Object

JWSDecodedHeader

A decoded JSON Web Signature (JWS) header containing transaction or renewal information.

App Store Server API 1.0+

```
object JWSDecodedHeader
```

Properties

alg
alg
The algorithm used for signing the JSON Web Signature (JWS).

x5c
x5c
The X.509 certificate chain that corresponds to the key that the App Store used to secure the JWS.

Mentioned in

App Store Server API changelog

Discussion

The types `JWSTransaction` and `JWSRenewalInfo` contain headers that are `JWSDecodedHeader` objects when decoded. Use the information in the `JWSDecodedHeader` to validate the JWS signature. For more information about validating signatures, see the JSON Web Signature (JWS) IETF RFC 7515 specification.

The App Store signs transaction and renewal information that you receive in `App Store Server Notifications V2` and in the App Store Server API. It uses the following `x5c` certificate chain, in the following order:

1. A certificate that contains the public key that corresponds to the key the App Store uses to digitally sign the JWS. Section 4.11.10 Mac App Store Receipt Signing Certificates of the Apple Inc. Certificate Practice Statement Worldwide Developer Relations document defines the custom extensions this certificate uses.
2. An Apple intermediate certificate that contains an extension with the extension ID for `Apple Worldwide Developer Relations (1.2.840.113635.100.6.2.1)`.
3. An Apple root certificate.

For more information, or to download Apple's root certificate, see Apple PKI.

Topics

Data types

`type alg`

An algorithm used to sign a JSON Web Signature.

`type x5c`

The JSON Web Signature (JWS) header parameter that contains the certificate chain that corresponds to the key used to digitally sign the JWS.

See Also

JWS headers and payloads

`type JWSAppTransaction`

App transaction information signed by the App Store, in JSON Web Signature (JWS) Compact Serialization format.

`object JWSAppTransactionDecodedPayload`

A decoded payload that contains app transaction information.

`type JWSTransaction`

Transaction information signed by the App Store, in JSON Web Signature (JWS) Compact Serialization format.

`object JWSTransactionDecodedPayload`

A decoded payload that contains transaction information.

`type JWSRenewalInfo`

Subscription renewal information, signed by the App Store, in JSON Web Signature (JWS) format.

`object JWSRenewalInfoDecodedPayload`

A decoded payload containing subscription renewal information for an auto-renewable subscription.

Data types

Refer to these data types for decoded transaction and renewal information payloads.