Annexes – My listing of Cipher Suites and AKM numbers

RSN Structure – Cipher Suites

OUI	Suite	Description	GTK	PTK	IGTK
IEEE (00:0F:AC)	0	Use the Group Cipher Suite	N	Y	N
	1	WEP-40	Y	N	N
	2	TKIP	Y	Y	N
	3	WRAP (Should not being implemented; Originally proposed for 802.11i-2004; Based on AES-OCB, but not released because of IPR issues)			
	4	CCMP 128	Y	Y	N
	5	WEP-104	Y	N	N
	6	BIP-CMAC-128	N	N	Y
	7	Group addressed traffic not allowed	Y	N	N
	8	GCMP-128	Y	Y	N
	9	GCMP-256	Y	Y	N

RSN Structure – Cipher Suites (cont.)

OUI	Suite	Description	GTK	PTK	IGTK
IEEE (00:0F:AC)	10	CCMP-256	Y	Y	N
	11	BIP-GMAC-128	N	N	Y
	12	BIP-GMAC-256	N	N	Y
	13	BIP-CMAC-256	N	N	Y
China Broadcast Wireless IP Standard Group (00:14:72)	0	Reserved			
	1	WAI Certificate or SMS4			
	2	WAI PSK			
Cisco (00:40:96)	0	CKIP			
	1	CKIP-CMIC			
	2	CMIC			
	255	KRK			

RSN Structure – Authentication Key Management

OUI	Suite	Handshake	Key Derivation	Authentication	Support of Fast Transition
IEEE (00:0F:AC)	0	Reserved (Deprecated crypto using ARC4 and MD5)			
	1	WPA	WPA's PRF with SHA-1	802.1x	No
	2	WPA	WPA's PRF with SHA-1	PSK	No
	3	WPA	WPA's PRF with SHA-256	802.1x	Yes
	4	WPA	WPA's PRF with SHA-256	PSK	Yes
	5	WPA	WPA's PRF with SHA-256	802.1x	No
	6	WPA	WPA's PRF with SHA-256	PSK	No

RSN Structure – Authentication Key Management (2)

OUI	Suite	Handshake	Key Derivation	Authentication	Support of Fast Transition
IEEE (00:0F:AC)	7	TDLS (Wi-Fi Direct)			
	8	SAE	SHA-2	PSK	No
	9	SAE	SHA-2	PSK	Yes
	10	AP-PEER-KEY			
	11	WPA Note: Uses NSA Suite-B EAP method *Deprecated!*	WPA's PRF with SHA-256	802.1x	No
	12	WPA Note: Uses CNSA EAP method Note: KCK is 192b long and KEK 256b	WPA's PRF with SHA-384	802.1x	No

RSN Structure – Authentication Key Management (3)

OUI	Suite	Handshake	Key Derivation	Authentication	Support of Fast Transition
IEEE (00:0F:AC)	13	WPA Note: KCK is 192b long and KEK 256b	WPA's PRF with SHA-384	802.1x	Yes
	14	Fast Initial Link Setup Using AES-SIV-256	SHA-256	802.1x	No
	15	Fast Initial Link Setup Using AES-SIV-512	SHA-384	802.1x	No
	16	Fast Initial Link Setup Using AES-SIV-256 And AES-128-CMAC	SHA-256	802.1x	Yes
	17	Fast Initial Link Setup Using AES-SIV-512 And AES-256-CMAC	SHA-384	802.1x	Yes

RSN Structure – Authentication Key Management (4)

OUI	Suite	Handshake	Key Derivation	Authentication	Support of Fast Transition
IEEE (00:0F:AC)	18	OWE May use AES with 128, 192 and 256b. Uses SHA-2			
	19	WPA Note: KCK is 192b long and KEK 256b	WPA's PRF with SHA-384	PSK	Yes
	20	WPA Note: KCK is 192b long and KEK 256b	WPA's PRF with SHA-384	PSK	No
	21	PASN (Do not protect EAPOL frames)	SHA-256	*N/A*	Yes

RSN Structure – Authentication Key Management (5)

OUI	Suite	Handshake	Key Derivation	Authentication	Support of Fast Transition
IEEE (00:0F:AC)	22	WPA Note: KCK is 192b long and KEK 256b	SHA-384	802.1x	Yes
	23	WPA Note: KCK is 192b long and KEK 256b	SHA-384	802.1x	No
	24	SAE But with a PSK of 384b	SHA-2	PSK	No
	25	SAE But with a PSK of 384b	SHA-2	PSK	Yes
Cisco (00:40:96)	0	CCKM			

RSN Structure – Authentication Key Management (6)

OUI	Suite	Handshake	Key Derivation	Authentication	Support of Fast Transition
Wi-Fi Alliance® (50:6F:9A)	1		OSEN		
	2		DPP		