kerberos-rbcd-s4u2proxy.annotated

🏛️ NDC (KDC, parent realm)	🖥️ WINC$ (service)	🏛️ TDC (KDC, child realm)

[1] 🔐 AS-REQ

🔒 PA-DATA	pA-PAC-REQUEST
📋 kdc-options	40810010
🏷️ Name type	ENTERPRISE-PRINCIPAL
👤 Client	ayala@nd
🌐 Realm	ND.C
🎯 SName	krbtgt
🎯 SName	ND.C

[2] ⚠️ KRB-ERROR PREAUTH-REQUIRED

🌐 Realm	ND.C
🔒 e-data PA-DATA	pA-ETYPE-INFO2
🧂 Salt	ND.Cayala
🔒 e-data PA-DATA	pA-ENC-TIMESTAMP
🔒 e-data PA-DATA	pA-PK-AS-REQ
🔒 e-data PA-DATA	pA-PK-AS-REP-19

[3] 🎫 TGS-REQ (S4U2Self)

🔒 PA-DATA	pA-TGS-REQ
🎯 SName	krbtgt
🎯 SName	ND.C
👤 CName	WINC$
👤 CName	WINC$
🔒 PA-DATA	pA-FOR-X509-USER
👤 On behalf of	ayala@nd
👤 On behalf of	ayala@nd
📋 kdc-options	40810000
🎯 SName	winc$

[4] ✅ TGS-REP

🔒 PA-DATA	pA-FOR-X509-USER
👤 Client	ayala@nd
🌐 Realm	ND.C
🎯 SName	winc$
🏷️ forwardable	False
🔑 Decrypted key type	AES256-CTS-HMAC-SHA1-96 (18)
👤 Client	ayala@nd
🪪 PAC name	ayala@nd
🔑 Decrypted key type	AES256-CTS-HMAC-SHA1-96 (18)
🏷️ forwardable	False
🎯 SName	winc$
🔒 PA-DATA	pA-SUPPORTED-ETYPES

[5] 🔐 AS-REQ

🔒 PA-DATA	pA-PAC-REQUEST
📋 kdc-options	40810010
🏷️ Name type	ENTERPRISE-PRINCIPAL
👤 Client	hagit@nd
🌐 Realm	ND.C
🎯 SName	krbtgt
🎯 SName	ND.C

[6] ⚠️ KRB-ERROR PREAUTH-REQUIRED

🌐 Realm	ND.C
🔒 e-data PA-DATA	pA-ETYPE-INFO2
🧂 Salt	ND.Chagit
🔒 e-data PA-DATA	pA-ENC-TIMESTAMP
🔒 e-data PA-DATA	pA-PK-AS-REQ
🔒 e-data PA-DATA	pA-PK-AS-REP-19

[7] 🔐 AS-REQ

🔒 PA-DATA	pA-PAC-REQUEST
📋 kdc-options	40810010
👤 Client	winc$

[Frame 1] Phase 1: find user ayala's realm. `WINC$` is the computer account of a Windows server that wants to act on behalf of domain users. Before asking for a ticket in a user's name, it checks which realm holds the account.

It sends an AS-REQ for the enterprise name `ayala@nd` with no pre-authentication. This is the lookup MS-SFU 3.1.5.1.1.2 describes for a user principal name: the KDC that holds the account answers `PREAUTH_REQUIRED`, any other refers the service onward.

[Frame 2] `PREAUTH_REQUIRED`: the account is here, in `ND.C`. The `ETYPE-INFO2` hint gives the salt for ayala's AES key, `ND.Cayala` (realm plus user name), and lists the pre-authentication methods the KDC accepts.

[Frame 3] S4U2Self for ayala. WINC$ asks NDC, the `ND.C` KDC, for a ticket to itself (`sname = winc$`) on behalf of `ayala@nd`, named in `PA-FOR-USER` and `PA-S4U-X509-USER`.

It authenticates with its own TGT in `PA-TGS-REQ`. That TGT was issued at 12:38:49, before the capture began; decrypted with the krbtgt key, it shows the forwardable TGT and PAC of WINC$.

[Frame 4] The KDC returns a ticket to WINC$ for client `ayala@nd`, with a PAC describing ayala. Its flags are `renewable` and `pre-authent`, but not `forwardable`. MS-SFU 3.2.5.1.2 ties that flag to whether the service is trusted to authenticate for delegation, so WINC$ evidently isn't, and its S4U2Self tickets can't be passed on through classic constrained delegation.

The capture shows no further use of ayala's ticket. The rest of the flow follows a second user, hagit, 229 seconds later.

[Frame 5] Phase 2: the same lookup for hagit. An AS-REQ for `hagit@nd`, no pre-authentication.

[Frame 6] `PREAUTH_REQUIRED` again, salt `ND.Chagit`: hagit's account is also in `ND.C`.

[Frame 7] Phase 3: WINC$ gets a fresh TGT, the textbook AS exchange. This time the AS-REQ names WINC$ itself, again without pre-authentication.

🏛️ NDC (KDC, parent realm)	🖥️ WINC$ (service)	🏛️ TDC (KDC, child realm)

🌐 Realm	ND.C
🎯 SName	krbtgt
🎯 SName	ND.C

[8] ⚠️ KRB-ERROR PREAUTH-REQUIRED

🌐 Realm	ND.C
🔒 e-data PA-DATA	pA-ETYPE-INFO2
🧂 Salt	ND.Chostwinc.nd.c
🔒 e-data PA-DATA	pA-ENC-TIMESTAMP
🔒 e-data PA-DATA	pA-PK-AS-REQ
🔒 e-data PA-DATA	pA-PK-AS-REP-19

[Frame 8] `PREAUTH_REQUIRED`. The salt `ND.Chostwinc.nd.c` is the computer-account form: realm, then `host`, then the host name.

[9] 🔐 AS-REQ

🔒 PA-DATA	pA-ENC-TIMESTAMP
⏱️ Decrypted timestamp	Feb 25, 2019 13:21:28.000000000 India Standard Time
🔒 PA-DATA	pA-PAC-REQUEST
📋 kdc-options	40810010
👤 Client	winc$
🌐 Realm	ND.C
🎯 SName	krbtgt
🎯 SName	ND.C

[Frame 9] The retry adds `PA-ENC-TIMESTAMP`, the current time encrypted with the WINC$ AES-256 key. Decrypted: 25 Feb 2019 13:21:28, the second this request left.

[10] ✅ AS-REP (TGT)

🔐 Enc-part etype	AES256-CTS-HMAC-SHA1-96 (18)	
👤 Client	WINC$	
🎯 SName	krbtgt	
🎯 SName	ND.C	
🔐 Enc-part etype	AES256-CTS-HMAC-SHA1-96 (18)	
🏷️ forwardable	True	
🔑 Decrypted key type	AES256-CTS-HMAC-SHA1-96 (18)	
👤 Client	WINC$	
⌛ endtime	Feb 25, 2019 23:21:28.000000000 India Standard Time	
🪪 PAC name	WINC$	
🔐 Enc-part etype	AES256-CTS-HMAC-SHA1-96 (18)	
🔑 Decrypted key type	AES256-CTS-HMAC-SHA1-96 (18)	
🏷️ forwardable	True	
⌛ endtime	Feb 25, 2019 23:21:28.000000000 India Standard Time	
🎯 SName	krbtgt...	
	1 more	

[Frame 10] The AS-REP. The keytab holds the krbtgt key, so even the TGT opens: client WINC$, flags `forwardable, renewable, initial, pre-authent,` a 10-hour lifetime, and a PAC with user RID 1115 in group 515 (Domain Computers). The enc-part, under the WINC$ key, gives the client the TGT session key.

[11] 🎫 TGS-REQ (S4U2Self)

🔒 PA-DATA	pA-TGS-REQ
🎯 SName	krbtgt
🎯 SName	ND.C
👤 CName	WINC$
👤 CName	WINC$
🔒 PA-DATA	pA-FOR-X509-USER
👤 On behalf of	hagit@nd
👤 On behalf of	hagit@nd
📋 kdc-options	40810000
🎯 SName	winc$

[Frame 11] Phase 4: S4U2Self for hagit, now using the new TGT from frame 10. `PA-FOR-USER` names `hagit@nd`.

[12] ✅ TGS-REP

🔒 PA-DATA	pA-FOR-X509-USER
👤 Client	hagit@nd
🌐 Realm	ND.C
🎯 SName	winc$
🏷️ forwardable	False
🔑 Decrypted key type	AES256-CTS-HMAC-SHA1-96 (18)
👤 Client	hagit@nd
🪪 PAC name	hagit@nd
🔑 Decrypted key type	AES256-CTS-HMAC-SHA1-96 (18)

[Frame 12] A ticket to WINC$ for `hagit@nd`, PAC for hagit, and again not `forwardable`. Keep this ticket: frame 13 hands it back to the KDC as evidence.

NDC (KDC, parent realm)	WINC$ (service)	TDC (KDC, child realm)

forwardable	False
SName	winc$
PA-DATA	pA-SUPPORTED-ETYPES

[13] TGS-REQ (S4U2Proxy)

PA-DATA	pA-TGS-REQ
Realm	ND.C
SName	krbtgt
SName	ND.C
CName	WINC$
PAC name	WINC$
CName	WINC$
PA-DATA	pA-PAC-OPTIONS
PAC-OPTIONS	resource-based-constrained-delegation
kdc-options	40830000 (cname-in-addl-tkt)
Realm	ND.C
SName	cifs
SName	ndc.nd.c
Additional tickets	1 item
Realm	ND.C...
	3 more

[Frame 13] Phase 5: S4U2Proxy to a service in the same realm. WINC$ asks for a ticket to `cifs/ndc.nd.c` (file sharing on the domain controller) for hagit. Three things make it S4U2Proxy:

- `kdc-options` sets `cname-in-addl-tkt` (bit 14, Wireshark shows it as `constrained-delegation`) : take the client name from the additional ticket, not from the TGT (MS-SFU 2.2.3),
- the additional ticket is hagit's S4U2Self ticket from frame 12, decrypted here with the WINC$ key: client `hagit@nd`, not forwardable,
- `PA-PAC-OPTIONS` (167) sets the `resource-based-constrained-delegation` bit (MS-SFU 2.2.5).

Without that bit, a non-forwardable evidence ticket would be refused with `KRB-ERR-BADOPTION` (MS-SFU 3.2.5.2.1). With it, the KDC checks the target instead: may WINC$ act on behalf of users to the account that owns `cifs/ndc.nd.c`? That list lives on the target, in `msDS-AllowedToActOnBehalfOfOtherIdentity`.

[15] ✅ TGS-REP

Client	hagit@nd
Realm	ND.C
SName	cifs
SName	ndc.nd.c
forwardable	True
Ticket flag	ok-as-delegate
Decrypted key type	AES256-CTS-HMAC-SHA1-96 (18)
Client	hagit@nd
PAC S4U2proxyTarget	cifs/ndc.nd.c
PAC transited service	winc$@ND.C
PAC name	hagit@nd
Decrypted key type	AES256-CTS-HMAC-SHA1-96 (18)
forwardable	True
Ticket flag	ok-as-delegate
SName	cifs...
	3 more

[Frame 15] ✅ Granted. A ticket to `cifs/ndc.nd.c` for client `hagit@nd`, so the target's account must list WINC$. The keytab holds the NDC$ key, so the ticket opens:

- flags `forwardable` and `ok-as-delegate`,
- hagit's PAC, plus an S4U delegation info buffer: `S4U2proxyTarget` `cifs/ndc.nd.c` and transited service `winc$@ND.C` (MS-SFU 3.2.5.2.4).

The file server sees hagit's identity and groups, and also that WINC$ obtained the ticket on hagit's behalf. hagit never sent a password or a ticket to anyone in this capture.

[16] TGS-REQ (S4U2Proxy)

PA-DATA	pA-TGS-REQ
Realm	ND.C
SName	krbtgt
SName	ND.C
CName	WINC$
PAC name	WINC$
CName	WINC$
PA-DATA	pA-PAC-OPTIONS
PAC-OPTIONS	resource-based-constrained-delegation
kdc-options	40830000 (cname-in-addl-tkt)
Realm	ND.C
SName	cifs
SName	tdc.td.nd.c
Additional tickets	1 item
Realm	ND.C...
	3 more

[Frame 16] Phase 6: S4U2Proxy across realms. The same request, with the same evidence ticket, for `cifs/tdc.td.nd.c`, a service in the child realm `TD.ND.C`.

[18] ✅ TGS-REP

Client	WINC$
Realm	ND.C
SName	krbtgt
SName	TD.ND.C
forwardable	True
Ticket flag	ok-as-delegate

[Frame 18] NDC can't issue a ticket for another realm's service, so it returns a referral: a TGT for `krbtgt/TD.ND.C`, encrypted with the inter-realm trust key (RC4; the keytab has it as `TD$`). Decrypted:

- client `WINC$`, but the PAC is hagit's, with client-info name `hagit@nd@ND.C`. This is the referral MS-SFU 3.2.5.1.1 describes: the service as client, the user in the PAC,
- delegation info already records `S4U2proxyTarget` `cifs/tdc.td.nd.c` and transited service

🏛️ NDC (KDC, parent realm)	🖥️ WINC$ (service)	🏛️ TDC (KDC, child realm)

🔑 Decrypted key type	ARCFOUR-HMAC-MD5 (23)
👤 Client	WINC$
🪪 PAC S4U2proxyTarget	cifs/tdc.td.nd.c
🪪 PAC transited service	winc$@ND.C
🪪 PAC name	hagit@nd@ND.C
🔑 Decrypted key type	ARCFOUR-HMAC-MD5 (23)
🏷️ forwardable	True
🏷️ Ticket flag	ok-as-delegate
🎯 SName	krbtgt...
	4 more

`winc$@ND.C.`

This referral becomes the evidence ticket for the `TD.ND.C` KDC.

[19] 🎫 TGS-REQ

🔒 PA-DATA	pA-TGS-REQ
🌐 Realm	ND.C
🎯 SName	krbtgt
🎯 SName	ND.C
👤 CName	WINC$
👤 CName	WINC$
🔒 PA-DATA	pA-PAC-OPTIONS
📋 kdc-options	40810000
🌐 Realm	ND.C
🎯 SName	cifs
🎯 SName	tdc.td.nd.c

[Frame 19] WINC$ also needs a TGT of its own that `TD.ND.C` will accept. It asks NDC for `cifs/tdc.td.nd.c` in its own name: no `cname-in-addl-tkt`, no additional ticket.

[20] ✅ TGS-REP

👤 Client	WINC$
🌐 Realm	ND.C
🎯 SName	krbtgt
🎯 SName	TD.ND.C
🏷️ forwardable	True
🏷️ Ticket flag	ok-as-delegate
🔑 Decrypted key type	ARCFOUR-HMAC-MD5 (23)
👤 Client	WINC$
🪪 PAC name	WINC$
🔑 Decrypted key type	ARCFOUR-HMAC-MD5 (23)
🏷️ forwardable	True
🏷️ Ticket flag	ok-as-delegate
🎯 SName	krbtgt
🎯 SName	TD.ND.C
🔒 PA-DATA	pA-USE-SPECIFIED-KVNO...
	2 more

[Frame 20] Another referral TGT for `krbtgt/TD.ND.C`, this one with WINC$'s own PAC.

[21] 🎫 TGS-REQ

🔒 PA-DATA	pA-TGS-REQ
🌐 Realm	ND.C
🎯 SName	krbtgt
🎯 SName	TD.ND.C
👤 CName	WINC$
👤 CName	WINC$
📋 kdc-options	40810000
🌐 Realm	TD.ND.C
🎯 SName	cifs
🎯 SName	tdc.td.nd.c

[Frame 21] Phase 7: the child realm's KDC. WINC$ now talks to TDC. With its referral TGT from frame 20, it first asks for `cifs/tdc.td.nd.c` for itself.

[22] ✅ TGS-REP

👤 Client	WINC$
🌐 Realm	TD.ND.C
🎯 SName	cifs
🎯 SName	tdc.td.nd.c
🔑 Decrypted key type	AES256-CTS-HMAC-SHA1-96 (18)
🏷️ forwardable	True
🏷️ Ticket flag	ok-as-delegate
🎯 SName	cifs
🎯 SName	tdc.td.nd.c
🔒 PA-DATA	pA-SUPPORTED-ETYPES

[Frame 22] TDC issues WINC$ a ticket to `cifs/tdc.td.nd.c` in its own name. The keytab lacks that service's key, so only the enc-part opens: `forwardable`, `ok-as-delegate`. Frame 23 does not use this ticket.

🏛️ NDC (KDC, parent realm)	🖥️ WINC$ (service)	🏛️ TDC (KDC, child realm)

[23] 🎫 TGS-REQ (S4U2Proxy)

🔒 PA-DATA	pA-TGS-REQ
🌐 Realm	ND.C
🎯 SName	krbtgt
🎯 SName	TD.ND.C
👤 CName	WINC$
🪪 PAC name	WINC$
👤 CName	WINC$
🔒 PA-DATA	pA-PAC-OPTIONS
🏷️ PAC-OPTIONS	resource-based-constrained-delegation
📋 kdc-options	40830000 (cname-in-addl-tkt)
🌐 Realm	TD.ND.C
🎯 SName	cifs
🎯 SName	tdc.td.nd.c
🎟️ Additional tickets	1 item
🌐 Realm	ND.C...
	6 more

[Frame 23] The S4U2Proxy request TDC decides on. `PA-TGS-REQ` carries WINC$'s referral TGT from frame 20; the additional ticket is hagit's referral from frame 18 (client WINC$, PAC `hagit@nd@ND.C`); `cname-in-addl-tkt` and the RBCD bit are set. TDC checks the target's own `msDS-AllowedToActOnBehalfOfOtherIdentity`.

[25] ✅ TGS-REP

👤 Client	hagit@nd
🌐 Realm	TD.ND.C
🎯 SName	cifs
🎯 SName	tdc.td.nd.c
🔑 Decrypted key type	AES256-CTS-HMAC-SHA1-96 (18)
🏷️ forwardable	True
🏷️ Ticket flag	ok-as-delegate
🎯 SName	cifs
🎯 SName	tdc.td.nd.c
🔒 PA-DATA	pA-SUPPORTED-ETYPES
🔒 PA-DATA	pA-PAC-OPTIONS

[Frame 25] ✅ A ticket to `cifs/tdc.td.nd.c` for client `hagit@nd` of realm `ND.C`, issued by `TD.ND.C`, flags `forwardable` and `ok-as-delegate`. The keytab can't open the ticket itself, but frames 15 and 18 showed what such a PAC records.

Nine exchanges across two realms, and hagit was never involved: that reach is why defenders watch which accounts may delegate.