ADR-HTTP Payload encryption

KPAPI Standard
Draft 10 november 2023

This version:
https://geonovum.github.io/KPAPI/

Latest published version:
https://github.com/Geonovum/KPAPI/adr/template/

Latest editor's draft:
https://geonovum.github.io/KPAPI/

Editor:
Peter Haasnoot (Logius)

Author:
KPAPI (KPAPI)

Participate:
GitHub Geonovum/KPAPI
File an issue
Commit history
Pull requests

Abstract

This ADR Module contains the requirements for ADR REST-API encryption based on JWE

Status of This Document

This is a draft that could be altered, removed or replaced by other documents. It is not a recommendation approved by de werkgroep.

Table of Contents

§ 1. ADR-HTTP Payload encryption

> NOTE: Status
>
> This module is under development

§ 1.1 Introduction

This module specifies the use of JWE for HTTP payload encryption.

§ 1.2 Notational Conventions

The key words "*MUST*", "*MUST NOT*", "*REQUIRED*", "*SHALL*", "*SHALL NOT*", "*SHOULD*", "*SHOULD NOT*", "*RECOMMENDED*", "*NOT RECOMMENDED*", "*MAY*", and "*OPTIONAL*" in this document are to be interpreted as described in "Key words for use in RFCs to Indicate Requirement Levels" [RFC2119]. The interpretation should only be applied when the terms appear in all capital letters.

§ 1.3 JWE encryption

For encryption JSON Web Encryption (JWE) is used as defined in [RFC7516];

§ 1.3.1 Basic JWE proces flow

The basic flow for encryption using JWE is :

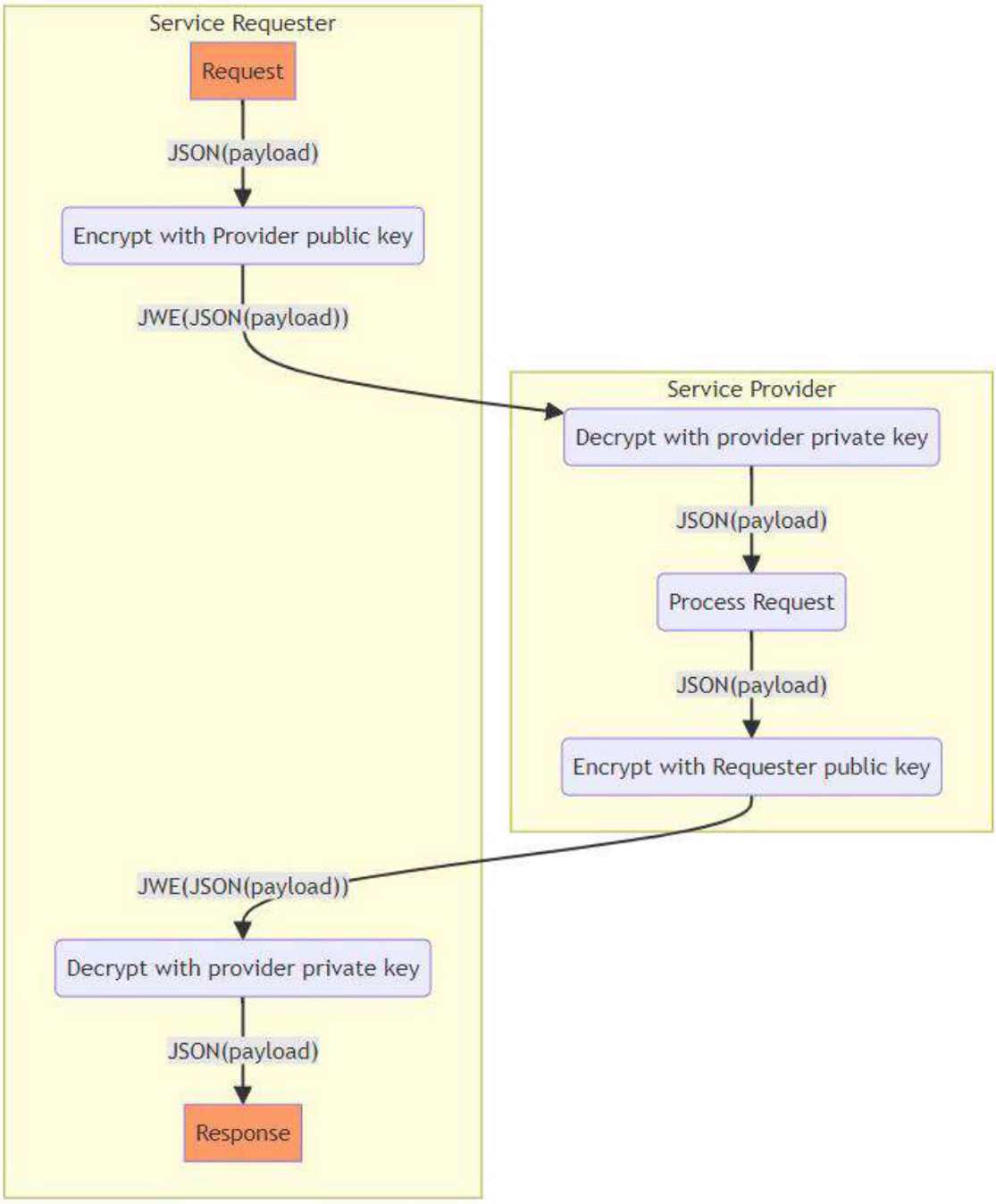


Figure 1

- 1 Service Requester encrypts payload using Service Provider public encryption key:
- 2 Service Provider decrypts the request using the corresponding Service Provider private encryption key.
- 3 Service Provider performs the request and then generates an encrypted response;
- 4 Service Requester decrypts response using providers public key

1.3.2 Parameters and requirements

The following specific requirements *MUST* be met:

- The request is sent to Service Provider with the content-type: application/jose+json.
- An encrypted request needs to pass application/jose+json as the value for the Content-Type and Accept headers:

```
Content-Type: application/jose+json
Accept: application/jose+json
```

- When the encrypted request uses an unsupported algorithm, the Service Provider rejects the request with a 400 HTTP response.
- Use for encryption the public key from the X.509 certificate of the other party
- Use the following parameters in the JWE protected header:

```
alg : "RSA-OAEP",
enc : "A256GCM",
typ : "JWE"
```

- JWE compact serialization format is used

1.4 Cryptographic Algorithms

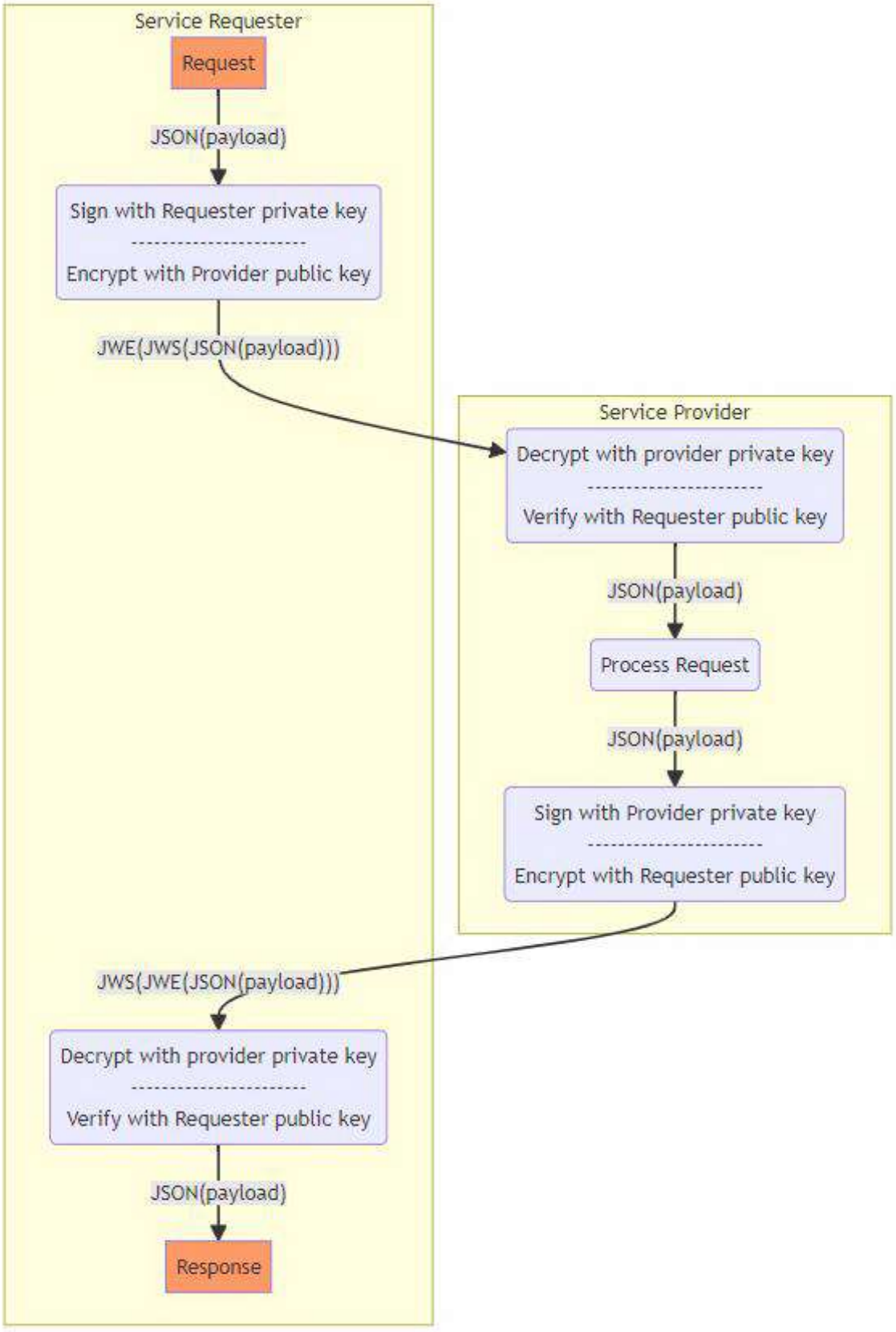
The following algorithms are used

- Key Management : RSA-OAEP
- Content encryption : A256GCM

As defined in [rfc7518]

1.5 Encryption in combination with signing

The following diagram shows the order in which encryption & signing must be applied when encryption is used in combination with signing


Service Requester
Request
JSON(payload)
Sign with Requester private key

Encrypt with Provider public key
JWE(JWS(JSON(payload)))
Service Provider
Decrypt with provider private key

Verify with Requester public key
JSON(payload)
Process Request
JSON(payload)
Sign with Provider private key

Encrypt with Requester public key
JWS(JWE(JSON(payload)))
Decrypt with provider private key

Verify with Requester public key
JSON(payload)
Response

Figure 2

§ 2. Conformance

As well as sections marked as non-normative, all authoring guidelines, diagrams, examples, and notes in this specification are non-normative. Everything else in this specification is normative.

The key words *MAY*, *MUST*, *MUST NOT*, *NOT RECOMMENDED*, *OPTIONAL*, *RECOMMENDED*, *REQUIRED*, *SHALL*, *SHALL NOT*, *SHOULD*, and *SHOULD NOT* in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

§ A. References

§ A.1 Normative references

[RFC2119]
Key words for use in RFCs to Indicate Requirement Levels. S. Bradner. IETF. March 1997. Best Current Practice. URL: https://www.rfc-editor.org/rfc/rfc2119

[RFC7516]
JSON Web Encryption (JWE). M. Jones; J. Hildebrand. IETF. May 2015. Proposed Standard. URL: https://www.rfc-editor.org/rfc/rfc7516

[rfc7518]
JSON Web Algorithms (JWA). M. Jones. IETF. May 2015. Proposed Standard. URL: https://www.rfc-editor.org/rfc/rfc7518

[RFC8174]
Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words. B. Leiba. IETF. May 2017. Best Current Practice. URL: https://www.rfc-editor.org/rfc/rfc8174