User | Authenticator | Authenticator Specific Modules | FIDO Client | User Agent | Web Server | FIDO Server

User clicks on any action required authentication on https://webapp?purchase

HTTP GET https://webapp?purchase

Generate CHALLENGE (c), Auth Policy (p), and Transaction Text (t)

Start UAF Authentication/Transaction Request

Send UAF Authentication/Transaction Request $= (c, p, t)$

t is present in transaction confirmation ONLY.

HTTP 200 OK ($a =$ APP_ID, c, p, t)

a, c, p, t

1. Select authenticator(s) according to p
2. Obtain the FACET_ID and TLS_DATA
3. Lookup the key handle (h) and access key (ak)
3. $fcp = (a, c, $ FACET_ID, TLS_DATA$)$

$h, ak, t, fc = $ hash$(fcp), ...$

Send Sign Command
($h, ak, t, fc, ...$)

Trigger local user verification

1. Unlock UAuth Key Pair $= (Auth.pub, Auth.priv)$ for this handle h by ak
2. Generate a nonce (n)
3. Generate the Sign Data $= SignData = (fc, n, cntr, t, sig = $ signature_by_$Auth.priv(fc, n, cntr, t))$

$cntr = $ Signature Counter.

User Verified

$SignData$

$SignData$

$SignData$

$SignData$

$SignData$

1. Verify the $SignData$ signature by $Auth.pub$

Return verification result

HTTP 200 OK (verification result) and session binding