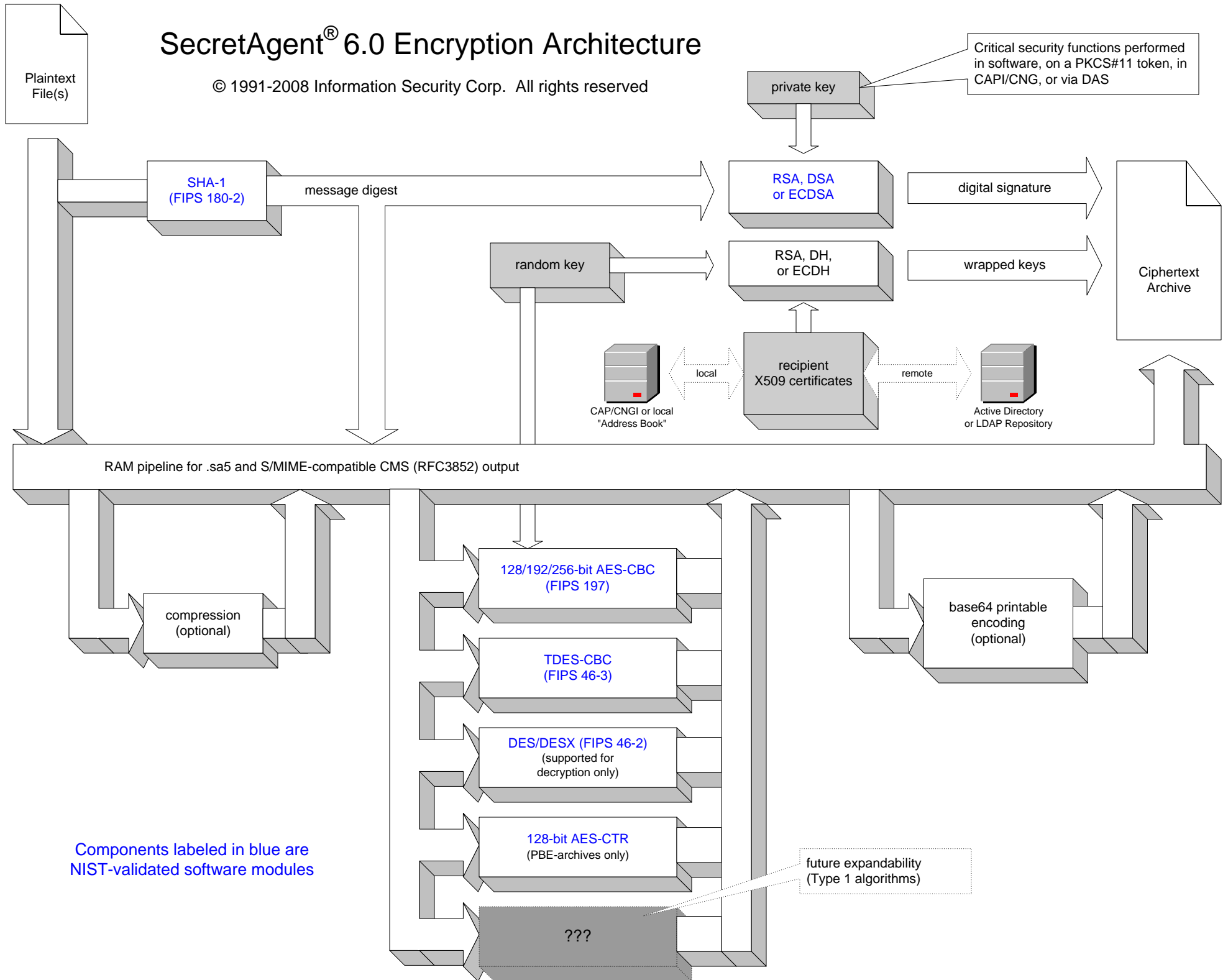


# SecretAgent® 6.0 Encryption Architecture

© 1991-2008 Information Security Corp. All rights reserved



Critical security functions performed in software, on a PKCS#11 token, in CAPI/CNG, or via DAS

Plaintext File(s)

SHA-1 (FIPS 180-2)

message digest

private key

RSA, DSA or ECDSA

digital signature

random key

RSA, DH, or ECDH

wrapped keys

Ciphertext Archive

CAP/CNGI or local "Address Book"

recipient X509 certificates

Active Directory or LDAP Repository

RAM pipeline for .sa5 and S/MIME-compatible CMS (RFC3852) output

compression (optional)

128/192/256-bit AES-CBC (FIPS 197)

TDES-CBC (FIPS 46-3)

DES/DESX (FIPS 46-2) (supported for decryption only)

128-bit AES-CTR (PBE-archives only)

base64 printable encoding (optional)

Components labeled in blue are NIST-validated software modules

future expandability (Type 1 algorithms)

???