Garzón Domínguez Gerardo Ismael & Sánchez Becerra Ernesto Daniel

Criptografía Híbrida - Servicios

Servicio	**Primitiva**	**Algoritmo**	**Seguridad en bits**	**Referencia**
Confidencialidad	Cifrado/Descifrado	AES256	256	[1]
Integridad	Firma / Verificación	SHA512	512 o 256 segun el ataque	[2]
No repudio	F/V + C/D	RSA4096, SHA512	140 bits. 512 o 256, segun el ataque	[3] [2]
Confidencialidad	Generación de llave	Diffie Hellman 2048	112 bits.	[4]

[1] https://csrc.nist.gov/publications/detail/fips/197/final
[2] https://link.springer.com/chapter/10.1007/978-3-031-17510-7_7
[3] https://csrc.nist.rip/library/NIST%20SP%20800-078-2%20Cryptographic%20Algorithms%20and%20Key%20Sizes%20for%20Personal%20Identification%20Verification%20(PIV),%202010-02.pdf
[4] https://www.rfc-editor.org/rfc/rfc2631