3emplate for comments and secretariat observations

Date: 14/X/2013	Document: CWA_XBRL_WI002-1 (E).doc	Project: **XBRL**

MB/ NC[1]	Line number (e.g. 17)	Clause/ Subclause (e.g. 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment[2]	Comments	Proposed change	Observations of the secretariat
SP/uc3m [1]	7	section 3.3.1	second paragraph	ge	In the page 7 section 3.3.1 second paragraph: "The function of the header file is describe the characteristics of the data files in the submission.".	"The function of the header file is to describe the characteristics of the data files in the submission.".	
SP/uc3m	7	section 3.4		ge	Page 7 section 3.4: "A Zip compressed file is a set of one or more files compressed together, that is generated in accordance with the standard set in: http://www.pkware.com/documents3/casestudies/APPNOTE.TXT..".	A Zip compressed file is a set of one or more files compressed together (Pkware (2012)).". And as reference: "[XX] Pkware (2012) .ZIP File Format Specification. September 1st, 2012. http://www.pkware.com/documents/casestudies/APPNOTE.TXT.".	
SP/uc3m	8	3.5.3		ge	Page 8 section 3.5.3: "An signed file is a file embedded and signed in an XML instance of the XML schema referred to at: http://uri.etsi.org/01903/v1.4.1/.".	"A signed file is a file embedded and signed in an XML instance of the XML schema (ETSI 2013)". And the reference "[XX] ETSI (European Telecommunications Standards Institute) 2009 XML Advanced Electronic Signatures (XAdES) (ETSI TS 101 903 V1.4.1). http://uri.etsi.org/01903/v1.4.1/ts_101903v010401p.pdf.".	
SP/uc3m	8	3.5.5		ge	Page 8 section 3.5.5: "External Hash of a file. To be added if required". What is the hash file? What is its use?	"To be added if required for guaranteeing the no modification".	
SP/uc3m	9	3.6.4	first paragraph	ge	Page 9 section 3.6.4 first paragraph: "…for comma seperated files etc.".	"…for comma separated files etc."	
SP/uc3m	11		figure 3	ge	Page 11 figure 3, why is the arrow broken? (--→). Moreover, according to the text, the response container is always recommended.		
SP/uc3m	12	5.1		ge	Page 12 section 5.1 "The present section describes the primitive functions required to put in place the this CWA.".	"The present section describes the primitive functions required to put in place of the this CWA.".	

[1] Carlos III University of Madrid.

1 **MB** = Member body / **NC** = National Committee (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

MB/ NC[1]	Line number (e.g. 17)	Clause/ Subclause (e.g. 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment[2]	Comments	Proposed change	Observations of the secretariat
SP/uc3m	12	5.2		ge	Page 12 section 5.2: “Compression is made in accordance with the standard set in: http://www.pkware.com/documents/casestudies/APPnotE.TXT.”.	“Compression is made in accordance with (Pkware (2012)).”.	
SP/uc3m	12	5.3.2		Ge	Page 12 section 5.3.2: “W3C Encryption http://www.w3.org/TR/xmlenc-core/, using key transport RSA-OAEP http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p and encrypting data with AES256. http://www.w3.org/2001/04/xmlenc#aes256-cbc”.	“As references of W3C Encryption (2002a), of using key transport RSA-OAEP and encrypting data with AES256 are in W3C Encryption (2002b).”. And two new references: “[XX] W3C Encryption 2002a XML Encryption Syntax and Processing. December 10th, 2002. http://www.w3.org/TR/xmlenc-core/. [XX] W3C Encryption 2002b XML Encryption Syntax and Processing. December 10th, 2002. http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/Overview.html#rsa-oaep-mgf1p.”.	
SP/uc3m	12	5.3.2	first paragraph out the box	ge	Page 12 section 5.3.2 first paragraph out the box: “…(there shall be no references to te file at an external location). …”.	“…(there shall be no references to the file at an external location). …”.	
SP/uc3m	13		paragraph sixth	ge	Page 13 paragraph sixth: “The embedded file is encrypted using a symmetric algorithm (AES-256) with a generated secret key. The Security strength of AES-256 is 256 (NIST SP 800-57 part1). http://csrc.nist.gov/publications/drafts/800-57/Draft_SP800-57-Part1-Rev3_May2011.pdf.”.	http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_part1_rev3_general.pdf. I would change by “The embedded file is encrypted using a symmetric algorithm (AES-256) with a generated secret key. The Security strength of AES-256 is 256 (NIST SP 800-57 part1 (2012))”. And a new reference: “[XX] NIST SP 800-57 part1 2012 Recommendation for Key Management – Part 1: General (Revision 3). Authors: Elaine Barker, William Barker, William Burr, William Polk, and Miles Smid. July 2012. http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_part1_rev3_general.pdf.”.	
SP/uc3m	12		paragraph eight	ge	Page 12 paragraph eight: “… decrypting keys . RSA-OAEP uses …”.	“… decrypting keys. RSA-OAEP uses …”.	
SP/uc3m	13		paragraph	ge	Page 13 paragraph ninth: “… (see NIST SP 800 131 A)). Also, RSA is acceptable, with |n|=2048,	“… (see NIST SP 800 131A (2011)).). Also, RSA is acceptable, with |n|=2048, for SP800-56B	

1 **MB** = Member body / **NC** = National Committee (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

MB/ NC[1]	Line number (e.g. 17)	Clause/ Subclause (e.g. 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment[2]	Comments	Proposed change	Observations of the secretariat
			ninth		for SP800-56B key agreement schemas. |n| is. …".	(2009) key agreement schemas. As |n| is …". And I would add the next references: "[XX] NIST SP 800 131A 2011 Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths. Authors: Elaine Barker and Allen Roginsky. January 2011. http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf.", [XX] SP800-56B 2009 Recommendation for Pair-Wise, Key Establishment Schemes Using Integer Factorization Cryptography. Authors: Elaine Barker, Lily Chen, Andrew Regenscheid, and Miles Smid. August 2009. http://csrc.nist.gov/publications/nistpubs/800-56B/sp800-56B.pdf.".	
SP/uc3m	13	5.3.3	paragraph second	ge	Page 13 section 5.3.3 paragraph second: "When an encryption is applied to a file that has no suffix, the reserved extended suffix .encrypted.xml shall be added to the filename.".	"When an encryption is applied to a file that has no suffix, the reserved extended suffix .encrypted.xml shall be added to the filename as the table 1 shows.".	
SP/uc3m	14	5.3.6	paragraph fifth	ge	Page 14 section 5.3.6 paragraph fifth: "be compliant with European Directive 1999/93/EC;".	"be compliant with European Directive 1999/93/EC (1999);", I would add the next reference: "[XX] Directive 1999/93/EC 1999 Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999. Chapter 13 Volume 038 P. 50 – 58. http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&numdoc=31999L0093&model=guichett.".	
SP/uc3m	14	5.3.7		ge	Page 14 section 5.3.7: "The file structure generated by the signature shall be XAdES-BES/EPES http://uri.etsi.org/01903/v1.4.1/ using RSA with SHA512 http://www.w3.org/2001/04/xmldsig-more#rsa-sha512".	"The file structure generated by the signature shall be XAdES-BES/EPES referenced in (ETSI 2013), and using RSA with SHA512 (2008)". And I would add "[XX] RSA with SHA512 2008 XML Security Algorithm Cross-Reference. http://www.w3.org/TR/2013/NOTE-xmlsec-algorithms-20130124/, http://www.w3.org/2001/04/xmldsig-more#rsa-	

1 **MB** = Member body / **NC** = National Committee (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

MB/ NC[1]	Line number (e.g. 17)	Clause/ Subclause (e.g. 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment[2]	Comments	Proposed change	Observations of the secretariat
						sha512, http://www.ietf.org/rfc/rfc4051.txt.".	
SP/uc3m	15		paragraph first	ge	Page 15 paragraph first: "XAdES-BES/EPES (which has been built up on W3C XML Digital Signature) shall be implemented according to COMMISSION DECISION of 25 February 2011 establishing minimum requirements for the cross-border processing of documents signed electronically by competent authorities under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:053:0066:0072:EN:PDF".	"XAdES-BES/EPES (which has been built up on W3C XML Digital Signature) shall be implemented according to COMMISSION DECISION of 25 February 2011 establishing minimum requirements for the cross-border processing of documents signed electronically by competent authorities under Directive 2006/123/EC (2006) of the European Parliament and of the Council on services in the internal market (Official Journal of EU (2011))." I would add the next references: "[XX] Directive 2006/123/EC 2006 Directive 2006/123/EC of the European Parliament and of the Counciel of 12 December 2006. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:376:0036:0068:en:pdf.". And, "[XX] Official Journal of EU 2011 Commission decision of 25 February 2011 establishing minimum requirements for the cross-border processing of documents signed electronically by competent authorities under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:053:0066:0072:EN:PDF.".	
SP/uc3m	15		paragraph eight	ge	Page 15 paragraph eight: "The length of the RSA modulus shall be at least 2048 (NIST SP 800-131A-1). http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf. Details on RSA can be found in RFC 3447 at: http://www.ietf.org/rfc/rfc3447.txt.. The hash function SHA-512 as specified in FIPS PUB 180-4. http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf. SHA-512 prov: http://csrc.nist.gov/publications/drafts/800-57/Draft_SP800-57-Part1-Rev3_May2011.pdf.".	"The length of the RSA modulus shall be at least 2048 (NIST SP 800-131A-1 (2011)). Details on RSA can be found in RFC 3447 (2003). The hash function SHA-512 as specified in FIPS PUB 180-4 (2012). SHA-512 (2008). With the next references: "[XX] NIST SP 800-131A-1 2011 Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths. January 2011. http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf.", "[XX] RFC 3447 2003 Public-Key Cryptography Standards (PKCS) #1:	

1 **MB** = Member body / **NC** = National Committee (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

MB/ NC[1]	Line number (e.g. 17)	Clause/ Subclause (e.g. 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment[2]	Comments	Proposed change	Observations of the secretariat
						RSA Cryptography Specifications Version 2.1. February 2003. http://www.ietf.org/rfc/rfc3447.txt.", "[XX] FIPS PUB 180-4 2012 Federal Information Processing Standards Publication, Secure Hash Standard (SHS). March 2012. http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf.",	
SP/uc3m	15		last paragraph	ge	Page 15 last paragraph: "When a signature is applied to a file that has no suffix, the reserved extended suffix .signed.xml shall be added to the filename".	"When a signature is applied to a file that has no suffix, the reserved extended suffix .signed.xml shall be added to the filename, as the table 2 shows.".	
SP/uc3m	16	5.4.2	first paragraph	ge	Page 16 section 5.4.2 first paragraph: "The structure of a header as described in this CWA is that of an ExtendedHeader that is to be defined as in Figure 5. Figure 5 shows an Extended Header structure importing the BasicHeader structure that optionally imports the RegisteredOrganisationVocabulary (formerly called « Core Business Vocabularies ») and/or other modules (to be developed in the future).".	"The structure of a header as described in this CWA is that of an ExtendedHeader that is to be defined as in Figure 5. This picture shows an Extended Header structure importing the BasicHeader structure that optionally imports the RegisteredOrganisationVocabulary (formerly called « Core Business Vocabularies ») and/or other modules (to be developed in the future). The table 3 shows the structure of the header. ".	
SP/uc3m	17		table 3, second row, second column	ge	Page 17, table 3, second row, second column: "… It has been revised and renamed into Registered Organization Vocabulary (RegOrg). It is described at http://www.w3.org/TR/vocab-regorg/. …".	"… It has been revised and renamed into Registered Organization Vocabulary (RegOrg (2013)). …". And, I would add the reference: "[XX] RegOrg 2013 Registered Organization Vocabulary. W3C Working Group Note 28 May 2013. http://www.w3.org/TR/vocab-regorg/.".	
SP/uc3m	17	5.4.3	first paragraph	ge	Page 17, section 5.4.3 first paragraph: "The following use-cases for creating an ExtendedHeader are explicitly defined by this CWA and may be used « as is ».".	"The following use-cases, table 4, for creating an ExtendedHeader are explicitly defined by this CWA and may be used « as is ».".	
SP/uc3m	17		table 4, second row, second column	ge	Page 17, table 4, second row, second column: "This header structure reflects the survey made within the Eurofiling BestPractices efforts which had given the results documented in http://www.wikixbrl.info/index.php?title=Best_Prac	"This header structure reflects the survey made within the Eurofiling BestPractices (2013). …". And, I would add the reference: "[XX] BestPractices 2013 Best Practices on Common European Reporting Structures. Eurofiling 21013.	

1 **MB** = Member body / **NC** = National Committee (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

MB/ NC[1]	Line number (e.g. 17)	Clause/ Subclause (e.g. 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment[2]	Comments	Proposed change	Observations of the secretariat
					tices_on_Common_European_Reporting_Structures. …".	http://www.wikixbrl.info/index.php?title=Best_Practices_on_Common_European_Reporting_Structures, http://www.xbrlwiki.info/images/c/c0/Eurofiling_header_questionnaire-results.xls.".	
SP/uc3m	18	5.4.4		ge	Page 18, section 5.4.4, first paragraph: "The guidelines for the creation of a specific ExtendedHeader schema are given in the external document « How to use the basic header? ».". Where is this document?		
SP/uc3m	20	6.3		Ge	Page 20, section 6.3, first paragraph: "The container feedback file should be added to the Response container.".	"The container feedback file should be added to the Response container, figure 7.".	
SP/uc3m	21	6.5		te	Page 21, section 6.5: "Reporting entity to NSA to ESA (1st and 2nd level)".	"Reporting entity to European Supervision Authority (NSA) to European Supervision Authority (ESA), 1st and 2nd level".	
SP/uc3m	21	6.5.1	first paragraph	Ge	Page 21, section 6.5.1, first paragraph: "… As a consequence, the ESA has all of the reporting entities it is forwarded data from as communication partner s and needs to know their public key / certificate.".	"… As a consequence, the ESA has all of the reporting entities it is forwarded data from as communication partners and needs to know their public key / certificate.".	
SP/uc3m	21	6.5.1	second paragraph	ge	Page 21, section 6.5.1, second paragraph: "Figure 8 shows a 2-layer submission using containers in containers to forward data to subsequent authorities and as well as feedback to the respective sender.".	"Figure 8 shows a 2-layer submission using containers to forward data to subsequent authorities and as well as feedback to the respective sender.".	
SP/uc3m	23	6.6		te	Page 23, section 6.6, paragraph first: "To be added if required". Is it correct?		
SP/uc3m	24	A.2		Te	Page 24, section A.2, row belongs to "Allow update containers ?"	explanations, maybe: "No, because, after creating the container ought to be manipulated.".	
SP/uc3m	25	A.4		ge	Page 25, section A.4, first paragraph: "A table composed of following information (defining codes accepted both for legal antities as for	"A table composed of following information (defining codes accepted both for legal entities as for persons) should explain which codes are	

1 **MB** = Member body / **NC** = National Committee (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

MB/ NC[1]	Line number (e.g. 17)	Clause/ Subclause (e.g. 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment[2]	Comments	Proposed change	Observations of the secretariat
					persons) should explain which codes are allowed:".	allowed:".	
SP/uc3m	25	A.4	paragraph second	ge	Page 25, section A.4, paragraph second: "A list of the applicable Destinees for potential subcontainers should be defined". The word "Destinees" in the Collins or in WordReference is a verb, the name is "destination".		
SP/uc3m	26		Table B.1	Ge	Page 26, table B.1, row third, second column: "Definition of the subcontainer types, the destinees of these subcontainers, …". The same with "destinees".		
SP/uc3m	27		first paragraph	ge	Page 27, first paragraph: "This section will be described in detail in the final version of this document. For now, the explanations cover the BasicHeaderOnly use-case:". When?		
SP/uc3m	27		table C.5, second row	te	Page 27, table C.5, second row, second column: "This field gives the relative URI to a file in the container (starting from top-level)".	"This field gives the relative Uniform Resource Identifier (URI) to a file in the container (starting from top-level)".	
SP/uc3m	28		first paragraph	ge	Page 28, first paragraph: "These are supplementary information for the elements provided in both tables for:".	"These are supplementary information (figure D.1) for the elements provided in both tables for:".	
SP/uc3m	28		first paragraph	ge	Page 28, first paragraph: "These are supplementary information for the elements provided in both tables for:".	"These are supplementary information (figure D.1) for the elements provided in both tables for:".	
SP/uc3m	28		figure D.1	ge	Page 28, figure D.1, the type of letter is small, I don't know if it is possible.		
SP/uc3m	29		first paragraph	ge	Page 29, first paragraph: "These are supplementary information for the elements provided in both tables for:".	"These are supplementary information, figure E.1, for the elements provided in both tables for:".	
SP/uc3m	28		figure E.1	ge	Page 28, figure E.1, the type of letter is small, I don't know if it is possible.		

1 **MB** = Member body / **NC** = National Committee (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial