## Document Security and Encryption

### Document Security Algorithms

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>11.0</td>
<td>No change except for enhancements to the encrypted and stored password</td>
<td>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.*</td>
<td>No change</td>
</tr>
<tr>
<td>10.0</td>
<td>No change except for enhancements to the encrypted and stored password</td>
<td>No change</td>
<td>No change</td>
</tr>
<tr>
<td>9.0</td>
<td>256-bit AES</td>
<td>256-bit AES</td>
<td>256-bit AES</td>
</tr>
<tr>
<td>8.1</td>
<td>Same as 7.0 except enabling FIPS mode disables password security</td>
<td>Same as 7.0 except enabling FIPS mode disables RC4</td>
<td>Same as 7.0</td>
</tr>
<tr>
<td>8.0</td>
<td>Same as 7.0</td>
<td>Same as 7.0</td>
<td>Same as 7.0</td>
</tr>
<tr>
<td>7.0</td>
<td>128-bit RC4/AES with options A, B, and C</td>
<td>128-bit RC4/AES with options A, B, and C</td>
<td>128-bit AES with options A, B, and C</td>
</tr>
<tr>
<td>6.0</td>
<td>Same as 5.0 with options A and B</td>
<td>Same as 5.0 (Self-sign &amp; 3rd-party certs) with options A and B</td>
<td>N/A</td>
</tr>
<tr>
<td>5.0</td>
<td>40 &amp; 128-bit RC4 with option A</td>
<td>40 &amp; 128-bit RC4 (Self-sign p7b &amp; apf files only) with option A</td>
<td>N/A</td>
</tr>
<tr>
<td>4.0</td>
<td>40-bit RC4 (64-bit decrypt) with option A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>2-3.0</td>
<td>40-bit RC4</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

* 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:

<table>
<thead>
<tr>
<th>Compatibility</th>
<th>Encryption</th>
<th>Encryption options</th>
<th>Password length limits</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.0 and later</td>
<td>40-bit RC4</td>
<td>Forces the encryption of strings and streams only and limits other features.</td>
<td>32 Roman (latin-1) characters</td>
</tr>
<tr>
<td>5.0 and later</td>
<td>128-bit RC4</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>6.0 and later</td>
<td>128-bit RC4</td>
<td>Allows encrypting the document independently of the metadata.</td>
<td></td>
</tr>
<tr>
<td>7.0 and later</td>
<td>128-bit AES</td>
<td>Allows encrypting all contents, all but metadata, or only attachments.</td>
<td>Unicode, up to 127 UTF-8 bytes.</td>
</tr>
<tr>
<td>9.0 and later</td>
<td>256-bit AES</td>
<td>Same options as 7.0.</td>
<td>Unicode, up to 127 UTF-8 bytes.</td>
</tr>
<tr>
<td>10.0 and later</td>
<td>256-bit AES</td>
<td>Same options as 7.0. The password algorithm was significantly strengthened. <strong>Note:</strong> The Acrobat 9.0 and later option is removed in Acrobat X.</td>
<td>Unicode, up to 127 UTF-8 bytes.</td>
</tr>
</tbody>
</table>

### 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.