# Auditable Authorization

## Abstract

Bearer tokens are vulnerable at rest and in transit when an attacker is able to intercept a token to illegally access private information. In order to mitigate some of the risk associated with bearer tokens, the Authorization Audit Trail (AAT) may be used instead of bearer tokens in the authorization process. AAT consists of cryptographically chained blocks of data bearing a chronological tamper-resistant records of all their possessors and the changes that have been made by them. A nested, chained MAC construction (e.g., HMAC) is used to ensure the authenticity and integrity of AAT. All sensitive information are encrypted to preserve confidentiality. The access control relies on a real-time auditability of AAT by the authorization server. The AAT concept is compatible with existing OAuth2 and UMA protocols.

## Conclusion

By utilizing simple cryptographic techniques, the AAT mechanism may be used instead of bearer tokens during the authorization process. This concept of auditable authorization mitigates the risk associated with bearer tokens to illegally access private information. In a broader scope of AAT, there is the possibility of using the recorded data for forensic analysis and verification of legal compliances.