

DOCUMENT SECURITY AND ENCRYPTION

Document security algorithms

V.	Password Security	Certificate Security	LiveCycle Security
11.0	No change except for enhancements to the encrypted and stored password	Prior to 11.0, RSA certificates were required. 11.0 allows ECDSA (Elliptic Curve) certificates. For multiple recipients, some may use RSA and others ECDSA. Sending a document where some recipients are ECDSA to Acrobat 9 or 10 is permitted but those recipients must have RSA certificates.*	No change
10.0	No change except for enhancements to the encrypted and stored password	No change	No change
9.0	256-bit AES	256-bit AES	256-bit AES
8.1	Same as 7.0 except enabling FIPS mode disables password security	Same as 7.0 except enabling FIPS mode disables RC4	Same as 7.0
8.0	Same as 7.0	Same as 7.0	Same as 7.0
7.0	128-bit RC4/AES with options A, B, and C	128-bit RC4/AES with options A, B, and C	128-bit AES with options A, B, and C
6.0	Same as 5.0 with options A and B	Same as 5.0 (Self-sign & 3rd-party certs) with options A and B	N/A
5.0	40 & 128-bit RC4 with option A	40 & 128-bit RC4 (Self-sign p7b & apf files only) with option A	N/A
4.0	40-bit RC4 (64-bit decrypt) with option A	N/A	N/A
2-3.0	40-bit RC4	N/A	N/A

* Support for ECDSA certificates with specific named curves (NIST): P256 with digest algorithm SHA256, P384 with digest algorithm SHA384, P521 with digest algorithm SHA512. **Not supported on Windows (MSCAPI) and Mac (Keychain):** P-192 (secp192r1), P-224 (secp224r1), P-256 (secp256r1), P-384 (secp384r1), P-521 (secp521r1), B-163 (sect163r2), K-163 (sect163k1), B-233 (sect233r1), K-233 (sect233k1), B-283 (sect283r1), K-283 (sect283k1), B-409 (sect409r1), K-409 (sect409k1), B-571 (sect571r1), K-571 (sect571k1)

Compatibility options

The compatibility options determine the available algorithm and encryption options as follows:

Compatibility	Encryption	Encryption options	Password length limits
3.0 and later	40-bit RC4	Forces the encryption of strings and streams only and limits other features.	32 Roman (latin-1) characters
5.0 and later	128-bit RC4	Allows the accessibility option to be selected independently of the copy option, restricts printing to 150-bit dpi, and expands the set of Changes Allowed options.	
6.0 and later	128-bit RC4	Allows encrypting the document independently of the metadata.	
7.0 and later	128-bit AES	Allows encrypting all contents, all but metadata, or only attachments.	
9.0 and later	256-bit AES	Same options as 7.0.	Unicode, up to 127 UTF-8 bytes.
10.0 and later	256-bit AES	Same options as 7.0. The password algorithm was significantly strengthened Note: The Acrobat 9.0 and later option is removed in Acrobat X.	Unicode, up to 127 UTF-8 bytes.


What to encrypt" options

Select Document Components to Encrypt

Encrypt all document contents

Encrypt all document contents except metadata (Acrobat 6 and later compatible)

Encrypt only file attachments (Acrobat 7 and later compatible)

 All contents of the document will be encrypted, and search engines will not be able to access the document's metadata.

Compatibility: Acrobat X and later ▼

Acrobat 6.0 and later

Acrobat 7.0 and later

Acrobat X and later