Comments on OBE JSON Web Signature Profile – v.0.10

13 Aug 2020

Ref	Source	Section / paragraph	Comment	Resolution
1	Hervé Robache - Stet	5.4.2 Rec.-15 Annex A example step 1	5.4.2 recommends the inclusion of "typ": "JOSE" in the header but this is missing from the example in Annex A step 1	Accepted in principle: RFC 7515 states against for Typ: " This is intended for use by the application when more than one kind of object could be present in an application data structure that can contain a JWS; the application can use this value to disambiguate among the different kinds of objects that might be present. It will typically not be used by applications when the kind of object is already known. This parameter is ignored by JWS implementations; any processing of this parameter is performed by the JWS application. Use of this Header Parameter is OPTIONAL." Thus, it should be optional in 5.4.2 and need not be included in the example.
2	Kornél Réti - Microsec	5.3.2	Both REQUIREMENT-7a and OPTION-11 contain this sentence: “Both "x5t#S256" and "x5t#o" may be present.” To avoid the repetition, OPTION-11 could be moved up just below REQUIREMENT-7a, the sentence could be deleted from REQUIREMENT-7a, and the requirements renumbered accordingly.	Accepted in principle Kept requirement in 7a and removed in 11 so that related requirements are kept together. Also, this has minimal change to requirement numbering.

Ref	Source	Section / paragraph	Comment	Resolution
3	Ralph Bragg – UK OBIE	5.3.2 option 9	I’m doing the compare and contrast to the OBIE specifications and this wording jumped out at me as being potentially challenging. The signature is only valid if it’s issued by a valid certificate from a valid QTSP. If the certificates aren’t validated as belonging to a QTSP and validity of the certificate isn’t checked then the signature isn’t valid. This to me implies that a RP doesn’t have to perform these checks.	This is not intended to overrule RFC 5280 requirements for certificate path validation by the relying up to a trust anchor. Replace with: OPTION-9: The "x5c" header parameter may include the full certificate path up to the trust anchor. If the full path is present, the relying party may choose to use an alternative path up to the trust anchor it trusts provided that at least the end-entity certificate provided in the header is used.
4	Ralph Bragg – UK OBIE	6.3.2 Req. 21 & 24	Recommendation of the OBE JWS spec; 21 says that SigD SHALL be present but recommendation 24 then says… when it’s not present do something else.	The aim of 24 is to facilitate interoperability with pre-OBE profile implementations which do not use SigD. Replace 24 with: In order to facilitate interoperability with earlier implementation not conforming to this profile, parties relying on JWS signatures (e.g. ASPSPs relying on signed HTTP requests from TPPs) should accept signatures where the sigD is not present. In such situations relying parties should consider the HTTP Body as the Data to be Signed.
5	JAdES Alignment	2.3	It should be clear that "data to be signed" is the JWS payload as this is the term used in JAdES	Update definition: *Data to be Signed*: the data used as the secured JWS Payload of the JSON Web Signature.
6	JAdES alignment	6.5.1 and 6.5.2	It should be possible for parties relying on signatures (e.g. ASPSPs relying on HTTP requests from TPPs) to use the JAdES etsiU header to support later re-validation of the signature	6.5.1 updated to describe how JAdES could be used to extend the signature with ore informative guidance in Annex C

Ref	Source	Section / paragraph	Comment	Resolution
7	Hervé Robache - Stet	6.3 and annex A	There is a contradiction between the capitalisation of "mID" as in 6.3 and "mId" in annex A example.	Corrected 6.3 to use mId which defined in JAdES
8	Hervé Robache - Stet	Annex A	In Annex A creation- step 1 & validation - step 3 sigT has spurious spaces in time after ":" mId has spurious spaces after "http: "	Annex A example to be corrected
9	OBE	Front pages	Acknowledgement of authors and contributors, and copyright statement to be added	Text added
10	Yann Grostete - Arkéa	6.3.1	Incorrect interpretation of "(request target)" from Cavage. This only include "path" and "query" elements of URL as in RFC 3986 section 3.	Clarification added to 6.3.1 and Annex A example updated to include "Host" HTTP header and path within the host.
11	OBE	Annex A steps	Update steps to better describe action to be taken	Annex A step titles updated
12	Manu Sporny - Digital Bazaar Inc (co editor of Cavage and subsequent HTTP signature drafts)	7	A common weakness is through the use of software packages which include weak algorithms	Recommendation added that weak, and any other cryptographic algorithms that are not required, are disabled or removed from implementations.