XML Enc v1.1 Review

1) Comments

- **Abstract:** This sentence is not logical or correct: “The data may be arbitrary data (including an XML document), an XML element, or XML element content.” The data that is being encrypted must be an XML document, one or more elements or a single element’s content. As a result, it is not arbitrary. This sentence is repeated in Section 1, where it is contradicted in the next few sentences. If the intent is to allow the encrypted result to span elements, that should be stated clearly. I suggest the text: “**The data that is being encrypted must be an XML document, one or more elements or a single element’s content**.” If this is incorrect, then a clear statement of the scope of the plain text that may be subjected to a cryptographic transform and appear as the content of a single EncryptedData element must be developed.

- **Section** 2: Since CipherValue and CipherReference can occur zero times in the CipherData, this contradicts the following sentence in section 2:  The CipherData element envelopes or references the raw encrypted data. “If enveloping, the raw encrypted data is the CipherValue element's content; if referencing, the CipherReference element's URI attribute points to the location of the raw encrypted data.” The if neither case is not mentioned. It also contradicts section 2.1.5 [s6]: ‘CipherData contains a CipherValue, which is a base64 encoded octet sequence. Alternately, it could contain a CipherReference, which is a URI reference along with transforms necessary to obtain the encrypted data as an octet sequence.” Finally, section 3.3 states that CipherData it must have some contents. As a result, the possibility of an empty CipherData element may cause an implementation to fail catastrophically.

- **Formalisms**:

In that case, you need to point out that their ?, +, \* formalism does not support enumerated types. As a result, they have no way of specifying A or B or C, but not empty.

If I am correct and there is no enum, it constitutes an underlying flaw in the XML schema definition. If not, they need to define all mandatory fields as enum, regardless of whether the empty element tag is allowable or not. If it is allowable, it should be one of the allowed enumerated values, otherwise not. In either case, a mandatory field containing nothing and with no indication will not be allowed and should fail a schema check. This protects simple implementations, like PDA or cheap CPE.

2) Admin/Edits

- Section 1.1 Editorial, paragraph 3,

From: “**they**

To: “They