CSIRO
[redacted]
csiro.au | ABN 41 687 119 230

May 22, 2026

To: The Account-to-Account Payments Roundtable

Response to the A2A Payments Vision Consultation Draft

Background: CSIRO has strong capability in cybersecurity, system security, quantum-safe transition, and critical infrastructure resilience. Recently, CSIRO organized a workshop "Planning the Quantum-Safe Transition for Australia's Financial Sector: A National Use Case in April 2026", addressing emerging challenges in the financial sector. In addition, CSIRO released a report, "Quantum Safe Transition: Reality, Hurdles and Pathways", highlighting the importance of quantum-safe transition and crypto-agility. These developments align closely with the A2A payment vision consultation and reinforce the importance of incorporating long-term cryptographic resilience into future payment infrastructure planning.

In the following, we provide our responses to the consultation questions, focusing on the security and long-term resilience of Australia's payments infrastructure, with particular emphasis on quantum resilience and crypto-agility.

1. Vision Resonance

We agree with the framing of the future A2A system as a trusted national asset and foundational component of Australia's economy. Trust in payment systems should be underpinned by security-by-design principles, interoperability, effective governance, and well-defined technical standards. We suggest making one additional aspect explicit in the vision: the future A2A system should be both crypto-agile and quantum-resilient. While the draft refers to encryption and cryptography, it does not explicitly address post-quantum cryptography or the broader quantum-safe transition. Given the long operational lifetime of payment infrastructure and the enduring sensitivity of financial data, explicit consideration of quantum resilience should form part of the system's long-term strategic vision.

2. End-User Objectives

We recognise the importance of safety and reliability, given that A2A payments support critical economic and social functions. Safety can be further strengthened by explicitly considering long-term cryptographic security, particularly the risks that quantum computing may pose to data confidentiality, authentication, and digital trust mechanisms. Reliability should also encompass the ability of the payment ecosystem to maintain continuity, interoperability, and operational stability throughout major technology transitions, including the transition to quantum-safe cryptography.

3. System Characteristics

For security and protection, we concur with the draft's emphasis on safety-by-design principles and alignment with global cryptographic standards. We suggest that the vision additionally incorporate explicit consideration of crypto-agility and the transition to quantum-safe cryptography, recognising that large-scale cryptographic migration itself may introduce operational and resilience risks if not carefully managed. Shared sector-wide guidance, common approaches to cryptographic asset discovery, and coordinated transition planning could help reduce implementation burden and support more consistent, secure, and resilient adoption across the payments ecosystem.

4. Priorities for Delivering the Vision

Aligning with the recommendations in CSIRO's report "Quantum Safe Transition: Reality, Hurdles and Pathways", we propose five priorities related to crypto-agility and quantum resilience in future payment infrastructure:

1) Establishing a dedicated security and quantum-safe transition workstream within the A2A governance and standards process;
2) Undertaking business-centric cryptographic asset discovery for priority A2A services, initially focusing on critical services and message flows. This approach starts with payment services, which complements the common approach starting from networks and security tools;
3) Prioritising business risk analysis for high-impact and long-lived assets;
4) Embedding crypto-agility into future A2A standards, protocols, and infrastructure design; and
5) Validating quantum-safe transition approaches through realistic testing and operational trial environments.

5. Other Feedback

We propose that the A2A vision incorporates measurable security and resilience outcomes, including cryptographic asset inventory coverage, post-quantum cryptography (PQC) readiness, adoption of crypto-agility principles, and validation of major infrastructure changes prior to deployment. We also recommend that the industry consider establishing a shared Open Cryptographic Asset Knowledge Base for payment services. Such a capability could assist institutions in identifying common cryptographic dependencies across shared standards, protocols, and message flows, while preserving the confidentiality of individual participants and reducing duplicated transition effort across the sector.