ENDL
TEXAS

Date: 18 July 2007
To: T10 Technical Committee
From: Ralph O. Weber
Subject: SA September CAP Decision Matrix

September CAP Decision

The July CAP working group agreed to choose between the two Security Strength columns in the following table when the group meets in Vancouver.

		Security Strength	
		128 Bits	256 Bits
Mandatory Algorithm Support	Key Exchange	2 048-bit MODP group (finite field D-H)	521-bit prime elliptic curve field P-521
	PRF	IKEv2-use based on SHA-256	IKEv2-use based on SHA-512
	Encryption	AES-CBC with 128-bit (16-byte) key	AES-CBC with 256-bit (32-byte) key
	Integrity	AUTH_HMAC_SHA2_ 256_128	AUTH_HMAC_SHA2_ 512_256
	Authentica-tion	RSA Digital Signature with 2 048-bit key support [a]	ECDSA with 512-bit SHA-2 on the P-521 elliptic curve [a]
		[a] Certificate support is optional.	

18484 Preston Road, Suite 102 PMB 178, Dallas, TX 75252 214-912-1373 972-596-2775 Fx ENDL_TX@computer.org