Global Encryption

Poly ATA 400 series

Completed by: Kevin Fang Date: 6/30/2023

Product Name and Model(s)	Poly ATA402, Poly ATA400
OS and Version	Linux 4.9.221
Product SW revision	4.0.1.6480

Application	Encryption Function	Description	Protocol Used	Encryption					Status (Russia)
				Cipher/Crypto Suites (SSL/TLS cipher suite code)	Sym Alg (Key len)	Asym Alg (Key len)	Key Exc Alg (Group Size)	Hash Alg (Size)	
Provisioning (client mode), Local WebUI (Server mode)	Confidentiality Integrity		HTTPS	ECDHE-RSA-AES256-GCM-SHA384 ECDHE-ECDSA-AES256-GCM-SHA384 ECDHE-RSA-AES256-SHA384 ECDHE-ECDSA-AES256-SHA384 ECDHE-RSA-AES256-SHA ECDHE-ECDSA-AES256-SHA SRP-DSS-AES-256-CBC-SHA SRP-RSA-AES-256-CBC-SHA SRP-AES-256-CBC-SHA DH-DSS-AES256-GCM-SHA384 DHE-DSS-AES256-GCM-SHA384 DH-RSA-AES256-GCM-SHA384 DHE-RSA-AES256-GCM-SHA384 DHE-RSA-AES256-SHA256 DHE-DSS-AES256-SHA256 DH-RSA-AES256-SHA256 DH-DSS-AES256-SHA256 DHE-RSA-AES256-SHA DHE-DSS-AES256-SHA DH-RSA-AES256-SHA DH-DSS-AES256-SHA ECDH-RSA-AES256-GCM-SHA384 ECDH-ECDSA-AES256-GCM-SHA384 ECDH-RSA-AES256-SHA384 ECDH-ECDSA-AES256-SHA384 ECDH-RSA-AES256-SHA ECDH-ECDSA-AES256-SHA AES256-GCM-SHA384 AES256-SHA256	AESGCM (256) AES(256) AESGCM(128) AES(128) RC4(128) 3DES(168) DES(56)	RSA ECDSA DSS SRP ECDH PSK	ECDH SRP DH RSA PSK	SHA256 SHA1 SHA384 AEAD MD5	N/A

Owner: I Jennings

Global Encryption

				AES256-SHA PSK-AES256-CBC-SHA ECDHE-RSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES128-GCM-SHA256 ECDHE-RSA-AES128-SHA256 ECDHE-ECDSA-AES128-SHA256 ECDHE-RSA-AES128-SHA ECDHE-ECDSA-AES128-SHA SRP-DSS-AES-128-CBC-SHA SRP-RSA-AES-128-CBC-SHA SRP-AES-128-CBC-SHA DH-DSS-AES128-GCM-SHA256 DHE-DSS-AES128-GCM-SHA256 DH-RSA-AES128-GCM-SHA256 DHE-RSA-AES128-GCM-SHA256 DHE-RSA-AES128-SHA256 DHE-DSS-AES128-SHA256 DH-RSA-AES128-SHA256 DH-DSS-AES128-SHA256 DHE-RSA-AES128-SHA DHE-DSS-AES128-SHA DH-RSA-AES128-SHA DH-DSS-AES128-SHA ECDH-RSA-AES128-GCM-SHA256 ECDH-ECDSA-AES128-GCM-SHA256 ECDH-RSA-AES128-SHA256 ECDH-ECDSA-AES128-SHA256 ECDH-RSA-AES128-SHA ECDH-ECDSA-AES128-SHA AES128-GCM-SHA256 AES128-SHA256 AES128-SHA PSK-AES128-CBC-SHA ECDHE-RSA-RC4-SHA ECDHE-ECDSA-RC4-SHA ECDH-RSA-RC4-SHA ECDH-ECDSA-RC4-SHA RC4-SHA RC4-MD5 PSK-RC4-SHA ECDHE-RSA-DES-CBC3-SHA ECDHE-ECDSA-DES-CBC3-SHA SRP-DSS-3DES-EDE-CBC-SHA SRP-RSA-3DES-EDE-CBC-SHA SRP-3DES-EDE-CBC-SHA EDH-RSA-DES-CBC3-SHA EDH-DSS-DES-CBC3-SHA DH-RSA-DES-CBC3-SHA DH-DSS-DES-CBC3-SHA ECDH-RSA-DES-CBC3-SHA ECDH-ECDSA-DES-CBC3-SHA DES-CBC3-SHA					

				PSK-3DES-EDE-CBC-SHA					
SRTP	Confidentiality			AES_CM_128, AES_CM_128_HMAC_SHA1_32 AES_CM_128_HMAC_SHA1_80 AES_CM_192_HMAC_SHA1_32 AES_CM_192_HMAC_SHA1_80 AES_CM_256_HMAC_SHA1_32 AES_CM_256_HMAC_SHA1_80 AES_192_CM_HMAC_SHA1_32 AES_192_CM_HMAC_SHA1_80 AES_256_CM_HMAC_SHA1_32 AES_256_CM_HMAC_SHA1_80 AEAD_AES_128_GCM AEAD_AES_256_GCM	AES(128) AES(192) AES(256)	NA	NA	NA	N/A
SIP over TLS	Confidentiality		TLS 1.2	ECDHE-RSA-AES256-GCM-SHA384-TLSv1.2 ECDHE-ECDSA-AES256-GCM-SHA384-TLSv1.2 ECDHE-RSA-AES256-SHA384-TLSv1.2 ECDHE-ECDSA-AES256-SHA384-TLSv1.2 DHE-DSS-AES256-GCM-SHA384-TLSv1.2 DHE-RSA-AES256-GCM-SHA384-TLSv1.2 DHE-RSA-AES256-SHA256-TLSv1.2 DHE-DSS-AES256-SHA256-TLSv1.2 ECDH-RSA-AES256-GCM-SHA384-TLSv1.2 ECDH-ECDSA-AES256-GCM-SHA384-TLSv1.2 ECDH-RSA-AES256-SHA384-TLSv1.2 ECDH-ECDSA-AES256-SHA384-TLSv1.2 AES256-GCM-SHA384-TLSv1.2 AES256-SHA256-TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256-TLSv1.2 ECDHE-ECDSA-AES128-GCM-SHA256-TLSv1.2 ECDHE-RSA-AES128-SHA256-TLSv1.2 ECDHE-ECDSA-AES128-SHA256-TLSv1.2 DHE-DSS-AES128-GCM-SHA256-TLSv1.2 DHE-RSA-AES128-GCM-SHA256-TLSv1.2 DHE-RSA-AES128-SHA256-TLSv1.2 DHE-DSS-AES128-SHA256-TLSv1.2 ECDH-RSA-AES128-GCM-SHA256-TLSv1.2 ECDH-ECDSA-AES128-GCM-SHA256-TLSv1.2 ECDH-RSA-AES128-SHA256-TLSv1.2 ECDH-ECDSA-AES128-SHA256-TLSv1.2 AES128-GCM-SHA256-TLSv1.2 AES128-SHA256-TLSv1.2	AESGCM (256) AES(256) AESGCM(128) AES(128)	RSA ECDSA DSS ECDH	ECDH DH RSA	SHA256 SHA384 AEAD	N/A
SIP Authentication	Authentication	Provides authentication of the product's SIP user agent credentials to the	Digest (RFC 2617)	NA	NA	NA	NA NA	MD5 (128)	NA

Global Encryption

		SIP Proxy/Registrar							
Local Web Server	Authentication	HTTP Digest	Digest (RFC 2617)	NA	NA	NA	NA	MD5 (128)	NA
LDAP Directory Client	Authentication Confidentiality Integrity	Provides enterprise directory information allowing product to add participants to conferences by name from an enterprise directory server.	TLS 1.2,	ECDHE-RSA-AES256-GCM-SHA384-TLSv1.2 ECDHE-ECDSA-AES256-GCM-SHA384-TLSv1.2 ECDHE-RSA-AES256-SHA384-TLSv1.2 ECDHE-ECDSA-AES256-SHA384-TLSv1.2 DHE-DSS-AES256-GCM-SHA384-TLSv1.2 DHE-RSA-AES256-GCM-SHA384-TLSv1.2 DHE-RSA-AES256-SHA256-TLSv1.2 DHE-DSS-AES256-SHA256-TLSv1.2 ECDH-RSA-AES256-GCM-SHA384-TLSv1.2 ECDH-ECDSA-AES256-GCM-SHA384-TLSv1.2 ECDH-RSA-AES256-SHA384-TLSv1.2 ECDH-ECDSA-AES256-SHA384-TLSv1.2 AES256-GCM-SHA384-TLSv1.2 AES256-SHA256-TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256-TLSv1.2 ECDHE-ECDSA-AES128-GCM-SHA256-TLSv1.2 ECDHE-RSA-AES128-SHA256-TLSv1.2 ECDHE-ECDSA-AES128-SHA256-TLSv1.2 DHE-DSS-AES128-GCM-SHA256-TLSv1.2 DHE-RSA-AES128-GCM-SHA256-TLSv1.2 DHE-RSA-AES128-SHA256-TLSv1.2 DHE-DSS-AES128-SHA256-TLSv1.2 ECDH-RSA-AES128-GCM-SHA256-TLSv1.2 ECDH-ECDSA-AES128-GCM-SHA256-TLSv1.2 ECDH-RSA-AES128-SHA256-TLSv1.2 ECDH-ECDSA-AES128-SHA256-TLSv1.2 AES128-GCM-SHA256-TLSv1.2 AES128-SHA256-TLSv1.2	AESGCM (256) AES(256) AESGCM(128) AES(128)	RSA ECDSA DSS ECDH	ECDH DH RSA	SHA256 SHA384 AEAD	N/A
802.1X Supplicant	Authentication Confidentiality Integrity	Allows product to authenticate to a Layer 2 switch that is using 802.1X for authentication	EAP-MD5 (RFC 3748) TLS 1.2,1.1,1.0	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c) TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024) TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) TLS_DH_DSS_WITH_AES_256_GCM_SHA384 (0x00a5) TLS_DHE_DSS_WITH_AES_256_GCM_SHA384 (0x00a3) TLS_DH_RSA_WITH_AES_256_GCM_SHA384 (0x00a1) TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x009f) TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x006b) TLS_DHE_DSS_WITH_AES_256_CBC_SHA256 (0x006a) TLS_DH_RSA_WITH_AES_256_CBC_SHA256 (0x0069) TLS_DH_DSS_WITH_AES_256_CBC_SHA256 (0x0068) TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039) TLS_DHE_DSS_WITH_AES_256_CBC_SHA (0x0038) TLS_DH_RSA_WITH_AES_256_CBC_SHA (0x0037) TLS_DH_DSS_WITH_AES_256_CBC_SHA (0x0036) TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384 (0xc032)	AES-GCM (256) AES-CBC (256) AES-GCM (128) AES-CBC (128) RC4 (128) 3DES_EDE_CBC	RSA (up to 16384) ECDSA (up to 571) DSA (up to 10000)	RSA (up to 16384) DH (up to 10000) DHE (up to 10000) ECDHE (up to 571) ECDH (up to 571)	SHA2 (384) SHA2 (256) SHA1 (160) MD5 (128)	N/A

Owner: I Jennings

Global Encryption

				TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02e) TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384 (0xc02a) TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384 (0xc026) TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f) TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005) TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d) TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d) TLS_RSA_WITH_AES_256_CBC_SHA (0x0035) TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b) TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023) TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) TLS_DH_DSS_WITH_AES_128_GCM_SHA256 (0x00a4) TLS_DHE_DSS_WITH_AES_128_GCM_SHA256 (0x00a2) TLS_DH_RSA_WITH_AES_128_GCM_SHA256 (0x00a0) TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x009e) TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x0067) TLS_DHE_DSS_WITH_AES_128_CBC_SHA256 (0x0040) TLS_DH_RSA_WITH_AES_128_CBC_SHA256 (0x003f) TLS_DH_DSS_WITH_AES_128_CBC_SHA256 (0x003e) TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033) TLS_DHE_DSS_WITH_AES_128_CBC_SHA (0x0032) TLS_DH_RSA_WITH_AES_128_CBC_SHA (0x0031) TLS_DH_DSS_WITH_AES_128_CBC_SHA (0x0030) TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256 (0xc031) TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02d) TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256 (0xc029) TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 (0xc025) TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e) TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004) TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c) TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c) TLS_RSA_WITH_AES_128_CBC_SHA (0x002f) TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011) TLS_ECDHE_ECDSA_WITH_RC4_128_SHA (0xc007) TLS_ECDH_RSA_WITH_RC4_128_SHA (0xc00c) TLS_ECDH_ECDSA_WITH_RC4_128_SHA (0xc002) TLS_RSA_WITH_RC4_128_SHA (0x0005) TLS_RSA_WITH_RC4_128_MD5 (0x0004) TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012) TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA (0xc008) TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x0016) TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA (0x0013) TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA (0x0010) TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA (0x000d) TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA (0xc00d) TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA (0xc003) TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a) TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)					

Owner: I Jennings

Global Encryption

WPA Supplicant	Authentication Confidentiality Integrity	For EAP extension over WPA/WPA2 see 801.1X supplicant section.	802.11 WEP/WPA WPA2 TLS1.0/1.1/ 1.2	TKIP CCMP	AES(256)/PSK	N/A	N/A	SHA1	N/A