OAuth 2.0 Step-up Authentication Challenge Protocol

Agenda

• Step-up refresher
• Updates since the last meeting
• Discussion items
Step-up Authentication for API

- Resource servers (RS) can reject “technically valid” tokens for any reason
  - Opaque risk engine decisions, local constraints (e.g., high risk transactions)
- Often what the RS wants is
  - a fresher token, or
  - A token obtained with a different authentication flow
- Today there’s no guidance on how
  - The RS can express its requirements to the client
  - The client can indicate those requirements to the authorization server
Proposal

• Extend RFC6750 with
  • error code insufficient_user_authentication
  • New WWW-Authenticate params acr_values, max_age

• Require support for AS request parameters acr_values, max_age

• Provide guidance for JWT ATs and Introspection response to express auth levels in interoperable fashion so that RS can read them
(1) GET https://example.com/api/highvaluemethod HTTP/1.1
authorization: Bearer eyJ0[..]5A

HTTP/1.1 401 Unauthorized
WWW-Authenticate: Bearer error="insufficient_user_authentication",
error_description="A different authentication level is required",
acr_values="myACR"

(3) GET https://authorizationserver.com/authorize
?client_id=xHMM_&response_type=code&scope=purchase&acr_values=myACR...

(4) 200 HTTP/1.1
{
    "access_token" : "eyJ0[..]4B",
    "expires_in" : 86400,
    "token_type" : "Bearer"
}

(5) GET https://example.com/api/highvaluemethod HTTP/1.1
authorization: Bearer eyJ0[..]4B

(6) 200 HTTP/1.1 ...
Happenings since IETF 113 Vienna

• WG Adoption!
• -01 (Many thanks to Filip and Pieter for their thorough reviews!)
  • Clarified that “step-up” tokens aren’t always a replacement for original tokens
  • Added AS Metadata section with pointer to OIDC’s `acr_values_supported`
    • Important: that indicates support for BOTH `acr_values` and `max_age` in incoming requests
  • Add examples showing `max_age`
• -02
  • Fix typos & begin to fill out the Acknowledgements Section
• Need to flesh out IANA and Security Considerations sections
• Is the current `acr_value_supported` behavior clear enough?
• Adoption is already happening, but discussion has been light
  • The proposal is already viable, if we want changes we should discuss and incorporate quickly