AES-128 PDF Encryption

Zero-dependency password protection using the PDF Standard Security Handler (Revision 4). Implemented entirely with System.Security.Cryptography.

How It Works

TerraPDF derives a 16-byte **File Encryption Key (FEK)** from your passwords using the PDF-mandated MD5 key-derivation algorithm (50 rounds). Each PDF object — pages, images, content streams — is then encrypted with a unique **per-object AES-128 CBC key** derived from the FEK plus the object number. A random 16-byte IV is prepended to every encrypted payload.

Component	Detail
Cipher	AES-128 CBC (per PDF §7.6.5)
IV	16 random bytes — unique per object
Key derivation	MD5 × 51 rounds (PDF §7.6.3.3 Algorithm 2)
O entry	Algorithm 3 — owner password verifier
U entry	Algorithm 5 (Rev 4) — user password verifier
Handler	PDF Standard Security Handler, Revision 4
PDF version	1.6 (minimum for AES encryption)
Dependencies	System.Security.Cryptography only — no packages

Four Protection Scenarios (see companion files)

File	User pwd	Owner pwd	Permissions	Use case
12a	user123	admin123	All	Protect authorship; allow all viewer operations
12b	(none)	ownerOnly	Accessibility	Distribute freely; prevent print / copy
12c	printme	printAdmin	Print only	Allow printing; prevent digital re-use
12d	viewonly	superadmin	None	Maximum restriction — view on screen only

TerraPDF — Encryption Showcase

PdfPermissions Reference & API

Overview

PdfPermissions Flags

Combine flags with bitwise-OR. Use PdfPermissions.All to grant everything or PdfPermissions.None to deny all.

Flag	PDF bit	Description
PdfPermissions.Print	Bit 3	High-quality printing
PdfPermissions.ModifyContents	Bit 4	Modify document contents
PdfPermissions.CopyText	Bit 5	Copy or extract text and graphics
PdfPermissions.ModifyAnnotations	Bit 6	Add or modify annotations and form fields
PdfPermissions.FillForms	Bit 9	Fill in interactive form fields
PdfPermissions.ExtractForAccessibility	Bit 10	Text extraction for screen readers
PdfPermissions.AssembleDocument	Bit 11	Insert, rotate, or delete pages
PdfPermissions.PrintLowResolution	Bit 12	Low-resolution (degraded) printing only
PdfPermissions.All	Bits 3-12	All flags combined — full viewer access
PdfPermissions.None	Bits 3-12	No flags set — view on screen only

EncryptionOptions API

Property	Type	Default	Description
UserPassword	string?	null	Password to open the document. Omit for no open prompt.
OwnerPassword	string?	null	Full-access password. Auto-generated when null.
Permissions	PdfPermissions	All	Bitwise flags controlling viewer operations.

Complete API Example

```
Document.Create(container =>
{
container.Encrypt(new EncryptionOptions
{
UserPassword  = "open123",
OwnerPassword = "admin456",
Permissions   = PdfPermissions.Print
| PdfPermissions.CopyText,
});

container.Page(page =>
{
page.Size(PageSize.A4);
page.Margin(2, Unit.Centimetre);
page.Content().Text("Confidential").Bold();
});
})
.PublishPdf("protected.pdf");
```