COVERING NOTE

GENERAL SECRETARIAT OF THE INTERNATIONAL TELECOMMUNICATION UNION

Geneva, 7 February 2013

ITU – TELECOMMUNICATION STANDARDIZATION SECTOR

Subject: Erratum 1 (02/2013) to Recommendation ITU-T H.235.6 (03/2009), *H.323 security: Voice encryption profile with native H.235/H.245 key management*

Table 4 does not reflect correctly the exponents in the formula for calculating prime numbers.

Modify Table 4 in clause 8.5 as shown below:

Table 4 – Diffie-Hellman groups

Encryption Algorithm OID	DH-OID	D-H group description
"X", "X1" (RC2-compatible), "Y", "Y1" (DES)	"DHdummy"	Mod-P, any suitable 512-bit prime
"Z", "Z1" (triple-DES), "Z2", "Z3" (AES)	"DH1024"	Mod-P, 1024-bit prime Prime = $2^{1024} - 2^{960} - 1 + 2^{64} \times \{ [2^{894} \text{ pi}] + 129093 \}$ ~~Prime = 21024 – 2960 – 1 + 264 × { [2894 pi] + 129093 }~~ Hexadecimal value = FFFFFFFF FFFFFFFF C90FDAA2 2168C234 C4C6628B 80DC1CD1 29024E08 8A67CC74 020BBEA6 3B139B22 514A0879 8E3404DD EF9519B3 CD3A431B 302B0A6D F25F1437 4FE1356D 6D51C245 E485B576 625E7EC6 F44C42E9 A637ED6B 0BFF5CB6 F406B7ED EE386BFB 5A899FA5 AE9F2411 7C4B1FE6 49286651 ECE65381 FFFFFFFF FFFFFFFF Generator (Note) = 2
"Z", "Z1" (triple-DES), "Z2", "Z3" (AES)	"DH1536"	Mod-P, 1536-bit prime Prime = $2^{1536} - 2^{1472} - 1 + 2^{64} \times \{ [2^{1406} \text{ pi}] + 741804 \}$ ~~Prime = 21536 – 21472 – 1 + 264 × { [21406 pi] + 741804 }~~ Hexadecimal value = FFFFFFFF FFFFFFFF C90FDAA2 2168C234 C4C6628B 80DC1CD1 29024E08 8A67CC74 020BBEA6 3B139B22 514A0879 8E3404DD EF9519B3 CD3A431B 302B0A6D F25F1437 4FE1356D 6D51C245

Table 4 – Diffie-Hellman groups

Encryption Algorithm OID	DH-OID	D-H group description
		E485B576 625E7EC6 F44C42E9 A637ED6B 0BFF5CB6 F406B7ED EE386BFB 5A899FA5 AE9F2411 7C4B1FE6 49286651 ECE45B3D C2007CB8 A163BF05 98DA4836 1C55D39A 69163FA8 FD24CF5F 83655D23 DCA3AD96 1C62F356 208552BB 9ED52907 7096966D 670C354E 4ABC9804 F1746C08 CA237327 FFFFFFFF FFFFFFFF Generator (Note) = 2
"Z2", "Z3", "Z4", "Z5" (AES)	"DH2048"	Mod-P, 2048-bit prime Prime = $2^{2048} - 2^{1984} - 1 + 2^{64} \times \{ [2^{1918} \text{ pi}] + 124476 \}$ ~~Prime = 22048 – 21984 – 1 + 264 × { [21918 pi] + 124476 }~~ Hexadecimal value = FFFFFFFF FFFFFFFF C90FDAA2 2168C234 C4C6628B 80DC1CD1 29024E08 8A67CC74 020BBEA6 3B139B22 514A0879 8E3404DD EF9519B3 CD3A431B 302B0A6D F25F1437 4FE1356D 6D51C245 E485B576 625E7EC6 F44C42E9 A637ED6B 0BFF5CB6 F406B7ED EE386BFB 5A899FA5 AE9F2411 7C4B1FE6 49286651 ECE45B3D C2007CB8 A163BF05 98DA4836 1C55D39A 69163FA8 FD24CF5F 83655D23 DCA3AD96 1C62F356 208552BB 9ED52907 7096966D 670C354E 4ABC9804 F1746C08 CA18217C 32905E46 2E36CE3B E39E772C 180E8603 9B2783A2 EC07A28F B5C55DF0 6F4C52C9 DE2BCBF6 95581718 3995497C EA956AE5 15D22618 98FA0510 15728E5A 8AACAA68 FFFFFFFF FFFFFFFF Generator (Note) = 2
"Z2", "Z3", "Z4", "Z5" (AES)	"DH3072"	Mod-P, 3072-bit prime Prime = $2^{3072} - 2^{3008} - 1 + 2^{64} \times \{ [2^{2942} \text{ pi}] + 1690314 \}$ ~~Prime = 23072 – 23008 – 1 + 264 × { [22942 pi] + 1690314 }~~ Hexadecimal value = FFFFFFFF FFFFFFFF C90FDAA2 2168C234 C4C6628B 80DC1CD1 29024E08 8A67CC74 020BBEA6 3B139B22 514A0879 8E3404DD EF9519B3 CD3A431B 302B0A6D F25F1437 4FE1356D 6D51C245 E485B576 625E7EC6 F44C42E9 A637ED6B 0BFF5CB6 F406B7ED EE386BFB 5A899FA5 AE9F2411 7C4B1FE6 49286651 ECE45B3D C2007CB8 A163BF05 98DA4836 1C55D39A 69163FA8 FD24CF5F 83655D23 DCA3AD96 1C62F356 208552BB 9ED52907 7096966D 670C354E 4ABC9804 F1746C08 CA18217C 32905E46 2E36CE3B E39E772C 180E8603 9B2783A2 EC07A28F B5C55DF0 6F4C52C9 DE2BCBF6 95581718 3995497C EA956AE5 15D22618 98FA0510 15728E5A 8AAAC42D AD33170D 04507A33 A85521AB DF1CBA64 ECFB8504 58DBEF0A 8AEA7157 5D060C7D B3970F85 A6E1E4C7 ABF5AE8C DB0933D7 1E8C94E0 4A25619D CEE3D226 1AD2EE6B F12FFA06 D98A0864 D8760273 3EC86A64 521F2B18 177B200C BBE11757 7A615D6C 770988C0 BAD946E2 08E24FA0 74E5AB31 43DB5BFC E0FD108E 4B82D120 A93AD2CA FFFFFFFF FFFFFFFF Generator (Note) = 2

Table 4 – Diffie-Hellman groups

Encryption Algorithm OID	DH-OID	D-H group description
"Z2", "Z3", "Z4", "Z5" (AES)	"DH4096"	Mod-P, 4096-bit prime Prime = $2^{4096} - 2^{4032} - 1 + 2^{64} \times \{ [2^{3966} \text{ pi}] + 240904 \}$ ~~Prime = 24096 – 24032 – 1 + 264 × { [23966 pi] + 240904 }~~ Hexadecimal value = FFFFFFFF FFFFFFFF C90FDAA2 2168C234 C4C6628B 80DC1CD1 29024E08 8A67CC74 020BBEA6 3B139B22 514A0879 8E3404DD EF9519B3 CD3A431B 302B0A6D F25F1437 4FE1356D 6D51C245 E485B576 625E7EC6 F44C42E9 A637ED6B 0BFF5CB6 F406B7ED EE386BFB 5A899FA5 AE9F2411 7C4B1FE6 49286651 ECE45B3D C2007CB8 A163BF05 98DA4836 1C55D39A 69163FA8 FD24CF5F 83655D23 DCA3AD96 1C62F356 208552BB 9ED52907 7096966D 670C354E 4ABC9804 F1746C08 CA18217C 32905E46 2E36CE3B E39E772C 180E8603 9B2783A2 EC07A28F B5C55DF0 6F4C52C9 DE2BCBF6 95581718 3995497C EA956AE5 15D22618 98FA0510 15728E5A 8AAAC42D AD33170D 04507A33 A85521AB DF1CBA64 ECFB8504 58DBEF0A 8AEA7157 5D060C7D B3970F85 A6E1E4C7 ABF5AE8C DB0933D7 1E8C94E0 4A25619D CEE3D226 1AD2EE6B F12FFA06 D98A0864 D8760273 3EC86A64 521F2B18 177B200C BBE11757 7A615D6C 770988C0 BAD946E2 08E24FA0 74E5AB31 43DB5BFC E0FD108E 4B82D120 A9210801 1A723C12 A787E6D7 88719A10 BDBA5B26 99C32718 6AF4E23C 1A946834 B6150BDA 2583E9CA 2AD44CE8 DBBBC2DB 04DE8EF9 2E8EFC14 1FBECAA6 287C5947 4E6BC05D 99B2964F A090C3A2 233BA186 515BE7ED 1F612970 CEE2D7AF B81BDD76 2170481C D0069127 D5B05AA9 93B4EA98 8D8FDDC1 86FFB7DC 90A6C08F 4DF435C9 34063199 FFFFFFFF FFFFFFFF Generator (Note) = 2
NOTE – The generator is used to generate the DH token.		