Authentication and Authorisation for Research and Collaboration

AARC Policy: Recommendations for Token Lifetimes

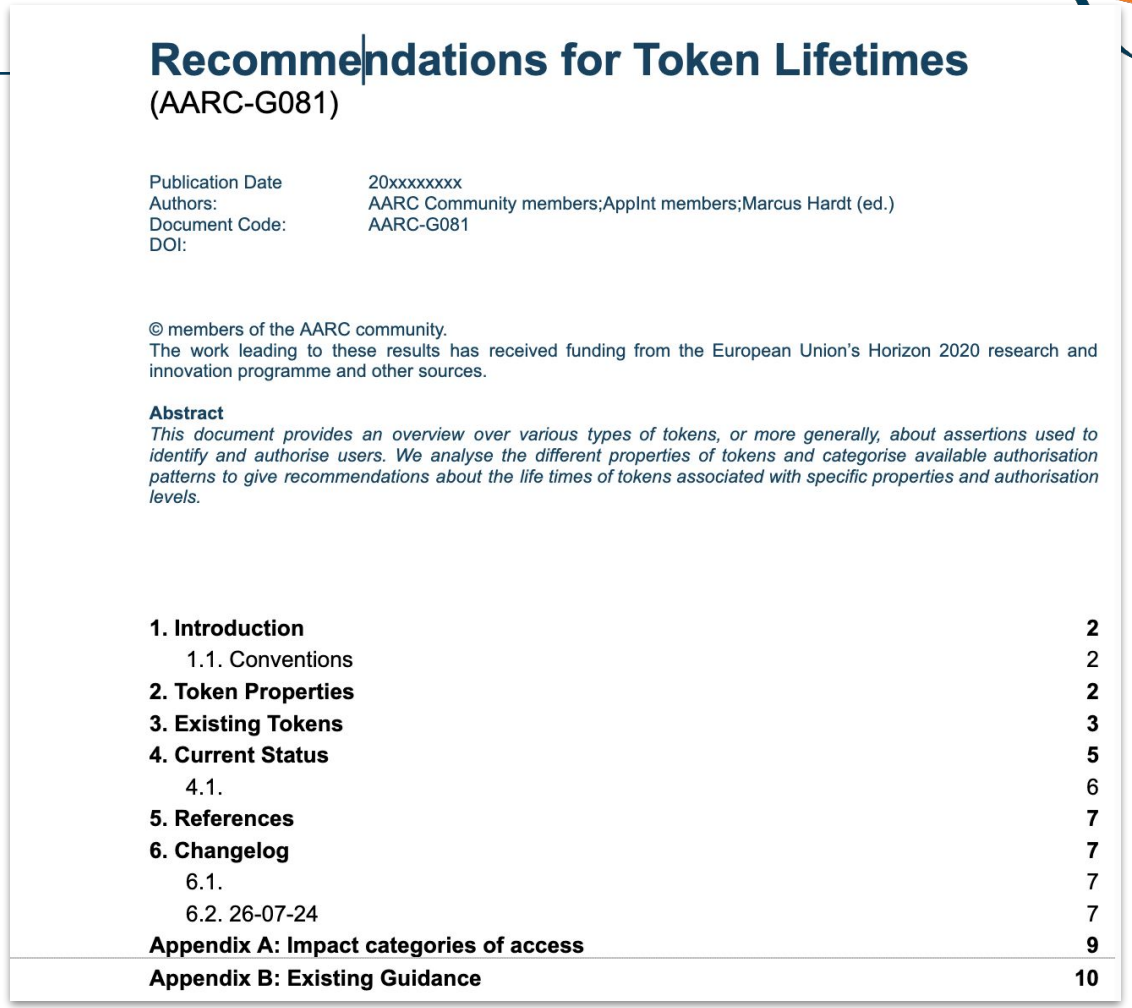
AARC-G081

Marcus Hardt (KIT)
Nicolas Liampotis (GRNET)

62nd EUGridPMA-AARC-EnCo-IGTF workshop
23 September, 2024

Introduction

- Goal: Provide recommendations for token lifetimes
- Importance: Token lifetimes are critical as they directly impact **security** and **usability**
- Factors influencing token lifetimes:
  - Token properties (e.g., revocation, rotation).
  - Impact of access (e.g., risk of compromise, sensitivity of resources)



Recommendations for Token Lifetimes
(AARC-G081)

Publication Date 20xxxxxxxx
Authors: AARC Community members;AppInt members;Marcus Hardt (ed.)
Document Code: AARC-G081
DOI:

The work leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme and other sources.

Abstract
This document provides an overview over various types of tokens, or more generally, about assertions used to identify and authorise users. We analyse the different properties of tokens and categorise available authorisation patterns to give recommendations about the life times of tokens associated with specific properties and authorisation levels.

1. Introduction **2**
1.1. Conventions 2
2. Token Properties **2**
3. Existing Tokens **3**
4. Current Status **5**
4.1. 6
5. References **7**
6. Changelog **7**
6.1. 7
6.2. 26-07-24 7
Appendix A: Impact categories of access **9**
Appendix B: Existing Guidance **10**

https://docs.google.com/document/d/1U9vvJfWuE8oO7u0FcGVGr3KySvBqwjnkzKO8TKzgoX4/edit

Token Properties Overview

Property	Description	Advantages	Disadvantages
Bound	Token is bound to a specific instance of a relying party	Mitigate impact of compromised tokens	Delegation scenarios may lack support
Rotation	Token can only be used once → New token issued with each use	Detect compromised tokens → Trigger revocation of related tokens	- Legitimate tokens may be erroneously revoked - Requires additional logic for token management, especially in parallel workflows
Revocable	Revoked tokens may no longer be used, regardless of initial lifetime	Longer lifetime acceptable	- Each token validation requires a network request, potentially causing delays - Availability issues with the issuer/revocation authority can disrupt access to resources, creating a single point of failure

Token Properties Overview (Contd.)

Property	Description	Advantages	Disadvantages
Opaque	Token contains no information → Requires validation from the issuing authority	- No embedded information reduces the risk of data exposure - Validations are managed by the issuer, ensuring up-to-date access permissions	- Each token validation requires a network request, potentially causing delays - Availability issues with the issuer can disrupt access to resources, creating a single point of failure
Structured	Contains information about subject	Essential information readily available, e.g. lifetime	Less private
Signed	Token can be cryptographically verified by recipient	- Tokens can be validated without contacting the issuer for each request (*but* periodic online access is still required to obtain and refresh the signing keys) - Protects against token tampering	- Cannot revoke unless revocation mechanisms are in place (e.g. CRL/OCSP for X.509 or RFC7009 for OAuth2)

Impact categories of access

See Appendix A

- **Low:**
  - Read protected data
  - Write low or medium value data, e.g. update wiki pages, write data with an appropriate backup in place.
  - Write heavily restricted high value data e.g. single file
  - Attackers may spam-fill wiki pages, or modify / delete low-impact data
  - Potential vulnerability identified, but not clear how to exploit it
- **Moderate:**
  - Read sensitive data
  - Write data in larger volume, or non backed-up data
  - Attackers may delete or modify important data
  - Problem where a user can cause disruption to services, but are easily traceable.
- **High:**
  - Access to remote computers
  - Start virtual machines
  - Attackers may abuse infrastructure to run own infrastructure or mine coins
  - Most Root or admin exploits
  - Most cases of identity theft and impersonation
  - Most cases in which an authorised user in principle can carry out widespread destruction of data belonging to another group
  - An Information leak which is illegal or embarrassing
- **Critical:**
  - Access to HPC
  - Consume expensive resources
  - An anonymous or unauthorised user can gain root or admin access
  - An anonymous or unauthorised user can carry out widespread damage, data destruction or access to confidential data
  - A public exploit is available allowing an authorised user to trivially gain root or admin access
  - A public exploit is available allowing unauthorised access
  - Usually for a vulnerability to be assessed as 'Critical' the problem needs to be widespread, and not only affect a small number of sites

Points for discussion

- Scope of AARC-G081: Current document covers several token types → Limit scope to specific tokens?
- Recommendation Approach: Determine factors influencing default/min/max lifetimes
- How to handle token lifetimes in chained token issuer scenarios

Points for discussion - Scope of AARC-G081

- Scope of AARC-G081: Current document covers several token types:
  - OAuth2/OpenID Connect access tokens & refresh tokens
  - X.509 certificates
  - SSH keys & certificates
  - Kerberos tickets
  - MyTokens, VAULT Tokens
- **Q:** Should AARC-G081 focus on the more commonly used token types in AARC BPA, such as OIDC/OAuth2 access and refresh tokens?

Scope of AARC-G081 - Recommendation Approach

Current approach to Basic Recommendations:

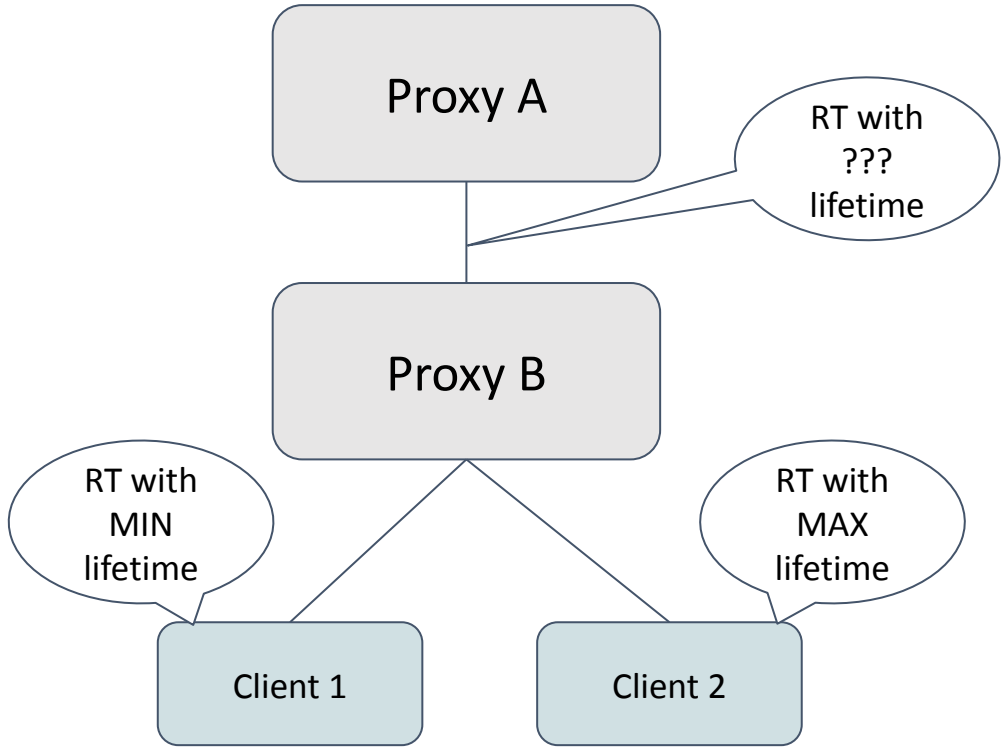
								Recommended lifetime				
Token	Bound	Rotation	Verified online	Revocable	Structured	Signed	Opaque*	Default	Minimal	Maximal	#yes	#no
Opaque Access Tokens	Yes	No	Yes	No	No	No	Yes				2	5
JWT Access Tokens	Yes	No	No	No	Yes	Yes	No				4	3
JWT Access Tokens	Yes	No	Yes	Yes	Yes	Yes	No				6	1
OIDC ID Tokens	Yes	No	No	No	Yes	Yes	No				4	3
OIDC Refresh Tokens	Yes	Yes	Yes	Yes	Yes	Yes	No				7	0
OIDC Refresh Tokens	Yes	No	Yes	Yes	Yes	Yes	No				6	1
											0	0

Points for discussion - Recommendation Approach

- Recommendation Approach: Determine factors influencing default/min/max lifetimes
  - Type & properties of the token?
  - Impact category of the intended access?
  - Other mitigating controls?
    - Allowing a longer refresh token expiry with stricter rotation policies
    - Requiring a shorter access token expiry with offline validation
    - Allowing 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
- **Q1:** Should we focus solely on token type and properties, or combine them with impact categories and mitigating controls?
- **Q2:** If default, minimum, and maximum lifetimes are established, what prevents the adoption of the maximum lifetime for all tokens?

Points for discussion - Token Lifetimes in Chained Token Issuer Scenarios

- Scenario Overview:
  - Proxy A: OAuth2 Token issuer
  - Proxy B: OAuth2 Token issuer connected as a client to Proxy A
  - Client 1: Requires minimum refresh token (RT) lifetime
  - Client 2: Requires maximum refresh token (RT) lifetime
- Key Challenge:
  - If the refresh token (RT) issued to each client must align with the RT lifetime between Proxy A & Proxy B, how can Proxy B assign the correct lifetime to each client?
- **Q1:** Should Proxy B dynamically adjust refresh token lifetimes based on the specific requirements of each client?
- **Q2:** How can Proxy B ensure that the RT lifetime issued by Proxy A does not conflict with the lifetimes required by Client 1 and Client 2?
- **Q3:** What mechanisms can be implemented to manage different lifetimes while maintaining consistency across the chain?
  - See also working document on Guidelines for Refreshing Tokens between OAuth 2.0 Proxies (AARC-G073)



Thank you

Any Questions?

davide@nikhef.nl

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