



Phụ lục I

**DANH MỤC TIÊU CHUẨN KỸ THUẬT VỀ CHỮ KÝ SỐ
TRÊN THÔNG ĐIỆP DỮ LIỆU DÙNG CHO PHẦN MỀM KÝ SỐ VÀ
PHẦN MỀM KIỂM TRA CHỮ KÝ SỐ**

(Ban hành kèm theo Thông tư số 15 /2025/TT-BKHCN ngày 15 tháng 8 năm 2025 của
Bộ trưởng Bộ Khoa học và Công nghệ)

Số TT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
1. Tiêu chuẩn bắt buộc áp dụng cho chữ ký số, chứng thư chữ ký số trên thông điệp dữ liệu dùng cho phần mềm ký số và phần mềm kiểm tra chữ ký số				
1.1	Mật mã đối xứng	TCVN 7816:2007	Công nghệ thông tin - Kỹ thuật mật mã thuật toán mã dữ liệu AES	Áp dụng một trong hai tiêu chuẩn
		FIPS PUB 197	Advanced Encryption Standard	
1.2	Mật mã phi đối xứng và chữ ký số	PKCS #1 (RFC 3447)	RSA Cryptography Standard	- Áp dụng một trong hai tiêu chuẩn. - Đối với tiêu chuẩn RSA: + Tối thiểu phiên bản 2.1; + Áp dụng lược đồ RSAES-OAEP để mã hoá và RSASSA-PSS để ký. + Độ dài khóa tối thiểu là 2048 bit - Đối với tiêu chuẩn ECDSA: độ dài khóa tối thiểu là 256 bit.
		ANSI X9.62-2005	Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)	
1.3	Yêu cầu cho hàm băm	FIPS PUB 180-4	Secure Hash Standard	Áp dụng một trong các hàm băm sau: SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256, SHA3-224, SHA3-256, SHA3-384,
		FIPS PUB 202	SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions	

				SHA3-512, SHAKE128, SHAKE256
1.4	Cú pháp thông điệp mật mã	PKCS #7 (RFC 2630)	Cryptographic Message Syntax Standard	Phiên bản 1.5
1.5	Chữ ký số cho PDF	ETSI EN 319 142-1	Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures	Áp dụng một trong hai bộ tiêu chuẩn: ETSI EN 319 142-1 Phiên bản V1.2.1 ETSI EN 319 142-2 Phiên bản V1.1.1 Hoặc ISO 14533-3:2017 ISO 32000-1:2008 ISO 32000-2:2020
		ETSI EN 319 142-2	Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 2: Additional PAdES signatures profiles	
		ISO 32000-1:2008	Document management - Portable document format - Part 1: PDF 1.7	
		ISO 14533-3:2017	Processes, data elements and documents in commerce, industry and administration — Long-term signature formats — Part 3: Long-term signature profiles for PDF Advanced Electronic Signatures (PAdES)	
		ISO 32000-2:2020	Document management - Portable document format - Part 2: PDF 2.0	
1.6	Chữ ký số cho XML	ETSI EN 319 132-1	Electronic Signatures and Infrastructures (ESI); XAdES digital	Phiên bản V1.2.1

			<i>signatures; Part 1: Building blocks and XAdES baseline signatures</i>	
		<i>ETSI EN 319 132-2</i>	<i>Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 2: Extended XAdES signatures</i>	<i>Phiên bản V1.1.1</i>
1.7	<i>Chữ ký số cho CMS</i>	<i>ETSI EN 319 122-1</i>	<i>Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures</i>	<i>Phiên bản V1.3.1</i>
		<i>ETSI EN 319 122-2</i>	<i>Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 2: Extended CAdES signatures</i>	<i>Phiên bản V1.1.1</i>
		<i>ETSI TS 119 122-3</i>	<i>Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 3: Incorporation of Evidence Record Syntax (ERS) mechanisms in CAdES</i>	<i>Phiên bản V1.1.1</i>
1.8	<i>Yêu cầu đối với phần cứng HSM</i>	<i>FIPS PUB 140-2</i>	<i>Security Requirements for Cryptographic Modules</i>	- Áp dụng một trong ba tiêu chuẩn. - Đối với các tiêu chuẩn FIPS PUB 140-2/ FIPS PUB 140-3: Yêu cầu tối
		<i>FIPS PUB 140-3</i>	<i>Security Requirements for Cryptographic Modules</i>	

		EN 419221-5:2018	Protection Profiles for TSP Cryptographic modules - Part 5: Cryptographic Module for Trust Services	thiếu mức 3 (level 3)
1.9	Yêu cầu đối với thẻ Token và Smart card	FIPS PUB 140-2	Security Requirements for Cryptographic Modules	- Áp dụng một trong hai tiêu chuẩn.
		FIPS PUB 140-3	Security Requirements for Cryptographic Modules	- Yêu cầu tối thiểu mức 2 (level 2)
1.10	Yêu cầu đối với thẻ SIM	FIPS PUB 140-2	Security Requirements for Cryptographic Modules	- Áp dụng một trong ba tiêu chuẩn.
		FIPS PUB 140-3	Security Requirements for Cryptographic Modules	- Đối với các tiêu chuẩn FIPS PUB 140-2/ FIPS PUB 140-3: Yêu cầu tối thiểu mức 2 (level 2);
		TCVN 8709 (ISO/IEC 15408)	Công nghệ thông tin – Các kỹ thuật an toàn – Các tiêu chí đánh giá an toàn công nghệ thông tin (Common Criteria for Information Technology Security Evaluation)	- Đối với tiêu chuẩn TCVN 8709 (ISO/IEC 15408): Yêu cầu tối thiểu EAL mức 4 (level 4)
1.11	Yêu cầu chính sách cho Tổ chức cung cấp dịch vụ tạo chữ ký số của khách hàng	ETSI TS 119 431-1	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD/SCDev	Phiên bản V1.2.1
		ETSI TS 119 431-2	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 2: TSP service	Phiên bản V1.2.1

			<i>components supporting AdES digital signature creation</i>	
1.12	<i>Giao thức tạo chữ ký số</i>	<i>ETSI TS 119 432</i>	<i>Electronic Signatures and Infrastructures (ESI); Protocols for remote digital signature creation</i>	<i>Phiên bản V1.2.1</i>
1.13	<i>Ứng dụng ký trên máy chủ ký số</i>	<i>EN 419241-1:2018</i>	<i>Trustworthy Systems Supporting Server Signing - Part 1: General system security requirements</i>	
1.14	<i>Yêu cầu cho mô đun ký số</i>	<i>EN 419241-2:2019</i>	<i>Trustworthy Systems Supporting Server Signing - Part 2: Protection Profile for QSCD for Server Signing</i>	
1.15	<i>Yêu cầu đối với phần cứng HSM</i>	<i>EN 419221-5:2018</i>	<i>Protection Profiles for TSP Cryptographic modules - Part 5: Cryptographic Module for Trust Services</i>	
1.16	<i>Giao thức truyền, nhận chứng thư chữ ký số và danh sách chứng thư chữ ký số bị thu hồi</i>	<i>RFC 2585</i>	<i>Internet X.509 Public Key Infrastructure - Operational Protocols: FTP and HTTP</i>	<i>Áp dụng một hoặc cả hai giao thức FTP và HTTP</i>
1.17	<i>Giao thức cho kiểm tra trạng thái chứng thư chữ ký số trực tuyến</i>	<i>RFC 6960</i>	<i>X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP</i>	
1.18	<i>Định dạng chứng thư chữ</i>	<i>RFC 5280</i>	<i>Internet X.509 Public Key Infrastructure</i>	

	<i>ký số và danh sách thu hồi chứng thư chữ ký số</i>		<i>Certificate and Certificate Revocation List (CRL) Profile</i>	
2. Tiêu chuẩn bắt buộc áp dụng cho phần mềm ký số, phần mềm kiểm tra chữ ký số				
2.1	<i>Bộ ký tự và mã hóa cho tiếng Việt</i>	<i>TCVN 6909:2001</i>	<i>TCVN 6909:2001 “ Công nghệ thông tin-Bộ mã ký tự tiếng Việt 16-bit ”</i>	<i>Bắt buộc áp dụng</i>
2.2	<i>Giao thức đường truyền</i>	<i>RFC 9110</i>	<i>HTTP Semantics</i>	<i>HTTP/1.1</i>
2.3	<i>Giao thức bảo mật tầng giao vận</i>	<i>RFC 5246</i>	<i>The Transport Layer Security (TLS) Protocol Version 1.2</i>	<i>Áp dụng tối thiểu TLS 1.2</i>
3. Tiêu chuẩn khuyến nghị áp dụng cho phần mềm ký số, phần mềm kiểm tra chữ ký số				
3.1	<i>Bộ ký tự và mã hóa</i>	<i>ASCII</i>	<i>American Standard Code for Information Interchange</i>	
3.2	<i>Trình diễn bộ ký tự</i>	<i>UTF-8</i>	<i>8-bit Universal Character Set (UCS)/ Unicode Transformation Format</i>	
3.3	<i>Ngôn ngữ định dạng thông điệp dữ liệu</i>	<i>XML v1.0 (5th Edition)</i>	<i>Extensible Markup Language version 1.0 (5th Edition)</i>	<i>Áp dụng tối thiểu XML v1.0</i>
		<i>XML v1.1 (2nd Edition)</i>	<i>Extensible Markup Language version 1.1</i>	
3.4	<i>Định nghĩa các lược đồ trong tài liệu XML</i>	<i>XML Schema version 1.1</i>	<i>XML Schema version 1.1</i>	
3.5	<i>Trao đổi dữ liệu đặc tả tài liệu XML</i>	<i>XML v2.4.2</i>	<i>XML Metadata Interchange version 2.4.2</i>	

3.6	Định dạng PDF	ISO 32000-1:2008	Document management - Portable document format - Part 1: PDF 1.7	Áp dụng tối thiểu PDF 1.7
		ISO 32000-2:2020	Document management - Portable document format - Part 2: PDF 2.0	
3.7	Định dạng JSON	RFC 7159	The JavaScript Object Notation (JSON) Data Interchange Format	
3.8	Cú pháp mã hóa và cách xử lý thông điệp dữ liệu định dạng XML	XML Encryption Syntax and Processing	XML Encryption Syntax and Processing	
		XML Signature Syntax and Processing	XML Signature Syntax and Processing	
3.9	Quản lý khóa công khai thông điệp dữ liệu định dạng XML	XKMS v2.0	XML Key Management Specification version 2.0	
3.10	Chữ ký số cho JSON	RFC 7515	JSON Web Signature (JWS)	