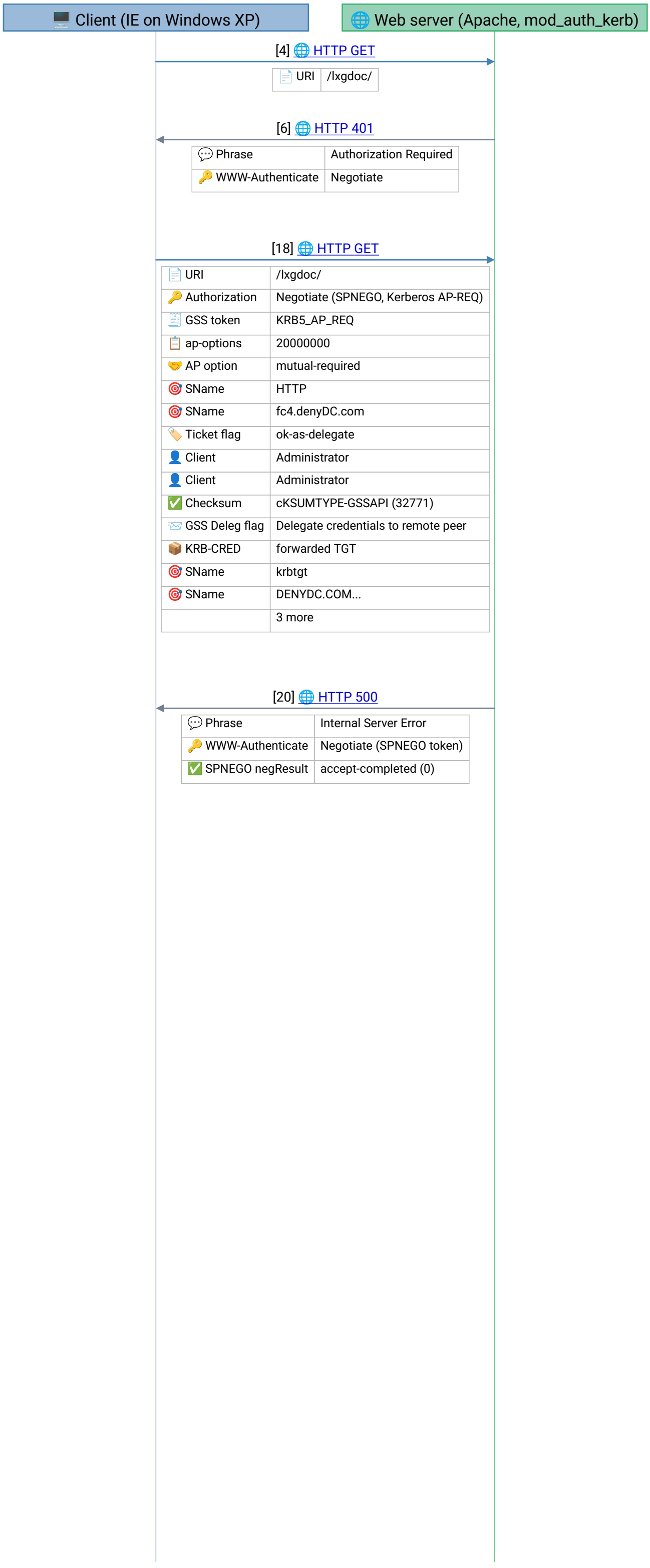


[Frame 4] The same web page, with delegation turned on. The client and server are the ones in the no-delegation capture; this time the user is `Administrator`. The first GET carries no credentials.

[Frame 6] `401` with `WWW-Authenticate: Negotiate`, exactly as before.

There is no AS or TGS exchange in this capture: the client already holds a TGT and a service ticket for `HTTP/fc4.denyDC.com`, so it goes straight to the AP-REQ.

[Frame 18] The AP-REQ carries the user's TGT. Opened with the web service's key, the service ticket shows client `Administrator` and one flag the no-delegation ticket lacked: `ok-as-delegate`. The KDC sets it when the service account is trusted for delegation (MS-KILE 3.3.5.1). It tells the client that this server may receive the user's credentials.

So the client sent them. The authenticator, decrypted with the ticket's session key:

- its GSS-API checksum (0x8003) has `Deleg` = 1, with `DlgOpt` 1 and 1232 bytes of delegation data (RFC 4121 4.1.1),
- that data is a `KRB-CRED` message: Administrator's TGT for `krbtgt/DENYDC.COM`, plus, encrypted with the session key, the TGT's own session key and flags `forwardable` and `forwarded`.

The web server can now ask the KDC for tickets to any service as Administrator until the TGT expires at 04:16, and renew it until 16 Feb. This is unconstrained delegation.

⚠️ The PAC shows what was handed over: user RID 500, the built-in Administrator, in groups 512 (Domain Admins), 518 (Schema Admins), 519 (Enterprise Admins), and 520 (Group Policy Creator Owners). Its account flags show `NOT_DELEGATED` clear, so nothing stopped the forwarding.

[Frame 20] As in the no-delegation capture, SPNEGO reports `accept-completed` and the page fails with `500` after authentication. Delegation did not change the result for the user; it changed what the server now holds.