PHỤ LỤC 01

TIÊU CHUẨN KỸ THUẬT VỀ TRIỂN KHAI OPEN API TRONG NGÀNH NGÂN HÀNG

(Ban hành kèm theo Thông tư số .../2024/TT-NHNN ngày ... tháng .... năm 2024 của Thống đốc Ngân hàng Nhà nước Việt Nam)

Số TT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Quy định áp dụng
1	**Tiêu chuẩn về kiến trúc**			
1.1	Trao đổi dữ liệu			
		REST	REpresentational State Transfer	Bắt buộc áp dụng
		SOAP	Simple Object Access Protocol	Khuyến nghị áp dụng đối với các API mở rộng của Ngân hàng.
1.2	Định dạng trao đổi dữ liệu			
		JSON	Javascript Object Notation	Bắt buộc áp dụng
		XML	Extensible Markup Language	Khuyến nghị áp dụng đối với các API mở rộng của Ngân hàng
1.3	Công cụ mô tả API			Khuyến nghị áp dụng một trong các tiêu chuẩn dưới đây
		SWAGGER	Real-time Streaming Protocol	
		OpenAPI Generator	Open Application Programming Interface Generator	
		RAML	RESTful API Modeling Language	
		API BLUEPRINT	Application Programming Interface Blueprint	

2	**Tiêu chuẩn về dữ liệu**			
2.1	Định dạng dữ liệu	ISO 20022	International Organization for Standardization 20022	Khuyến khích áp dụng một trong các tiêu chuẩn chuẩn
		ISO 8583	International Organization for Standardization 8583	
		OFX	Open Financial Exchange	
3	**Tiêu chuẩn về an toàn thông tin**			
3.1	Giải pháp xác thực, ủy quyền người sử dụng	RFC 6749	The OAuth 2.0 Authorization Framework	- Bắt buộc áp dụng theo RFC 6749, RFC 6750. - Có thể kết hợp RFC 6749, RFC 6750 với các tiêu chuẩn RFC 7636, OIDC tùy theo các trường hợp áp dụng
		RFC 6750	The OAuth 2.0 Authorization Framework: Bearer Token Usage	
		RFC 7636	Proof Key for Code Exchange by OAuth Public Clients	
		OIDC	Open Identity Connect	
		SAML v2.0	Security Assertion Markup Language version 2.0	Khuyến nghị áp dụng đối với các API mở rộng của Ngân hàng.
3.2	An toàn tầng giao vận	SSH v2.0	Secure Shell version 2.0	Bắt buộc áp dụng
		HTTPS	Hypertext Transfer Protocol Secure	Bắt buộc áp dụng
		TLS v1.2 trở lên	Transport Layer Security version 1.2+	Bắt buộc áp dụng cho kết nối giữa TPP và Bank theo cơ chế xác thực chéo mTLS
3.3	Giải thuật mã hóa	TCVN 7816:2007	Công nghệ thông tin. Kỹ thuật mật mã thuật toán mã dữ liệu AES	Khuyến nghị áp dụng
		PKCS #1 V2.1	RSA Cryptography Standard - version 2.1	Khuyến nghị áp dụng, sử dụng lược đồ RSAES-OAEP để mã hóa. Độ dài khóa tối thiểu là 2048 bit

		ECC	Elliptic Curve Cryptography	Khuyến nghị áp dụng. Độ dài khóa tối thiểu 256 bit
		JWE	JSON Web Encryption	Khuyến nghị áp dụng theo RFC 7516
		TCVN 11367-2:2016	Công nghệ thông tin – Các kỹ thuật an toàn – Thuật toán mật mã phi đối xứng.	Khuyến nghị áp dụng
3.4	Thuật toán chữ ký số	PKCS #1	RSA Cryptography Standard - version 2.1 hoặc cao hơn	- Áp dụng một trong các tiêu chuẩn. - Độ dài khóa tối thiểu là 2048 bit đối với RSA và 256 bit đối với ECDSA
		ECDSA	Elliptic Curve Digital Signature Algorithm	
		TCVN 7635:2007	Các kỹ thuật mật mã – Chữ ký số	
3.5	Giải thuật băm cho chữ ký số	FIPS PUB 180-4	Secure Hash Algorithms	Áp dụng một trong các hàm băm sau: SHA2-56, SHA-384, SHA-512, SHA-512/256, SHA3-256, SHA3-384, SHA3-512, SHAKE128, SHAKE256
		FIPS PUB 202	SHA-3 Standard: Permutation Based Hash and Extendable Output Functions	

3.6	Toàn vẹn dữ liệu	JWS - JSON Web Signature	Javascript Object Notation Web Signature	Bắt buộc áp dụng: - Theo chuẩn RFC 7515. - Độ dài khóa tối thiểu là 2048 bit đối với RSA và 256 bit đối với ECDSA.
3.7	An toàn Hệ thống thông tin	ISO27001:2013	International Organization for Standardization 27001:2013	Bắt buộc áp dụng một trong hai tiêu chuẩn.
		TCVN 11930:2017	Công nghệ thông tin – Các kỹ thuật an toàn – Yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ	