X9 Informative Report

Title: ASC X9 Financial PKI Use-Cases

Released Date: April 1, 2025

By: X9 PKI Policy Group

This page left intentionally blank

Table of Contents

Forward

This Informative Report has been approved and released by the Accredited Standards Committee X9, Incorporated, 275 West Street, Suite 107, Annapolis, MD 21401. This document is copyrighted by X9 and is not an American National Standard and the material contained herein is not normative in nature. Comments on the content of this document should be sent to: Attn: Executive Director, Accredited Standards Committee X9, Inc., 275 West Street, Suite 107, Annapolis, MD 21401,

This Informative Report is a product of the Accredited Standards Committee X9 Financial Industry Standards and was generated by the Public Key Infrastructure (PKI) Study Group created by the X9 Board of Directors in 2018 to research the state of the PKI industry, summarizing the findings of the group.

Suggestions for the improvement or revision of this Informative Report are welcome. They should be sent to the X9 Committee Secretariat, Accredited Standards Committee X9, Inc., Financial Industry Standards, 275 West Street, Suite 107, Annapolis, MD 21401 USA or emailed to admin@x9.org.

Published by

Accredited Standards Committee X9, Incorporated
Financial Industry Standards
275 West Street, Suite 107
Annapolis, MD 21401 USA
X9 Online http://www.x9.org

Introduction

This Informative Report is a product of the Accredited Standards Committee X9 Financial Industry Standards and was generated by the X9 Public Key Infrastructure (PKI) Policy Group. This Informative Report is a list of PKI use-cases relevant to the Financial Services industry.

As information and communication technologies evolve, services and applications become more reliant on the Internet and other high-speed communication. Similarly, reliance increases on cryptographic methods used to protect the confidentiality, integrity, availability and authentication of data, messages, and transactions exchanged over these channels. Further, short-term and long-term data storage requires interoperable confidentiality, integrity, availability, and authentication. These security, technical and business needs are often addressed by Public Key Cryptography (PKC) technologies resulting in broad deployments of Public Key Infrastructures (PKIs). Many PKI are publicly trusted, while others are privately trusted.

Financial information is often reliant on PKIs, where the PKIs can be either public or private. However, these PKI are frequently designed for general use across many diverse industries rather than being focused on the financial services industry, a highly regulated industry. Consequently, PKI users rely on these general-use PKIs for specialized protection. Accordingly, the X9 PKI Policy Group performed the following major tasks:

1) Analyzed how various PKI are being used in the financial services community through a collection of existing and trending Use Cases,
2) Made recommendations and propose new standards where X9 can lead the financial services community in the use of PKI technologies, and

3) Explored the feasibility of developing an X9 sponsored PKI for its members.

The X9 PKI Policy Group will continue to research, analyze, and formulate recommendations relating to PKI policy and practices for the financial services industry. This group will also continue to maintain and develop PKI related policies.

Suggestions for the improvement or revision of this Informative Report are welcome. They should be sent to the X9 Committee Secretariat, Accredited Standards Committee X9, Inc., Financial Industry Standards, 275 West Street, Suite 107, Annapolis, MD 21401 USA or emailed to admin@x9.org.

1 Scope

The scope of this Informative Report is to provide Public Key Infrastructure (PKI) Use Cases for the financial services industry, employed to determine recommendations for PKI policy and practices, X9 standards, and an X9 sponsored PKI. This report represents the consensus of the X9F PKI Study Group. The use of publicly trusted (non-web browser) PKI solutions in the financial community has recently caused substantial issues to surface which affect the availability of financial transactions. Browsers control the use of "public" CA roots and the certificates that can be issued from them. Historically, the financial community has made use of these publicly trusted roots in payment terminals and other transaction-oriented devices.

As financial services evolve, the list of these services continues to expand and the priority of some of the use cases has changed.

2 Purpose

The purpose of this Informative Report is to identify Use Cases of PKI in the Financial Services industry and identify which are potentially harmed (or benefited) by the continued use of the public internet PKI and other evolving communication. Upon analyzing these Use Cases, the group will make recommendations which may involve a further standards, technical reports, or other reports.

2.1 Background

X9F has a 25-year history in developing and maintaining PKI-related standards.

- X9.57 and X9.55 were developed by X9F1 and published in 1997, submitted to TC68 and transitioned by TC68/SC2/WG8 as ISO 15782 parts 1 and 2 in 2003 and 2001.
- X9.79-1 was developed by X9F5 and published in 2001, submitted to TC68 and transitioned by TC68/SC2/WG8 as ISO 21188 in 2006.
- Subsequently, X9F5 was disbanded and its PKI work migrated to X9F4.
- ISO 21188 was merged with ISO 15782 by TC68/SC2/WG8 with X9F4 participation and published as ISO 21188 in 2018.
- Consequently, ISO 15782 was withdrawn by SC2.
- Afterwards, JTC1/SC27 attempted to transfer ISO 21188 from TC68/SC2 but ANSI/X9, OASIS/CS1 and others opposed the effort, so ISO 21188 will remain within TC68/SC2.

AICPA[1] and the CICA[2] collaborated to develop WebTrust for CA[3] published in 1999 using the control objectives and evaluation criteria from the draft X9.79-1 standard. Browser manufacturers (e.g. Microsoft, Google, and Apple) adopted WebTrust for CA audits as a prerequisite to allow a public CA's PKI certificates in their products. The auditing standard has been licensed in multiple countries and adopted in many legal jurisdictions. Subsequently WebTrust for CA incorporated ISO 21188:2006 and continues to be maintained by the joint WebTrust/PKI Assurance[5] task force and the CA Browser Forum.

Meanwhile, the PKI Forum was established in 1999 as a marketing and technology program, published multiple PKI Notes whitepapers, but eventually transitioned as OASIS IDtrust[4] member section in 2003. During its lifespan the

---

[1] American Institute of Certified Public Accountants www.aicpa.org

[2] Canadian Institute of Chartered Accountants www.cica.org

[3] WebTrust for Certification Authorities www.webtrust.org

[4] OASIS Identity Trust www.oasis-idtrust.org

PKI Forum held a Certification Authority Industry Summit Meeting in June 2002 to address several major industry issues:

1) Obtain feedback regarding Levels of Assurance Assigned to Certificates and Identification and Authentication Procedures Required.
2) Discuss Cross Certification of CA's to WebTrust Certified CA's.
3) Discuss CA's Subordinate to WebTrust Certified Root CA's and build consensus.

The CA Browser Forum[5] (CABF) was organized in 2005, consisting of Certification Authorities (48), Internet browser software vendors (8), and other software application developers, to manage TLS and Code Sign certificate usage. However, the CABF is industry agnostic; it does not address the specific needs of any particular industry, including financial services.

In addition to the CABF, individual root programs have their own set of rules for roots that are embedded in the browsers (e.g. Firefox[6], Chrome[7]) or operating systems (e.g. Apple[8], Microsoft[9]). Implementation of rules in both the browser root programs and the CABF happen irrespective of timelines associated with the financial community (e.g. holiday blackout periods, equipment technology upgrades). This has caused problems in the past, for example, when one browser suddenly announced it would no longer accept issuance of SHA-1 certificates from publicly trusted CAs (effective immediately), this caused turmoil with the tens of thousands of payment terminals that had not yet upgraded. While some browsers are more amicable to the needs of the financial community, the rules for the web PKI are determined by the most restrictive root program.

2.2 PKI types and Use Case Considerations and Issues

PKI architectures and Use Cases have particular concerns that need to be taken into consideration for a successful integration of PKI features. The following is a short list of architectures and Use Case concerns.

2.2.1 PKI Architectures

Today, there are numerous PKI implementations, some obvious to the user and some below the surface and quite opaque to users, with various pros and cons that can have a real impact on the security of the application relying on the PKI. Some of the more notable areas are:

1. Raw public keys:

   Public keys distributed with no authentication or certification. Without third-party authentication, there is no trusted party on which to rely providing assurances that the private key is not compromised, that it belongs to the claimed owner, and that the claimed owner has been verified (they may be verified out of band). No reliance can be made on such a public key that even the communication session is protected from compromise.

2. End-point self-signed certificates:

   Products often allow self-signed certificates for TLS connections or other uses. For cons, an endpoint selfsigned certificate does not provide any data integrity or authentication. The certificate signature is generated using the subject private key and verified using the subject public key. However, an adversary can replace the subject public key and re-sign the certificate using the adversary's private key. Consequently, any

---

5 CA Browser Forum https://cabforum.org/

6 http://www.mozilla.org/projects/security/certs/policy/

7 https://www.chromium.org/Home/chromium-security/root-ca-policy

8 http://www.apple.com/certificateauthority/ca_program.html

9 https://aka.ms/rootcert

information in the certificate such as the issuer CA name or certificate key usages can also be modified. Further, software that supports self-signed certificates has a fundamental validation design flaw. The only pro is that self-signed certificates are easy to issue and use.

3. Embedded product CA:

   An attempt to avoid end-point self-signed certificates is to embed a CA within the product. For cons, the CA is implemented in software, so the CA private key is not protected using a cryptographic hardware security module (HSM) though may have been protected in secure silicon chips. The CA keys might be generated during installation, but often cannot be replaced. The embedded CA generates a CA self-signed certificate and end-point certificates that must be installed on end-point equipment. The end-point keys might be generated on the equipment with a certificate signing request (CSR) submitted, or the product CA might provision the equipment keys. Embedded CA products typically do not offer revocation services and X.509 extensions are often limited with default values. Often certificate (and private key) issuance are done using manual procedures with limited auditing capabilities. Embedded CA products tend to proliferate within an organization, each instance is usually managed by application teams versus a centralized PKI team, and no certification practice statement (CPS) is available. If the embedded product CA is compromised there may be no way to replace the CA and Certificates on the devices. An advantage is that end-point self-signed certificates are not used; an out-of-band verification is not required. Refer to #2 End-point Self-Signed Certificates for more information.

4. Vendor private PKI:

   An alternative is an external private PKI provided by the vendor consisting of at least a root CA, possibly one or more intermediary CA, and an issuing CA for the product and end-point certificates. The vendor private PKI issues various certificates for the product and corresponding end-point certificates. For cons, the end-point equipment might generate keys but needs to submit a CSR to the vendor private PKI. Further, the vendor private PKI might support revocation but distributing certificate revocation lists (CRL) or connecting to an online certificate status protocol (OCSP) responder is problematic. The PKI certificates need to be installed with the product and the end-point equipment. The vendor private PKI may offer a CPS with subscriber agreements, warranty statements, and relying party agreements but these documents vary greatly among vendors and analyzing them can be very time consuming and expensive. However, the vendor private PKI might not undergo a WebTrust for CA audit for assurance or any audit at all, so assessing the security of the PKI is an open question. For pros, the vendor private PKI might offer a CPS with corresponding agreements, certificate status, and cyclic WebTrust for CA audits.

5. Customer private PKI:

   Another alternative to an embedded CA product or vendor private PKI is a customer private PKI that issues various certificates for the product and corresponding end-point certificates. For cons, the customer private PKI might not be compatible with the vendor's product, it should offer a CPS with corresponding agreements, and should undergo a WebTrust for CA audit. For pros, the customer private PKI is known internally to the organization, it offers a CPS with corresponding agreements, certificate status, and should submit to cyclic WebTrust for CA audits. An example of customer private PKIs is certificate-based Point-of-Interaction merchant bank card terminals that encrypt their bank card data between the merchant terminal and their bank card processor.

6. Generic public PKI:

   Another option to using a vendor or customer private PKI is reliance on a public PKI that issues various certificates for the product and corresponding end-point certificates. For cons, the public PKI is generic; it does not address the specific needs of the financial services industry. Further, the vendor needs to test its products with many public PKIs for compatibility. The product may not be able to access the public CRL or OCSP responder from a private network firewalled from the Internet by a DMZ. If the Generic public PKI was to go out of business, the financial services organizations relying on these certificates would have to scramble to replace them within their infrastructure with a competing brand. The pros include wide and public distribution of trust anchor CA root certificates, a CPS with corresponding agreements, certificate status, and cyclic WebTrust for CA audits. An example of generic public PKIs are SSL / TLS certificates whose roots are embedded in browsers.

2.2.2 Use Case and Implementation Issues

1. PKI used as the basis for Cryptocurrencies and Blockchain Implementations:

   An emerging challenge regarding PKI trustworthiness stems from the recent rise and proliferation in cryptocurrencies and the use of Blockchain to protect and verify a wide variety of transactions and provide the basis for electronic record keeping. Immediate investigation into how PKI is being implemented and used with Blockchain systems would be beneficial. The current lack of standards regarding how PKI is deployed within these new technologies creates considerable concerns. Financial institutions often need to trust vendor proprietary CA or private PKI without the benefit of transparency or independent assessments (e.g. WebTrust for CA audits).

2. Revocation Issues:

   A basic PKI operational control is the ability to terminate usage of an asymmetric key pair prior to its expiration date by revoking the certificate. When the relying party checks the certificate status using the associated CRL or OCSP server, and discovers that the certificate is no longer valid, the certificate should not be used. Data should no longer be encrypted nor should digital signatures be verified, just as if the certificate had expired. However, when the CRL or OCSP is unavailable or not supported, the certificate status cannot be checked. CRLs or OCSP might not be available within a private network when the public CRL or OCSP cannot be accessed. Also, CRLs and OCSP usage may not be possible with a public connection when the private CRL or OCSP cannot be accessed. Finally, the CA may simply not provide CRL or OCSP support. There are risk-based decisions that need to be made regarding the choice and use of PKI systems in light of the availability and effectiveness of their revocation systems.

   Recent advances have shown that it is practical to perform secure, efficient, private, and reliable certificate revocation without relying upon CRL or OCSP services (https://cabforum.org/wp-content/uploads/CABF_F2Fpreso_030518_vmf.pdf). This eliminates the need to move to shorter and shorter certificate lifetime periods, and reduces the need to frequently access high availability systems for certificate replacement, reducing the risk of unintended downtime when certificate replacement does not go smoothly.

3. Quantum Computing Risks:

   Some mathematical problems are sufficiently difficult to solve on classical computers that they are the basis for cryptographic algorithms. For example, RSA is based on factoring N (a product of primes) and Diffie-Hellman is based on discrete logarithms (the inverse of exponentiation), both computationally intensive. However, the advent of quantum computers will allow some cryptographic problems to be solved, such that the asymmetric private key can be determined from the public key. Hence, some of the existing algorithms will need remediation with post-quantum cryptography (PQC) or other methods. The NIST Post-Quantum Cryptography project released the PQC algorithms with new standards in August 2024. See: (https://csrc.nist.gov/Projects/Post-Quantum-Cryptography)". X9 has recently published a report on Quantum Computing risks to the Financial Sector. That report can be obtained through the X9 website at: https://x9.org/download-qc-ir/

   By contrast, having a dedicated PKI for the financial services industry should resolve many issues of PKI trustworthiness. However, a private PKI might need to interoperate over an X9-based financial PKI Bridge. This study group will research various PKI strategies and operational tactics.

3 Normative References

The following referenced documents are indispensable for the application of this document. For dated references, only the specific edition cited applies. For undated references, the most recent edition of the referenced document (including any amendments) applies.

2.1. ISO 21188-2018 Public key infrastructure for financial services -- Practices and policy framework

2.2. X9.24-2-2016 Retail Financial Service Symmetric Key Management Part 2: Using Asymmetric Techniques for the Distribution of Symmetric Keys

2.3. CA Browser Forum: Baseline Requirements for the Issuance and Management of Publicly Trusted TLS Server Certificates,

2.4. CA Browser Forum: Baseline Requirements for the Issuance and Management of Publicly Trusted Code Signing Certificates,

2.5. CA Browser Forum: Guidelines for the Issuance and Management of Extended Validation [EV] Certificates,

4 Symbols and abbreviated terms

For the purposes of this report, the following symbols and abbreviations apply.

4.1 FI
Financial Institution

4.2 IETF
Internet Engineering Task Force www.ietf.org

4.3 Financially Trusted Certificate
Public key certificate issued by the X9 Financial PKI

4.4 PKC
Public Key Cryptography

4.5 PKI
Public Key Infrastructure

4.6 Publicly Trusted Certificate
A certificate that is trusted by virtue of the fact that its corresponding Root Certificate is distributed as a trust anchor in widely available application [browser] software. [2.3]

4.7 TLS
Transport Layer Security

TLS is defined in the Internet Engineering Task Force (IETF) specifications:

- IETF RFC 2246 TLS v1.0
- IETF RFC 4346 TLS v1.1
- IETF RFC 5246 TLS v1.2
- IETF RFC 8446 TLS v1.3

5 PKI Use Cases

5.1 Introduction

This is not an exhaustive list of Use Cases but represents those that the group members felt were the most important and visible in the community.

5.2 Financial TLS Web Services

Publicly Trusted Certificates are certificates trusted by virtue that its corresponding Root Certificate is distributed as a trust anchor in widely available application [browser] software. [4.6]

Financially Trusted Certificates are public key certificates issued by the X9 Financial PKI. [4.3]

Server certificates used in typical TLS environment for consumer/customer sessions. In this configuration, the certificate is used for basic server authentication and securing the session without client authentication. Services may extend to bill payment, account review, small transaction/funds transfer, etc. These services should always be accompanied by customer authentication protected within the TLS session. TLS web server certificates are issued in three categories: Domain Validated (DV), Organizationally Validated (OV), and Extended Validation (EV). The CA/B Forum has published definitions for TLS certificates[10]. The PCI SSC has published a document titled, Best Practices for Securing E-commerce[11] which contains recommendations on the type of certificates useful for e-commerce, similar to that noted below:

DV: The lowest level of authentication, where only the domain name is verified, for situations only where trust and credibility have low risk, e.g., B2B or machine-to-machine type of communication where a consumer is not directly involved. DV certs are acceptable when used between entities that have a formal business relationship and contract in place (which authenticates and documents the relationship between the entities), and the DV cert's role is that of encrypting data-in-motion between the parties.

OV: A more secure step where the CA vets the business before issuance of the certificate, recommended for public-facing websites not dealing with personally identifiable information (PII) or financial information.

EV: The highest level of authentication of the business by the CA, recommended for websites handling CHD, PII, PHI and other sensitive data.

It is recommended the certificates (certs) be configured to use the highest level of security available regardless of the type of certificate used.

Section 5.6 Financial TLS Point-of-Interaction (POI) Services outlines the use case for a private PKI for financial TLS POI.

5.3 Financial TLS Aggregator Services

This is used by financial services aggregator portals. Two distinct types of communication are included in this Use Case. To their users, these portals appear as servers. To financial services

---

[10] https://cabforum.org/about/information/consumers/#what-are-the-different-types-of-ssl-certificates

[11] https://www.pcisecuritystandards.org/pdfs/best_practices_securing_ecommerce.pdf

providers, these services appear as users. When connecting to service providers, a standard Financial TLS connection as a client can be established as defined in §5.2 Financial TLS Web Services. The aggregator appears as a server to users/clients of the service as defined in the Financial TLS Use Case.

5.4 Financial TLS Host Services

Host-to-Host services operating within TLS offer additional protection through mutual authentication of the entities in the session. Services operating within this mutual authentication environment may include FI-to-FI transfers, business-to-business exchanges, business-to-FI exchanges, and consumer-to-FI sessions. Interactions within this environment are typically higher value or risk and require additional entity authentication, such as EV or Qualified Website Authentication Certificates (QWAC)

5.5 Financial TLS Message Queue (MQ) Services

Message Queue (MQ) software enables asynchronous communication between applications within serverless and microservices architectures. This means that they enable applications to seamlessly process requests, manage workloads, and handle complex workflows, without a developer having to couple or integrate them. To achieve this, the MQ software receives messages from the sending application called a producer, and adds those messages to a queue, where they wait to be processed by a receiving application. These receiving applications, also called consumers, process the messages in the queue and perform necessary actions based on the content of the message. The Top 10 Message Queue Software[12] include:

- Amazon Simple Queue Service (SQS)
- Anypoint MQ
- Apache Kafka
- Azure Service Bus
- EMQ Technologies EMQX
- IBM MQ
- RabbitMQ
- Red Hat AMQ
- Solace PubSub+ Event Broker
- TIBCO Enterprise Message Service

MQ is widely used in financial institutions due to its reliability, security, and ability to handle high volumes of transactions. It provides reliable messaging between its components - queue manager, message queues, applications that can be run on different platforms, including mainframe, distributed systems and cloud environment. It uses TLS to secure the communication channel between the queue manager and the application. Mutual authentication is commonly used with message queue systems due to the stringent security requirement of financial transactions, where it is crucial to verify the identities of both parties to prevent unauthorized access and ensure data integrity. MQ itself does not issue certificates. They are typically issued by a trusted third-party CA.

5.6 Financial TLS Point-of-Interaction (POI) Services

Point-of-Interaction (client) device, such as ATM or other Point-of-Interaction (POI) devices, to a remote processing host (server) system using TLS to provide an encrypted session that may use TLS mutual authentication techniques.

---

[12] https://expertinsights.com/insights/the-top-message-queue-mq-software/

5.7 Financial Virtual Private Cloud (VPC)

Cloud server access, while often utilizing TLS connections, distinguish themselves by including a separate multi-tenant environment, may be managed by a third party for data storage and/or processing. Access can be direct between a client and the cloud environment or utilized by an application to backup data. The third-party cloud provider can be unknown to the client. The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

See Special Publication 800-145: https://csrc.nist.gov/pubs/sp/800/145/final

In a VPC, the previously described mechanism, providing isolation within the cloud, is accompanied with a virtual private network (VPN) function (again, allocated per VPC user) that secures, by means of authentication and encryption, the remote access of the organization to its VPC resources.

5.8 Financial File Transfer Protocol Secure (FTPS) Services

Financial File Transfer Protocol Secure FTP (FTPS) originally used SSL (FTP-SSL) but now uses TLS for encryption and authentication. FTPS uses extensions to FTP that add support for the TLS protocols. Like FTP, FTPS uses two connections: a command channel and a data channel, either or both can be encrypted.

5.9 Financial Secure File Transfer Protocol (SFTP) Services

Secure File Transfer Protocol (SFTP or SSH-FTP) uses Secure Shell (SSH) for encryption and authentication. SFTP uses extensions to SSH that add support for FTP. SFTP is a separate protocol, replacing Secure Copy (SCL) not to be confused with FTPS or running FTP over an SSH connection.

5.10 Financial SSH Services

Secure Shell (SSH) is a cryptographic protocol for network administration, replacing Telnet, and is used to secure other unsecured administrative protocols. SSH is typically used over any network connection, allowing an administration client to connect to a server.

5.11 Financial Device Remote Key Load (RKL)

Asymmetric public keys are used for remote key load (RKL) of symmetric keys between a Key Distribution Host (KDH) and one or more Key Receiving Devices (KRD). The KRD asymmetric key pair is used to encrypt and decrypt the symmetric key block containing the encrypted symmetric keys. The KDH asymmetric key pair is used to sign and verify the symmetric key block containing the encrypted symmetric keys. For more information, see:

- ANS X9.24 Retail Financial Services Symmetric Key Management – Part 2: Using Asymmetric Techniques for the Distribution of Symmetric Keys
- X9-TR-34-2012 Interoperable Method For Distribution Of Symmetric Keys Using Asymmetric Techniques: Part 1 - Using Factoring-Based Public Key Cryptography Unilateral Key

5.12 Financial Device Authentication

PKI used in this application can assist in the authentication of devices used in financial processing, or for initiating or processing financial transactions. These can include merchant point-of-interaction / point-of-sale devices, ATMs, customer service terminals within FI facilities and third-party operated terminals in a shared service environment. This may also include session security between a 1)

merchant service provider (or merchant processing system) and an acquiring services provider, 2) communication between ATM service providers (ATM switches), 3) large transaction processors and FIs.

5.13 Financial Device Component Authentication

PKI used in this application can assist in the authentication of components such as cash dispenser module, depositor module, recycling module, Encrypting PIN Pad (EPP), card reader, etc. within a device (e.g. ATM, POS, or cash register). The certificates can be used to ensure that the component is genuine and has not been substituted.

5.14 Financial Device TLS Communications

PKI used in this application can be used to establish secure communications between devices (e.g. ATM, POS, or cash registers) and the local host processing system. Transactions, data, configuration, or other information might be encrypted and authenticated.

5.15 Financial Manufacturer Code Sign

This type of PKI is used to determine the validity of manufacturer or legitimate vendor Point of Interaction device software or firmware upgrades to secure devices (such as SCD, HSM, EPP, PEDs, etc.).

5.16 Financial Application Code Sign

Code signing of applications developed (CI/CD) within the Financial institution for distribution to customers for use on mobile or personal use devices. This could include Software Bill of Materials (SBOM), Crypto Bill of Materials (CBOM) as part of the developed product. See section 5.28 Financial Software Bill of Materials (SBOM) and section 5.29 Financial Cryptographic Bill of Materials (CBOM) for details.

5.17 Financial ISO 20022 Messages

ISO 20022-based XML messages are related to financial activity. To provide a more credible message authentication and content verification, digital signatures can be computed on the message. The digital signature will only be as reliable as the infrastructure under which the signing party is authenticated. Since these messages carry financial value, the infrastructure should be related to the financial industry, managed to financial industry standards and requirements. See www.iso20022.org

ISO 20022 messages might be digitally signed, messages might be encrypted, and some message elements (e.g. PIN) might be individually encrypted using Cryptographic Message Syntax (CMS).

Note that ISO 20022 supports XML and ASN.1 but many implementations use JSON.

The ISO 20022 Message Catalogue is maintained and updated by the X9 ISO 20022 Message Catalogue and Use Case Matrix Meeting WG and updates have occurred on a regular basis and shall be checked for current status of the messages to be used for testing and validation. With the status of the effort moving to “Phase 2” in August of 2024, it is essential that the Message Matrix be current and up to date

Catalog ISO 20022 Message Definitions – see https://www.iso20022.org/iso-20022-message-definitions

The ISO 20022 catalog gives access to the documentation related to the ISO 20022 message definitions. Note that the Message Definition Reports (MDRs) and Message Usage Guidelines (MUG) are available at the level of the message set, not at the level of the message definition itself.

BUSINESS DOMAIN CATALOGUES

- Payments
- Securities
- Trade Finance
- Cards
- Foreign Exchange (FX)

ADDITIONAL CONTENT FOR THE MESSAGES

- Business application header (BAH)
- Business message envelope
- Data Source Scheme
- External Code Sets
- ISO 20022 Real-Time Payments Group
- Supplementary Data Extension
- Variants

5.18 Financial ID Certificates

Identity certificates are used with email (S/MIME) for internal communications (using mostly private PKI) within an organization and for external communications (using mostly public PKI) with consumers, small businesses, third-party service providers, and banking regulators. Sensitive information might be embedded in the body of the email, included as an attachment to the email, or referenced in the email as a link to a web site. Authentication often refers to security credentials which include public key (digital) certificates. Other communications such as financial transactions are composed of one or messages (e.g. notification, request, response, etc.) used for payments, mobile financial services, digital currencies, blockchain, etc. using digital signatures relying on public key certificates.

Certificates issued for this Use Case are typically issued to individuals rather than organizations.

ISO 3531 Financial services — Financial Information eXchange session layer

ISO 5201:2024 Financial services — Code-scanning payment security

ISO 8583:2023 Financial-transaction-card-originated messages — Interchange message specifications

ISO/DTS 9546 Guidelines for security framework of information systems of third-party payment services

ISO 11568:2023 Financial services — Key management (retail)

ISO 12812-1:2017 Core banking — Mobile financial services – Part 1: General framework

ISO 23195:2021 Security objectives of information systems of third-party payment services

ISO 13491-1:2016 Financial services — Secure cryptographic devices (retail) – Part 1: Concepts, requirements and evaluation methods

ISO/TR 14742:2010 Financial services — Recommendations on cryptographic algorithms and their use

ISO 19092:2023 Financial services — Biometrics — Security framework

ISO 20022-1:2013 Financial services — Universal financial industry message scheme – Part 1: Metamodel

ISO 21188:2018 Public key infrastructure for financial services — Practices and policy framework

ISO/TR 21941:2017 Financial services — Third-party payment service providers ISO/TS 23526:2023 Security aspects for digital currencies

ISO/TR 24374:2023 Financial services — Security information for PKI in blockchain and DLT implementations

5.19 Financial Distributed Ledger Technology (DLT)

By Distributed Ledger Technology (DLT) we refer to a diverse and growing class of algorithms and methods that aim to provide *computational integrity* for stakeholders across digital environments that often include adversarial actors. DLT becomes useful at and beyond boundaries of centrally controlled systems. They are also providing augmentative benefits for well-regulated federated liability and settlement networks (generally closed) that have the benefit of known counterparties bound by adjacent legal and social trust mechanisms. Over recent decades, these methods are opening new applications above and beyond the traditional distributed computing challenge spaces providing the promise of distributed or fully decentralized or centerless financial utilities. Below we highlight how PKI remains integral to the capability enabled by ten example types of DLT. While the list is not meant to be exhaustive it does highlight the variety and types of ways PKI is an adjacent necessity for the functioning of DLT.

Nakamoto Consensus-Based Algorithms: inspired by the original design used in Bitcoin, focusing on probabilistic finality and decentralized operation. Examples include Proof of Work (PoW), Stake (PoS), and Authority (PoA) as well as Delegated Proof of Stake (DPoS). PKI ensures the authenticity of transactions and block proposals through digital signatures.

Classical Byzantine Fault Tolerance (BFT) Algorithms: these algorithms (PBFT, FBA, Tendermint BFT) focus on ensuring consensus in the presence of Byzantine faults (malicious nodes). PKI is used to authenticate messages between nodes, ensuring secure communication and reliable consensus in Byzantine environments.

Leader-Based Consensus: in methods like Paxos, Raft and variants, long used in distributed database synchronization, PKI secures leader election and communication, allowing nodes to verify the integrity of proposals and prevent tampering.

Directed Acyclic Graph (DAG) Consensus: Tangle, Block-lattice and Hashgraph leverage PKI to validate transactions as linked in the DAG structure. It is integral to ensuring each transaction's authenticity and preventing double-spending.

Hybrid Consensus Mechanisms: like Algorand, Casper (Ethereum's PoS w/ slashing conditions) and Ouroboros rely on PKI to support secure delegation and validation, ensuring trust and fairness in combined mechanisms like Algorand's cryptographic sortition.

Proof-Based Consensus Variants: in PoB, PoC/PoS, PoET, PoH (Proof of Burn, Capacity/Space, Elapsed Time and History respectively); PKI authenticates participation in

mechanisms like Proof of Capacity or Proof of History, ensuring that only legitimate contributors influence consensus.

Voting-Based Consensus: used in private blockchains and Ripple consensus VBCs rely on PKI to secure node votes, prevent tampering and ensure consensus decisions are based on authenticated participation.

Randomized Consensus: methods like HoneyBadgerBFT, Snowflake/Snowball/Avalanche use PKI to validate randomized processes and ensure authenticated node participation in their probabilistic algorithms.

Tokenomics-Driven Consensus: like Proof of Activity (PoA) which combines PoW and PoS for mining, are underpinned by PKI for staking and slashing mechanisms. PKI is needed to securely link economic incentives to verified identities and actions.

Custom and Application-Specific Algorithms: like Filecoin's Proof of Replication and NEO's dBFT (which combines DPoS with BFT) rely on PKI to ensure the integrity and reliability of specialized functions, such as Filecoin's proof of data replication. PKI authenticates nodes and actions.

Note that there are many workgroups from several industry committees including ASC X9, ISO TC46, ISO TC68 and ISO TC307 including a few joint workgroups. These working groups include:

ASC X9A1 Distributed Ledger Technology

ISO TC46/SC11/JWG1 Joint ISO TC46/SC11 & ISO TC307 Blockchain

ISO TC68/AG5 Digital currencies

ISO TC68/SC2/WG17 Security aspects of digital currencies

ISO TC68/SC8/WG3 Digital Token Identifier (DTI)

ISO TC 307 Blockchain and distributed ledger technologies

ISO TC307/AG3 Digital currencies

ISO TC307/AHG4 DLT and carbon markets

ISO TC307/JWG4 Joint ISO TC307 & ISO/IEC JTC1/SC27 Security, privacy and identity for Blockchain and DLT

ISO TC307/WG3 Smart contracts and their applications

ISO TC307/WG8 Non-Fungible Tokens (NFT)

ANSI X9.138:2020 Distributed Ledger Technologies (DLT) Terminology

ISO/TR 21941:2017 Financial services — Third-party payment service providers

ISO/TS 23526:2023 Security aspects for digital currencies

ISO/TR 24374:2023 Financial services — Security information for PKI in blockchain and DLT implementations

5.20 Financial PSD2 Certificates

The European Payments Council (EPC) is an international not-for-profit association of payment service providers (PSP) for the Single Euro Payments Area (SEPA) schemes. Directive 2007/64/EC of the European Parliament and of the European Council, commonly called the Payment Services Directive (PSD) established the rules for six categories of payment service provider concerning transparency of conditions and information requirements for payment services, and the respective rights and obligations of payment service users and payment service providers in relation to the provision of payment services as a regular occupation or business activity.

European Payments Council (EPC) https://www.europeanpaymentscouncil.eu/

The revised Payment Services Directive (PSD2) Directive (EU) 2015/2366 of the European Parliament and of the Council, expanded the previous scope for new services and participants, including third-party providers, wider range of payment transactions, and created two new payment services. Qualified Trusted Service Providers (QTSP) are regulated to provide trusted digital certificates under the electronic Identification and Signature (eIDAS) regulation for the European Union (EU) Revised Payment Services Directive (PSD2).

European Commission eIDAS Dashboard https://eidas.ec.europa.eu/efda/tl-browser/#/screen/home

The Open Banking Implementation Entity (OBIE) program is for trusted digital certificates analogous to the electronic Identification and Signature (eIDAS) regulation for the European Union Revised Payment Services Directive (PSD2). Per BREXIT (British Exit) from the EU the QTSP can no longer be used and so the United Kingdom (UK) deployed its own Trustis Limited Open Banking CA. European Telecommunications Standards Institute (ETSI) standards are used for PSD2 certification.

ETSI TS 119 495 V1.6.1 (2022-11) Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Certificate Profiles and TSP Policy Requirements for Open Banking

ETSI TR 119 476 V1.1.1 (2023-08) Electronic Signatures and Infrastructures (ESI); Analysis of selective disclosure and zero-knowledge proofs applied to Electronic Attestation of Attributes

ETSI EN 319 412 1 V1.5.1 (2023-09) Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures

ETSI TR 119 000 V1.3.1 (2023-05) Electronic Signatures and Infrastructures (ESI); The framework for standardization of digital signatures and trust services; Overview

The following is excerpt from https://seon.io/resources/psd3-payment-services-directive-update/ :

On May 10, 2022, the European Commission (EC) published an initiative/call for consultation on its 2nd Payment Services Directive – PSD2 for short – which is currently in force. The goal? To use the takeaways to inform the update of what will be called PSD3.

What is PSD3?

The 3rd Payment Services Directive, PSD3, is an upcoming framework that regulates electronic payments and the banking ecosystem within the European single market area (EEA). The PSD3 will be decided by the EC after a round of consultations.

Just like its predecessor, PSD3 is going to address Strong Customer Authentication (SCA) and open banking standards and protocols, aiming to make it easier for consumers to transact with confidence in the digital landscape, both with merchants and with banks.

Moreover, the open finance and banking protocols will address sharing of customer information between competent authorities and banks the consumer has accounts with, including tax authorities, payment processors, and more.

PSD3 vs PSD2: Differences

PSD3 is upcoming legislation set to regulate the provision of electronic payments and the banking ecosystem within the EU's single market, while PSD2 is the older version of this framework, which has been in use in the European Union and European Economic Area since 2019/2020, when the extended deadline for its implementation passed.

PSD2 governs all digital payments and open finance in the EU and EEA, and PSD3 is expected to do the same, potentially broadening its scope.

UK's Equivalent

In the UK PSD2 is largely implemented through the Payment Services Regulations 2017, which was published by HM Treasury.

The Financial Conduct Authority (FCA) is the competent authority for PSD2. The FCA has published the PSD2 Policy Statement which explains the changes we are making to our proposals following consultation and confirms amendments to our Handbook

Payment Services Regulations 2017 and Electronic Money Regulations 2011 form the basis for the Financial Conduct Authority (FCA) rulings complying with PSD2.

5.21 Verified Mark Certificates

Verified Mark Certificates indicate that a visual depiction of a trademark or service mark (included in the certificate) has been verified to belong to the subject named in the certificate by a Mark Verifying Authority (MVA). The identity of the subject is rigorously vetted using the Extended Validation (EV) Guidelines, and then the ownership of the mark is validated using the appropriate national trademark database. Verified Mark Certificates allow application software suppliers to securely display a visual indication of the trademark or service mark associated with a domain name, helping assure the user that the email comes from the trusted brand they expect. Trademarks have a long history and extensive legal background in preventing confusion between entities, products, or services with similar names, and there is an existing legal infrastructure that can be leveraged to help prevent attackers from exploiting confusing domain names to trick customers[13].

5.22 Financial SCD Authentication

PKIs are used for device keys for Secure Cryptographic Devices (SCDs). This includes HSMs, ATM EPPs, and POS terminals. The keys are typically used to authenticate the devices as genuine and untampered to external parties. A private key is securely held in a SCD, and the corresponding public key - in the form of a certificate - is either stored in the SCD in a way that and can be read or is stored outside the SCD in a place where it can be reliably retrieved. Higher-end SCDs usually generate the key pair internally and send out the public key to be certified. Less-capable SCDs may have their key pair generated by some other device, and then injected into the SCD in a secure facility

[13] Reference: "Minimum Security Requirements for Issuance of Mark Certificates, Version 1.6, March 7, 2024". (https://bimigroup.org/supporting-documents/)

Some SCD manufacturers have their own specialized in-house CAs and PKIs for this purpose, while others rely on commercial CAs and PKIs for some or all the key hierarchy.

The PCI HSM Security Requirements document describes secure cryptographic devices/hardware security modules in the context of financial services. See: https://www.pcisecuritystandards.org/document_library/?category=pts&document=PCI_HSM_Security_Requirements

Network Trust Links (NTLs) are secure, authenticated network connections between the SafeNet Luna Network HSM appliance and clients. NTLs use two-way digital certificate authentication and TLS data encryption to protect your sensitive data during all communications between HSM partitions on the appliance and its clients.

See SafeNet Luna Network HSM 7.4 Product Documentation:

https://thalesdocs.com/gphsm/luna/7.4/docs/network/Content/Product_Overview/networking/ntls_and_stc.htm

5.23 Financial Application Communications

Financial applications often encrypt individual data elements such as authentication credentials (e.g. PIN, passwords, and biometrics) or whole messages (e.g. request, response) and not solely rely on lower layer security protocols (e.g. TLS, IPsec). For example, Cryptographic Message Syntax (CMS) uses a content encryption key (CEK) that might be established using key transport (e.g. RSA, Named Key) or key agreement (e.g. DH, ECDH).

5.24 Financial ISO 17442 Legal Entity Identifier (LEI)

Legal Entity Identifier (LEI) is used with an optional value or possibly required value in a client certificate DN or certificate extension. A PKI in this Use Case would be used to authenticate the identity of each legal entity in communication and business transactions as defined under the Global Legal Entity Identity Foundation.

5.25 Financial X9.129 Legal Order Exchange (LOE)

X9.129 Electronic File Format Standards for Presentment and Remittance of Legal Orders: this is the methodology for responding electronically to subpoenas (as opposed to faxing paper documents). X9F4 submitted security material to the X9AB workgroup but it ended up in informative (vs normative) Annex A: Security Considerations. X9AB allowed X9F4 to mention encryption but not digital signatures. Nonetheless, certificates might be used for key management to establish encryption keys, and for digital signatures over the data, receipts, or agreements.

5.26 Financial IPsec Host Services

Relies primarily on DH key agreement where the static DH public keys can be encapsulated within an X.509 certificate. For government connections, many agencies require a certificate from the External Certification Authority (ECA) Program. Some connections rely on pre-shared keys which are actually authentication strings used with anonymous DH without certificates.

5.27 Financial X9.100-187 Check21

The Check Clearing for the 21st Century Act (Check 21) was signed into law on October 28, 2003. Check 21 is designed to foster innovation in the payments system and to enhance its efficiency by reducing some of the legal impediments to check truncation. The law facilitates check truncation by creating a new negotiable instrument called a substitute check, which permits banks to truncate original checks, to process check information electronically, and to deliver substitute checks to banks that want to continue receiving paper checks. A substitute check is the legal equivalent of the original check and includes all the information contained on the original check. The law does not require banks to accept checks in electronic form nor does it require banks to use the new authority granted by the Act to create substitute checks. Check 21 applies to "Substitute Checks" which are image reprints of original paper checks, but considered a new legal payment instrument, designed to be processed exactly as if it were the original paper check. Substitute Checks allows unilateral decision to truncate checks, so does not require bilateral agreement between parties.

See https://www.federalreserve.gov/paymentsystems/regcc-faq-check21.htm

X9.100-187:2021 Specifications for Electronic Exchange of Check and Image Data allows for the use of digital signatures and certificates over the check image data. Prior to the enactment of Check 21 and the fully electronic exchange of checks, paper checks were accepted as payment by consumers, businesses (i.e. merchants) and government entities, typically known as the payee, forwarded to the payee's bank (also known as Depositary Bank, Bank of First Deposit (BOFD) or collecting bank), bundled and sent for clearing either directly to the paying bank, through another bank, processor or through the Federal Reserve Bank. The check was forwarded to the paying bank, who provided either the original check, a description of that check or an image of that check to the bank customer who wrote the check, with the monthly statement. Settlement occurs through the Federal Reserve typically as a Fedwire transfer from paying banks to collecting banks, who would credit money to the payee's account, and the paying bank would debit money from the customer's account. Electronic checks truncated the paper check at a collecting bank or payee location by capturing a check image and initiating an electronic check to its collecting bank.

Check 21 captures information from the check image and protects the data using a digital signature.

5.28 Financial Software Bill of Materials (SBOM)

The ECMA-424 CycloneDX Bill of Materials Specification defines various bill of material (BOM) objects for supply chain management for reducing cybersecurity risks, capable of representing software, hardware, services, and other types of inventory, including:

- Software Bill of Materials (SBOM)
- Software-as-a-Service Bill of Materials (SaaSBOM)
- Hardware Bill of Materials (HBOM)
- Machine Learning Bill of Materials (ML-BOM)
- Cryptography Bill of Materials (CBOM)
- Operations Bill of Materials (OBOM)
- Manufacturing Bill of Materials (MBOM)
- Bill of Vulnerabilities (BOV)
- Vulnerability Disclosure Report (VDR)
- Vulnerability Exploitability eXchange (VEX)
- CycloneDX Attestations (CDXA)
- Common Release Notes Format

See https://ecma-international.org/wp-content/uploads/ECMA-424_1st_edition_june_2024.pdf

Cybersecurity & Infrastructure Security Agency (CISA) defines Software Bill of Materials (SBOM) as a formal record containing the details and supply chain relationships of various components used in building software. **Error! Reference source not found.** – see CISA SBOM HYPERLINK "https://www.cisa.gov/sbom"https://www.cisa.gov/sbom

These objects can be signed with a digital signature or trusted time stamp.

5.29 Financial Cryptographic Bill of Materials (CBOM)

The ECMA-424 CycloneDX Bill of Materials Specification defines various bill of material (BOM) objects for supply chain management for reducing cybersecurity risks, capable of representing software, hardware, services, and other types of inventory, including Cryptographic Bill of Materials (CBOM).

These objects can be signed with a digital signature or trusted time stamp.

5.30 Financial Time Stamp Token (TST) X9.95

Trusted timestamps consist of a Time Stamp Token (TST) issued by a Time Stamp Authority (TSA) whose clocks are calibrated to National Measurement Institute (NMI) clocks and ultimately to the International Timing Authority (ITA). The Bureau International des Poids et Mesures (BIPM) near Paris, France is the official ITA who calibrates the clocks with each NMI. Each NMI subsequently calibrates the clocks of other Master Clocks (MC) or Time Stamp Authorities (TSA). Note that calibrated clocks cannot be synchronized with other clocks.

IEFT RFC-3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP), August 2001

ISO/IEC 18014 Information technology — Security techniques — Time-stamping services

- Part 1:2008 Framework
- Part 2:2021 Mechanisms producing independent tokens
- Part 3:2009 Mechanisms producing linked tokens
- Part 4:2015 Traceability of time sources

ANSI X9.95:2022 Trusted Time Stamp Management and Security

Document providers submit a hash of a document to a TSA who issues a TST consisting of (a) the hash, (b) a timestamp from its calibrated clock, and (c) a cryptographic binding. Any recipient of the TST and the original document can verify the cryptographic binding to confirm the integrity of the document at that specific time. This prevents modification or creation of backdated documents. Further, when the TST contains a hash of signed document, the signature date is preserved, which is especially useful for code signing.

The primary cryptographic binding used with TST are digital signatures. The TSA signs the TST and provides a public key certificate for signature verification. Note that the TSA signature is different than the document signature. Also note that the TSA is NOT a CA and therefore does not issue certificates.

5.31 Financial QR Codes

QR Codes (Quick Response code) are a type of matrix barcode, also called two-dimensional (2-D) barcode, to encode some data types such as Uniform Resource Locator (URL) used with financial payments. QR Codes are read and executed using a QR Code scanner on devices, such as a mobile smartphone. QR Codes can be used for payments between a consumer (payer) using a mobile device and a merchant (payee) using a payment terminal. While the QR Code might be protected as

a data element within a message, the QR Code does not protect itself from modification, duplication, or masquerading. The following material is from the Faster Payments Council QR Code whitepaper

> *Dynamic QR codes are ones which can be formatted using the latest up-to-date information plus optional transaction-specific information. Dynamic QR code presentment requires a smart phone, POS QR enhanced device, or dynamic version of the QR code using website checkout-specific information.*
>
> *Static QR codes can be printed and displayed at convenient locations, such at the point of sale, on a menu, on a bill, on a website checkout page, etc. Static codes include point-of-time information. They can include transaction information, such as the bill they are printed on.*

QR Code content might be protected using encryption and/or digital signatures. QR Code protection can be achieved using CMS with detached protection. Cryptographic Message Syntax (CMS) is a scheme for constructing cryptographically protected data, including data encryption, message authentication, digital signatures, and the corresponding key management supporting a sender and one or more receivers.

QR Codes might contain payer (payment authorizer), payee (payment recipient), and payment (transfer of funds) information vulnerable to modification, duplication, or masquerading resulting in fraud. Altering payer information can transfer funds from the wrong account, changing payee information can transfer funds to the wrong account, and modifying payment information can affect the transfer amount. QR Codes might be static or dynamic. Static codes might be printed and posted publicly (e.g. parking meters) for payments. Dynamic codes might be generated by the payer and presented to the payee, or generated by the payee and presented to the payer, such as a cardholder using a mobile device to purchase goods or services from a merchant using a POI device.

Faster Payments Council: QR Codes for Faster Payments, July 2022
https://fasterpaymentscouncil.org/

ANSI X9.73:2017 Cryptographic Message Syntax (CMS)

ANSI X9.148:2024 Quick Response (QR) Code Protection using Cryptographic Solutions

ISO/IEC 15417:2007, Information Technology – Automatic Identification And Data Capture Techniques – Code 128 Bar Code Symbology Specification

ISO 5201:2024 Financial services — Code-scanning payment security

ISO/IEC 18004:2015 Information Technology – Automatic Identification And Data Capture Techniques – QR Code Bar Code Symbology Specification

5.32 Digital Currencies

A digital currency is an asset represented in electronic form having some monetary characteristics. Anyone can create one, but the challenge is getting others to accept them. Whether created by nations or other stakeholder groups, a functioning digital currency must allow measure, account, storage and transfer of value. Our current financial system sees digital currency taking many context specific digital forms. Currencies which fail to provide a consistent measure over significant intervals or otherwise fails to provide proper accounting or robust store of value relative to adversarial agents or add frictions to transactions are dropped for alternatives that meet these axiomatic requirements.

This is illustrated by a quick consideration of examples from the money supply aggregation classifications. Overnight deposits (M1); fixed-term and deposits with notice (M2); and the variety of money market funds, repurchase agreements and debt instruments all include digital currency in

forms and formats that often rely on extra digital adjacent legal and institutional mechanisms. Whether in a resting state as a liability in a ledger or in transit between custodial of bank accounts across a variety of payment service providers, digital currency technologies display a diverse mostly bespoke to localized functional ecologies of more to less sophisticated systems.

Digital currencies are almost ever present in and across both traditional as well as emerging distributed or decentralized frontiers. A full list of how PKI is critical to these would be nearly coterminous with the scope of this document. Even the most 'exogenous' open banking transactions between individuals using open wallets connecting over NFCs to transfer a private currency they have agreed to use; even in this scenario, you would require PKI to maintain measure, account, storage and transfer of such private digital coinage. Going forward, as national currencies in the form of central bank liabilities become amendable to tokenization, PKI will still play a critical role in securing containerized handles and functionality associated with the basic units of commerce.

Digital currency is any currency that's available exclusively in electronic form. Electronic versions of currency already dominate most countries' financial systems. What differentiates digital currency from the electronic currency that's already in Americans' bank accounts is that digital currency never takes physical form.

5.33 Digital Wallets and Vaults

A digital wallet, also known as an e-wallet or mobile wallet, is an electronic device, online service, or software program that allows one party to make electronic transactions with another party bartering digital currency units for goods and services. This can include purchasing items either online or at the point of sale in a brick and mortar store, using either mobile payment (on a smartphone or other mobile device) or (for online buying only) using a laptop or other personal computer. Money can be deposited in the digital wallet prior to any transactions or, in other cases, an individual's bank account can be linked to the digital wallet. Users might also have their driver's license, health card, loyalty card(s) and other ID documents stored within the wallet. The credentials can be passed to a merchant's terminal wirelessly via near field communication (NFC).

See https://en.wikipedia.org/wiki/Digital_wallet

Ten Best Digital Wallets

Digital wallets are becoming an increasingly popular alternative to cash or using a debit or credit card to make payments. But what are the best digital wallets and which one is right for you? As you consider which option you should use, it's important to evaluate the features and fees of today's most popular digital wallets so you can choose the solution that best fits your needs. See https://wellkeptwallet.com/digital-wallets/

- Amazon Pay
- Apple Pay
- Cash App
- Dwolla
- Facebook Pay
- Google Pay
- PayPal
- Venmo
- Walmart Pay
- Zelle

5.34 Cryptographic Message Syntax (CMS)

Cryptographic Message Syntax (CMS) can be used to protect financial transactions and other information from accidental or deliberate disclosure, alteration, substitution, or destruction of data. The syntax provides support for data confidentiality, data integrity, data origin authentication, and non-repudiation services needed to provide strong, mutual authentication. Flexibility of key management techniques is provided through support for a variety of key establishment mechanisms, including key exchange, key agreement, password-based encryption and constructive key management.

See 5.17 Financial ISO 20022 Messages

See 5.19 Financial Distributed Ledger Technology (DLT)

See 5.23 Financial Application Communications

See 5.31 Financial QR Codes

ANSI X9.73:2017 Cryptographic Message Syntax (CMS)

IETF RFC 5652 Cryptographic Message Syntax (CMS), September 2009

5.35 Financial TLS Content Delivery Network (CDN)

Financial services rely on Content Delivery Networks (CDN) to offload access to public information relating to publicly accessible applications (PAA) such as online banking and wealth investment management (WIM) services. Customers accessing the bank URL on their browsers are redirected to a CDN over a TLS connection (see §5.2) for public information, and when accessing a PAA the CDN forwards the access to the financial server over a second TLS connection, while maintaining the first TLS connection for access to public information. Since the CDN is not an aggregator (see §5.3) or another host system (see §5.4) this scenario is another PKI financial use case.

End of Document

