

EPHEMERAL DIFFIE-HELLMAN OVER COSE (EDHOC)

••••••••••

IETF99 ACE, JUL 17 2017 SELANDER, MATTSSON, PALOMBINI DRAFT-SELANDER-ACE-COSE-ECDHE-07

SEVERAL REVIEWS



• Presented for CFRG at Eurocrypt by Jim Schaad

- Security reviews by Dan Harkins and Ilari Liusvaara
 - All comments taken into account in -07

"This is a very well-written draft and I am happy to see SIGMA being applied to every layer of the stack".

Dan Harkins

NEW IN VERSION -06



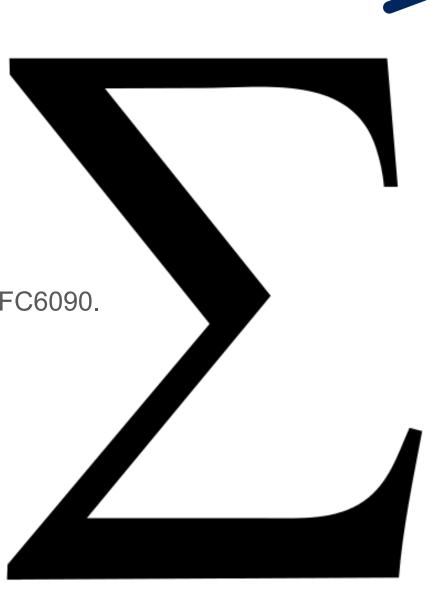
- Changes:
 - Error Message (MSG_TYPE = 0)
 - Verification of common preferred ECDH curve
 - Renamed "extension" → "opaque application data"
 - Removed encryption and integrity protection in message_1
 - Application unique strings now in field AlgorithmID.
 - Default CoAP Uri-Path: "/.well-known/edhoc"
 - PSK Chaining



NEW IN VERSION -07



- Changes:
 - AlgorithmID is a tstr
 - Better explanation of session identifiers
 - Compact representation of EC2 points according to RFC6090.
 - ID_V, CERT_V replaced with ID_V, HINT_ID_V sent in the protected field of COSE_SIG_V.
 - Point validation of EC2 points



IMPLEMENTATIONS

• One implementation by Jim Schaad.

• A second implementation by SICS (work-in-progress).

• Test vectors to be added after interop testing.

	2	0 8		2	~	4	5	10	-	00	07
D	FICATION	OF	-	2	3	47	5 5	9 9	-	00	
-40003	CAT	OR	-	2 2	~	4	5	9	-	00	07
2	-	0 %		2	~	1	555	9999999	-	00	0
÷.		0 10	-	2	~	-7	5 5		-	00	
		0 0	-	2 2	33	4	102	6	-	8 8 3 8	G
		002		2 3	3	-3	5	6	-	00	đ
		0 1	-	2	~	4	LO	6	~	00	J
		0 2	-	2	3	-	22	9 9	-	00	0
		0 0		23	53	4	10	6	-	8 8 8 8	a
		00	-	2	3	-	5	0	-	00	đ
		0 3	-	2	6.3	4	5	60	-	00	0
		0 8	-	2	3	4	22	6	-	00	0
		0 0	_	2	3	-	5	6	-	00	0
		0 3	-	2	~	-	5	0	-	00	a
		0 5	-	2	~ ~	45	5	60	-	00	0
		0 9		2	3		5	0	2	00	0
		0 8	_	2	3	4	10	6	-	00	0
		0 5	-	3	3	-	50	60	-	00	0
		0 8		2	3	42	5	-	-	00	C
		0 8		5	3	4	5	0	-	00	0
	1	0 3	_	2 2	3	-	10	6	-	00	0
	-	0 3	-	2	57	4	117	60	-	00	0
	7	0 5		2	~	-	5	6	-	00	0
	1.1	0 3	-	2	~	4	5	60	-	60	C
	1 H	0.9		2	~		10	60	-	00	-
	2	00		2	3	-	10	6	-	60	0
	L	0 0	-	3	3	-	5	0	-	00	C
	1 1-	0 17	-	~	3	-7	5	60	-	60	C
	1	0 3	-	2	3	-7	10	0	-	00	C
		00	-	2	3	-7	10	60	2	00	
	F	0 5	-	2	57	-5	10	60	-	00	0
	STATEMENT	0 2	-	2	3		5	60	-	00	C
		08		~	3	42	5	60	-	00	000
		0 0		2	~	4	10	0	2	00	0
	7	0 8	-	2	~	4	10	4	-	00	0
	1	OR		2	3	-	5	60	-	00	0 0
	2	0 7	-	2	3	12	5	6	-	00	C
	LLL L	000	-	2	3	-	5	6	-	00	0
	F	0 5	-	2	~		10	60	2	00	0
	1 CC	OR	-	~	5	-	10	60	-	00	0
	0	0 %	-	2	~	-1-	100	60	~	00	C
	FORTRAN	00		2	3	44	10	60	-	00	0000000
	4	0 8		2	5	-	10	60	2	00	0
		0 1		2	3	-	5	60	-	00	0
		0 7	-	2	3	-	5	60	-	00	C
		0 1	-	5	3	47	477	60	-	00	0
	-	0	-	2	33		1.07	60	-	00	0
		0 8	-	~	3	-	100	10	-	00	0
-		0.2	-	2	3		-	60	-	-	3
		0		2 2	3		10	-	~	60	0
-		0 1	-	2	3	4	5	0	-	00	0
		0 1		3	3	-	10	5	-	00	G
		2		2	3	-	10	63	-	-	9
		00		2 2	3	-4	5	60	-	00	G
		0		0	0	-	100	10	~	-	C
	-	0 2		2	17	-	-	40	-		0
-		0 .	-	~	~	4	50	60	-	00	a
		-		2 2	3	44	-	40	-	-	000000000000000000000000000000000000000
-	MERCENTRYLWEST	0.		04	3		5	2 2	-	00	-
	2 5-	0 .	-	~	3	49	100	60	-	60	0
	Sec. 38	0.	-	5	3		103	60	-	60	or
	C+2mments			212 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	ala a a a a a a a a a a a a a a a a a a	**************************************	5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5	56666			0
	O E	0-		24					-		9



ERICSSON