VĂN BẢN QUY PHẠM PHÁP LUẬT

BỘ QUỐC PHÒNG

BỘ QUỐC PHÒNG	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 76/2025/TT-BQP	*Hà Nội, ngày 18 tháng 7 năm 2025*

THÔNG TƯ

Ban hành "Quy chuẩn kỹ thuật quốc gia về xác thực lưu trữ tài liệu số lâu dài của các cơ quan Đảng, Nhà nước"

Căn cứ Luật Tiêu chuẩn và Quy chuẩn kỹ thuật ngày 29 tháng 6 năm 2006;

Căn cứ Luật Giao dịch điện tử ngày 22 tháng 6 năm 2023;

Căn cứ Luật Lưu trữ ngày 21 tháng 6 năm 2024;

Căn cứ Nghị định số 127/2007/NĐ-CP ngày 01 tháng 8 năm 2007 của Chính phủ quy định chi tiết thi hành một số điều của Luật Tiêu chuẩn và Quy chuẩn kỹ thuật; Nghị định số 78/2018/NĐ-CP ngày 16 tháng 5 năm 2018 của Chính phủ sửa đổi, bổ sung một số điều của Nghị định số 127/2007/NĐ-CP ngày 01 tháng 8 năm 2007 của Chính phủ quy định chi tiết thi hành một số điều của Luật Tiêu chuẩn và Quy chuẩn kỹ thuật;

Căn cứ Nghị định số 09/2014/NĐ-CP ngày 27 tháng 01 năm 2014 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Ban Cơ yếu Chính phủ;

Căn cứ Nghị định số 01/2022/NĐ-CP ngày 30 tháng 11 năm 2022 của Chính phủ quy định chức năng, nhiệm vụ, quyền hành và cơ cấu tổ chức của Bộ Quốc phòng; Nghị định số 03/2025/NĐ-CP ngày 28 tháng 02 năm 2025 của Chính phủ sửa đổi, bổ sung một số điều của Nghị định số 01/2022/NĐ-CP ngày 30 tháng 11 năm 2022 của Chính phủ quy định chức năng, nhiệm vụ, quyền hành và cơ cấu tổ chức của Bộ Quốc phòng;

Căn cứ Nghị định số 68/2024/NĐ-CP ngày 25 tháng 6 năm 2024 của Chính phủ quy định về chữ ký số chuyên dùng công vụ;

Theo đề nghị của Trưởng ban Ban Cơ yếu Chính phủ;

Bộ trưởng Bộ Quốc phòng ban hành Thông tư quy định Quy chuẩn kỹ thuật quốc gia về xác thực lưu trữ tài liệu số lâu dài của các cơ quan Đảng, Nhà nước.

Điều 1. Ban hành kèm theo Thông tư này Quy chuẩn kỹ thuật quốc gia về xác thực lưu trữ tài liệu số lâu dài của các cơ quan Đảng, Nhà nước.

Ký hiệu: QCVN 16:2025/BQP.

Điều 2. Thông tư này có hiệu lực thi hành kể từ ngày 02 tháng 9 năm 2025.

Điều 3. Trưởng ban Ban Cơ yếu Chính phủ, Thủ trưởng các cơ quan, đơn vị, tổ chức và cá nhân có liên quan chịu trách nhiệm thi hành Thông tư này./.

BỘ TRƯỞNG

Đại tướng Phan Văn Giang

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM

QCVN 16:2025/BQP

QUY CHUẨN KỸ THUẬT QUỐC GIA VỀ XÁC THỰC LƯU TRỮ TÀI LIỆU SỐ LÂU DÀI CỦA CÁC CƠ QUAN ĐẢNG, NHÀ NƯỚC

National technical regulation on authentication long-term in digital document archives of party and state agencies

HÀ NỘI - 2025

MỤC LỤC

1 QUY ĐỊNH CHUNG
1.1 Phạm vi điều chỉnh
1.2 Đối tượng áp dụng
1.3 Tài liệu viện dẫn
1.4 Giải thích từ ngữ
1.5 Chữ viết tắt
1.6 Ký hiệu
2 QUY ĐỊNH KỸ THUẬT
2.1 Quy định về khuôn dạng chữ ký số
2.1.1 Khuôn dạng chữ ký số
2.1.2 Thông tin bắt buộc phải có trong các khuôn dạng chữ ký số
2.2 Quy định về khuôn dạng dữ liệu phục vụ xác thực lâu dài
2.3 Quy định về thuật toán mật mã
2.3.1 Quy định về các thuật toán mật mã được sử dụng
2.3.2 Quy định về thời gian sử dụng các thuật toán mật mã
3 QUY ĐỊNH VỀ QUẢN LÝ
4 TRÁCH NHIỆM CỦA CƠ QUAN, TỔ CHỨC, CÁ NHÂN
5 TỔ CHỨC THỰC HIỆN
TÀI LIỆU THAM KHẢO

Lời nói đầu

QCVN 16:2025/BQP do Cục Chứng thực số và Bảo mật thông tin - Ban Cơ yếu Chính phủ biên soạn, Ban Cơ yếu Chính phủ trình duyệt, Bộ Khoa học và Công nghệ thẩm định, Bộ trưởng Bộ Quốc phòng ban hành theo kèm Thông tư số 76/2025/TT-BQP ngày 18 tháng 7 năm 2025.

QUY CHUẨN KỸ THUẬT QUỐC GIA VỀ XÁC THỰC LƯU TRỮ TÀI LIỆU SỐ LÂU DÀI CỦA CÁC CƠ QUAN ĐẢNG, NHÀ NƯỚC

National technical regulation on authentication long-term in digital document archives of party and state agencies

1 QUY ĐỊNH CHUNG

1.1 Phạm vi điều chỉnh

Quy chuẩn kỹ thuật quốc gia này quy định mức giới hạn các đặc tính kỹ thuật về xác thực trong hoạt động nghiệp vụ lưu trữ đối với tài liệu lưu trữ số được ký số bằng chứng thư chữ ký số chuyên dùng công vụ.

1.2 Đối tượng áp dụng

Quy chuẩn kỹ thuật quốc gia này áp dụng đối với các cơ quan, tổ chức, cá nhân có liên quan khi quản lý, sử dụng dịch vụ chứng thực chữ ký số chuyên dùng công vụ trong hoạt động nghiệp vụ lưu trữ đối với tài liệu lưu trữ số.

1.3 Tài liệu viện dẫn

Các Tài liệu viện dẫn sau là cần thiết cho việc áp dụng Quy chuẩn này. Trường hợp các Tài liệu viện dẫn được sửa đổi, bổ sung hoặc thay thế thì áp dụng phiên bản mới nhất.

Tiêu chuẩn ISO 14533-1:2022, Quy trình, phần tử dữ liệu và tài liệu trong thương mại, công nghiệp và quản trị - hồ sơ chữ ký dài hạn, Phần 1: Hồ sơ chữ ký điện tử nâng cao CMS (CAdES).

Tiêu chuẩn ISO 14533-2:2021, Quy trình, phần tử dữ liệu và tài liệu trong thương mại, công nghiệp và quản trị - hồ sơ chữ ký dài hạn, Phần 2: Hồ sơ chữ ký điện tử nâng cao XML (XadES).

Tiêu chuẩn ISO 14533-3:2017, Quy trình, phần tử dữ liệu và tài liệu trong thương mại, công nghiệp và quản trị - Hồ sơ chữ ký dài hạn, Phần 3: Hồ sơ chữ ký dài hạn cho Chữ ký Điện tử Nâng cao PDF (PAdES).

Tiêu chuẩn ISO 14533-4:2019, Quy trình, phần tử dữ liệu và tài liệu trong thương mại, công nghiệp và quản trị - Hồ sơ chữ ký dài hạn, Phần 4: Thuộc tính trỏ đến đối tượng chỉ bằng chứng (bên ngoài) của sự tồn tại được sử dụng trong các định dạng chữ ký dài hạn (PoEAttributes).

TCVN 11816-3:2017 (ISO/IEC 10118-3:2004) "Công nghệ thông tin - Các kỹ thuật an toàn - Hàm băm - Phần 3: Hàm băm chuyên dụng".

Khuyến nghị RFC 3161, Giao thức dấu thời gian (TSP).

Khuyến nghị RFC 6960, Giao thức kiểm tra trạng thái chứng thư chữ ký số trực tuyến (OCSP).

Tiêu chuẩn của Viện tiêu chuẩn và Công nghệ quốc gia Hoa Kỳ, FIPS 186-4, Tiêu chuẩn về chữ ký số (DSS), tháng 7 năm 2013.

Tiêu chuẩn của Viện tiêu chuẩn và Công nghệ quốc gia Hoa Kỳ, FIPS 180-4, Tiêu chuẩn về Hàm băm an toàn (SHS), tháng 8 năm 2015.

Tiêu chuẩn của Viện tiêu chuẩn và Công nghệ quốc gia Hoa Kỳ, FIPS 202, Tiêu chuẩn SHA-3: Hàm băm dựa trên hoán vị và hàm đầu ra có thể mở rộng, tháng 8 năm 2015.

Tiêu chuẩn của tổ chức IETF, Bảo vệ dữ liệu bằng mật mã trên thiết bị lưu trữ theo khối, tháng 10 năm 2018.

1.4 Giải thích từ ngữ

Trong Quy chuẩn này, các từ ngữ dưới đây được hiểu như sau:

1.4.1. Khuôn dạng dữ liệu phục vụ xác thực lâu dài

Là một loại dữ liệu có cấu trúc, được tham chiếu đến hồ sơ, tài liệu lưu trữ nhằm chứng minh sự tồn tại (thời điểm bắt đầu đưa vào lưu trữ), toàn vẹn của hồ sơ, tài liệu đó.

1.4.2. Mật mã

Là những quy tắc, quy ước riêng dùng để thay đổi hình thức biểu hiện thông tin nhằm bảo đảm bí mật, xác thực, toàn vẹn của nội dung thông tin.

1.4.3. Kỹ thuật mật mã

Là phương pháp, phương tiện có ứng dụng mật mã để bảo vệ thông tin.

1.4.4. Mã hóa

Là quá trình dùng kỹ thuật mật mã để thay đổi hình thức biểu hiện thông tin.

1.4.5. Giải mã

Là phép biến đổi ngược của quá trình mã hóa tương ứng.

1.4.6. Khóa

Là dãy ký tự điều khiển hoạt động của biến đổi mật mã.

1.4.7. Mật mã không đối xứng

Là mật mã trong đó khóa được sử dụng cho phép mã hóa hoặc giải mã gồm hai thành phần là khóa công khai và khóa bí mật với đặc tính có thể dễ dàng tính toán được khóa công khai nếu biết khóa bí mật nhưng không khả thi về mặt tính toán để tính được khóa bí mật từ khóa công khai.

1.4.8. Thuật toán băm

Là thuật toán thực hiện quá trình biến đổi chuỗi dữ liệu đầu vào có độ dài bất kỳ thành một chuỗi dữ liệu đầu ra đặc trưng có độ dài cố định.

1.4.9. Tổ chức cung cấp dịch vụ chứng thực chữ ký số chuyên dùng công vụ

Là Cục Chứng thực số và Bảo mật thông tin trực thuộc Ban Cơ yếu Chính phủ.

1.4.10. Chứng thư chữ ký số

Là chứng thư chữ ký điện tử đối với chữ ký số.

1.5 Chữ viết tắt

Chữ viết tắt	Tên tiếng anh	Tên tiếng việt
EC	Elliptic Curve	Đường cong Elliptic
ECDSA	Elliptic Curve Digital Signature Algorithm	Thuật toán chữ ký số dựa trên đường cong Elliptic
FIPS	Federal Information Processing Standards	Tiêu chuẩn xử lý thông tin liên bang (Hoa Kỳ)
FIPS PUB	Federal Information Processing Standards Publication	Công bố tiêu chuẩn xử lý thông tin liên bang (Hoa Kỳ)
NIST	National Institute of Standards and Technology	Viện Tiêu chuẩn và Kỹ thuật quốc gia (Hoa Kỳ)
QCVN		Quy chuẩn kỹ thuật quốc gia (Việt Nam)

Chữ viết tắt	Tên tiếng anh	Tên tiếng việt
RFC	Request for Comments	Đặc tả kỹ thuật do tổ chức IETF (Internet Engineering Task Force) công bố
RSA	Rivest - Shamir - Adleman	Thuật toán, phương pháp mã hóa và chứng nhận thông tin điện tử do 3 nhà khoa học Rivest, Shamir và Adleman phát minh
SHA	Secure Hash Algorithm	Thuật toán băm an toàn
TCVN		Tiêu chuẩn kỹ thuật quốc gia (Việt Nam)

1.6 Ký hiệu

Ký hiệu	Mô tả
nlen	Đối với thuật toán RSA: *nlen* là độ dài modulo theo bit; Đối với thuật toán ECDSA: *nlen* là độ dài theo bit của cấp của phần tử sinh

2 QUY ĐỊNH KỸ THUẬT

2.1 Quy định về khuôn dạng chữ ký số

2.1.1 Khuôn dạng chữ ký số

Sử dụng khuôn dạng chữ ký số trong danh sách sau:

Bảng 1 - Danh mục các khuôn dạng chữ ký số được phép sử dụng

STT	Loại	Tham chiếu
1	CAdES	ISO 14533-1:2022
2	XadES	ISO 14533-2:2021
3	PAdES	ISO 14533-3:2017

2.1.2 Thông tin bắt buộc phải có trong các khuôn dạng chữ ký số

- Chứng thư chữ ký số chuyên dùng công vụ của chủ thể thực hiện ký số và danh sách chứng thư chữ ký số bị thu hồi (CRL) hoặc trạng thái chứng thư chữ ký số trực tuyến (OCSP) được công bố bởi Tổ chức cung cấp dịch vụ chứng thực chữ ký số chuyên dùng công vụ tại thời điểm đưa vào lưu trữ;

- Chứng thư chữ ký số chuyên dùng công vụ trung gian (nếu có) và danh sách chứng thư chữ ký số bị thu hồi (CRL) hoặc trạng thái chứng thư chữ ký số trực tuyến (OCSP) được công bố bởi Tổ chức cung cấp dịch vụ chứng thực chữ ký số chuyên dùng công vụ tại thời điểm đưa vào lưu trữ;

- Chứng thư chữ ký số chuyên dùng công vụ gốc và danh sách chứng thư chữ ký số bị thu hồi (CRL) hoặc trạng thái chứng thư chữ ký số trực tuyến (OCSP) được công bố bởi Tổ chức cung cấp dịch vụ chứng thực chữ ký số chuyên dùng công vụ tại thời điểm đưa vào lưu trữ.

- Dấu thời gian hợp lệ trước thời điểm đưa vào lưu trữ; địa chỉ máy chủ dấu thời gian được công bố bởi Tổ chức cung cấp dịch vụ chứng thực chữ ký số chuyên dùng công vụ.

2.2 Quy định về khuôn dạng dữ liệu phục vụ xác thực lâu dài

Sử sụng khuôn dạng dữ liệu của thành phần phục vụ xác thực lâu dài cho tài liệu lưu trữ như sau:

Bảng 2 - Khuôn dạng dữ liệu phục vụ xác thực lâu dài được phép sử dụng

STT	Loại	Tham chiếu
1	PoEAttributes	ISO 14533-4:2019

2.3 Quy định về thuật toán mật mã

2.3.1 Quy định về các thuật toán mật mã được sử dụng

2.3.1.1 Thuật toán mật mã không đối xứng

Sử dụng thuật toán trong danh sách sau:

Bảng 3 - Danh mục thuật toán mật mã không đối xứng được phép sử dụng

STT	Thuật toán	Tham chiếu
1	RSA	[FIPS 186-4], [SP 800-56B Rev. 2]
2	ECDSA	[FIPS 186-4]

2.3.1.2 Thuật toán băm

Sử dụng thuật toán băm trong danh sách sau:

Bảng 4 - Danh mục thuật toán băm được phép sử dụng

STT	Thuật toán	Tham chiếu
1	SHA-256, SHA-384, SHA-512/256, SHA-512	[TCVN 11816-3], [FIPS 180-4]
2	SHA3-256, SHA3-384, SHA3-512	[FIPS 202]

2.3.2 Quy định về thời gian sử dụng các thuật toán mật mã

2.3.2.1 Thuật toán mật mã không đối xứng

Sử dụng thuật toán mật mã không đối xứng phải tuân thủ các quy định sau:

Bảng 5 - Quy định về đặc tính kỹ thuật và thời gian áp dụng đối với thuật toán mật mã không đối xứng

STT	Thuật toán	Kích thước tham số theo bit	Sử dụng đến năm	Tài liệu tham chiếu
1	RSA	*nlen* ≥ 3072	2027	QCVN 15:2023/BQP
2	ECDSA	*nlen* ≥ 256	2027	QCVN 15:2023/BQP
CHÚ THÍCH: Các tiêu chuẩn cho tham số an toàn, các thuật toán sinh, các bộ tham số cụ thể cho các thuật toán RSA, ECDSA trong quy chuẩn này áp dụng theo tiêu chuẩn FIPS 186-4.				

2.3.2.2 Thuật toán băm

Sử dụng thuật toán băm phải tuân thủ quy định sau:

Bảng 6 - Quy định về đặc tính kỹ thuật và thời gian áp dụng đối với thuật toán băm

STT	Thuật toán	Sử dụng đến năm	Tài liệu tham chiếu
1	SHA-256, SHA-384, SHA-512/256, SHA-512	2027	QCVN 15:2023/BQP
2	SHA3-256, SHA3-384, SHA3-512	2027	QCVN 15:2023/BQP

3 QUY ĐỊNH VỀ QUẢN LÝ

3.1 Các mức giới hạn đặc tính kỹ thuật của chữ ký số chuyên dùng công vụ nêu tại Quy chuẩn này phục vụ quản lý tài liệu lưu trữ số lâu dài theo quy định của Luật Lưu trữ số 33/2024/QH15 ngày 21 tháng 6 năm 2024.

3.2 Dịch vụ chứng thực chữ ký số chuyên dùng công vụ thuộc phạm vi điều chỉnh trong Mục 1.1 Quy chuẩn này phải đáp ứng quy định kỹ thuật trong Quy chuẩn này.

3.3 Hoạt động kiểm tra, đánh giá tình hình sử dụng chữ ký số chuyên dùng công vụ phục vụ xác thực tài liệu lưu trữ số lâu dài của các cơ quan Đảng, Nhà nước được thực hiện theo quy định tại Nghị định số 68/2024/NĐ-CP ngày 25 tháng 6 năm 2024 của Chính phủ quy định về chữ ký số chuyên dùng công vụ.

4 TRÁCH NHIỆM CỦA CƠ QUAN, TỔ CHỨC, CÁ NHÂN

4.1 Các cơ quan, tổ chức, cá nhân liên quan khi sử dụng dịch vụ chứng thực chữ ký số chuyên dùng công vụ để xác thực trong hoạt động nghiệp vụ lưu trữ của các cơ quan Đảng, Nhà nước phải tuân thủ quy định trong Quy chuẩn này.

4.2 Các cơ quan, tổ chức, cá nhân liên quan có trách nhiệm thực hiện các quy định về chứng nhận hợp quy, công bố hợp quy và chịu sự kiểm tra của cơ quan quản lý nhà nước theo các quy định hiện hành.

5 TỔ CHỨC THỰC HIỆN

5.1 Ban Cơ yếu Chính phủ chỉ đạo Cục Chứng thực số và Bảo mật thông tin hướng dẫn, tổ chức triển khai quản lý theo Quy chuẩn này.

5.2 Trong trường hợp các văn bản quy phạm pháp luật quy định tại Quy chuẩn kỹ thuật này có sự thay đổi, bổ sung hoặc được thay thế thì thực hiện theo các văn bản mới. Trong trường hợp các tiêu chuẩn được viện dẫn trong Quy chuẩn này có sự thay đổi, bổ sung, thay thế thì thực hiện theo hướng dẫn của Bộ Quốc phòng.

5.3 Trong quá trình triển khai thực hiện Quy chuẩn này, nếu có vấn đề phát sinh, vướng mắc, các cơ quan, đơn vị, tổ chức, cá nhân có liên quan kịp thời phản ánh bằng văn bản về Bộ Quốc phòng (qua Ban Cơ yếu Chính phủ) để xem xét, quyết định./.

TÀI LIỆU THAM KHẢO

[1]. National Institute of Standards and Technology, Special Publication 800-131A *“Transitioning the Use of Cryptographic Algorithms and Key Lengths”,* March 2019.

[2]. *ISO 17068:2017 Information and documentation - Trusted third party repository for digital records*

[3]. *ISO 14721:2012 The Reference Model for an Open Archival Information System (OAIS)*

[4]. *Recommendation ITU-T X.509 (2008)/ISO/IEC 9594-8 (2008): "Information technology - Open Systems Interconnection - The Directory: Public-key and Attribute Certificate frameworks".*

[5]. *ETF RFC 3280 (2002): "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".*

[6]. *IETF RFC 2560 (1999): "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP".*

[7]. *IETF RFC 3852 (2004): "Cryptographic Message Syntax (CMS)".*

[8]. *IETF RFC 3161 (2001): "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)".*

[9]. *Recommendation ITU-T X.680 (2008): "Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation".*

[10]. *Recommendation ITU-T X.501 (2008)/ISO/IEC 9594-1 (2008): "Information technology - Open Systems Interconnection - The Directory: Models".*

[11]. *IETF RFC 3370 (2002): "Cryptographic Message Syntax (CMS) Algorithms".*

[12]. *Recommendation ITU-T F.1: "Operational provisions for the international public telegram service".*

[13]. *Recommendation ITU-T X.500: "Information technology - Open Systems Interconnection - The Directory: Overview of concepts, models and services".*

[14]. *IETF RFC 3281 (2002): "An Internet Attribute Certificate Profile for Authorization".*

[15]. *Recommendation ITU-T X.208 (1988): "Specification of Abstract Syntax Notation One (ASN.1)".*

[16]. *IETF RFC 5035 (2007): "Enhanced Security Services (ESS) Update: Adding CertID Algorithm Agility".*

[17]. *IETF RFC 4998 (2007): "Evidence Record Syntax (ERS)".*

[18]. *ETSI TS 101 733: "Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)".*

[19]. *W3C/IETF Recommendation: "XML-Signature Syntax and Processing".*

[20]. *IETF RFC 2119: "Key words for use in RFCs to Indicate Requirement Levels".*

[21]. *ETSI TR 102 038: "TC Security - Electronic Signatures and Infrastructures (ESI); XML format for signature policies".*

[22]. *IETF RFC 3261: "Internet X.509 Public Key Infrastructure Time-Stamp protocol".*

[23]. *ISO 32000-1: "Document management - Portable document format - Part 1: PDF 1.7". http://www.adobe.com/devnet/acrobat/pdfs/PDF32000_2008.pdf.*

[24]. *ETSI EN 319 122-1: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures".*

[25]. *IETF RFC 5652 (2009): "Cryptographic Message Syntax (CMS)".*

[26]. *IETF RFC 5280 (2008): "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".*

[27]. *IETF RFC 6960 (2013): "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP".*

[28]. *W3C Recommendation (May 2008): "Canonical XML Version 1.1".*

[29]. *IETF RFC 5816 (2010): "ESSCertIDv2 Update for RFC 3161".*

[30]. *IETF RFC 2315: "PKCS #7: Cryptographic Message Syntax Version 1.5".*

[31]. *ETSI EN 319 142-1: "Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures".*

[32]. *ETSI EN 319 132-1: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures".*

[33]. *ETSI EN 319 132-2: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 2: Extended XAdES signatures".*