Public Review: Comments on Draft ETSI SR 019 020 V0.0.4 (2013-11)

Rationalised Framework of Standards for Advanced Electronic Signatures in Mobile Environment>

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**OBSERVATIONS** on each comment submitted
OASIS TC DSS-X			General	The document is a good description of possible signing scenarios in mobile environments! But we miss the focus on the required building blocks of these scenarios. The blocks are shown in the diagrams explicitly ... why is there no further discussion on this granularity level? These blocks define the required (remote) interfaces and can be matched against existing interface definitions easily. Some of the interfaces are defined by DSS (the signature requesting interface and presumably the digest encryption unit), other may need to be defined. In our opinion all the scenarios can be implemented by an aggregation of local and remote instances of these interfaces. This would ease the aspect discussed in 5.4 (Applicability to General Computing Devices).		
OASIS TC DSS-X			General	The aspects of verification should be discussed a bit more in detail. In analogy the the private key in signing the trust anchor is the crucial part of the verification. The selection of trust roots could vary widely in different scenarios. Sometimes a company / internal root must be used, sometimes a qualified root is required, and sometimes the browser-accepted root set will do. Should this be handled by verification policies? Or does the client match the verification result against his root set? Especially in the mobile environment it should be considered to have a special verification mode for any 'often verified' documents. For e. g. code snippets or apps it shouldn't be necessary to do a full-scale verification each-and-every time when there		

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	OBSERVATIONS on each comment submitted
				is a huge advantage of caching, especially on the mobile provider level.		
OASIS TC DSS-X			General	Also regarding verification the aspect of document privacy and network load / latency should be discussed. In analogy to the signing process a pre-hashed variant of the verification could be useful. A more paranoid aspect of privacy is the disclosure of the signer certificate. Maybe it's a valid use case to do basic signature verification locally and just do the upper level of chain verification for remote services.		
OASIS TC DSS-X			General	We missed the aspect of trust setup (how to create trust regarding the different CA's).		
OASIS TC DSS-X	3.1 Page 9	Def mobile device	Editorial	The phrase 'This is typically the tablet'. This might be confused with a signing tablet, only used to record the handwriting. (The icon used for this in the scenario's is a bit confusing.) If a handheld tablet is meant, such as an Apple iPad or MS Surface, a different icon should be used. (Figure 1 on page 13)		
OASIS TC DSS-X	3.1 Page 9	Def mobile signature service	Technical	It tries to define the service but uses almost the same words. What does the 'mobile signing process' mean?	"Facility that coordinates and manages the process by which an end user can sign a document, or other information, using a mobile device."	
OASIS TC DSS	4.1 Page 10		Editorial	Under a) capital letters 'M' for Mobile		
OASIS TC DSS	4.2	Under f) sentence "Note: Use of software for …."	Editorial	Do you mean: "The use of secure signing software is not required by this standard." (emphasis on 'required' instead of 'supported').		
OASIS TC	4.3.1	Sentence "Throughout	Editorial	This sounds like a definition of digital signature value, but it differs from the	Extend the definition?	

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	OBSERVATIONS on each comment submitted
DSS	Page 11	this clause the term "digital signature value" refers to the result of"		actual definition.		
OASIS TC DSS	4.3.1 Page 11	Sentence For generation the set of scenarios range from those where	Editorial	Strange sentence. Reformulate…?	"To generate the set of scenario's, ranging from..."	
OASIS TC DSS	4.3.2.2 Figure 1 Page 13	Use of icons	Editorial	The icons that are used, for instance for the MSSP and tablet give the wrong impression.		
OASIS TC DSS	4.2.2.3	Title	Editorial	Should the title exclude the words "or complete"? Because what does it mean? (Does it actually create scenario R3?)		
OASIS TC DSS	4.2.2.3	First par. Phrase "the AdES structure is built by the MSSP. "	Editorial	The title assumes something else as well: 'the complete generation of AdES in mobile devices…'		
OASIS TC DSS	4.2.2.3 Page 15	First par.	Editorial	The term SCD is used but there is no definition given.		
OASIS TC DSS	4.3.2.4		Technical	Does this clause also support a mobile device with an 'app' that contains the signing key? Section 5.4 states: "Only scenario L3 is specific to mobile devices, although variations of all the local scenarios (L1, L2, and L3) and potential		

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	OBSERVATIONS on each comment submitted
				options within the remote signing scenario R2 can require mobile devices connected to a mobile network". So, the other scenario's do not necessarily need a mobile device?? (I thought they were intended for mobile devices...) Is this scenario only applicable to mobile devices just because of the wireless icon, indicating by 'Mobile service'? By definition the Mobile device needs an antenna, so why is only L3 specific to mobile devices? Or is it assumed that mobile devices can be connected to something by means of a wire (suchg as USB cable)? This is not explicitely mentioned in the definition.		
OASIS TC DSS	4.3.2.4 Page 16	Paragraph below figure 3	Editorial/Technical	Is it the SIM that generates the AdES? Could it also be an application on the device?		
OASIS TC DSS	4.3.2.4 Page 16	2nd par. Sentence: For example, the mobile device may generate only a digital signature, leaving extension to an AdES to the signing server.	Editorial/Technical	Are you referring to other scenario's than the scenario's of the previous sections? This alternative sounds like scenario R2...		
OASIS TC DSS	4.3.2.4 Page 17 1st par.	Sentence: '..meaning that the signing key may have to be stored in another (secure)	Technical	What is meant by 'another (secure) environment'? Do you refer to the 'remote device' (the one that it not held by the user, but contains the private key and is located in another (secure) environment. This is actually another scenario: one where the SCD is		

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**OBSERVATIONS** on each comment submitted
		environment.’		NOT part of the mobile device.		
OASIS TC DSS	4.3.3.1	Sentence The following scenarios are where the AdES is created using a using a signing key…	Editorial	Please rephrase		
OASIS TC DSS	4.3.3.2 Page 18 6th par.	Term SDO	Editorial	What is an “SDO format”?		
OASIS TC DSS	4.3.3.2 Page 18 8th par.	Sentence: The authentication of the user to the signing service provider may involve an external identity provider.	Technical	In some cases the SSP will initiate the authentication (the current scenario assumes that the authentication is done before the request is sent to the SSP).		
OASIS TC DSS	5.3 Page 29	Sentence **EN 319 431** For remote signing s	Editorial	Rephrase ‘are not subject to the open to hostile attack .’		
OASIS TC DSS	4.2		Editorial	The wording should be improved. For instance “a) Whether document created on to the mobile…”		

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**OBSERVATIONS** on each comment submitted
OASIS TC DSS			Editorial	Sometime the term ‘digital signature’ is used but usually (?) ‘digital signature value’.		
OASIS TC DSS						
OASIS TC DSS						
OASIS TC DSS						
OASIS TC DSS						
OASIS TC DSS						