



Australia's National
Science Agency

Planning the cyber quantum-safe transition for Australia's financial sector: a national use case

Summary report of the April 2026 workshop

08 September 2026

A MORE
RESILIENT AUSTRALIA
THROUGH CYBER
QUANTUM-SAFE TRANSITION



Citation

Planning the cyber quantum-safe transition for Australia's financial sector:
a national use case, CSIRO 2026

Australia's National
Science Agency

Copyright

© Commonwealth Scientific and Industrial Research Organisation 2026. To the extent permitted by law, all rights are reserved and no part of this publication covered by copyright may be reproduced or copied in any form or by any means except with the written permission of CSIRO.

Important disclaimer

CSIRO advises that the information contained in this publication comprises general statements based on scientific research. The reader is advised and needs to be aware that such information may be incomplete or unable to be used in any specific situation. No reliance or actions must therefore be made on that information without seeking prior expert professional, scientific and technical advice. To the extent permitted by law, CSIRO (including its employees and consultants) excludes all liability to any person for any consequences, including but not limited to all losses, damages, costs, expenses and any other compensation, arising directly or indirectly from using this publication (in part or in whole) and any information or material contained in it.

CSIRO is committed to providing web accessible content wherever possible. If you are having difficulties with accessing this document please contact csiro.au/contact.

Acknowledgement of Country

CSIRO the Traditional Owners of the lands, seas and waters of the area that we live and work on across Australia and pays its respects to Elders past and present. CSIRO recognises that Aboriginal and Torres Strait Islander peoples have made, and will continue to make, extraordinary contributions to Australian life including in cultural, economic, and scientific domains.

Acknowledgements

We acknowledge the valuable input, advice and review provided by workshop participants and subject matter experts. With their agreement, selected individuals and organisations are acknowledged by name: CSIRO team (Dongxi Liu, Sharif Abuadbbba, Sid Chau, Surya Nepal, Jiafan Wang, The Anh Ta, Nazatul Sultan), May Lam and Michael Egan, Emerging Payments Association Asia, David Walker, Former CTO at Westpac, DBS, and ANZ. Other contributors have not been identified due to confidentiality and sensitivity considerations.

Executive Summary.....	3
1 Introduction and Context.....	5
2 Background: Cryptographic in Payment Systems	7
3 Key Findings from the Workshop.....	8
Ecosystem and engagement.....	8
Migration approaches and challenges.....	9
Technical and governance collaboration.....	9
4 Approaches to Cryptographic Asset Discovery	10
Infrastructure-centric approach	10
Business-centric approach.....	11
Concluding Remarks	12
5 Technical Appendix	13
Payment Ecosystem and Cryptographic Dependencies	13
Case Study One: Cryptographic Asset Discovery in W3C’s Web Payment APIs	14
Case Study Two: Cryptographic Asset Discovery in EMV	16
Case Study Three: Cryptographic Asset Discovery in NPP/FSS	18

Executive Summary

Advances in quantum computing present a significant emerging risk to the public-key cryptography underpinning Australia's payment and financial systems. While international and Australian guidance has established the need to transition to post-quantum cryptography (PQC), translating high-level roadmaps into practical and actionable transition plans remains a significant challenge for financial institutions and payment operators. In Australia, the Australian Signals Directorate (ASD) has stipulated expectations for Australian organisations to provide PQC transition plans in place by 2026 and to phase out quantum-vulnerable cryptography by 2030, reinforcing the need for organisations to begin preparing for the transition.

To help address this challenge, CSIRO's post-quantum cryptography researchers have undertaken a national use case focused on planning the quantum-safe transition for Australia's financial sector, with payment systems as a key area of investigation. Drawing on CSIRO's expertise in PQC and working in collaboration with financial-sector stakeholders, the team examined the practical challenges associated with the preparation for the transition, including cryptographic asset discovery, migration planning, ecosystem dependencies, and the application of quantum-safe approaches to critical payment services.

As part of this work, CSIRO convened a workshop in April 2026 bringing together representatives from 17 organisations across Australia's payments ecosystem. The workshop provided a forum for stakeholders to discuss the challenges, priorities and practical considerations associated with PQC transition and to identify opportunities for coordinated actions and knowledge sharing. Discussions covered governance and strategy, migration approaches, technical challenges and future industry coordination.

The research and stakeholder engagement highlighted three overarching considerations for Australia's quantum-safe transition:

1. **The PQC transition will be a complex, multi-year to a decade undertaking requiring early preparation and ecosystem-wide coordination.** Australia's payment infrastructure is highly interconnected, with dependencies spanning financial institutions, payment operators, technology providers, vendors, standards bodies and international payment networks. Successful migration will require strong governance and planning, cryptographic asset discovery, vendor readiness, testing, stakeholder coordination and phased deployment to maintain security, interoperability, trust and operational continuity.
2. **A business-centric, risk-based approach provides a pragmatic starting point for transition planning.** Beginning with critical business services and tracing their underlying standards, cryptographic requirements and technology dependencies can help organisations prioritise migration according to business criticality and risk. This can be complemented by infrastructure-centric discovery and provides an opportunity to establish crypto-agility as a long-term architectural capability.
3. **Detailed domain- and application-specific assessments are essential.** High-level frameworks alone cannot capture the distinct cryptographic dependencies, architectures, standards and operational constraints of individual payment systems. Transition planning therefore needs to progress from ecosystem-level guidance to detailed assessments of specific payment domains, applications and systems, with migration strategies tailored to their specific requirements.

Together, these findings reinforce that the quantum-safe transition should be approached not simply as a replacement of cryptographic algorithms, but as a coordinated transformation of the trust infrastructure underpinning Australia's payments ecosystem. Early preparation provides an opportunity not only to address quantum risk, but also to strengthen cryptographic governance, improve cyber resilience and embed crypto-agility into future financial-system architectures.

The report is structured to distinguish the findings arising from stakeholder discussions from the supporting technical analysis prepared by the CSIRO team. Section 2 provides background on cryptography in payment systems to establish the technical context for the workshop discussions. Section 3 summarises the key findings from the workshop. Sections 4 and 5 present more detailed analysis prepared by the CSIRO team and presented during the workshop to examine practical approaches to cryptographic asset discovery and illustrate relevant dependencies across the payments ecosystem. The Appendix provides deeper case studies demonstrating how these approaches may be applied to specific payment systems.

1 Introduction and Context

Cryptography plays a critical role in modern payment and financial systems by ensuring the confidentiality, integrity, authenticity, and non-repudiation of sensitive communications, such as payment requests and confirmations, as well as clearing and settlement instructions. However, the rapid advancement of quantum computing poses a significant threat to the widely deployed public-key cryptographic algorithms, such as RSA and ECDSA for digital signatures and ECDH for key establishment.

In response to the emerging threats of quantum computing, in 2024, the National Institute of Standards and Technology (NIST) standardized new Post Quantum Cryptographic (PQC) algorithms, as US Federal Information Processing Standards (FIPS), (FIPS 203, Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM); FIPS 204 Module-Lattice-Based Digital Signature (ML-DSA); FIPS 205 Stateless Hash-Based Digital Signature (SLH-DSA). These algorithms are intended to replace the quantum-vulnerable public-key algorithms.

In Australia, the Australian Signals Directorate (ASD) has advised Australian organisations to prepare for the migration to PQC and introduced controls in the Information Security Manual (ISM) to support PQC transition planning and implementation (Control: ISM-2073). In addition, the ASD outlined an update to the ASD-Approved Cryptographic Algorithms (AACA) such that many common public-key cryptographic algorithms will no longer be approved beyond 2030¹. While a cryptographically relevant quantum computer has not yet been built, the “harvest now, decrypt later” threat creates urgency for transition.

This was followed by an update of the Protective Security Policy Framework (PSPF) in July 2026, that prescribes what Australian Government entities must do to protect their people, information and resources, both domestically and internationally. This update included the adoption of PQC algorithms and PQC-compatible technology during the procurement of new cryptographic equipment and software to align with the ASD ISM.

The global finance industry is aware of the quantum threat and the need for a quantum-safe transition. In January 2026, the G7 Cyber Expert Group published a roadmap for the PQC transition in the financial sector, and the roadmap aims to be a guidance for G7 Finance Ministers and Central Bank Governors². The Emerging Payments Association Asia (EPAA) has established the Quantum Safe Cryptography Working Group to coordinate the efforts of PQC transition for payment systems³. Mastercard also has a whitepaper discussing the PQC transition⁴. In Project Leap Phase 2, the Bank

¹ <https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism/cyber-security-guidelines/guidelines-for-cryptography>

² G7 Cyber Expert Group (CEG). Advancing a Coordinated Roadmap for the Transition to Post-Quantum Cryptography in the Financial Sector, <https://home.treasury.gov/system/files/136/G7-CEG-Quantum-Roadmap.pdf>

³ EPAA. Quantum Safe Payment: Why the Payments Industry Must Act Now, <https://emergingpaymentsasia.org/wpcontent/uploads/2025/10/Quantum-Safe-Payments-Why-the-Payments-Industry-Must-Act-Now-updated.pdf>

⁴ MasterCard. Migration to post-quantum cryptography, https://www.mastercard.com/content/dam/mccom/shared/news-and-trends/stories/2025/quantum-explainer-and-white-paper/Migration-to-post-quantum-cryptography-WhitePaper_2025.pdf

for International Settlements developed a prototype of integrating post-quantum signatures into payment messages of the Eurosystem's T2 payment system⁵.

While existing transition roadmaps help raise awareness, they fall short of providing operational steps that financial institutions can follow to identify a starting point and prepare an actionable plan for the transition.

Beyond addressing emerging quantum threats, the transition presents an opportunity for financial institutions and payment operators to modernise trust infrastructure, improve cyber resilience, strengthen governance of cryptographic assets and embed crypto-agility into future technology architectures. Organisations that begin preparing early are likely to reduce long-term operational risk while improving their ability to respond to future cryptographic advances.

The purpose of this report is to address this gap by identifying suitable approaches to support the implementation of cryptographic transition roadmaps, including the G7 CEG roadmap. To gain a deeper understanding of the associated challenges and opportunities, CSIRO organised a workshop in April 2026 bringing together representatives from 17 organisations across Australia's payments ecosystem. This report summarises the key findings arising from the workshop and presents supporting technical analysis prepared by the CSIRO team to inform the discussions and illustrate practical approaches to quantum-safe transition planning. It recognises that successful transition depends on coordinated leadership across payment operators, financial institutions, technology providers, regulators and international standards bodies.

⁵ Bank for International Settlements (BIS). Project Leap: Quantum-proofing payment systems, <https://www.bis.org/publ/othp107.pdf>

2 Background: Cryptographic in Payment Systems

Public-key cryptography underpins many critical security functions in payment systems, including secure communications, authentication, digital signatures, and the protection of payment messages. Key establishment enables two parties to derive a shared secret over an untrusted network, while digital signatures provide authentication, integrity, and non-repudiation by allowing a party to prove its identity and sign messages. These capabilities are embedded throughout financial infrastructure, from customer-facing applications and payment gateways to interbank clearing and settlement systems. However, widely deployed algorithms in current financial systems, such as RSA, ECDSA, and ECDH, are expected to become vulnerable to sufficiently capable quantum computers attacks using the Shor's algorithm.

To address this risk, NIST has recently standardized several PQC algorithms, including ML-KEM for key encapsulation and ML-DSA for digital signatures. These algorithms are designed to replace quantum-vulnerable public-key cryptography while preserving the security functions required by modern digital systems. These encryption algorithms are foundational and industry bodies are building on these standards to develop quantum-safe versions of widely used security protocols. For example, the Internet Engineering Task Force (IETF) has developed quantum-safe IKEv2 for IPsec VPN connections⁶, while the standardisation of quantum-safe TLS 1.3 is ongoing⁷.

The transition to quantum-safe cryptography extends beyond replacing the foundational cryptographic algorithms. Payment systems rely on cryptography which is implemented through a wide range of protocols, standards, applications, and operational processes. As a result, organisations must identify where cryptographic functions are used, understand their business significance, and assess the dependencies involved in migrating to quantum-safe alternatives.

In addition to secure communication protocols such as TLS and IPsec, payment systems employ cryptography in domain-specific functions including transaction authentication, card verification, payment message signing, and clearing and settlement processes. The X9F5 Financial PKI workgroup is developing X9.146 Quantum TLS⁸ to support PQC readiness and crypto-agility for financial services. Similarly, the BIS Project Leap initiative highlights the critical role of digital signatures in payment systems and financial market infrastructures, where they provide message integrity, sender authentication, and protection against message manipulation. Understanding these cryptographic dependencies is therefore a critical prerequisite for effective quantum-safe transition planning.

Key Takeaways

- Quantum-safe transition should address both algorithms and protocols. Replacing RSA, ECDH, and ECDSA with PQC algorithms such as ML-KEM and ML-DSA is necessary, but these

⁶ Multiple Key Exchanges in IKEv2: <https://www.ietf.org/archive/id/draft-ietf-ipsecme-ikev2-multiple-ke-08.html>

⁷ Post-Quantum Cryptography Recommendations for TLS-based Applications: <https://datatracker.ietf.org/doc/draft-ietf-uta-pqc-app/>

⁸ X9F5 Financial PKI. X9.146 Quantum TLS - PQC Readiness and Crypto-Agility for Financial Services, https://pkic.org/events/2025/pqc-conference-austin-us/THU_BREAKOUT_1230_X9-146-QTLS-20241220.pdf

algorithms must also be integrated into operational protocols such as TLS, IPSec, PKI, and payment messaging systems.

- Financial sector quantum-safe migration requires domain specific planning. Payment infrastructures depend on specialised standards, trust relationships, and operational processes, so quantum-safe transition must be tested and phased carefully across applications, institutions, and industry protocols, while maintain existing systems.

3 Key Findings from the Workshop

Building on the technical context outlined in Section 2, this section summarises the key findings from the stakeholder workshop. In April 2026, CSIRO convened a workshop with representatives from 17 organisations across Australia's payments ecosystem as part of the national use case, Planning the Quantum-Safe Transition for Australia's Financial Sector. The workshop was organised to bring together diverse stakeholders from across the payments ecosystem to develop a deeper understanding of the challenges, priorities, and practical considerations associated with the transition to PQC, and to identify opportunities for coordinated action and knowledge sharing. The workshop explored key issues relevant to the preparation phase of the PQC transition, including governance and strategy, migration approaches, technical challenges, and future industry coordination. Participants identified three overarching priorities:

- strengthening ecosystem-wide coordination,
- adopting risk-based migration planning, and
- fostering industry collaboration on practical transition tools and knowledge sharing.

The key findings arising from these discussions are summarised below. Sections 4 and 5 present more detailed analysis prepared by the CSIRO team and presented during the workshop to provide context and practical examples, with deeper payment-system case studies provided in the Appendix.

Ecosystem and engagement

The PQC transition in the financial sector requires the migration of a complex, interconnected ecosystem, comprising financial institutions, service providers, customers, and standardisation development organisations. Financial institutions may have a mix of systems, some of which they have developed themselves and some of which are operational legacy. In addition, many financial institutions will also have a mix of different vendors, on premise and cloud, to supply and maintain application and network infrastructures. Vendors will have their own prioritisations and resource limitations and may follow their own timelines for upgrading their products to support PQC. Similarly, international organisations, such as SWIFT, Wise, Airwallex and the increasingly significant Chinese, Cross-border Interbank Payment System (CIPS) will establish their own PQC transition schedules.

Small and medium-sized enterprises play an important role in Australia's financial ecosystem. However, they may not be well-equipped and well-motivated for the PQC transition, as they often struggle to implement standards in a timely manner. As a result, ongoing engagement and collaboration across the ecosystem are essential to develop a shared understanding, of both the technical possibilities and the practical constraints of PQC transition. Such collaboration can

establish a common knowledge base and support realistic, coordinated transition planning across all stakeholders.

Migration approaches and challenges

The business-centric approach was well-received during the discussion and is described in more detail in the next section. One financial institution described its adoption of a business-first, top-down, and risk-centric approach. Participants broadly agreed that planning from a business-centric perspective, followed by an infrastructure-centric transition approach, could provide a more effective strategy. A business-centric and risk-based transition strategy helps identify which assets should be prioritized for migration and helps manage the costs of this transition. Budget constraints were also identified as a factor that may influence transition timelines, and participants emphasised that quantum safety should be integrated into a broader cybersecurity strategy. Participants emphasized that not all quantum vulnerable assets are of high value and therefore may not require immediate transition, as lower-priority assets can often be migrated through routine technology refresh cycles.

For cryptographic asset discovery, participants highlighted the complexity of cryptographic dependencies, making accurate dependency mapping an essential prerequisite for planning and executing the transition. Given the diversity of financial-sector infrastructure, the maturity, coverage, and usability of off-the-shelf discovery tools remain key concerns.

Maintaining consumer trust requires financial institutions to ensure the long-term security and resilience of their systems. To support this objective, organisations should minimise reliance on legacy cryptographic systems during the transition and adopt crypto-agility as a long-term design principle, enabling cryptographic mechanisms to be updated efficiently as standards and threats evolve.

Participants also emphasised that successful transition planning requires a clear understanding of the cryptographic algorithms, protocols, and standards that underpin payment systems. Since cryptographic assets are embedded within these technologies, organisations must first understand where and how cryptography is used before they can identify dependencies and develop effective migration plans. Building on the technical background in Section 2, Section 4 examines approaches to cryptographic asset discovery and considers how cryptographic dependencies can be identified and prioritised to support transition planning.

Technical and governance collaboration

The workshop participants discussed the importance of engagement and knowledge sharing to support the PQC transition across the economy and the finance industry and not only in Australia. The group also discussed the challenges that other countries may have in moving to PQC and in being ready for the depreciation or weaker cryptographic approaches, as this may have an impact on international trade in the Asian and Pacific regions

The connection between the technical challenge and the governance challenge was also discussed in the context of a need for collaboration to more broadly understand the technical transition challenges throughout the ecosystem. The workshop also considered the roles that could be played by organisations like CSIRO, EPAA, ASIC, APRA, ASD and academia. Issues of awareness, regulation, preparation and sharing of technical expertise and standards identification and development were

discussed. CSIRO researchers proposed the idea of an Open Cryptographic Asset Catalog to support the sharing of cryptographic asset information and transition knowledge.

4 Approaches to Cryptographic Asset Discovery

Cryptographic asset discovery and inventory are foundational activities for quantum-safe transition planning. Organisations cannot prioritise, assess, or migrate quantum-vulnerable cryptography without first understanding where cryptographic functions are used and how they support critical business services. Consequently, cryptographic asset discovery is identified as a key early activity in transition guidance from many organisations, including both the G7 Cyber Expert Group and the ASD⁹. Note that Microsoft and NIST are already moving towards continuous posture management, not one-off inventories.

To support the workshop discussion, the CSIRO team presented two complementary approaches to cryptographic asset discovery: infrastructure-centric and business-centric approaches. Broadly, approaches to cryptographic asset discovery can be categorised as infrastructure-centric or business-centric. While both approaches have value, the workshop participants broadly agreed that a business-centric approach provides a more practical starting point for payment systems because it aligns cryptographic asset discovery with business risk, operational priorities, and industry standards.

Infrastructure-centric approach

This approach begins with an organisation's IT infrastructure and employs a range of tools to identify cryptographic algorithms, protocols, certificates, and their implementations within that environment. During the discovery process, this approach does not consider the associated business contexts of these assets; risk analysis is a separate step.

⁹ ASD. Planning for post-quantum cryptography, <https://defencescienceinstitute.com/wp-content/uploads/2025/10/Planning-for-post-quantum-cryptography-September-2025.pdf>

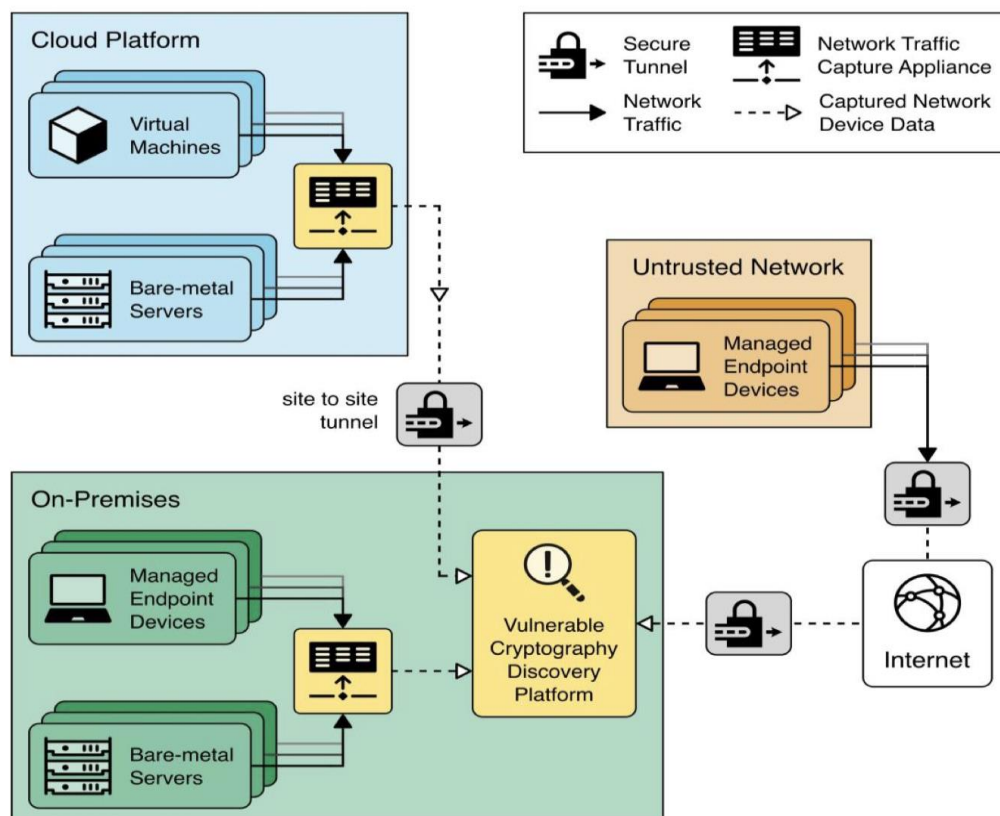


Figure F4-1 An IT Infrastructure for Discovery [source: NIST SP 1800-38B⁸]

This approach has been piloted in the NIST project, Migration to Post-Quantum Cryptography¹⁰, which involves numerous technology partners, including IBM and Cisco. These partners use their tools to discover cryptographic assets in pre-defined IT infrastructures, such as the example in Fig. F4-1. For example, Cisco Mercury is used to capture and analyse quantum-vulnerable network packet metadata in this NIST project.

Similarly, Microsoft's cryptographic posture management covers cryptographic asset discovery from various infrastructure components, including code, storage, networks, and runtime domains¹¹. While it operates as a continuous monitoring process, it still focuses on infrastructure-level elements. For example, GitHub Advanced Security generates cryptographic signals for cryptographic algorithms in code.

Business-centric approach

A business-centric approach starts with critical business services rather than technology assets. While business-centric transition planning has been promoted as a general strategy for PQC

¹⁰ NIST. Migration to Post-Quantum, <https://www.nccoe.nist.gov/applied-cryptography/migration-to-pqc>

¹¹ Aviram Shemesh and Jennifer Rutzer. Building your cryptographic inventory: A customer strategy for cryptographic posture management, <https://www.microsoft.com/en-us/security/blog/2026/04/16/building-your-cryptographic-inventory-a-customer-strategy-for-cryptographic-posture-management/>

migration¹², this report extends the concept to cryptographic asset discovery by defining a structured method that links business services, industry standards, cryptographic requirements, and infrastructure implementations, in payments.

The following are the top-down steps of our business-centric approach.

- Identify business capabilities that are critical to customers, financial stability and operational resilience (for example real-time payments, card payments, settlement, fraud management and customer authentication).
- Identify the standards, protocols, and regulatory requirements that govern those services.
- Determine the cryptographic functions, algorithms, and security requirements specified by those standards.
- Build the cryptographic asset inventory with the usage context to enrich Cryptographic Bill of Materials (CBOM).
 - “e.g., in this service, this message uses ECDSA or RSA signature for what purposes according to which standard”
- Continue with the inventory to identify deployed products that handle cryptographic messages
 - The priority can be made with the importance of services and the relevant messages
- Optionally, further map the corresponding assets into system implementations or products in IT infrastructure; tools used in infrastructure-centric can be applied here, but within a clearer business context.

In the above steps, the inventory is built progressively following a top-down approach from business-critical services to implementations and infrastructure levels. This hierarchy provides executives with a clearer basis for investment prioritisation because migration decisions are aligned to business outcomes rather than technology assets alone. Our approach can be modular and hierarchical to address the complexity of PQC transition. The approach can be applied to application-layer messages to construct application inventories or independently applied to develop inventories for network-layer messages and then establish links between these inventories.

Concluding Remarks

Taken together, the preceding sections highlight that preparing for the quantum-safe transition requires more than replacing individual cryptographic algorithms. It requires an understanding of where cryptography is used, how it supports critical business services, and the technical and organisational dependencies that will affect migration. The workshop discussions reinforced the importance of early preparation, ecosystem coordination and risk-based prioritisation, while the approaches outlined in this section provide practical ways to begin identifying and organising cryptographic assets. Building on these considerations, Section 5, Technical Appendix, examines the broader payments ecosystem and the dependencies that need to be understood when applying these approaches in practice through selected use cases.

¹² Unsung. Why Post-Quantum Cryptography Is a Business Transformation, Not an Algorithm Swap, <https://www.unsungltd.com/blog-posts/why-post-quantum-cryptography-is-a-business-transformation-not-an-algorithm-swap>

5 Technical Appendix

Payment Ecosystem and Cryptographic Dependencies

The payment ecosystem comprises of a complex set of interconnected services, platforms, and infrastructures that collectively enable the initiation, processing, clearing, and settlement of transactions. Understanding this ecosystem is an important step in cryptographic asset discovery because cryptographic functions are embedded throughout the payment lifecycle.

The three case studies presented below illustrate how the business-centric approach may be applied to identify cryptographic assets within different payment systems. These examples were prepared by the CSIRO team and presented during the workshop to demonstrate the approach rather than represent a complete discovery process.

The payment ecosystem is a multi-layered architecture that connects user-initiated transactions to a wide range of interconnected underlying systems, as illustrated in the high-level overview in Fig. F5-1. These systems are often operated by different organisations; for instance, the New Payments Platform (NPP) is managed by Australia Payments Plus (AP+), while Visa and MasterCard networks are run by global providers. The payment ecosystem engages with virtually all entities with economic activities in a society, including banks, payment service providers, technology vendors, and businesses of all sizes that send or receive payments. The broad scope and diverse participants of this ecosystem present significant complexity for preparing and implementing the PQC transition.

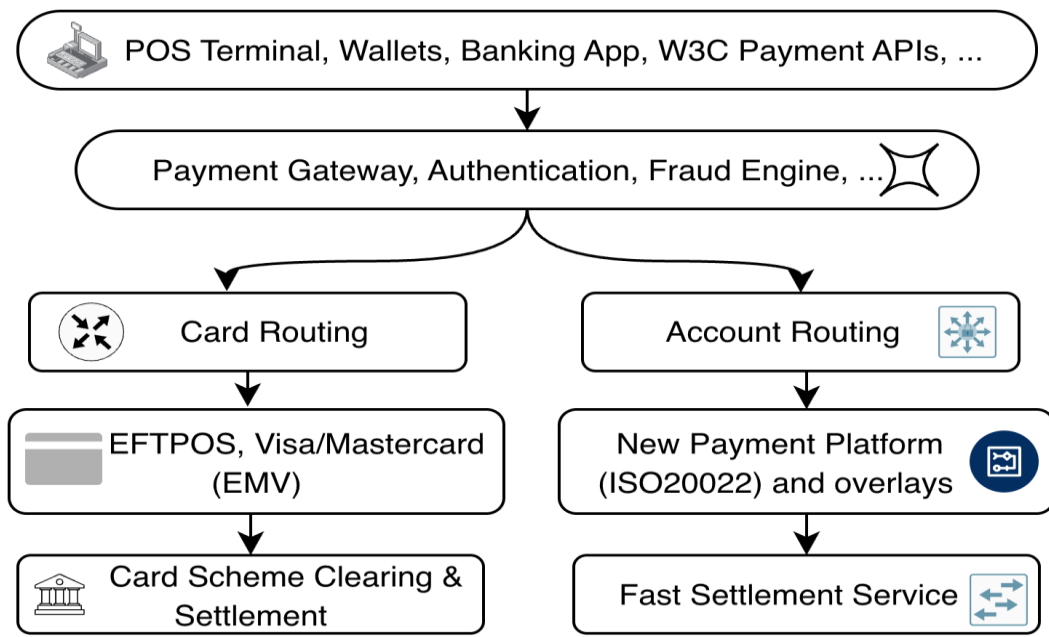


Figure F5-1 High-level Overview of Payment Networks

As exemplified in Fig. F5-1, many of these supporting capabilities are shared across multiple payment rails. Consequently, migrating cryptography within individual payment systems alone will not eliminate systemic quantum risk. For example, payments can be initiated through various channels, including point-of-sale terminals, digital wallets, banking applications, or browser-based W3C Web Payment APIs. Payment requests are supported by intermediate services such as payment

gateways, authentication services, and fraud detection engines. Card-based payments and account-based payments are then subsequently routed into different infrastructures for clearing and settlement. Preparing for the quantum-safe transition therefore requires identifying cryptographic assets and dependencies across the entire payment ecosystem.

To illustrate how the business-centric approach can be applied in practice, the CSIRO team prepared and presented the following three payment-system case studies during the workshop. The case studies provide deeper examples of cryptographic asset discovery across W3C Web Payment APIs, EMV card payments, and Australia’s NPP/FSS infrastructure.

Case Study One: Cryptographic Asset Discovery in W3C’s Web Payment APIs

The W3C Web Payment APIs (WPAs)¹³ provide a standardised framework for supporting web-based payment experiences across browsers, merchants, payment handlers, and payment service providers. This case study illustrates how the business-centric approach can be applied to identify cryptographic assets associated with a modern web payment service.

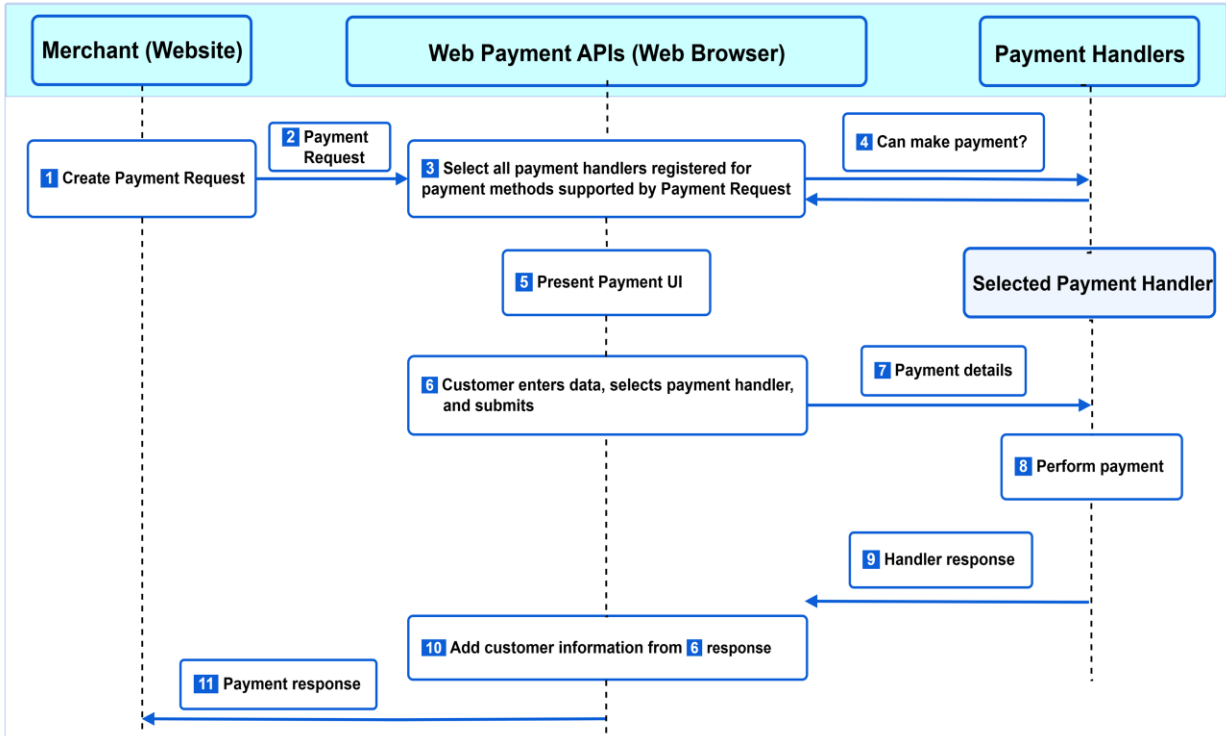


Figure F6-1: Message flow of W3C Web Payment APIs

Overview of W3C’s Web Payment APIs

Following the business-centric approach, the discovery process begins by identifying a business-critical service: web-based payment processing. The relevant standards are the W3C Payment Request API, Web Authentication (WebAuthn), and associated payment handler specifications.

In the W3C’s WPA payment architecture, the web browser acts as a secure intermediary between the merchant, the user’s payment handler, and the payment gateway. This intermediary relies on

¹³ Web Payments Working Group. Payment Request API: W3C Candidate Recommendation Draft, 2026

public key cryptography, for example JSON Web Encryption (JWE)¹⁴, to encrypt credit card information making it only readable by the payment gateway, and digital signatures (FIDO2¹⁵ and WebAuthn¹⁶) for robust, biometric based transaction authorisation. Compared to legacy web payment methods where users manually type Primary Account Numbers (PANs) into merchant checkout forms, the W3C's approach significantly improves data confidentiality and reduces the merchant's Payment Card Industry Data Security Standard (PCI-DSS) compliance scope.

Cryptographic Asset Discovery in W3C's WPAs

Following the identification of the relevant standards and business service, cryptographic assets can be discovered by analysing the payment message flow shown in Fig. F6-1.

In this protocol, the merchant first creates a payment request and invokes a Web Payment API that identifies payment handlers registered for the merchant's supported payment methods. The browser then presents the payment user interface, and the customer selects a payment handler. At this stage, the selected payment handler may authenticate the user through WebAuthn or FIDO2. After successful authentication, and if the payment can proceed, the payment handler returns a response containing payment authorisation information. In the example shown in Fig. F6-1, Message 9 includes a signature from the customer's financial institution to confirm the validity of the payment request.

This message flow reveals several cryptographic assets and dependencies:

- User authentication through WebAuthn or FIDO2 relies on public-key credentials and digital signatures.
- Payment confirmation relies on digital signatures that provide authenticity and integrity for the transaction.
- Payment handlers may protect card or token data using JSON Web Encryption (JWE).
- Trust relationships between participants rely on certificates, public keys, and secure communication protocols.

For example, JWE commonly uses RSA or ECDH for key establishment and AES for payload encryption. From a quantum-safe transition perspective, JWE payload protection may need to replace RSA or ECDH with ML-KEM or other approved PQC key-establishment mechanisms, while retaining AES-256 for data encryption. Similarly, WebAuthn and FIDO2 authentication, as well as payment confirmation signatures, may require migration to post-quantum digital signature algorithms such as ML-DSA or SLH-DSA, potentially using hybrid deployment approaches during the transition period.

This example illustrates how the business-centric approach can identify cryptographic assets directly from payment services, standards, and message flows before examining specific products or infrastructure implementations.

¹⁴ Internet Engineering Task Force (IETF), JSON Web Encryption (JWE), 2015

¹⁵ FIDO Alliance, User Authentication Specifications Overview, <https://fidoalliance.org/specifications/>

¹⁶ Web Payments Working Group, Web Authentication: An API for accessing Public Key Credentials Level 1: W3C Recommendation, 2019

Key Takeaways

Cryptographic asset discovery for web payment APIs should begin with the payment business process, rather than solely with infrastructure inventories. In web payment flows, cryptographic dependencies arise in user authentication, payment authorisation, data protection, and trust establishment between merchants, browsers, payment handlers, payment gateways, and financial institutions. Mapping these dependencies to business processes provides a more practical basis for assessing transition priorities and operational risks.

Quantum-safe migration in web payment ecosystems is not merely an algorithm replacement exercise. It requires coordinated transition across multiple stakeholders, merchants, browsers, payment handlers, payment gateways, financial organisations. The migration will involve transitional phases, hybrid cryptographic deployments, and extensive testing to ensure security, compatibility, and operational continuity.

Case Study Two: Cryptographic Asset Discovery in EMV

Card-based payments remain one of the most widely used payment services globally. EMV is the international standard governing interactions between payment cards, payment terminals, acquiring institutions, and issuing banks. This case study illustrates how the business-centric approach can be applied to identify cryptographic assets within a card-payment service.

Overview of EMV

Following the business-centric approach, the discovery process begins by identifying a business-critical service: card-based payments. The relevant standard is EMV, which defines how payment cards, terminals, and financial institutions authenticate one another and process transactions securely.

The EMV protocol has been described in the technical specification documents¹⁷ and summarised by Basin et al.¹⁸ for their formal security analysis. Fig. F7-1 shows a high-level overview of a card-based transaction process. A typical EMV contact transaction runs as a sequence of command response exchanges and can be viewed in four phases: 1) the terminal selects the payment application on the card and reads the card records needed for processing, 2) the terminal may perform offline data authentication to confirm the card's authenticity using one of three methods: SDA (static data authentication), DDA (dynamic data authentication), or CDA (combined dynamic data authentication), 3) the terminal verifies the cardholder using a mutually supported method such as "Offline Plaintext PIN", "Offline Enciphered PIN", or "Online Enciphered PIN", 4) the terminal and card perform risk management and generate a transaction cryptogram. Depending on terminal rules and card decisions, the transaction is either approved offline, declined offline, or sent online for issuer authorisation.

¹⁷ EMVCo. Book 2: Security and Key Management. EMVCo, Oct. 2022.

¹⁸ David Basin, Ralf Sasse, and Jorge Toro-Pozo. The emvstandard: Break, fix, verify. In 2021 IEEE Symposium on Security and Privacy (SP), pages 1766–1781, 2021.

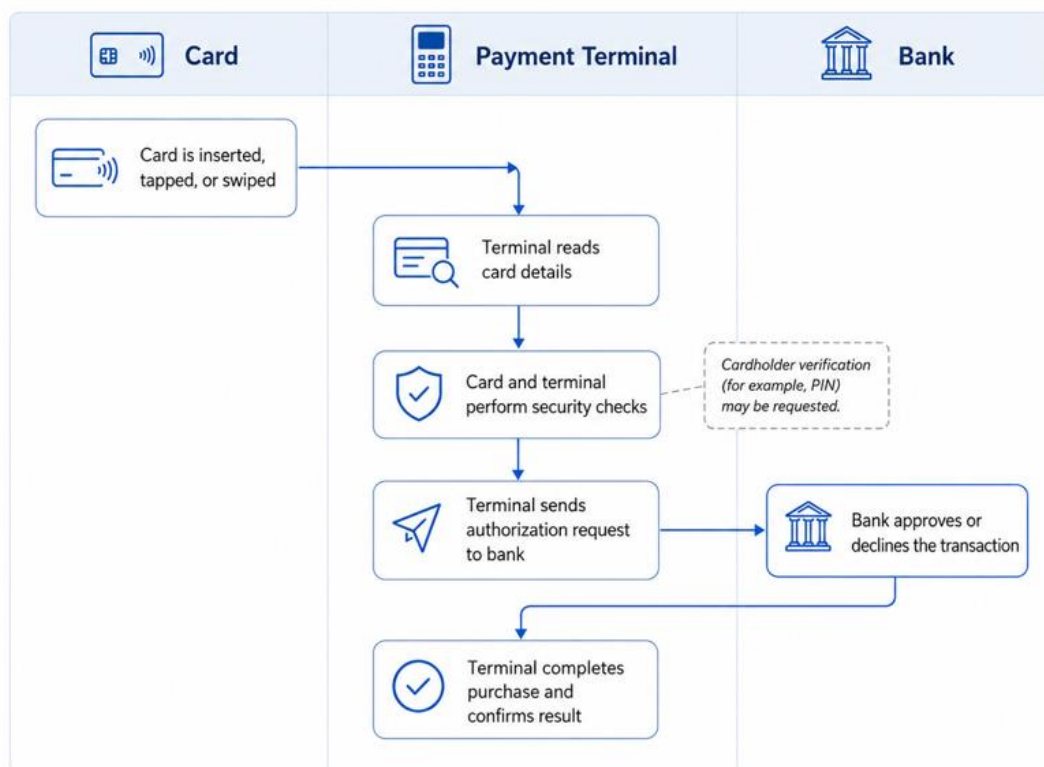


Figure F7-1: An Overview of Card-Based Transaction

Cryptographic Asset Discovery in EMV

Following the identification of the relevant standard and transaction flow, cryptographic assets can be discovered by analysing the security mechanisms used throughout the EMV transaction.

The security of EMV relies on a mix of asymmetric and symmetric cryptography. Asymmetric cryptography underpins the certificate chain and signatures used in offline authentication and some offline PIN modes. Symmetric cryptography underpins the application cryptograms used for authorisation, where the card and issuer share secret keys and derive session keys per transaction.

This design allows EMV to support both offline capable acceptance and online authorisation, while keeping the issuer in control of final approval when needed.

Key cryptographic assets in an EMV transaction include the certificates, public keys, digital signatures, and encrypted data used to prove that the card is genuine, the transaction is valid, and sensitive information is protected. These assets should be identified because some EMV implementations still rely on RSA or ECC, which may become vulnerable in a post-quantum environment. The transaction flow reveals several important cryptographic assets and dependencies:

- **Certificate chain and public keys provided to the terminal:** During the transaction, the card provides certificate material that helps the terminal verify the issuer and, where applicable, the card itself. The terminal uses trusted payment-network or issuer public keys to validate this chain.

- Static card authentication data: Some EMV transactions rely on signed static card data to confirm that the card information has not been altered.
- Dynamic card authentication: In stronger EMV modes, the terminal sends a fresh challenge to the card, and the card responds with a digitally signed response. This helps prove that the physical card is genuine.
- Transaction-bound signatures: Some EMV transactions use signatures that bind card authentication to the specific transaction details. These signatures are important because they help prevent replay or substitution of transaction data.
- Encrypted PIN data, where used: In some transaction flows, PIN data may be encrypted before being sent for authorisation.
- Symmetric cryptographic keys and transaction cryptograms used for transaction authorisation.

These cryptographic assets are important because some EMV implementations continue to rely on RSA or elliptic-curve cryptography for authentication and digital signatures. Such public-key mechanisms may become vulnerable to sufficiently capable quantum computers. Consequently, certificate chains, authentication signatures, and other public-key components represent potential migration targets for post-quantum cryptography. In contrast, the symmetric cryptographic mechanisms used for transaction cryptograms are generally expected to remain secure with appropriate key lengths.

This example illustrates how the business-centric approach can identify cryptographic assets directly from EMV transaction flows and standards before examining specific terminal, card, or banking infrastructure implementations.

Key Takeaways

The case study of EMV demonstrates that cryptographic asset discovery is most effective when it begins with the business-critical payment service and traces the end-to-end transaction flow across cards, terminals, payment networks, and issuing institutions. This process identifies the key cryptographic dependencies that support card authentication, cardholder verification, transaction authorisation, and trust management. It also enables the prioritisation of post-quantum migration efforts: public-key assets such as certificate chains, RSA/ECC keys, and authentication signatures are likely to require closer attention, while symmetric transaction cryptograms may remain suitable if implemented with appropriate key lengths.

Case Study Three: Cryptographic Asset Discovery in NPP/FSS

The New Payments Platform (NPP) is Australia's real-time payment infrastructure and represents a critical component of the national financial system. This case study illustrates how the business-centric approach can be applied to identify cryptographic assets within a payment service that supports interbank clearing and settlement. It also illustrates the importance of ecosystem-wide coordination. Migration cannot be undertaken independently by individual participants because cryptographic interoperability must be maintained across financial institutions, payment service providers and settlement infrastructure throughout the transition period.

Overview of NPP/FSS

Following the business-centric approach, the discovery process begins by identifying a business-critical service: real-time account-to-account payments. The relevant standards include the NPP API Framework, ISO 20022 payment messaging standards, and the supporting security protocols used by participating financial institutions.

Fig. F8-1 shows the message flows of the NPP and FSS infrastructure¹⁹. The payment is initiated by payers through their financial institutions, which rely on payment gateways to locate the payee's account via the NPP address service. After the payee's account is determined, clearing messages are exchanged among financial institutions, and settlement messages are with FSS. The NPP API Framework²⁰ states that NPP APIs follow RESTful API concepts, use JSON/JSON Schema for data representation, use Swagger/OpenAPI as the interface description language, and use ISO 20022 message for payload where available.

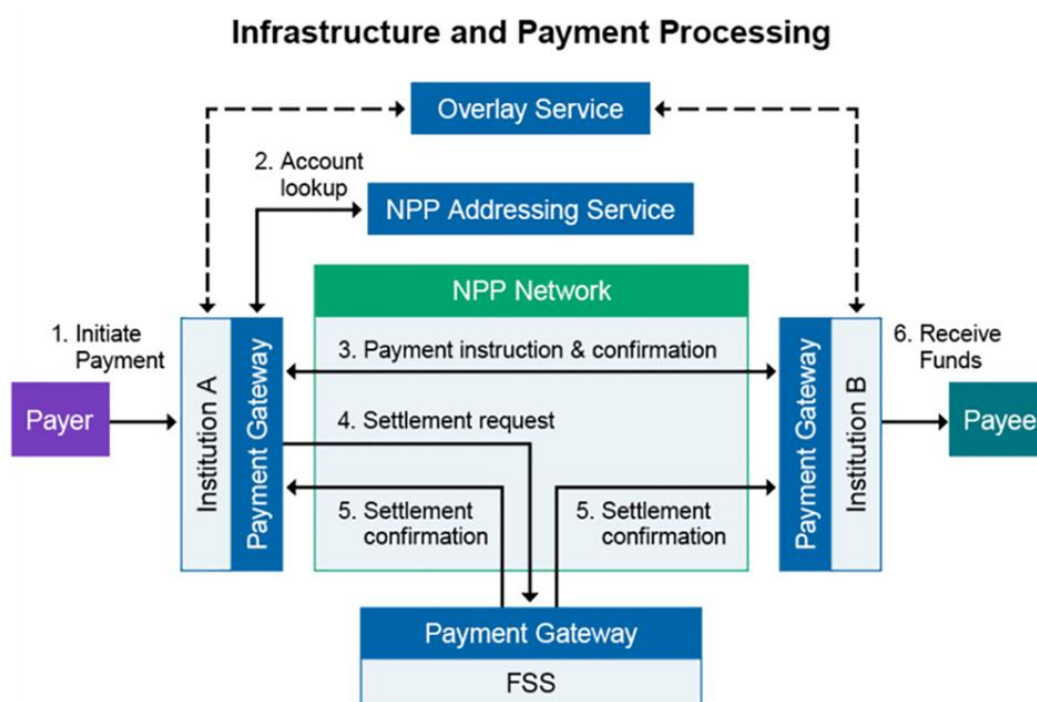


Figure F8-1 NPP and FSS Infrastructure [source: Bulletin – September 2018¹⁷]

Cryptographic Assets Discovery in NPP/FSS

Following the identification of the relevant standards and payment flows, cryptographic assets can be discovered by analysing the security mechanisms used to protect payment messages, communications, and participant authentication.

¹⁹ Alexandra Rush and Riaan Louw, The New Payments Platform and Fast Settlement Service, <https://www.rba.gov.au/publications/bulletin/2018/sep/the-new-payments-platform-and-fast-settlement-service.html>

²⁰ NPP Australia Limited and SWIFT SCRL. New Payments Platform API Framework. <https://www.auspayplus.com.au/wp-content/uploads/2025/05/NPP-API-Framework-v5.0-1.pdf>

In the NPP ecosystem, publicly identifiable cryptographic dependencies include TLS-secured or IPSec-protected communication channels, PKI/certificates for endpoint or participant authentication, institution-specific API authentication mechanisms, and authorisation based on token or credential. Although some ISO 20022 message families contain security-related structures, they should not be treated as NPP/FSS cryptographic assets without NPP-specific evidence. Based on industry feedback, these structures are more relevant to card payments. Therefore, the NPP/FSS analysis should focus on the underlying infrastructure that enables financial institutions to authenticate each other, protect payment instructions, exchange clearing messages, and maintain settlement consistency.

From the perspective of quantum transition, the most relevant exposure is the classical cryptographic assets supporting these trust relationships. If PKI, certificates, communication channels, or authentication mechanisms were compromised by quantum-capable adversaries, it could lead to endpoint impersonation, fraudulent payment initiation, transaction inconsistency, or manipulation of interbank obligations.

This example illustrates how the business-centric approach can identify cryptographic assets directly from payment services, standards, and message structures before examining specific technology products or infrastructure implementations.

Key Takeaways

The case study of NPP/FSS demonstrates the value of applying cryptographic asset discovery to a real-time payment infrastructure that connects customer-facing payment initiation through financial institutions with interbank clearing and central-bank settlement. A unique challenge is that cryptographic dependencies are distributed across several layers, including API-based payment initiation, ISO 20022-aligned message structures, participant authentication, secure communication channels, interbank clearing, and FSS settlement. As a result, the relevant assets cannot be identified by looking at a single protocol or implementation component in isolation. Instead, they must be traced along the end-to-end payment flow, from payment initiation and submission through clearing messages to final settlement instructions. This case study illustrates how cryptographic asset discovery can begin with publicly available payment processes, standards, and message structures to identify likely cryptographic dependencies before progressing to institution-specific implementations.