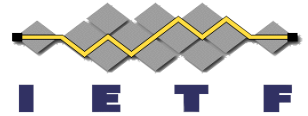


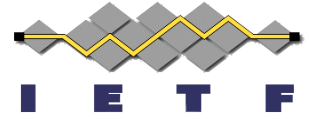
Enhanced JWE Security with Detached AAD



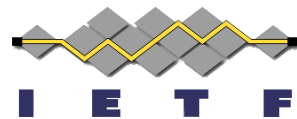
[draft-reddy-jose-detached-aad-00](#)

Tirumaleswar Reddy, Hannes Tschofenig
IETF 122, Bangkok

Introduction

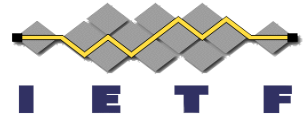


- Introduce a mechanism for detached AAD in JWE.



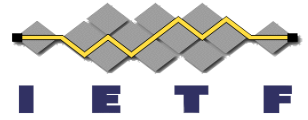
Motivation and Use Cases

- Introduces detached AAD in JWE, allowing the AAD to be derived from context-specific information rather than being transmitted in-band.
- Use Case: OpenID for Verifiable Credentials (OID4VC), where a verifier must validate context information without depending on in-band AAD.
 - Prevents attacks such as phishing, replay, and tampering attacks.



Benefits of Detached AAD

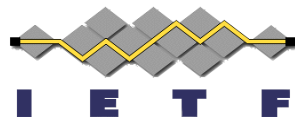
- Improved Security: By deriving AAD directly from the context, the need to transmit and validate in-band AAD is eliminated. This minimizes the attack surface and reduces the risks of tampering and replay.
- Enhanced Flexibility: AAD is transmitted only when necessary and otherwise derived out-of-band.
- Consistency Across Serializations: Works with JWE JSON and Compact Serialization.



Detached AAD parameter

- 'detached_aad' optional parameter set to true in the protected header indicates AAD is derived from context.
- If the "aad" parameter contains data and the "detached_aad" parameter is not present or set to false, it is used directly as the AAD for encryption.
- If both exist, they are combined.

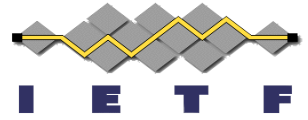
Deriving Detached AAD



- Identify context elements (e.g., session_id, sender identifier, receiver identifier).
- A JSON-based data structure is proposed to standardize the AAD information.
- Normalize and serialize elements in canonicalized JSON format.

ASCII(Encoded Protected Header || '.' || BASE64URL(Detached AAD)) => **Compact JWE and JWE JSON Serialization without an explicit JWE AAD**

ASCII(Encoded Protected Header || '.' || BASE64URL(JWE AAD) || '.' || BASE64URL(Detached AAD))
=> **JWE JSON Serialization with an explicit JWE AAD**



Security Considerations

- Consistency: Both sender and receiver must derive AAD identically.
- Synchronization: Handle potential mismatches due to time-sensitive data.

Next Steps

- Consider for WG adoption
- Comments and suggestions are welcome