TCA Group – Updated Use Case Complexity Matrix (v2 – DIA-Aligned)

This document provides a consolidated view of potential digital credential use cases, assessed through the lenses of complexity, impact, ecosystem readiness and alignment with DIA's public Digital Credentials Research (October 2025). It is intended as a neutral, evidence-based working draft to support TCA Group Session 3 discussions. The purpose is to assist the group in prioritising use cases for communications development, UX/UI principles and future-phase planning. This is not intended to be a policy position, but a collaborative input into ongoing cross-sector design work.

Complexity Scoring Method – Explanation

The complexity ratings in the below use case matrix are derived from a combined lens of **TCA Group direction**, **ecosystem expectations** and insights from the **DIA Digital Credentials Research**. Each use case has been assessed against several dimensions that influence how difficult it would be to design, implement, govern and scale within Aotearoa's emerging digital credentials ecosystem. These dimensions include:

- **Technical complexity:**
  The degree of technical sophistication required (e.g., biometric binding, liveness checks, issuer onboarding workflows, verifiable presentation flows, multi-party interactions, and cross-credential dependency). More advanced patterns or multiple system integrations increase complexity.
- **Ecosystem maturity & sector readiness:**
  Whether the relevant sector (e.g., banking, education, health, telco) has the standards, systems, issuers, and governance structures in place to support digital credentials at scale. Mature sectors reduce complexity; fragmented or low-readiness sectors increase it.
- **Policy & regulatory dependency:**
  The extent to which a use case relies on legislation, regulatory approval, or policy change (e.g., AML/CFT for banking, WorkSafe requirements, telco identity regulations). High dependency increases complexity and timelines.

- **Trust & public comfort:**
  Informed by the Verian research, this considers how acceptable, intuitive, or risky a use case feels to the public. Use cases that touch on sensitive topics (e.g., phone loss, delegated authority, income data) require stronger safeguards and clear design patterns, increasing complexity.
- **Dependency on DIA's three priority government use cases:**
  Age Verification, Photo ID, and Bank Onboarding form the baseline patterns for the ecosystem. Use cases that extend or rely on these foundational patterns are generally less complex; those requiring novel or untested patterns are more complex.
- **Interoperability with existing government systems:**
  The complexity of integrating with current government identity, credential-issuing, or verification systems. Use cases requiring cross-agency data flows or integration with legacy systems tend to increase overall complexity.

Together, these criteria provide a structured, transparent method for comparing use cases and identifying which are best suited for early adoption, which require further ecosystem development and which represent longer-term opportunities.

TCA Group Use Case Matrix

Use Case	Description	Complexity (Revised)	Impact / Public Value	NZ Policy / Trust Framework Dependencies	Notes / DIA Research Alignment
Lost Phone / SIM Recovery	Restore identity + SIM using digital wallet + VC	High (device binding, recovery patterns not yet defined)	High – Strong consumer demand; real-world pain point	• No prepaid SIM regulation today • Trust Framework does not yet define recovery flows	Public highly concerned about lost/stolen phone lockout (pp. 18–20) — high-value but high-risk.

Health & Safety Worker Verification	Verify induction, certification, compliance	Medium–High (multiple issuers, inconsistent standards)	High – Significant NZ business cost saving	• Requires sector credential standards • Likely WorkSafe alignment	High relevance; trust impacted by forgery fears (p. 19) – needs strong assurance pattern.
Age Verification (Alcohol, Controlled Goods)	Over-18 proof without revealing PII	Low–Medium (already a DIA priority use case)	Medium–High	• Already one of DIA's three use cases • Requires liveness + photo ID	Ranked lower in public value (p. 37); concerns about "too many steps for bars" (p. 40).
Bank Account Opening / KYC	Verified identity + address + AML controls	High (AML/CFT, bank assurance requirements)	High	• DIA priority use case • Bank accreditation + high assurance reqs	High trust requirement; strong public demand for proof of address + income verification (p. 37).
Visitor / Meeting Registration	Quick check-in using VC	Low	Medium (friction reduction)	• Minimal regulatory constraint	Public sees strong "convenience" appeal (pp. 11–13).
School Zoning / Education Entitlement	Confirm parent/student location/eligibility	Medium	High	• Must align with MoE address + enrolment evidence	Top-ranked public value: proof of address is #1 most helpful use case (p. 37).
Sports / Volunteer Vetting	Coach/volunteer identity + police vetting	Medium–High	Medium–High	• Requires Police Vetting API + Trust Framework roles	Public worried about delegation & authority misuse (p. 38–39).

Travel Identity / Domestic Photo ID Replacement	Wallet-based photo ID (domestic only)	Medium–High (airline & govt integration)	Medium	• Within DIA reference architecture	Older users find digital travel docs highly valuable (p. 37).
Small Business / Contractor Access Credentials	Issue/consume workforce creds	Medium	Medium–High	• Simplified issuer onboarding • Tiered assurance	Strong "productivity" theme but high issuer-onboarding lift.
Energy Sector Credentialing	Identity + entitlement for energy operators	High	Medium	• EA regulatory alignment	Cited in mining/energy discussions; narrow audience.
Telecommunications Customer Identity	Telco identity for onboarding + fraud	High (similar complexity to SIM recovery)	High	• Optional regulatory environment	Strong alignment with security concerns in research (pp. 18–20).
School / University Qualifications	Verified certificates, diplomas	Medium	Medium–High	• Needs education issuer standards	Strong public value for job applicants (p. 37–38).
Income / Employment Verification	Verified employment + income	Medium–High	High	• Requires IR / employer integration	High public demand for "verified income" (p. 37).
Proof of Address	Verified bank/utility/provider address	Medium	Very High – #1 use case	• Requires standardised "verified address issuer"	Highest public appeal; easiest to explain.

Delegated Authority (parent, POA, business)	Acting on behalf of others	High (high trust, risk, UX complexity)	Medium	• Requires binding legal authority + verifier trust	Research: least helpful overall and raises high concern (p. 37–38).

Complexity Category Summary:

Complexity	Use Cases
Low	Visitor / Meeting Registration Simple age checks (if tied to DIA base pattern)
Medium	Proof of Address School Enrolment / Zoning Skills / Qualifications Small Business Credentials
High	SIM Recovery Telecommunications Customer Identity Bank Onboarding / KYC Delegated Authority Energy Sector Credentialing

Shortlisted Use Cases for TCA Group Consideration and Decision-Making

This shortlist reflects use cases that best balance impact, feasibility, ecosystem readiness, and alignment with government research. It is intended to guide the TCA Group's decision-making as it confirms which use cases will proceed into communications development, user experience design, and future implementation planning.

Complexity with High Impact	Use Cases
Low	Proof of Address Visitor / Meeting Registration Age Verification
Medium	Job Application Credential Pack School / Childcare Enrolment Pack School Zoning / Education Entitlement
High	Bank KYC Lost Phone / SIM Recovery Income / Employment Verification (Optional) Delegated Authority

Draft for TCA Group discussion – based on publicly available DIA Digital Credentials Research (October 2025). This document is not a policy statement and should be treated as a working draft for collaborative exploration.