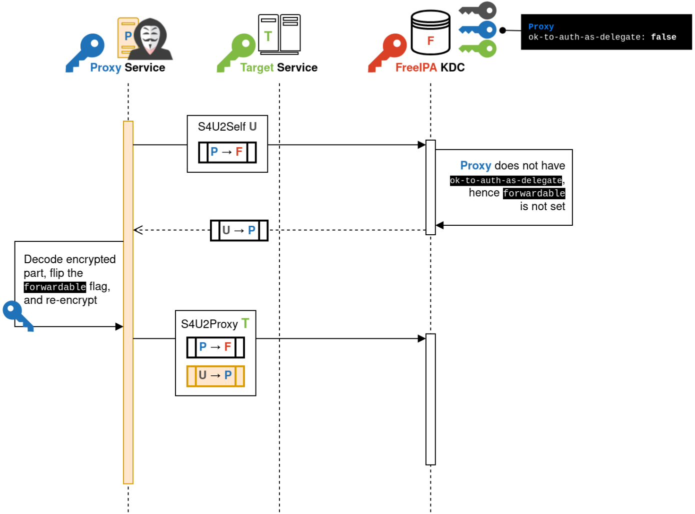
```
Proxy
ok-to-auth-as-delegate: false
```

Proxy does not have `ok-to-auth-as-delegate`, hence `forwardable` is not set

Decode encrypted part, flip the `forwardable` flag, and re-encrypt

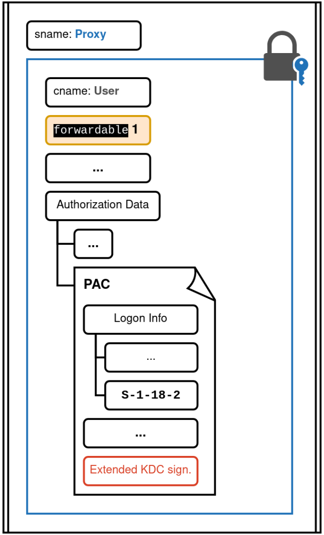


Bronze-Bit attack detection with PAC extended KDC signature

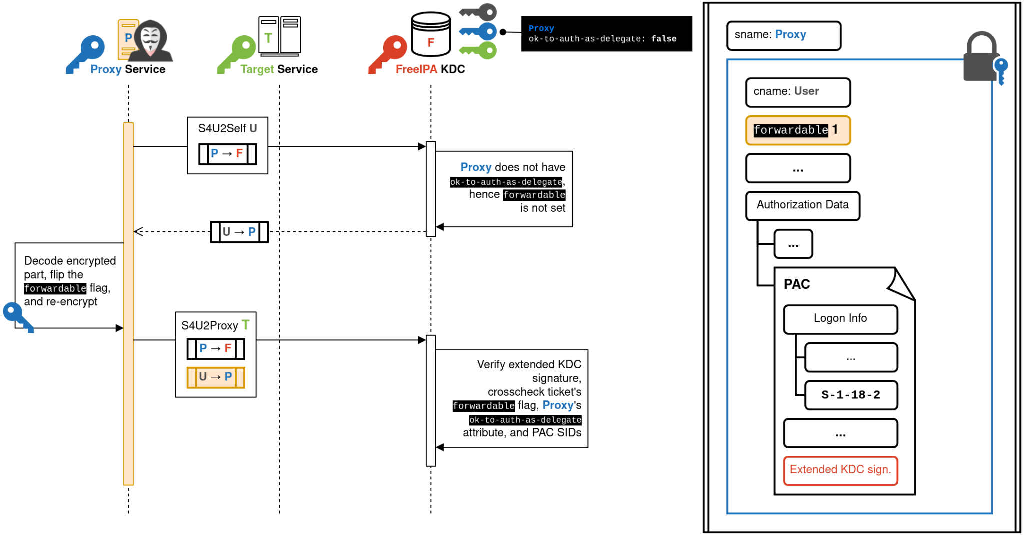


```
Proxy
ok-to-auth-as-delegate: false
```

Proxy Service
P
Target Service
T
FreeIPA KDC
F
S4U2Self U
P → F
Proxy does not have ok-to-auth-as-delegate, hence forwardable is not set
U → P
Decode encrypted part, flip the forwardable flag, and re-encrypt
S4U2Proxy T
P → F
U → P



Bronze-Bit attack detection with PAC extended KDC signature



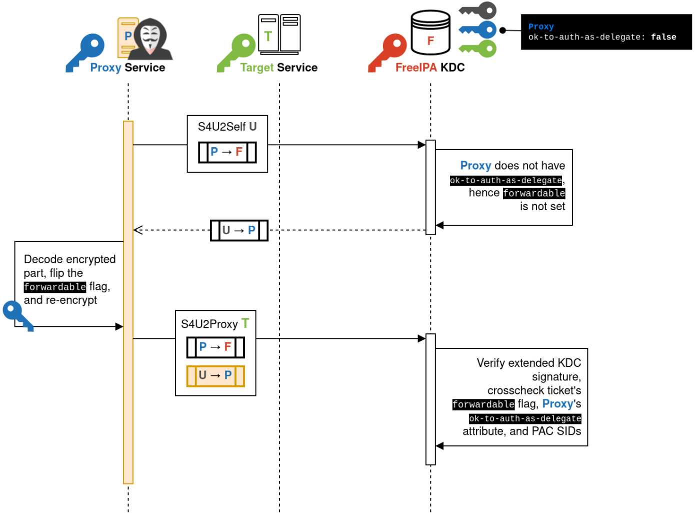
```
Proxy
ok-to-auth-as-delegate: false
```

Proxy does not have ok-to-auth-as-delegate, hence forwardable is not set

Decode encrypted part, flip the forwardable flag, and re-encrypt

Verify extended KDC signature, crosscheck ticket's forwardable flag, Proxy's ok-to-auth-as-delegate attribute, and PAC SIDs

Bronze-Bit attack detection with PAC extended KDC signature

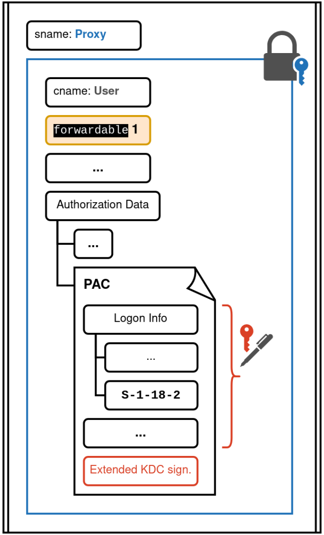


```
Proxy
ok-to-auth-as-delegate: false
```

Proxy does not have ok-to-auth-as-delegate, hence forwardable is not set

Decode encrypted part, flip the forwardable flag, and re-encrypt

Verify extended KDC signature, crosscheck ticket's forwardable flag, Proxy's ok-to-auth-as-delegate attribute, and PAC SIDs



sname: Proxy

cname: User

forwardable 1

...

Authorization Data

...

PAC

Logon Info

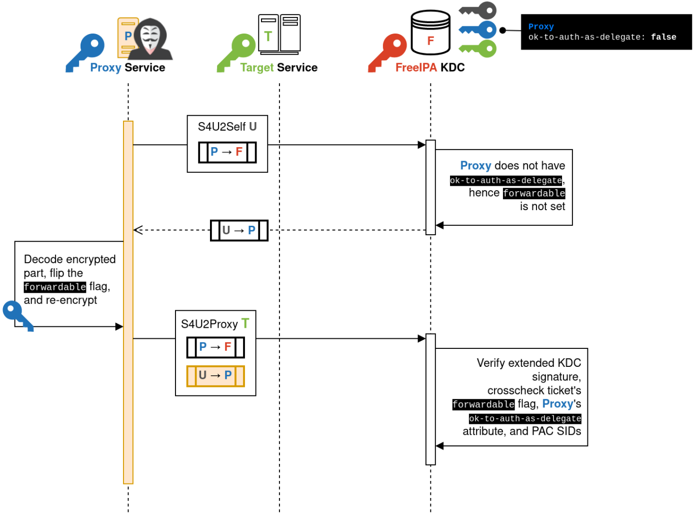
...

S-1-18-2

...

Extended KDC sign.

Bronze-Bit attack detection with PAC extended KDC signature

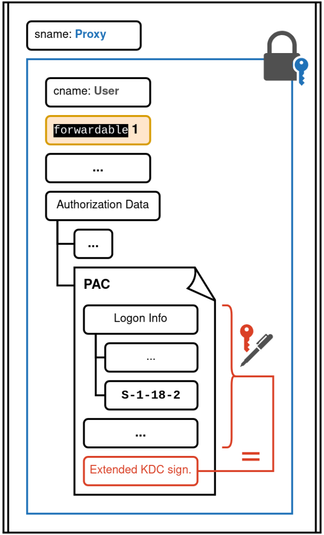


Proxy
ok-to-auth-as-delegate: **false**

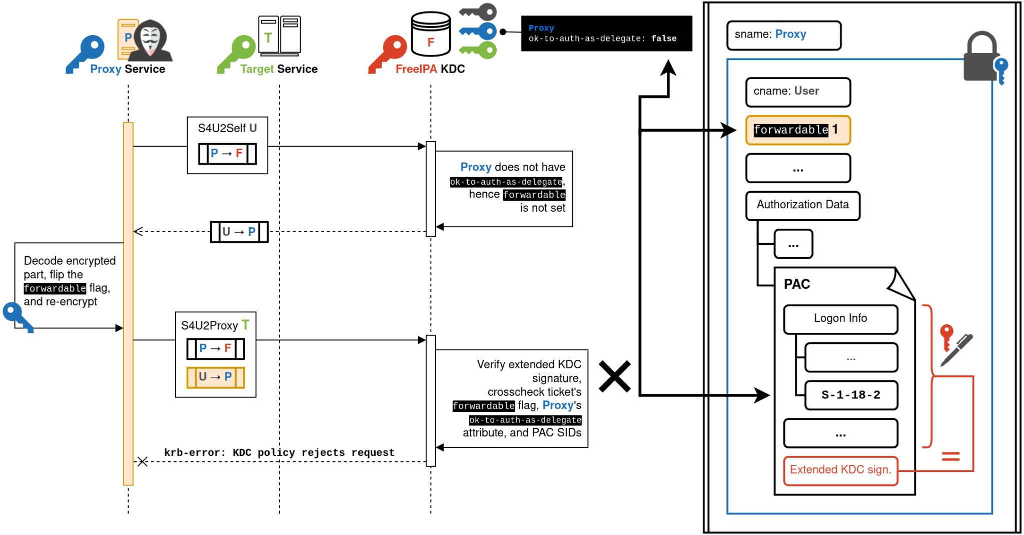
Proxy does not have ok-to-auth-as-delegate, hence forwardable is not set

Decode encrypted part, flip the forwardable flag, and re-encrypt

Verify extended KDC signature, crosscheck ticket's forwardable flag, Proxy's ok-to-auth-as-delegate attribute, and PAC SIDs



Bronze-Bit attack detection with PAC extended KDC signature



Proxy Service

Target Service

FreeIPA KDC

```
Proxy
ok-to-auth-as-delegate: false
```

S4U2Self U

P → F

Proxy does not have ok-to-auth-as-delegate, hence forwardable is not set

U → P

Decode encrypted part, flip the forwardable flag, and re-encrypt

S4U2Proxy T

P → F

U → P

Verify extended KDC signature, crosscheck ticket's forwardable flag, Proxy's ok-to-auth-as-delegate attribute, and PAC SIDs

krb-error: KDC policy rejects request

sname: Proxy

cname: User

forwardable 1

...

Authorization Data

...

PAC

Logon Info

...

S-1-18-2

...

Extended KDC sign.

Conclusion

Conclusion

- Good example of the typical tribulations of **long-term support**
    - Especially for security-related network protocols
- MS-SFU is the continuation of Kerberos' gradual shift
    - From authentication only to **authentication and authorization**

References

1. MS-SFU: Service for User and Constrained Delegation Protocol
   https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-sfu/
2. FreeIPA General Constrained Delegation
   https://freeipa.readthedocs.io/en/ipa-4-10/designs/rbcd.html#general-constrained-delegation-design
3. [Blog] Kerberos: How does delegation work? (Tarlogic)
   https://www.tarlogic.com/blog/kerberos-iii-how-does-delegation-work/
4. [Blog] Kerberos constrained delegation with protocol transition (Phackt)
   https://phackt.com/en-kerberos-constrained-delegation-with-protocol-transition
5. [Blog] Kerberos Delegation (Hackndo)
   https://en.hackndo.com/constrained-unconstrained-delegation/
6. [Blog] Kerberos Constrained Delegation (ired.team)
   https://www.ired.team/offensive-security-experiments/active-directory-kerberos-abuse/abusing-kerberos-constrained-delegation
7. `KDC-REQ-BODY` signature (RFC4120)
   https://datatracker.ietf.org/doc/html/rfc4120#section-5.2.7.1
8. RFC8009: AES Encryption with HMAC-SHA2 for Kerberos 5
   https://datatracker.ietf.org/doc/html/rfc8009
9. `impacket#1684`: Implement Kerberos encryption types from RFC8009 (AES HMAC-SHA2 familly)
   https://github.com/fortra/impacket/pull/1684
10. MS-PAC: ticket signature
    https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-pac/76c10ef5-de76-44bf-b208-0d8750fc2edd
11. Microsoft KB4598347 update
    https://support.microsoft.com/en-us/topic/kb4598347-managing-deployment-of-kerberos-s4u-changes-for-cve-2020-17049-569d60b7-3267-e2b0-7d9b-e46d770332ab
12. MIT Kerberos upstream pull request for PAC ticket signature
    https://github.com/krb5/krb5/pull/1225
13. RHEL8 Compatibility Levels
    https://access.redhat.com/articles/rhel8-abi-compatibility
14. MIT Kerbreos 1.18.2 KDB plugin API
    https://github.com/krb5/krb5/blob/krb5-1.18.2-final/src/include/krb5/kdcpolicy_plugin.h#L120-L126
15. AD special identity groups
    https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-special-identities-groups
16. Service Asserted Identity SID set by FreeIPA for S4U2Self
    https://github.com/freeipa/freeipa/blob/release-4-9-12/daemons/ipa-kdb/ipa_kdb_mspac.c#L386-L390
17. Kerberos' RC4-HMAC broken in practice: spoofing PACs with MD5 collisions
    https://i.blackhat.com/EU-22/Thursday-Briefings/EU-22-Tervoort-Breaking-Kerberos-RC4-Cipher-and-Spoofing-Windows-PACs-wp.pdf
18. MS-PAC: exteneded KDC signature
    https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-pac/9cf6f6ad-6b76-44b3-aefa-901aa1ff5a08
19. MIT Kerberos upstream pull request for PAC extended KDC signature (aka. PAC full checksum)
    https://github.com/krb5/krb5/pull/1284
20. Bronze-Bit attack detection for FreeIPA
    https://github.com/freeipa/freeipa/commit/a847e2483b4c4832ee5129901da169f4eb0d1392
21. Build conditions for Bronze-Bit attack detection in FreeIPA
    https://github.com/freeipa/freeipa/commit/67ca47ba4092811029eec02f8af9c34ba7662924
22. Bronze-Bit attack detection patch for CentOS 8 Stream
    https://gitlab.com/redhat/centos-stream/rpms/ipa/-/merge_requests/58/

Questions?

Thank you!