API Security Session

Session discussing customer issues around securing an API:

1. Focus:
    a. Protect APIs
        i. No security on REST APIs
    b. Evolution
        i. OAuthm Token-types (SAML)

ii. Questions:

    a. Question: Security end-to-end:

        i. How to obtain proof-of-possession (of token)
    b. Question: Upgrading a token with OAuth?
        i. A user access the web application (and authenticates). This web application calls different web services to deliver the service passing on access tokens. However at some point an access token might not have the right scope/claim. Looking for a way to challenge the user sitting in front of his web browser for a session upgrade and subsequently access tokens which appropriate scopes.
        ii. Joachim: I think this is a valid use case, but I don't know if there is a flow to combine