Svenska Läkaresällskapet

2011-08-31

SIS, Swedish Standards Institute
Sankt Paulsgatan 6
SE-118 80 Stockholm

Remiss SIS-9158 Hälso- och sjukvårdsinformatik

Svenska Läkaresällskapet (SLS) är en politiskt och fackligt obunden organisation, som arbetar för förbättrad hälsa och sjukvård med patientens bästa för ögonen.

Efter hörande från Språkvårdskommittén och Sektionen för medicinsk informatik vill SLS avge följande yttrande. Se bifogad svarsblankett.

För Svenska Läkaresällskapet

Stockholm den 31 augusti 2011

Margareta Troein Töllborn
Ordförande

Magnus Fogelberg
Ordf. i Kommittén för medicinsk språkvård

e-post: git.eliasson@sis.se

SIS
Remissvar
Git Eliasson
118 80 STOCKHOLM

SIS/TK 334, Hälso- och sjukvårdsinformatik
Svar på   SIS-remiss 9158
avseende   prEN ISO 21091

Senaste   **2011-09-05**
svarsdatum

Uppgifter om svarslämnaren

☒ Företag/Organisation/Myndighet   ☐ Enskild person

Företag/Organisation/Myndighet   Svenska Läkaresällskapet (SLS)

Handläggare (namn, telefon)   Anna Borgström, 08-440 88 92

Datum   2011-08-31

Remissvar

☐ Avstår

☐ Tillstyrker utan kommentarer

☒ Tillstyrker med kommentarer

☐ Avstyrker med motivering

☐ Har erfarenhet inom det område förslaget täcker

☐ Har tillämpat förslaget

☐ Ej berörd

☐ Kommentarer till föreslagen svensk titel

SIS, Swedish Standards Institute   *SIS is the Swedish member of ISO and CEN*

Postadress: 118 80 STOCKHOLM   Besöksadress: Sankt Paulsgatan 6, Stockholm   Organisationsnr: 8024100151
Telefon: 08-555 520 00 Telefax: 08-555 520 01   E-post: info@sis.se

Postal address: 118 80 STOCKHOLM, Sweden   Office address: Sankt Paulsgatan 6, Stockholm   V.A.T. No. SE802410015101
Phone: +46 8 555 520 00 Telefax: +46 8 555 520 01   E-mail: info@sis.se   **www.sis.se**

Svarslämnare: Svenska Läkaresällskapet   2011-08-30

Kommentarer på: SIS-remiss 9158 SLS   Förslag: prEN ISO 21091 – svar Språkkommittén/mf

1	2	(3)	4	5	(6)	(7)
ID	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/N ote (e.g. Table 1)	Type of comm ent	Comment (justfication for changes)	Proposed change	Fylls i av SIS
SE	Entire document		ed	The use of "s" and "z" in words containing "-ise" or "-isation" is not consequent. As this is an (draft) International Standard, and especially as it is a Vienna Agreement project together with CEN, British English should be used and not US English.	Change "z" to "s" in appropriate positions and make a linguistic consistency check of the entire document.	
SE	Entire document		ed	Space is repeatedly wrongly inserted in words, which is probably the effect of transforming the original template-built Word document to Adobe pdf format.	Check the master document and make corrections if the mistake occurs.	
SE	3	Entire clause	te	Appendix A (informative) of ISO 10241-1 should be respected concerning format of the terms and definition list: referred terms should be highlighted and numbered, preferably in italics.	Update the entire clause. Example: **3.14** **certificate verification** verifying that a *certificate* (3.8) is authentic	
SE	3	Entire clause	te	Definitions must not end with a period.	Delete the period after each definition.	
SE	3	3.3, 3.4	te	The definitions of these two concepts are circular (highlighting by commenter): **3.3** **attribute authority (AA)** authority which assigns privileges by issuing **attribute certificates** [X.509] **3.4** **attribute certificate** data structure, digitally signed by an **attribute authority**, that binds some attribute values with identification about its holder [X.509] This kind of definition does not comply with ISO 704, and, moreover, it is meaningless. The important thing is to find the essential characteristic(s). In 3.4 it seems that the binding of attribute values, and even if this was performed by someone else than the attribute authority, the concept would remain an attribute certificate. So in	Keep 3.3. Change the definition of 3.4 to: digitally signed data structure that binds some attribute values with identification about its holder [X.509]	

1	2	(3)	4	5	(6)	(7)
ID	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/N ote (e.g. Table 1)	Type of comm ent	Comment (justfication for changes)	Proposed change	Fylls i av SIS
				3.4, the attribute authority is not an essential characteristic.		
SE	3	3.5	te	The definition includes a comment.	Change the term entry to: **3.5** **authentication** process of reliably identifying security subjects by securely associating an identifier and its authenticator [ISO 7498-2] NOTE See also data origin authentication and peer entity authentication	
SE	3	3.8	te	Worst kind of circular definition, with the term used even within the definition of itself! Substitution will create a never-ending recursion. Unfortunately, even ISO 17090-1 uses this terminologically unacceptable definition. Lack of formal definitions in available standards makes prEN ISO 21091 the appropriate place to hold a correct definition.	Change the definition to: digital document assuring the identity of the only individual who can access and refer to that document	
SE	3	3.10	te	The definition includes a comment.	Change the term entry to: **3.10** **certificate issuer** authority trusted by one or more relying parties to create and assign *certificates* [ISO 9594-8] NOTE Optionally the certification authority may create the relying parties' keys.	
SE	3	3.11	te	The extensional definition is not quite logically worded. The last item in the list should have the same formulation as the preceding ones.	In the definition, add "certificate" before "revocation": procedures relating to *certificates* such as: certificate generation, *certificate distribution*, certificate archiving and *certificate revocation*	
SE	3	3.12	te	The definition includes non-essential characteristics. A certificate may be revoked regardless the reason. The second part of the definition is however an important explanation why certificates are revoked.	Change the term entry to: **3.12** **certificate revocation** act of removing any reliable link between a *certificate* and its related owner (or security subject owner)	

1	2	(3)	4	5	(6)	(7)
ID	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/N ote (e.g. Table 1)	Type of comm ent	Comment (justfication for changes)	Proposed change	Fylls i av SIS
					NOTE A certificate may be revoked because it is not trusted any more even though the time and date are within the certificate validity period.	
SE	3	3.13	te	The acronym CRL is a synonym and should be treated as one according to ISO 10241-1. Text in brackets in the definition seems unnecessary (unless the digital signature is optional, and in that case the text in brackets should be deleted). The use of capital initial letters in multi-word terms should be deprecated in this clause. This is something used in naming attributes in information models to mark separate word when they are written together in a one-word label. This notation has no justification in a concept list.	Change the term entry to: **3.13** **certificate revocation list** CRL published list of the suspended and revoked certificates digitally signed by the CA	
SE	3	3.15	te	The acronym CA is a synonym and should be treated as one according to ISO 10241-1. We agree that *certificate issuer* may be, or even is, a better term, and in that case it should be suggested as a synonym. The use of capital initial letters in multi-word terms should be deprecated in this clause. This is something used in naming attributes in information models to mark separate word when they are written together in a one-word label. This notation has no justification in a concept list.	Change the term entry to: **3.15** **certification authority** CA certificate issuer entity that issues *certificates* by signing certificate data with its private signing key NOTE: Authority in the certification authority term does not imply any government authorization, only that it is trusted. Certificate issuer may be a better term but CA is used very broadly.	
SE	3	3.18	te	1) Cryptography is not mentioned in this prEN/DIS and should not be referred to in the definition. 2) A definition must not include examples. That makes it extensional, and in that case the list of examples must be exhaustive.	Delete the text in brackets and the example. Change the term entry to: **3.18** **digital signature** data appended to, or a cryptographic transformation of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect	

1	2	(3)	4	5	(6)	(7)
ID	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/Note (e.g. Table 1)	Type of comment	Comment (justfication for changes)	Proposed change	Fylls i av SIS
					against forgery [ISO 7498-2]	
SE	3	3.24	te	The acronym should be handled as a synonym.	Change the term to: **lightweight directory access protocol** LDAP	
SE	3	3.25	te	The acronym should be handled as a synonym.	Change the term to: **object identifier** OID	
SE	3	3.26	te	The definition includes a non-essential characteristic: about the record. Even if the person is not registered in a health information system, she/he is still a subject of care as long as the first characteristics apply. Why not adopt the definition of prEN ISO 13940?	Change the definition to: person seeking to receive, receiving, or having received health care	
SE	3	3.27	te	The definition in ISO 2382, quoted also in ISO 17090, is far too narrow for use in prEN ISO 21091. The definition means that privacy does not exist until it has been violated. It does not comply with its use in paragraph 5.3, where "privacy" (a broader concept to be explained further down) may be violated even if the *gathering of data* is not illegal. Neither does it comply with its use in clause 6, first paragraph after the three bullet points. It says "... sensitive nature of health related and privacy information ...". The current definition does not know of privacy information until it has been "unduly or illegally" gathered. A suggested definition adapted from an explanation in Wikipedia-EN does not delimit the concept to occasions when information is used in an unauthorised way. That definition points out that 1) the individual/group has total control of the boundaries 2) information about the individual(s) is included within the boundaries controlled by themselves 3) the right to reveal information about the individual(s) is kept by themselves 4) it does not prevent violation of privacy, but other concepts have to cover the kind of violation, legal (emergency matter) or illegal.	Change the definition to: ability of an individual or group to seclude themselves or information about themselves and thereby reveal themselves selectively	
SE	3	3.28	te	The text in brackets is not defining, should be a	Change the term entry to:	

1	2	(3)	4	5	(6)	(7)
ID	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/Note (e.g. Table 1)	Type of comment	Comment (justfication for changes)	Proposed change	Fylls i av SIS
				comment.	**3.28** **private key** key that is used with an asymmetric cryptographic algorithm and whose possession is restricted [ISO 10181-1] NOTE The possession of a private key is usually restricted to only one entity.	
SE	3	3.30	te	The term entry does not comply with ISO 704. If the term has to be defined in clause 3, the term entry has to be completely reworded.	Suggested wording of the term entry: **3.30** **public key certificate** X.509 public key certificate PKC certificate binding an identity and a public key NOTE The identity may be used to support identity-based access control decisions after the client proves that it has access to the private key that corresponds to the public key contained in the PKC [RFC3280]	
SE	3	3.31	te	The acronym should be handled as a synonym.	Change the term to: **3.31** **public key infrastructure** PKI	
SE	3	3.34	te	The reference is written "(CEN)". The appropriate standard/TS/TR has to be stated.	Provide the correct reference, if necessary by aid of the CEN TC 251 secretariat.	
SE	3	3.40	te	The acronym should be handled as a synonym.	Change the term to: **3.40** **trusted third party** TTP	
SE	3	3.41	te	This is not a term to be defined, it is the title of a reference.	Delete the term entry and move the information to the bibliography.	
SE	3	3.42	te	This is not a term to be defined, it is the title of a	Delete the term entry and move the	

1	2	(3)	4	5	(6)	(7)
ID	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/N ote (e.g. Table 1)	Type of comm ent	Comment (justfication for changes)	Proposed change	Fylls i av SIS
				reference.	information to the bibliography.	
SE	4		ed	Line feed is missing before the entry "CRL Certificate revocation list" (at least in the pdf version).	Check and correct.	
SE	4		te	As SOA is mentioned in clause 5, it should be explained in clause 4.	Add: SOA Service-oriented architecture	
SE	5	5.1, second sentence	ed	Seems not well worded, the meaning is unclear.	Last part of the sentence may be better: "... are not fully addressed by X.500 defined attributes." Or maybe complete rewording of the sentence: X.500 defined attributes do not completely fill the requirements to manage and distinguish health professionals, subjects of care, organizations, and other health entities engaged in health care communications and security decisions. .	
SE	5	5.3, middle of first paragraph	ed	In the sentence " Within an organization, and individual may operate under differing roles depending upon the care setting or other factors." the word "and" seems to be wrong. Should probably read "an".	Change "and" to "an".	
SE	6	First paragraph last sentence	ed	Isn't one word missing? "While the following standards are not directory specific, should be adhered to for the protection of Directory Infrastructures..." Shouldn't there be a "they" after comma before "should"?	Check and possibly correct.	
SE	6	Last paragraph	te	Whilst the first paragraph clearly states which documents have to be respected (in order to achieve compliance to the objectives of prEN ISO 21091), the paragraph after the bullet points talks about what is outside the scope , yet to be considered. That text is not normative within the scope of the standard.	Move the last paragraph to the scope as last paragraph of clause 1.	
SE	7	7.2.4, 7.2.5	te	Whilst 7.2.2 is specified to be required and 7.2.3 to be optional, nothing is said about 7.2.4 and 7.2.5	Add statement whether organisation and organisation unit are required or optional. (Figure 1 implies that both are required.)	
SE	8	8.1.2, 8.3.1	te	There is an attribute called "mail" designating electronic	Attribute name "mail" to be replaced by	

Kommentarer på: SIS-remiss 9158 SLS   Förslag: prEN ISO 21091 – svar Språkkommittén/mf

1	2	(3)	4	5	(6)	(7)
ID	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/N ote (e.g. Table 1)	Type of comm ent	Comment (justfication for changes)	Proposed change	Fylls i av SIS
				mail. Even if several languages use "mail" (or words with local spelling resulting in the same pronunciation) for this phenomenon, in regular English the usual word is "e-mail" to mark the difference from old-fashioned mail (Royal Mail). "Mail" could therefore be ambiguous. Equally to the attribute named "homePostalAddress" the logic designation would be eMailAddress.	"eMailAddress".	
SE	8 (and annex B)	8.1.2 (and B.1)	te	Mobile phone number has got the attribute name "mobile", very short compared to other phone numbers, e.g. facsimileTelephoneNumber (which would have been understandable as "fax"). The word "mobile" is used in other meanings (mobile user, mobile environment). Better clarity would be achieved with a standardised naming of telecom attributes.	Change the attribute name "mobile" to "mobileTelephoneNumber".	
SE	8	8.1.2	te	Only when the table showing the HL7 attribute names it becomes clear that "telephoneNumber" means business (=work?) telephone, whilst "homePhone" means home telephone. Naming of attributes should be standardised.	Change the attribute name "homePhone" to "homeTelephoneNumber" and "telephoneNumber" to "businessTelephoneNumber".	
SE	9	9.1 second paragraph	ed	The sentence "A common mistake is to assume that every search the directory is based on the attributes used in the distinguished name.." is not clear. Is there a word missing: "...search **in** the directory..."? Moreover, there are two trailing periods.	Check and consider amendment. Delete one period.	