BÀI TẬP VỀ NHÀ – MÔN: AN TOÀN VÀ BẢO MẬT THÔNG TIN

Chủ đề: Chữ ký số trong file PDF Giảng viên: Đỗ Duy Cốp Thời điểm giao: 2025-10-24 11:45

Đối tượng áp dụng: Toàn bộ sv lớp học phần 58KTPM

Hạn nộp: Sv upload tất cả lên github trước 2025-10-31 23:59:59

I. CÁC YÊU CẦU CỤ THỂ

1) Cấu trúc PDF liên quan chữ ký (Nghiên cứu)

- Mô tả ngắn gọn: Catalog, Pages tree, Page object, Resources, Content streams, XObject, AcroForm, Signature field (widget), Signature dictionary (/Sig),

/ByteRange, /Contents, incremental updates, và DSS (theo PAdES).

- Liệt kê object refs quan trọng và giải thích vai trò của từng object trong lưu/truy xuất chữ ký.
- Dầu ra: 1 trang tóm tắt + sơ đồ object (ví dụ: Catalog → Pages → Page
 → /Contents; Catalog → /AcroForm → SigField → SigDict).

Object	Mô tả	Vai trò liên quan chữ ký		
Catalog (/Root)	Gốc của tài liệu PDF.	Chứa tham chiếu đến /Pages và có thể đến		
		/AcroForm.		
Pages Tree	Cấu trúc cây quản lý các	Không trực tiếp chứa chữ ký, nhưng xác định thứ		
(/Pages)	trang.	tự trang được hiển thị.		
Page Object	Đại diện cho mỗi trang.	Tham chiếu đến /Resources, /Contents (nội dung		
		trang).		
Resources	Font, ånh, XObject	Cung cấp tài nguyên cho nội dung trang.		
Content Stream Dòng lệnh vẽ nội dung		Không chứa chữ ký, nhưng thay đổi nội dung sẽ		
	trang (text, hình).	làm invalid chữ ký.		
XObject	Object có thể tái sử dụng	Có thể chứa con dấu đồ họa (visible signature		
	(ånh, form).	appearance).		
AcroForm	Biểu mẫu tương tác PDF.	Gốc chứa các Form Field, bao gồm Signature		
		Field.		
Signature Field	Một field trong AcroForm	Liên kết trực tiếp đến Signature Dictionary.		
(Widget)	có kiểu /Sig.			
Signature	Object chứa thông tin chữ	Đây là phần trọng tâm , định nghĩa các khóa như:		
Dictionary (/Sig)	ký.	/Filter, /SubFilter, /Name, /M, /ByteRange,		
		/Contents,		
/ByteRange	Mảng chỉ định các đoạn	Xác định vùng dữ liệu được hash → phục vụ xác		
	byte của file được ký.	minh chữ ký.		

/Contents	Chứa chữ ký (thường là	Là dữ liệu nhị phân kết quả ký.	
	CMS/PKCS#7 DER).		
Incremental	Cơ chế thêm nội dung mà	à Mỗi chữ ký mới là một incremental update mới,	
Update	không ghi đè file cũ.	giúp ký nhiều lần.	
DSS (Document	Phần lưu trữ dữ liệu xác	Lưu chứng thư, OCSP, CRL, timestamp, v.v.	
Security Store) minh lâu dài (PAdES-		phục vụ xác minh lâu dài.	
	LTV).		

2) Thời gian ký được lưu ở đâu?

- Nêu tất cả vị trí có thể lưu thông tin thời gian:
- +/M trong Signature dictionary (dạng text, không có giá trị pháp lý).
- + Timestamp token (RFC 3161) trong PKCS#7 (attribute timeStampToken).
- + Document timestamp object (PAdES).
- + DSS (Document Security Store) nếu có lưu timestamp và dữ liệu xác minh. Giải thích khác biệt giữa thông tin thời gian /M và timestamp RFC3161

Vị trí	Định dạng / Ý nghĩa	Giá trị pháp lý	
/M trong	Dạng chuỗi text, ví dụ:	Không có giá trị pháp lý, chỉ do	
Signature	D:20251031120000+07'00'	phần mềm ký ghi vào.	
Dictionary			
Timestamp Token	Attribute timeStampToken	Có giá trị pháp lý, vì được TSA	
(RFC 3161)	trong CMS/PKCS#7	(Time-Stamp Authority) ký xác	
		nhận.	
Document	Một chữ ký đặc biệt dùng	Là chữ ký thời gian độc lập,	
Timestamp	SubFilter=/ETSI.RFC3161	không gắn với người ký.	
(PAdES)			
DSS (Document	Có thể chứa timestamp và dữ	Hỗ trợ xác minh lâu dài (LTV).	
Security Store)	liệu xác minh (OCSP/CRL)		

❖ Giải thích khác biệt giữa thông tin thời gian /M và timestamp RFC3161.

So sánh	/M	RFC 3161 Timestamp
Nguồn phát sinh	Phần mềm ký tự điền	Cấp bởi máy chủ TSA có chứng thư riêng
Dạng dữ liệu	Chuỗi văn bản (PDF text)	Token ASN.1 trong PKCS#7
Mức tin cậy	Không được bảo vệ, có thể sửa	Được ký số, có thể xác minh
Vai trò	Thông tin hiển thị	Dấu thời gian xác thực, có giá trị pháp lý

> Tóm lại:

- Chữ ký PDF nằm trong /Sig dictionary, tham chiếu từ một signature field trong AcroForm.
- Nội dung ký được xác định qua /ByteRange, dữ liệu ký là /Contents.
- Thời gian ký có thể xuất hiện ở nhiều nơi, nhưng chỉ timestamp RFC3161 hoặc Document Timestamp (PAdES) là hợp lệ để chứng minh thời điểm ký.
- DSS dùng để duy trì xác minh chữ ký lâu dài (LTV Long Term Validation).

❖ Rủi ro bảo mật

Nhóm	rủi ro	Mô tả chi tiết	Ảnh hưởng	
1) Chỉnh sửa nội dung		PDF cho phép incremental update,	Làm sai lệch nội dung	
	sau khi ký	nghĩa là thêm phần mới mà không xoá	hiển thị mà vẫn giữ chữ ký	
	(Incremental	phần cũ. Kẻ tấn công có thể chèn nội	"hợp lệ" theo phần mềm	
	Update Abuse)	dung mới (text/ảnh) sau vùng	đọc PDF yếu.	
	,	/ByteRange mà người dùng không để	,	
		ý.		
2)	Invisible Signature	Có thể tạo form field vô hình hoặc	Gây hiểu nhầm nội dung	
	Fields / Hidden	xObject che phủ nội dung thật \rightarrow lừa	tài liệu đã ký, đặc biệt	
	Appearance	người đọc xem nội dung giả.	trong họp đồng hoặc hóa	
			đơn.	
3)	ByteRange	/ByteRange xác định phần dữ liệu	Có thể bị chèn mã độc	
	Manipulation	được hash. Nếu bị thay đổi (hoặc khai	hoặc nội dung giả ngoài	
		báo sai), trình xem PDF yếu có thể vẫn	vùng được ký.	
		hiển thị "valid signature".		
4) Lỗi xác thực của M		Một số viewer (như bản cũ của Adobe	Có thể khiến chữ ký giả	
	trình xem PDF	Reader, Foxit, v.v.) chỉ kiểm tra một	hoặc không hợp lệ vẫn	
		phần chữ ký hoặc bỏ qua lỗi nhỏ trong	hiển thị "hợp lệ".	
		PKCS#7.		
5) Lạm dụng XObject		Chữ ký hiển thị đồ họa (con dấu, tên,	Người xem tin vào hình	
	/ Appearance	ngày) nằm trong appearance	ảnh con dấu "giả" mà	
	Stream	stream, không phải dữ liệu ký. Kẻ tấn	không kiểm tra chữ ký	
		công có thể thay đổi hình ảnh con dấu	thực.	
		hoặc tên mà không ảnh hưởng chữ ký.		
6)	Fake Timestamp /	Trường /M có thể bị sửa bằng tay, vì	Mất tính pháp lý về thời	
	/M Field	không được ký. Nếu không có	điểm ký.	
		timestamp RFC3161 thật, người ký có		
		thể "lùi ngày" hoặc "giả thời gian ký".		
7)	DSS và LTV giả	Nếu phần DSS chứa dữ liệu chứng thư	Rủi ro trong xác minh lâu	
	mạo	hoặc OCSP không được xác thực dài (PAdES-LTV).		
		đúng, có thể dẫn đến xác minh sai hoặc		
		lưu dữ liệu giả.		