Chương V. YÊU CẦU VỀ KỸ THUẬT

1. Giới thiệu chung về dự án/dự toán mua sắm, gói thầu:

1.1. Giới thiệu về dự toán mua sắm

- **Tên dự toán mua sắm:** Hỗ trợ chữ ký số công cộng, hóa đơn điện tử cho doanh nghiệp thành lập mới và chi phí thuê kế toán cho các hộ kinh doanh chuyển đổi lên doanh nghiệp trên địa Thành phố Huế" năm 2026.

- **Quyết định phê duyệt Kế hoạch lựa chọn nhà thầu:** Quyết định số 1022/QĐ-STC ngày 03/02/2026 của Sở tài chính thành phố Huế.

1.2. Giới thiệu về gói thầu

- **Chủ đầu tư:** Sở tài chính thành phố Huế.

- **Tên gói thầu:** Gói thầu số 03: Hỗ trợ sử dụng chữ ký số công cộng và hoá đơn điện tử.

- **Hình thức lựa chọn nhà thầu:** Đấu thầu rộng rãi trong nước, qua mạng.

- **Phương thức lựa chọn nhà thầu:** Một giai đoạn, một túi hồ sơ.

Nguồn vốn: Ngân sách địa phương.

- **Thời gian thực hiện hợp đồng:** 365 ngày kể từ ngày ký hợp đồng.

- **Loại hợp đồng:** Hợp đồng trọn gói.

2. Mục tiêu công việc: Hỗ trợ sử dụng chữ ký số công cộng và hoá đơn điện tử cho doang nghiệp thành lập mới và chi phí thuê kế toán cho các hộ kinh doanh chuyển đổi lên doanh nghiệp

3. Yêu cầu kỹ thuật của gói thầu:

3.1. Danh mục các tài liệu tham chiếu:

- Luật Giao dịch điện tử số 51/2005/QH11 ngày 29/11/2005 của Quốc Hội khóa 11;

- Luật Công nghệ thông tin số 67/2006/QH11 ngày 29/6/2006 của Quốc Hội khóa 11 và Văn bản hợp nhất Luật công nghệ thông tin số: 10/VBHN-VPQH ngày 12/12/2017 của Văn phòng Quốc Hội;

- Nghị định 130/2018/NĐ-CP ngày 27/09/2018 quy định chi tiết về chữ ký số và dịch vụ chứng thực chữ ký số;

- Nghị định số 123/2020/NĐ-CP ngày 19/10/2020 của Chính phủ quy định về hóa đơn, chứng từ;

- Thông tư số 78/2021/TT-BTC ngày 17/9/2021 của Bộ Tài Chính hướng dẫn thực hiện một số điều của Nghị định 123/2020/NĐ-CP ngày 19/10/2020 của Chính phủ qui định về hóa đơn, chứng từ.

3.2. Yêu cầu kỹ thuật Hệ thống hóa đơn điện tử

3.2.1 Yêu cầu chức năng phần mềm

STT	Nội dung yêu cầu	Tiêu chí kỹ thuật
1	Chức năng Hệ thống	
1.1	Hệ thống cần có chức năng quản lý và phân quyền người sử dụng: - Thêm mới/Sửa/Xóa, Khóa người sử dụng. - Phân quyền người sử dụng theo vai trò - Tìm kiếm thông tin người sử dụng	Bắt buộc
1.2	Có chức năng quản trị danh mục hệ thống: - Danh mục người sử dụng - Danh mục sản phẩm - Danh mục khách hàng	Bắt buộc
1.3	Có chức năng quản lý và cấu hình thông tin đơn vị bao gồm: - Thông tin chung về đơn vị: tên, địa chỉ, mã số thuế, điện thoại, email - Cấu hình thông tin chứng thư số để phát hành hóa đơn điện tử	Bắt buộc
1.4	- Hỗ trợ nhiều loại thiết bị ký số HSM, USB Token	Bắt buộc
2	Đăng ký phát hành và Mẫu hóa đơn	
2.1	Có chức năng hỗ trợ thủ tục đăng ký phát hành hóa đơn điện tử: - Hỗ trợ đơn vị tạo lập/quản lý hồ sơ đăng ký phát hành với cơ quan thuế: Thông báo phát hành và đăng ký phát hành - Theo dõi được tình hình sử dụng hóa đơn.	Bắt buộc
2.2	Có chức năng hỗ trợ xây dựng và quản lý mẫu hóa đơn điện tử: - Hỗ trợ nhiều mẫu hóa đơn điện tử, hỗ trợ nhiều loại hóa đơn khác nhau.	Bắt buộc

	- Hỗ trợ hóa đơn nhiều trang	
	- Mẫu hóa đơn theo định dạng XML , Chữ ký số theo chuẩn XML DSign	
3	Phát hành và Phân phối hóa đơn	
3.1	Hỗ trợ nhiều hình thức phát hành hóa đơn:	Bắt buộc
	- Tạo lập hóa đơn bằng nhập dữ liệu trực tiếp trên giao diện	
	- Tạo lập hóa đơn thông qua Webservice.	
	- Tạo lập hóa đơn thông qua upload file excel hoặc XML	
3.2	Hỗ trợ linh động các phương án phát hành hóa đơn : Phát hành hóa đơn lẻ hoặc theo lô nhiều hóa đơn	Bắt buộc
3.3	Năng lực phát hành: Hệ thống có khả năng đáp ứng năng lực phát hành tối thiểu 10 triệu hóa đơn/tháng.	Bắt buộc
3.4	Hỗ trợ phương án phân phối hóa đơn đến khách hàng thông qua các hình thức:	Bắt buộc
	- Email	
	- Cổng tra cứu hóa đơn	
	- Webservice	
3.5	Chức năng cho phép gửi thông tin phát hành hóa đơn cho người mua hàng và cho phép người mua hàng in chuyển đổi hóa đơn để lưu trữ	Bắt buộc
4	Chức năng xử lý hóa đơn	
4.1	- Có chức năng điều chỉnh (tăng, giảm thông tin) và thay thế hóa đơn điện tử	Bắt buộc
	- Có chức năng quản lý/tìm kiếm các hóa đơn điều chỉnh/thay thế.	
	- Chức năng hỗ trợ quản lý các biên bản điều chỉnh/thay thế hóa đơn	

4.2	- Có chức năng xóa bỏ hóa đơn trong trường hợp có lỗi khi lập hóa đơn.	Bắt buộc
	- Có chức năng hủy dải hóa đơn đăng ký không dùng hết:	
	+ Hỗ trợ tìm kiếm và tra cứu thông tin hóa đơn đã bị xóa bỏ trên hệ thống.	
	+ Hóa đơn bị xóa bỏ chỉ bị đánh dấu xóa nhưng vẫn lưu đầy đủ thông tin ban đầu phục vụ tra cứu.	
5	Yêu cầu về báo cáo	Bắt buộc
	- Bảng kê chi tiết hóa đơn phát hành:	
	+ Hệ thống phải cung cấp tính năng cho phép kết xuất bảng kê chi tiết hóa đơn bán hàng	
	+ Báo cáo được lập có thể được kết xuất ra tệp điện tử theo định dạng Excel, pdf, ra máy in	
	- Báo cáo tình hình sử dụng hóa đơn	
	+ Hệ thống phải cung cấp tính năng cho phép lập báo cáo tình hình sử dụng hóa đơn theo kỳ của doanh nghiệp.	
	+ Báo cáo được lập có thể được kết xuất ra tệp điện tử theo định dạng Excel, XML	
6	Cổng thông tin để tra thông tin hóa đơn	
	- Thông tin của khách hàng	
	- Tra cứu hóa đơn: Hiển thị danh sách các hóa đơn điện tử đã được phát hành tới tài khoản của đơn vị tiếp nhận	
	- Cho phép Xem/Ký số/Download hóa đơn điện tử	

3.2.2 **Yêu cầu phi chức năng phần mềm**

1	Yêu cầu về kiến trúc hệ thống: Hỗ trợ tích hợp với các hệ thống phần mềm bên ngoài thông qua API	
2	Yêu cầu ngôn ngữ, mỹ thuật, tính chính xác số học của hệ thống:	
2.1	- Hỗ trợ tối đa khả năng nhập dữ liệu của người dùng.	Bắt buộc

	- Ngôn ngữ sử dụng trong chương trình là tiếng Việt. Font chữ sử dụng là Unicode.	
	- Định dạng các trường dữ liệu hiển thị: Định dạng hiển thị của ngày và tháng là DD/MM/YYYY	
2.2	Yêu cầu về tính chính xác của hệ thống: - Các số thực cần được lưu trữ được ít nhất 2 chữ số phần thập phân (sau dấu phẩy 2 chữ số). - Lưu trữ số liệu trong CSDL: Số tiền VNĐ chính xác đến đơn vị từng đồng.	Bắt buộc
2.3	Giao diện chương trình cần phải hiển thị và hoạt động đúng trên các phiên bản mới của các trình duyệt internet phổ biến: Firefox, Chrome. Ưu tiên giao diện phát triển dựa trên công nghệ HTML 5.	Bắt buộc

3.2.3 **Yêu cầu khác**

1	Yêu cầu về bảo mật	
1.1	Yêu cầu về đăng nhập: - Tên truy cập/mật khẩu có chiều dài tối thiểu là 8 ký tự, trong đó phải có cả ký tự chữ và ký tự số. - Không được phép tạo 2 tên truy cập trùng nhau và mỗi người dùng chỉ có 1 mật khẩu duy nhất. - Không cho phép có khoảng trắng trong tên truy cập và mật khẩu.	Bắt buộc
1.2	Yêu cầu phân quyền: Các chức năng trong hệ thống chỉ được phép thực hiện bởi những người sử dụng có đủ quyền.	Bắt buộc
1.3	Các giao tiếp giữa các thành phần hệ thống hoặc giữa hệ thống và các hệ thống khách của Đơn vị phải được bảo mật đường truyền bằng việc hỗ trợ giao thức bảo mật SSL	Bắt buộc
2	Yêu cầu hạ tầng triển khai	
2.1	Các trung tâm dữ liệu phải đạt các điều kiện tương đương Tier 3 hoặc tương đương - Tiêu chuẩn hạ tầng về trung tâm dữ liệu	Bắt buộc

2.2	Đảm bảo các hoạt động của hệ thống server phải được ghi log để phục vụ các công việc bảo hành, bảo trì.	Bắt buộc
2.3	Bảo đảm hệ thống hoạt động 24/7	Bắt buộc
2.4	Sao lưu và phục hồi dữ liệu: Hệ thống cần có cơ chế sao lưu dữ liệu thường xuyên đề phòng trường hợp hư hỏng thì vẫn có đủ dữ liệu để khôi phục lại hệ thống như trước lúc xảy ra sự cố. Đồng thời hệ thống cũng cần có cơ chế phục hồi nhanh chóng từ các dữ liệu được sao lưu	Bắt buộc
2.5	Có chứng nhận hệ thống quản lý an toàn thông tin theo tiêu chuẩn: ISO/IEC 27001:2013 HOẶC chứng nhận hệ thống quản lý chất lượng ISO 9001:2015 về các l nh vực hoạt động: + Phát triển cung cấp các sản phẩm phầm mềm trong l nh vực: Quản trị doanh nghiệp, quản lý tài chính. + Trung tâm hạ tầng IDC	Bắt buộc
3	Yêu cầu về phần mềm	
	Hệ thống có thể đáp ứng: Thời gian xử lý tối đa cho một giao dịch không quá 60 giây	Bắt buộc

3.3. Yêu cầu kỹ thuật của chữ ký số từ xa.

3.3.1 Yêu cầu đáp ứng quy chuẩn, tiêu chuẩn kỹ thuật được áp dụng

- Đơn vị cung cấp dịch vụ đáp ứng đầy đủ các tiêu chuẩn bắt buộc áp dụng về chữ ký số và dịch vụ chứng thực chữ ký số theo mô hình ký số trên thiết bị di động và ký số từ xa theo thông tư số 16/2019/TT-BTTTT được Bộ Thông tin truyền thông ban hành ngày 05 tháng 12 năm 2019.

- Đơn vị cung cấp dịch vụ chứng thực chữ ký số từ xa phải được đánh giá bởi các Tổ chức audit quốc tế uy tín (Trung tâm Chứng thực điện tử Quốc gia khuyến nghị trong Danh mục các đơn vị đủ điều kiện đánh giá đáp ứng tuân thủ tiêu chuẩn về hệ thống thiết bị quản lý khóa bí mật, chứng thư số và tạo chữ ký số theo mô hình ký số trên thiết bị di động và ký số từ xa – Kèm theo công văn số 105/NEAC-TĐPC ngày 26/03/2021 của Trung tâm Chứng thực điện tử quốc gia) và trực tiếp được cấp chứng chỉ quốc tế cho các tiêu chuẩn sau:

- Tiêu chuẩn yêu cầu về Module ký số bao gồm tiêu chuẩn: EN 419241-2:2019 and ISO 15408 (Mục 2.7.4 Danh mục tiêu chuẩn bắt buộc áp dụng về chữ ký số và dịch vụ chứng thực chữ ký số theo mô hình ký số trên thiết bị di động và ký số từ xa).

- Yêu cầu về chính sách và an ninh cho máy chủ ký số bao gồm tiêu chuẩn: ETSI TS 119 431-1; ETSI TS 119 431-2 (Mục 2.7.1 Danh mục tiêu chuẩn bắt buộc áp dụng về chữ ký số và dịch vụ chứng thực chữ ký số theo mô hình ký số trên thiết bị di động và ký số từ xa).

- Giao thức tạo chữ ký số bao gồm tiêu chuẩn: ETSI TS 119 432 (Mục 2.7.2 Danh mục tiêu chuẩn bắt buộc áp dụng về chữ ký số và dịch vụ chứng thực chữ ký số theo mô hình ký số trên thiết bị di động và ký số từ xa)

- Ứng dụng ký trên máy chủ ký số bao gồm tiêu chuẩn: EN 419241- 1:2018 (Mục 2.7.3 Danh mục tiêu chuẩn bắt buộc áp dụng về chữ ký số và dịch vụ chứng thực chữ ký số theo mô hình ký số trên thiết bị di động và ký số từ xa).

- Các tiêu chuẩn khác cần đáp ứng bao gồm:

+ ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers

+ ETSI EN 319 412-1 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures

+ ETSI EN 319 412-5 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements

Danh mục tiêu chuẩn bắt buộc áp dụng về chữ ký số và dịch vụ chứng thực chữ ký số theo mô hình ký số trên thiết bị di động và ký số từ xa.

Số TT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
1	**Chữ ký số và dịch vụ chứng thực chữ ký số theo mô hình ký số trên thiết bị di động (Mobile PKI)**			
1.1	**Tiêu chuẩn mật mã và chữ ký số**			
1.1.1	Mật mã phi đối xứng và chữ ký số	PKCS #1	RSA Cryptography Standard	- Áp dụng một trong hai tiêu chuẩn. - Đối với tiêu chuẩn RSA:
		ANSI X9.622005	Public Key Cryptography for the Financial Services Industry: The Elliptic	+ Phiên bản 2.1 + Áp dụng lược đồ RSAES-OAEP để mã hóa và RSASSA-PSS để ký.

			Curve Digital Signature Algorithm (ECDSA)	+ Độ dài khóa tối thiểu là 1024 bit - Đối với tiêu chuẩn ECDSA: độ dài khóa tối thiểu là 256 bit
1.1.2	Mật mã đối xứng	TCVN 7816:2007 (FIPS PUB 197) NIST 800- 67	Công nghệ thông tin - Kỹ thuật mật mã - Thuật toán mã hóa dữ liệu AES (Advanced Encryption Standard) Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher	Áp dụng một trong hai tiêu chuẩn
1.1.3	Hàm băm an toàn	FIPS PUB 180-4	Secure Hash Standard	Áp dụng một trong các hàm băm sau: SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256, SHA3224, SHA3-256, SHA3-384,
		FIPS PUB 202	SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions	
Số TT	**Loại tiêu chuẩn**	**Ký hiệu tiêu chuẩn**	**Tên đầy đủ của tiêu chuẩn**	**Quy định áp dụng**
				SHA3512,SHAKE128, SHAKE256
1.2	**Tiêu chuẩn thông tin, dữ liệu**			

1.2.1	Định dạng chứng thư số và danh sách thu hồi chứng thư số	RFC 5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	
1.2.2	Cú pháp thông điệp mật mã	PKCS #7	Cryptographic Message Syntax Standard	Phiên bản 1.5
1.2.3	Cú pháp yêu cầu chứng thực	PCKS #10	Certification Request Syntax Standard	Phiên bản 1.7
1.3	**Tiêu chuẩn chính sách và quy chế chứng thực chữ ký số**			
1.3.1	Khung quy chế chứng thực và sách Practices	RFC 3647 Certificate Policy and Certification Practices Framework	Internet X.509 Public Key Infrastructure - chính	
1.4	**Tiêu chuẩn giao thức lưu trữ và truy xuất chứng thư số**			
1.4.1	Lược đồ Giao thức truy nhập	RFC 2587	Internet X.509 Public Key Infrastructure LDAPv2 Schema	Áp dụng một trong hai tiêu chuẩn
		RFC 4523	Lightweight Directory Access Protocol (LDAP) Schema Definitions for X.509 Certificates	
1.4.2	Giao thức truy nhập thư mục	RFC 2251	Lightweight Directory Access Protocol (v3)	Áp dụng tiêu chuẩn RFC 2251 hoặc bộ bốn tiêu chuẩn: RFC 4510, RFC

		RFC 4510	Lightweight Directory Access Protocol (LDAP): Technical specification Road Map	4511, RFC 4512, RFC 4513
		RFC 4511	Lightweight Directory Access Protocol (LDAP): The Protocol	
		RFC 4512	Lightweight Directory Access Protocol (LDAP): Directory Information Models	
		RFC 4513	Lightweight Directory Access Protocol (LDAP): Authentication	
Số TT	**Loại tiêu chuẩn**	**Ký hiệu tiêu chuẩn**	**Tên đầy đủ của tiêu chuẩn**	**Quy định áp dụng**
			Methods and Security Mechanisms	
1.5	**Tiêu chuẩn kiểm tra trạng ái chứng thư số th**			
1.5.1	Giao thức truyền, nhận chứng thư số và danh sách chứng thư số bị thu hồi	RFC 2585	Internet X.509 Public Key Infrastructure - Operational Protocols: FTP and HTTP	Áp dụng một hoặc cả hai giao thức FTP và HTTP

1.5.2	Giao thức cho kiểm tra trạng thái chứng thư số trực tuyến	RFC 2560	X.509 Internet Public Key Infrastructure - On-line Certificate status protocol	
1.6	**Tiêu chuẩn bảo mật cho M quản lý khóa bí mật của tổ chức cung cấp HS vụ chứng thực chữ ký dịch số**			
1.6.1	Yêu cầu an ninh đối với khối an ninh phần cứng HSM	FIPS PUB 140-2	Security Requirements for Cryptographic Modules	Yêu cầu tối thiểu mức 3 (level 3)
1.7	**Tiêu chuẩn hệ thống thiết bị của khách hàng**	**quản lý khóa bí mật**	**, ch**	**ứng thư số và tạo chữ ký số**
1.7.1	Yêu cầu bảo mật cho thẻ SIM	FIPS PUB 140-2	Security Requirements for Cryptographic Modules	- Áp dụng một trong hai tiêu chuẩn. - Đối với tiêu chuẩn FIPS PUB 140-2: Yêu cầu tối thiểu mức 2 (level 2) - Đối với tiêu chuẩn TCVN 8709 (ISO/IEC 15408): Yêu cầu tối thiểu EAL mức 4 (level 4)
		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)	

1.7.2	Yêu cầu về chức năng, nghiệp vụ	ETSI TR 102 203	Mobile Commerce (M-COMM); Mobile Signatures; Business and Functional Requirements	Phiên bản V1.1.1
1.7.3	Giao diện dịch vụ Web	ETSI TS 102 204	Mobile Commerce (M-COMM); Mobile Signature Service;	Phiên bản V1.1.4

Số TT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
			Web Service Interface	
1.7.4	Khung bảo mật	ETSI TR 102 206	Mobile Commerce (M-COMM); Mobile Signature Service; Security Framework	Phiên bản V1.1.3
1.7.5	Thông số kỹ thuật chuyển vùng	ETSI TS 102 207	Mobile Commerce (M-COMM); Mobile Signature Service; Specifications for Roaming in Mobile Signature Services	Phiên bản V1.1.3
2	**Chữ ký số và dịch vụ chứng thực chữ ký số theo mô hình ký số từ xa (Remote signing)**			
2.1	**Tiêu chuẩn mật mã và chữ ký số**			
2.1.1	Mật mã phi	PKCS # 1	RSA Cryptography	- Áp dụng một trong

	đối xứng và chữ ký số		Standard	hai tiêu chuẩn. - Đối với tiêu chuẩn RSA: + Phiên bản 2.1 + Áp dụng lược đồ RSAES-OAEP để mã hóa 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)	
2.1.2	Mật mã đối xứng	TCVN 7816:2007 (FIPS PUB 197)	Công nghệ thông tin - Kỹ thuật mật mã - Thuật toán mã hóa dữ liệu AES	Áp dụng một trong hai tiêu chuẩn
		NIST 800-67	Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher	
2.1.3	Hàm băm an toàn	FIPS PUB 180-4	Secure Hash Standard	Áp dụng một trong các hàm băm sau: SHA-224, SHA256, SHA-384, SHA-512, SHA-512/224, SHA-512/256, SHA3224, SHA3-256, SHA3-384, SHA3512,SHAKE128, SHAKE256
		FIPS PUB 202	SHA-3 Standard: Permutation-Based Hash and ExtendableOutput Functions	
2.2	**Tiêu chuẩn thông tin, dữ liệu**			

2.2.1	Định dạng chứng thư số và danh sách thu hồi	RFC 5280	Internet X.509 Public Key Infrastructure Certificate and Certificate	

Số TT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
	chứng thư số		Revocation List (CRL) Profile	
2.2.2	Cú pháp thông điệp mật mã	PKCS #7	Cryptographic Message Syntax Standard	Phiên bản 1.5
2.2.3	Cú pháp yêu cầu chứng thực	PCKS #10	Certification Request Syntax Standard	Phiên bản 1.7
2.2.4	Cú pháp thông tin khóa riêng	PKCS #8	Private-Key Information Syntax Standard	Phiên bản 1.2
2.2.5	Giao diện giao tiếp với các thẻ mật mã	PKCS #11	Cryptographic token interface standard	Phiên bản 2.20
2.2.6	Cú pháp trao đổi thông tin cá nhân	PKCS #12	Personal Information Exchange Syntax Standard	Phiên bản 1.0
2.3	**Tiêu chuẩn chính sách và quy chế chứng thực chữ ký số**			
2.3.1	Khung quy chứng Key thực và and chính chứng thư	Internet RFC 3647 sách Practices Framework	X.509 Public chế Infrastructure - Certificate Policy Certification	

2.4	**Tiêu chuẩn giao thức lưu trữ và truy xuất chứng thư số**			
2.4.1	Lược đồ Giao thức truy nhập thư mục	RFC 2587	Internet X.509 Public Key Infrastructure LDAPv2 Schema	Áp dụng một trong hai tiêu chuẩn
		RFC 4523	Lightweight Directory Access Protocol (LDAP) Schema Definitions for X.509 Certificates	
2.4.2	Giao thức truy nhập thư mục	RFC 2251	Lightweight Directory Access Protocol (v3)	Áp dụng tiêu chuẩn RFC 2251 hoặc bộ bốn tiêu chuẩn: RFC 4510, RFC 4511, RFC 4512, RFC 4513
		RFC 4510	Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map	
		RFC 4511	Lightweight Directory Access Protocol (LDAP): The Protocol	
		RFC 4512	Lightweight Directory Access Protocol (LDAP): Directory Information Models	
Số TT	**Loại tiêu chuẩn**	**Ký hiệu tiêu chuẩn**	**Tên đầy đủ của tiêu chuẩn**	**Quy định áp dụng**

		RFC 4513	Lightweight Directory Access Protocol (LDAP): Authentication Methods and Security Mechanisms	
2.5	**Tiêu chuẩn kiểm tra trạng thái chứng thư số**			
2.5.1	Giao thức truyền, nhận chứng thư số và danh sách chứng thư số bị thu hồi	RFC 2585	Internet X.509 Public Key Infrastructure - Operational Protocols: FTP and HTTP	Áp dụng một hoặc cả hai giao thức FTP và HTTP
2.5.2	Giao thức cho kiểm tra trạng thái chứng thư số trực tuyến	RFC 2560	X.509 Internet Public Key Infrastructure - On-line Certificate status protocol	
2.6	**Tiêu chuẩn bảo mật cho HSM quản lý khóa bí mật của tổ chức cung cấp dịch vụ chứng thực chữ ký số**			
2.6.1	Yêu cầu an ninh đối với khối an ninh phần cứng HSM	FIPS PUB 140-2	Security Requirements for Cryptographic Modules	- Áp dụng một trong hai tiêu chuẩn. - Đối với tiêu chuẩn FIPS PUB 140-2: Yêu cầu tối thiểu mức 3 (level 3)
		EN 419221-5:2018	Protection Profiles for TSP Cryptographic modules - Part 5: Cryptographic Module for Trust Services	
2.7	**Tiêu chuẩn hệ thống thiết bị quản lý khóa bí mật, chứng thư số và tạo chữ**			

	ký số của khách hàng			
2.7.1	Yêu cầu chính sách và an ninh cho máy chủ ký số	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	Áp dụng cả bộ tiêu chuẩn 2 phần; Phiên bản V1.1.1 (12/2018)
		ETSI TS 119 431-2	Electronic Signatures and Infrastructures (ESI); Policy and security requirements	
Số TT	**Loại tiêu chuẩn**	**Ký hiệu tiêu chuẩn**	**Tên đầy đủ của tiêu chuẩn**	**Quy định áp dụng**
			for trust service providers; Part 2: TSP service components supporting AdES digital signature creation	
2.7.2	Giao thức tạo chữ ký số	ETSI TS 119 432	Electronic Signatures and Infrastructures (ESI); Protocols for remote digital signature creation	V1.1.1 Phiên bản (03/2019)
2.7.3	Ứng dụng ký trên máy chủ ký số	EN 419241-1:2018	Trustworthy Systems Supporting Server Signing - Part 1: General system security requirements	

2.7.4	Yêu cầu cho mô đun ký số	EN 419241-2:2019	Trustworthy Systems Supporting Server Signing - Part 2: Protection Profile for QSCD for Server Signing	
2.7.5	Yêu cầu an ninh đối với khối an ninh phần cứng HSM	EN 419221-5:2018	Protection Profiles for TSP Cryptographic modules - Part 5: Cryptographic Module for Trust Services	

3.3.2 Yêu cầu đáp ứng quy chuẩn, tiêu chuẩn kỹ thuật được áp dụng

STT	Nội dung yêu cầu	Tiêu chí kỹ thuật
I	**Yêu cầu đảm bảo về nghiệp vụ**	
1	Tích hợp với các hệ thống hiện hành: Hệ thống thuế, hệ thống kho bạc nhà nước, hệ thống hải quan,...	Bắt buộc
2	Yêu cầu ký số trên nhiều định dạng file như pdf, docx, xml, pptx, txt	Bắt buộc
3	Có thể quản lý thông tin chứng thư số đang sử dụng: thông tin chứng thư số, trạng thái chứng thư số.	Bắt buộc
4	Có thể tra cứu lịch sử giao dịch ký số trên smartphone và xuất thông tin tài liệu ký số khi cần (xuất tài liệu ký số *với trường hợp ký số theo file)*	Bắt buộc
5	Có thể tự kích hoạt lại khóa qua ứng dụng trên smartphone, máy tính bảng bằng hình thức xác thực	Bắt buộc
	điện tử thay cho việc phải gặp trực tiếp nhân viên của nhà cung cấp dịch vụ chứng thực chữ ký số mà vẫn đáp ứng đầy đủ quy định pháp luật.	

II	**Tính năng bắt buộc trên ứng dụng xác thực ký số để đáp ứng nghiệp vụ ký số**	
1	Chức năng ký số cho phép xác thực ký số từng file riêng lẻ hoặc theo từng lô tùy vào yêu cầu của cán bộ, giáo viện. Trước khi ký số cần xem được tên ứng dụng gửi yêu cầu ký số, xem chi tiết file ký số	Bắt buộc
2	Xác thực giao dịch ký số thông qua thiết bị smartphone với một trong các hình thức như sinh trắc học, mã PIN.	Bắt buộc
3	Chức năng xem lịch sử ký số: cần lưu được toàn bộ lịch sử ký số của người sử dụng cả trên giao diện web và ứng dụng trên thiết bị di động.	Bắt buộc
4	Yêu cầu có giao diện web quản lý thông tin chứng thư số để theo dõi trạng thái chứng thư số và thông tin chứng thư số. Có tính năng ký số trên giao diện web, tìm kiếm và xuất lịch sử ký số	Bắt buộc
5	Cung cấp giao diện API mở để có thể tích hợp với các phần mềm khi có nhu cầu với đầy đủ các tính năng cơ bản như ký số, xác thực văn bản ký số, quản lý thông tin chứng thư số của người dùng, tra cứu lịch sử giao dịch ký số của người dùng, phục hồi mật khẩu đăng nhập của người dùng.	Bắt buộc

3.4 Yêu cầu kỹ thuật đối với chữ ký số USB token:

3.4.1 Yêu cầu chung

Thiết bị do các nhà thầu cung cấp phải đảm bảo các yêu cầu kỹ thuật sau:

- Mới 100% chưa qua sử dụng, được sản xuất từ năm 2025 trở lại đây, có nguồn gốc xuất xứ rõ ràng, có mác mã, thông số kỹ thuật rõ ràng.

- Đảm bảo tính đồng bộ, tương thích về công nghệ với các thiết bị đang sử dụng tạo doanh nghiệp được hỗ trợ.

- Đối với hàng hóa chào thầu là tương đương hoặc tốt hơn phải kèm theo tài liệu của nhà sản xuất chứng minh.

- Hàng hóa phải được bảo đảm theo tiêu chuẩn của nhà sản xuất.

- Có hệ thống trang hỗ trợ hướng dẫn sử dụng online giúp người dùng dễ dàng tìm kiếm xử lý khi có vấn đề phát sinh.

- Thời gian bảo hành: Tối thiểu 12 tháng

- Cam kết cung cấp đầy đủ tài liệu chứng minh tính hợp lệ của hàng hóa:

+ Giấy chứng nhận xuất xứ (C/O) và giấy chứng nhận chất lượng (C/Q) của hàng hóa (nếu là hàng hóa nhập khẩu)

+ Giấy chứng nhận xuất xưởng, giấy chứng nhận hợp chuẩn, hợp quy (nếu là hàng hóa sản xuất trong nước)

3.4.2 Yêu cầu kỹ thuật chi tiết

STT	Nội dung kỹ thuật	Thông số kỹ thuật
1	***Yêu cầu vật lý đối với Token***	
1.1	Bộ xử lý	Tối thiểu 16 bit
1.2	Bộ nhớ Flash	Tối thiểu 2 MB
1.3	Memory Space	Tối thiểu 64 KB
1.4	Điện năng của Token	250 mW hoặc thấp hơn
1.5	Nhiệt độ thiết bị	Hoạt động tốt ở nhiệt độ 0 đến 50 độ C
1.6	Nhiệt độ lưu trữ	Hoạt động tốt từ -20 đến 60 độ C
1.7	Connectivity	Hỗ trợ USB 1.1, 2.0 trở lên
1.8	Interfaces	CCID, ISO 7816
1.9	Thời gian sống của bộ nhớ	Tối thiểu 10 năm
1.10	Hỗ trợ các chuẩn	Tuân theo chuẩn CE, FCC, RoHS
1.11	Khả năng chống ẩm	Hoạt động tốt tại độ ẩm từ 0–100% không ngưng tụ thành giọt
1.12	Yêu cầu về chứng nhận quốc tế	Có chứng nhận đạt chuẩn FIPS PUB 140-2 level 2 trở lên.
2	***Yêu cầu môi trường hỗ trợ***	
2.1	Hỗ trợ các hệ điều hành	- Windows Server từ bản 2003 trở lên
		- Windows từ bản XP trở lên
		- Mac OS X từ bản 10.6 trở lên

		- Hỗ trợ cả 32 và 64bit cho Windows và Mac OS
2.2	Hỗ trợ các trình duyệt	Hỗ trợ plugin cho phép tương tác các trình duyệt IE, Firefox, Chrome, Safari với thiết bị trong Windows và Firefox, Chrome, Safari trong MAC OS
2.3	Hỗ trợ tiêu chuẩn API	PKCS#11v2.2, Microsoft CSP, Microsoft CNG, PC/SC, X.509 v3 certificate storage, SSL v3, IPSec/IKE
2.4	Thuật toán hỗ trợ	RSA 1024-bit, RSA 2048-bit, 3DES, AES (128, 192, 256 bit), SHA-1, SHA-2 (SHA224, SHA-256, SHA-384, SHA-512)
3	***Các yêu cầu về hỗ trợ Client Token Manager và Thư viện***	

STT	**Nội dung kỹ thuật**	**Thông số kỹ thuật**
3.1	Cài đặt tự động	Hỗ trợ tự động cài đặt chứng thư vào IE, Firefox, Thunderbird, Chrome, Trust root CA của Windows
3.2	Thông báo trước khi chứng thư hết hạn	- Thông báo trước khi chứng thư hết hạn.
		- Hỗ trợ customize số ngày Thông báo trước khi hết hạn.
3.3	Thay đổi PIN,	Cho phép
3.4	Các yêu cầu lưu trữ	Phải lưu được Certificate
3.5	Hỗ trợ chức năng mở khóa token từ xa	Liên kết với WS của hệ thống quản lý token để cho phép quản trị viên có thể mở khóa token của khách hàng từ xa

3.6	Hỗ trợ xóa, thay đổi, cập nhật chứng thư cho khách hàng	Phải hỗ trợ cho phần mềm quản lý chứng thư tại Trung tâm/các đại lý CA, để có thể thực hiện tính năng xóa, thay đổi, cập nhật chứng thư cho khách hàng (Admin tool PC).
3.7	Hỗ trợ các phần mềm CA	EJBCA, Entrust, RSA,VeriSign
3.8	Hỗ trợ các ứng dụng khác	Hỗ trợ tất cả các ứng dụng sử dụng phương thức PKCS#11 hoặc CSP cụ thể:
		- Microsoft Office (từ bản Office 2003 trở lên)
3.9	Chỉ sinh được chứng thư số của Nhà cung cấp	Chỉ sinh được chứng thư số của Nhà cung cấp vào Token Nhà cung cấp
3.10	Khởi tạo Token	Phải khởi tạo Token trước khi chuyển qua cho Nhà cũng cấp
3.11	SOPIN	SOPIN phải khác nhau trên mỗi loại thiết bị Token, SOPIN phải được cung cấp tương ứng với mỗi serial của token.
3.12	Yêu cầu cung cấp SOPIN, số Serial của mỗi Token để phục vụ việc phát triển	Đáp ứng đầy đủ các yêu cầu của nội dung kỹ thuật
3.13	Token có thể chạy được với người sử dụng không có quyền Quản trị (Administrator)	Đáp ứng đầy đủ các yêu cầu của nội dung kỹ thuật
3.14	Yêu cầu có sự hỗ trợ lâu dài với thiết bị.	Đáp ứng đầy đủ các yêu cầu của nội dung kỹ thuật
3.15	Token phải được đặt trong hộp bìa cứng, có lót xốp bên trong.	Đáp ứng đầy đủ các yêu cầu của nội dung kỹ thuật
3.16	Ngôn ngữ hỗ trợ	Tiếng Việt và Tiếng Anh trên cả 3 phiên
STT	**Nội dung kỹ thuật**	**Thông số kỹ thuật**
		bản cho Windows, MacOS

3.17	Yêu cầu về bộ cài đặt	Hỗ trợ bộ cài đặt trên windows. MACOSX
3.18	Yêu cầu sử dụng	Có thể sử dụng cho các hệ thống của Tổng Cục Thuế, Tổng Cục Hải quan, Bộ Y tế, BHXH, Ủy Ban Chứng Khoán
3.19	Yêu cầu bảo mật thông tin	Nhà cung cấp phải cam kết bảo mật toàn bộ thông tin, dữ liệu về các token đã cung cấp

3.5. Yêu cầu về triển khai thực hiện gói thầu:

- Trình bày kế hoạch triển khai dịch vụ đến doanh nghiệp thành lập mới thuộc Sở Tài chính thành phố Huế.

- Trình bày biện pháp đảm bảo cung cấp dịch vụ chữ ký số và hóa đơn điện tử đúng qui trình, bàn giao đến từng doanh nghiệp thành lập mới trong năm 2026.

- Nhà thầu phải cam kết việc cung cấp dịch vụ cho các doanh nghiệp mới trong vòng 02 tháng kể từ ngày kí kết hợp đồng phải đạt 80% số lượng doanh nghiệp thành lập.

4. Giải pháp và phương pháp luận:

Nhà thầu chuẩn bị đề xuất giải pháp, phương pháp luận tổng quát thực hiện dịch vụ theo các nội dung quy định tại Chương này, gồm các phần như sau:

1. Giải pháp và phương pháp luận;

2. Kế hoạch công tác.

5. Quy định về kiểm tra, nghiệm thu sản phẩm:

Văn bản xác nhận nghiệm thu của doanh nghiệp nhận hỗ trợ sử dụng dịch vụ.