

DR #	Description of Defect	Part # and clause	DR doc #	Source	Status
157	ModifyDN and UnitOfReplication	4/19.1.4	8N363	Germany	4-TC1 (3rd)
159	targetObject in Search (I) procedure	4/19.3.2.2.1	8N363	Germany	4-TC1 (3rd)
162	APIInfo procedure	4/20.4.5	8N363	Germany	4-TC1 (3rd)
163	Shadowed information procedure	9/7.2, 9.Fig.3	8N363	Germany	Accepted Source solution
164	<i>ASN.1 of SupplierUpdateMode</i>				<i>Rejected</i>
166	Alias control by alias dereferencing	3/7.11.1	8N363	Germany	3-TC1 (3rd)
168	<i>Protected password</i>				<i>Rejected</i>
169	Permutable property for PKCS	8/Clause 7, 8/10.2, 8/10.3		UK	Accepted Not in DTC
170	Entry selection in search procedure	3/Fig. B-11		UK	Open
173	NSSRs in the root entry	2/18.5		ITU Rapp.	2-TC1 (3rd)
176	Access controls on aliases	3/7.11.1		ITU Rapp.	Open
177	Distinguished encoding of UTCTime	8/Clause 9		ISO Rapp.	8-TC3
178	Duplicate of 209				
179	Clarification in returnDN handling	2/Table K-1 3/7.4.11, B4, B5		Germany	2-TC1 (3rd) 3-TC1 (3rd)
180	entryOnly inconsistency	3/7.3 4/10.3(g)-(o)		Germany	Rejected But editorial to part 4 was

DR #	Description of Defect	Part # and clause	DR doc #	Source	Status
					accepted - 4-TC1 (3rd)
181	<i>Shadowing access controls</i>				<i>Withdrawn</i>
182	Shadowing and one-level searching	9/7.2.2.3 and 9.2		IETF	9-TC1 (3rd)
183	Public key usage	8/12.2.2..3		UK	8-TC1 (3rd)
184	<i>CertificationPath</i>	8/8		UK	Rejected Helsinki97
185	Forward and reverse certificates	8/8		UK	8-TC4 (3rd)
186	Entry ACI and shadowing	9/7.2.2		UK	9-TC1 (3rd)
187	sdseType of root	9/7.2.1.1		UK	9-DTC2(3rd)
188	Add permission and prescriptive ACI	3/11.1.5 (3)		UK	3-TC1 (3rd)
189	Modify operational binding	2/24.3		UK	2-TC1 (3rd)
190	Access controls	4/19.3.1.2.2 1b		UK	4-TC1 (3rd)
191	Alias loops	4/18.3.1		UK	Rejected
192	Collective attributes and content rules	2/11.7, 2/12.7.1, 2/13.6		UK	Open
193	<i>Policy constraints</i>				<i>Rejected</i>
194	Validity date	?			8-TC1 (3rd)
195	Shadowing agreement parameters	9/9.1		UK	<i>Rejected</i>
196	<i>Validity period</i>				<i>Withdrawn</i>
197	DSE type bits	2/19.4.2		Defect Group	Open

DR #	Description of Defect	Part # and clause	DR doc #	Source	Status
		4/24.3.1.2			
198	Additions to chaining arguments	4/17.3.3.1		UK	4-TC1 (3rd)
199	Presence Filter	3/7.8.2		US	Accepted with mod Not in DTC!!
200	CRL dist pts & full crls	8/12.6.2		Defect Group	8-TC3 (3rd)
201	Issuing distribution point	8/12.6.3.1		UK	8-TC3 (3rd)
202	Clarification of CertificationPath in SecurityParameters	3/7.10		Defect Group	3-TC1 (3rd)
203	Entry Information Selection	3/7.6		Defect Group	Rejected
204	Revoked certificates on CRL past expiry time	8/12.6.3.1 and 8/11.2		Defect Group	8-TC5 (3rd)
205	Definition of Superior Reference			US	2-TC1 (3rd)
206	Handling extensions for search results	3/10.1.3 4/21		EIDQ/FDAS & ISSS/WS DIR	3-TC1 (3rd) 4-TC1 (3rd)
207	Problem in the use of the Algorithm object Class	8/8 & Annex A		Rapporteur	8-DTC6(97) ?
208	Needed ACI when processing List using knowledge held in superior DSA	9/7.2.2.3 & 9.2.4.1		IETF IDS	9-DTC2(3rd)

DR #	Description of Defect	Part # and clause	DR doc #	Source	Status
209	DSA referrals (duplicate registration 178)			ITU rapporteur	4-TC1 (3rd)
210	Shadowing attribute selection			Defect Group	Open
211	Y2K corrections	Parts 2, 3,4, & 6		US	2-TC2, 3-TC3, 6-TC1 (3rd)
212	CRL matching rules	8/12.7.6		US	8-TC3 (3rd)
213	CRL matching rules	8/12.7.6d		US	8-TC3 (3rd)
214	Use of the term “canonical”	8/		Rapporteur	8-DTC6(97) ?
215	Access control to changing RDN			Rapporteur (UK)	Open
216	<i>CertificateAssertion</i>			<i>Australia</i>	<i>rejected</i>
217	Use of Operation and Error Code in Security Parameters	3/7.10		UK	3-TC1 (3rd)
218	Certificate Policy Match	8/12.7.2		UK	8-TC3 (3rd)
219	CA certificate and Basic Constraints	8/		IETF	<i>rejected</i>
220	CRL version number	8/		IETF/ISO rapporteur	8-TC3 (3rd)
221	Conformance for Certificate Extensions	5/9		Rapporteur's meeting	5-TC1 (97 3rd)
222	Policy Mapping	8/12.1 & 12.4.3		US (Santosh and Moses)	8-TC7 (3rd)

DR #	Description of Defect	Part # and clause	DR doc #	Source	Status
223	The naming attribute for an entry should always be shadowed.	9/9.2.2		UK	Open
224	The evaluation of a filter to UNDEFINED needs to be made consistent for the case where access control is/is not present.	3/7.8.2		UK	3-DTC5(3rd)
225	Entry Information Selection and extraAttributes	3/7.6		Australia	Open
226	CA system operational characteristics	8/11.2		Editor	8-DTC8(3rd)
227	Authority Key Identifier format	8/12.2.2.1		US	8-DTC8(3rd)
228	ASN.1 errors in protection feature in X.501	2/15.3.2, P		Editor	1-DTC1(3rd), 2-DTC4(3rd), 3-DTC5(3rd), 4-DTC5(3rd), 5-DTC3(3rd), 9-DTC4(3rd)
229	Wrong references and minor ASN.1 errors in X.501	2/17.4.3, 18.1.2 – 3, B, F, P		Editor	2-DTC3(3rd)
230	The X.501 ASN.1 type Issuer is unknown	2/18.1.2.1		Editor	2-DTC3(3rd)
231	Simple credential ASN.1 error in X.511	3/8.1.1, A		Editor	3-DTC3(3rd)
232	Small ASN.1 editorial errors in X.511	3/7.2, 8.11, 9.3, A		Editor	3-DTC3(3rd)
233	Minor ASN.1 editorials in the import section of X.518 ASN.1 Module	4/ A		Editor	4-DTC3(3rd)
234	Wrong limitation on request decomposition	4/15.3.1		Editor	4-DTC4(3rd)
235	Error in X.518 ASN.1 datatype AccessPointInformation	4/10.8		Editor	4-DTC3(3rd)

DR #	Description of Defect	Part # and clause	DR doc #	Source	Status
236	Editorial mistakes in X.519 ASN.1 modules	5/A, B,C, D, G		Editor	5-DTC2(3rd)
237	ASN.1 errors in X.520	6/5.2.9, 7.6, A		Editor	6-DTC2(3rd)
238	Wrong reference of string types in X.520	6/6.1.1 - 6		Editor	6-DTC2(3rd)
239	Missing imports in X.521 ASN.1 module	7/A		Editor	7-DTC1(3rd)
240	Miscellaneous errors in X.509	A		Editor	8-DTC8(3rd)
241	SerialNumber attribute	6/5.2.9		Rapporteur	6-DTC2(3rd)
242	Size constraint on SET OF and SEQUENCE OF	8/		Rapporteur	2-DTC4(3rd), 3-DTC5(3rd), 4-DTC5(3rd), 5-DTC3(3rd), 9-DTC4(3rd)
243	Miscellaneous errors in X.525	9/2.1, 6, 9.2, 11.1-3, A		Editor	9-DTC2(3rd)
244	Clarification of conformance to criticality	8/see proposal		Sharon	8-DTC9(3rd), 8-DTC1(4th)
245	Duplicate Tags	9/9.2		Erik	9-DTC3(3rd)
246	Miscellaneous errors	6/5.12.2, 5.12.5, 6.8, A, C		Erik	
247	Miscellaneous errors	3/Introduction, 12.4		Erik	3-DTC4(3rd)
248	ASN.1 error in NHOBSubordinateToSuperior	4/25.1.4, D		Erik	4-DTC4(3rd)
249	Miscellaneous errors	3/3.7.4, 7.3.2, 7.7, 7.8.2, 7.8.3		Erik	3-DTC1(4th)
250	Miscellaneous errors	2/various		Erik	2-DTC1(4th)

DR #	Description of Defect	Part # and clause	DR doc #	Source	Status
251	AdministrativeLimit	4/16.1.4.4, 6/5.12.1		Erik	4-DTC1(4th), 6-DTC1(4th)
252	ASN.1 errors	10/A.9		Erik	10-DTC1(3rd)
253	Hierarchy selections problems	4/19.3.3.2.4 (old 19.3.3.2.1. 6/5.12.		Erik	4-DTC1(4th), 6-DTC1(4th)
254	chainingRequired component misplaced	4/10.4, 10.8, A		Erik	4-DTC1(4th)
255	Inconsistency in CONTENT-RULE information object class	2/12.7.2		Erik	2-DTC4(3rd)
256	Populating reverse element	8/		Sharon	8-DTC9(3rd), 8-DTC1(4th)
257	Renaming forward & reverse	8/		Sharon	8-DTC9(3rd), 8-DTC1(4th)
258	Certificate path loops	8/		Sharon	8-DTC9(3rd), 8-DTC1(4th)
259	PartialOutcomeQualifier and ContextCombination errors	4 th 2/13.6.1, 16.10		Erik	2-DTC1(4th)
260	Ambiguity in AttributeTypeAndDistinguishedValue	2/9.3, B		Erik	2-DTC4(3rd)
261	CommonResults is wrong data dtype	2/26.5		Erik	2-DTC4(3rd)
262	Signal hierarchy selection not supported	4 th 3/13.3		Erik	3-DTC1(4th)
263	Incorrect clause references; test does not match ASN.1 for SimpleCredentials	3/7.1, 8.12		Erik	3-DTC5(3rd)
264	Optionally signal chaining; search constrained by service specific administrative area	4 th 4/16.1.4.2, 19.3.2.2.4		Erik	4-DTC1(4th)

DR #	Description of Defect	Part # and clause	DR doc #	Source	Status
265	Various errors	4/14.5, 15.3.1, 19.3.1.1.3		Erik	4-DTC5(3rd)
266	Invalid updates of conformance clause	5/9		Erik	5-DTC3(3rd)
267	Various errors	2/14.7.3, 14.7.10, 25.2, 22.2.1.2		Erik	2-DTC4(3rd)
268	noSubtypeSelection in Entry information selection	4 th 3/7.6		Erik	3-DTC1(4th)
269	Error in MatchingRuleDescription data type	2/12.5.2 b), 14.7.3		Erik	2-DTC4(3rd)
270	Data types in attribute syntaxes and matching rule assertion syntaxes	6/5.8.1, 6.1.1, 6.1.10, 6.5.3.1		Erik	6-DTC3(3rd), 6-DTC1(4th)
271	Use of term "packet"	4 th 5/9.7		Erik	5-DTC1(4th)
272	Certification Path Length	3 rd 8/12.4.2.1 & 4 th 8/8.4.2, 15.5.2.1		Sharon	8-DTC10(3rd), 8-DTC2(4th)
273	Name constraints conformance	3 rd 12.4.2.2 4 th 8.4.2.2		Sharon	8-DTC10(3rd), 8-DTC2(4th)
274	Attribute Certificate version	4 th 12.1, A		Sharon	8-DTC2(4th) vote for confirmation of solution already incorporated into published 4th edition
275	ExtendedKeyUsage	3 rd 8/12.2.2.4 & 4 th 8/8.4.2.1,		Sharon	8-DTC10(3rd), 8-DTC2(4th)

DR #	Description of Defect	Part # and clause	DR doc #	Source	Status
		15.5.2.1			
276	Use of anyPolicy in self issued certificates	4 th 8/8.1.5, 8.4.2.4, 10.5		Sharon	8-DTC2(4th)
277	Requires explicit policy skip certificates value	3 rd 8/12.4.2.3 & 4 th 8/8.4.2.3, 10		Sharon	8-DTC10(3rd), 8-DTC2(4th)
278	FreshestCRL extension	4 th 8/8.6.2.6		Sharon	8-DTC2(4th)
279	Certification path syntaxes	4 th 8/7, 11.1.6, 11.2.10, 11.3.9		Sharon/Mullan	8-DTC2(4th)
280	IDP extension: CA/AA split in CRLs	4 th 8/8.6.2.2		Sharon/Polk/Housley/Cooper	8-DTC3(4th)
281	FreshestCRL extension	4 th 8/8.6.2.6 and B.5.1.4		Cooper	8-DTC3(4th)
282	Invalid references to 4 th edition of X.519/9594-5	4 th 8/7, 7.3 & 12.1		Sharon	8-DTC3(4th)
283	Additional IDM-PROTOCOL needed for the second DISP Application Context	To be written		Anthony Hodson	
284	CRL Scope deprecation	4 th 8/8.5.2.5		Sharon	8-DTC4(4th)
285	Self-signed certs & path processing	3 rd 8/12.4.3 4 th 8/10.5.1-2		Sharon	8-DTC4(4th) 8-DTC11(3rd)
286	AC Exact Match discrepancy	4 th 8/17.3.1 & A		Sharon / Chadwick	8-DTC4(4th)
287	BitStringMatch rule & trailing bits	3 rd 6/6.2.4		Kesterson /	6-DTC4(3rd), 6-DTC3(4th)

DR #	Description of Defect	Part # and clause	DR doc #	Source	Status
		4 th 6/6.2.4		Legg	
288	Matching rule for facsimile telephone number	3 rd 6/5.7.4 4 th 6/5.7.4		Kesterson / Chadwick	6-DTC4(3rd), 6-DTC3(4th)
289	Certification Path Processing	4 th 8/10.5.4 3 rd 8/		Sharon/FPKI	8-DTC5(4th) 3rd ?
290	telephoneNumber syntax and matching rule (including substring)	To be written		Skip/Geneva2002	approved
291	Remove “encipherment” from definition of public-key certificate	3 rd 8/3.3.3 4 th 8/3.3.44 To be written		Sharon/Geneva2002	approved
292	Non-commutative matching rule problem	To be written		Kesterson/Legg/Geneva2002	
293	Filtermatch reveals presence of entry without permission	To be written		Chadwick/Legg/Geneva2002	
294	Replace specification of distinguished encoding rules with reference to ASN.1 DER & constrain extensibility for BIT STRING	3 rd 8/ 4 th 8/ 3 rd & 4 th 5/ To be written		Kesterson/Geneva2002	
295	Last day of month and year for TimeSpecification	3 rd 6/ 4 th 6/ To be written		Kesterson/Houlsley/Geneva2002	Approved
296	Default distribution point	4 th 8/ To be written		Cooper/Geneva2002	8-DTC5(4th) (TC3)

DR #	Description of Defect	Part # and clause	DR doc #	Source	Status
297	Remove bullet F which requires creation of full CRLs	3 rd 8/12.6.1 To be written		Sharon/Geneva 2002	8-DTC12(3rd) (TC5)
298	Clarify that the complete set of partitioned CRLs must cover the same set of certificates that would be covered by the full CRL	3 rd 8/ 4 th 8/ To be written		Sharon/Geneva 2002	8-DTC5(4th)
299	Clarify digitalSignature and NonRepudiation in the Key Usage extension	3 rd 8/12.2.2.3 4 th 8/8.2.2.3		Sharon/NIST2 002	8-DTC13(3rd), 8-DTC6(4th)
300	Basic Constraints requirement for path processing	4 th 8/10.5.1		Sharon/NIST2 002	8-DTC6(4th)
301	Base CRL window	4 th 8/B.5.2		Sharon/NIST2 002	8-DTC6(4th)
302	Skip Certs in policy constraints	4 th 8/8.4.2.3		SharonEmail London 2001	8-DTC7(4th) tbw laura
303	Attribute value preserved as supplied	3 rd 2/ 8/ 4 th 2/ 8.5. 8.8.1 6/6.1		Sharon Email London 2003 written by Hoyt	
304	old RSA encryption algorithm OID	3 rd 8/H 4 th 8/F		Sharon Email 14 March 03	8-DTC14(3rd) 8-DTC7(4th) tbw laura
305	IDP Extension	4 th 8/8.6.2.2		Sharon Email 12 March 03	8-DTC7(4th) tbw David Cooper
306	ASN.1 Error introduced by DR255	3 rd 2/12.7.2, I.4 4 th 2/13.8.2, K.4		Erik Email 1 Feb 04	2-DTC5(3rd) 2-DTC2(4th) Erik

DR #	Description of Defect	Part # and clause	DR doc #	Source	Status
307	Incorrect clause cross reference	4 th 4/14.2		Erik Email 9 March 04	4-DTC2(4th) Erik
308	validity in SimpleCredentials missing OPTIONAL	3 rd 3/8.1.1 Cor 2 4 th 3/8.1.1		Erik Email 12 March 04	3-DTC6(3rd) 3-DTC2(4th) Erik
309	Mandating that unavailableCriticalExtension be returned if extension not supported	3 rd 3/7.3.1 4 th 3/7.3.1		UK ballot #5 October 2004	3-DTC6(3rd) 3-DTC2(4th) Erik
310	Unrecognized CRL and CRL entry extensions	4 th 8/7.3 Note 4		Sharon email 9 March 2005	
311	Differences between crl and crl entry extensions	4 th 8/7.3 Note 5		Sharon email 9 March 2005	
312	ASN.1 errors in ITU-T Rec. X.501 ISO/IEC 9594-2 and ITU-T Rec. X.520 ISO/IEC 9594-6	4 th 2/13.6.2 4 th 6/ 6.8		Erik email 19 April 2005	
313	ServiceProblem error in ITU-T Rec. X.511 ISO/IEC 9594-3 and ITU-T Rec. X.520 ISO/IEC 9594-6	4 th 3/12.6 4 th 6/6.8		Erik email 19 April 2005	