AARC

Authentication and Authorisation for Research and Collaboration

AARC Policy: Token life time and revocation guidance

Sub title

Marcus Hardt (KIT)
Nicolas Liampotis (GRNET)

61st EUGridPMA+ and AARC Policy meeting (in conjunction with IGTF, GN5-1 EnCo)
30 May, 2024

Introduction

- Goal: Determine the information needed to provide communities with guidance on token lifetimes
- Focus: Balancing security with user experience
- Key Considerations:
    - Risk Assessment: Understanding the level of risk associated with data access
    - Use Cases:
        - Data Sensitivity (CIA): Confidentiality, Integrity, and Availability of the data being accessed
        - Interaction Model: How users interact with the application (frequent vs. infrequent)
- Mitigating Controls:
    - Existing security measures that might influence token lifetime (e.g., revocation, rotation)

Token Properties Overview

Property	Description	Advantages	Disadvantages
Bound	Token is bound to a specific client or audience	Mitigate impact of compromised tokens	Delegation scenarios may lack support
Rotatable	Token can only be used once. New token issued with each use	Detect compromised tokens	More work on clients Revoking the last token in chain needs more thought Good potential to break production runs
Revocable	Revoked tokens may no longer be used, regardless of initial lifetime	Longer lifetime acceptable	Depending on underlying tech. needs additional implementation work (e.g. OIDC)
Opaque	No information for client or rp in token	Privacy, Performance	Contact issuer for every bit of information

Token Properties Overview (Contd.)

Property	Description	Advantages	Disadvantages
Structured, Signed	Often a signed JWT that contains information about subject	Essential information readily available: Name, Expiry, **Issuer**, Scope	Less Private
Verified Online	Tokens are verified with the issuer to ● verify them ● obtain data for authorisation decision	Essential information readily available: ... **issuer**, ...	● Increased network traffic ● Increased load on issuer/AS
Verified Offline	Tokens contain enough information to ● verify them ● take authorisation decision	Extended information readily available: Assurance, Entitlements	● Authorisation granted based on potentially expired information. ● New groups not communicated timely ● **Revocation can not be supported**

Token Types Overview

Type	Description	Properties
X.509 Certificates	● Used for grid authentication. ● Each job carries a short-lived proxy certificate (valid for ~11 days). ● Rely on CRLs for revocation.	● Revocable (via CRLs) ● Structured + Signed ● Not bound ● Verified offline
OAuth2 Access Tokens	● Used by applications to make API requests on behalf of a user, authorising access to specific parts of the user's data. ● Need to be validated by Resource Servers (RS) ● Must be kept confidential in transit and storage, visible only to the application, AS, and RS. ● OAuth 2.0 Token Introspection defines a protocol that returns information about an access token. ● Content can be either: ○ Opaque: A simple string without embedded information, requiring validation from the issuer. ○ Structured: Some embed basic information such as issuer, subject, expiry details, relying on the issuer for validation, while others encode all the information, allowing offline validation. Example profiles: JWT Profile for OAuth 2.0 Access Tokens (RFC 9068), AARC, WLCG 1.0	● Revocable by Issuer & Client via OAuth 2.0 Token Revocation (RFC 7009) ○ However, offline validation by RSs will not reflect revocation ● Structured + Signed in the case of JWT access tokens ● Bound ● No rotation ● Verified online

Token Types Overview (Contd.)

Type	Description	Properties
OIDC ID Tokens	- Security tokens containing information about a user's successful authentication. - Formated as JWTs that MUST be signed using JWS and optionally encrypted using JWE - Primarily include claims about the user's authentication. - Optionally may also include additional claims	- Structured + Signed - Not Revocable - Bound - Not rotated
OAuth2/OIDC Refresh Tokens	- Used to acquire new access tokens, typically after the original access token expires. - To minimise the impact of compromise, refresh tokens are: ○ Bound to a Specific Client: This restricts their use to the authorised application that obtained them. ○ Rotatable: Issuing a new refresh token upon each use enhances security by rendering compromised tokens useless.	- Structured + Signed - Revocable (MUST) - Bound - Rotatable: ○ Public Clients: MUST use refresh token rotation or sender-constrained tokens (see OAuth2 Security BCP)
Mytokens	New Tokens that provide well defined restrictions and capabilities to give Access Tokens to the right people	- Structured + Signed - Revocable - Bound - Rotatable - Scoped - Restrictions + Capabilities

Existing Guidance on Token Lifetime

Type	Recommended Lifetime	Min Lifetime	Max Lifetime
OAuth2 Access Tokens	● OAuth2/OIDC: Short ● WLCG: 20 min	● OAuth2/OIDC: Short ● WLCG: 5 min	● OAuth2/OIDC: Short ● WLCG: 6 hours
OIDC ID Tokens	● OAuth2/OIDC: Short ● WLCG: 20 min	● OAuth2/OIDC: Short ● WLCG: 20 min	● OAuth2/OIDC: Short ● WLCG: 20 min
OAuth2/OIDC Refresh Tokens	● OAuth2/OIDC: Long ● WLCG: 10 days	● OAuth2/OIDC: Long ● WLCG: 1 day	● OAuth2/OIDC: Long ● WLCG: 30 days
Mytokens	● 10 days	● 7 days	● 1 Year

Summary

- There's no one-size-fits-all answer for token lifetimes
- Security best practices recommend:
  - Short-lived access tokens
  - Refresh token rotation
- Consider risk assessment, user interaction, and offline usage needs when setting lifetimes:
  - Setting a longer refresh token expiry with stricter rotation policies
  - Setting a shorter access token expiry with offline validation
  - Longer lifetimes for audience-restricted access tokens: Tokens restricted to a specific audience or set of resources reduce the potential damage if compromised, as they cannot be used universally
  - Combining a longer refresh token lifetime with *inactivity timeouts* mitigates risks from compromised or stale tokens by reducing their usable lifespan and enhancing revocation

Thank you

Any Questions?

davidg@nikhef.nl

The work leading to these results has received funding from the European Union (GAP 101131237) and other sources