Industry Demand for Trusted Identity Evidence and Standardised Network APIs

STATEMENT OF REQUIREMENTS (SOR) FOR GSMA FUSION AND GSMA OPEN GATEWAY

Version: 3.0 (Public External Version) | **Date:** 16th September 2026

© 2026 WeVerify B.V. All rights reserved. "WeVerify" and "Verified Existence Credential (VEC)" are trade names of WeVerify B.V. All other product, standard and organisation names are the property of their respective owners. This document is provided "as is", for information purposes only, without warranties of any kind.

CONTENTS

CONTENTS 2
EXECUTIVE SUMMARY 3
DEFINITIONS 3
MARKET DEMAND 3
ALIGNMENT WITH EXISTING FRAMEWORKS 3
DEPLOYMENT SCOPE 4
PURPOSE 4
ILLUSTRATIVE USE CASES 4
STANDARDS & TECHNOLOGY ORIGIN 5
CURRENT POLICY & REGULATORY ENVIRONMENT 5
1.1 Current regulatory environment 5
1.2 Barriers affecting the adoption of Know Your Customer (KYC) network APIs 5
1.3 Importance and benefits of stronger identity credentials 5
NETWORK API REQUIREMENTS 5
2.1 Essential Open Gateway / CAMARA APIs requirements 5
2.2 Secondary priority Open Gateway / CAMARA APIs requirements 6
EXPECTED IMPACT USING STANDARDISED NETWORK APIs 6
CALL TO ACTION 6
COLLABORATION AND NEXT STEPS 7

EXECUTIVE SUMMARY

- **Problem:** People without reliable identity and authorisation checks may be excluded from payment accounts, remittances and essential services, while service providers face fraud, impersonation and operational risk.
- **What is required:** Standardised CAMARA network APIs availability that enables relying parties to make proportionate, risk-based decisions using minimal network signals, such as boolean results, timestamps and limited freshness metadata.
- **What this Statement of Requirements (SoR) provides:** A public enterprise demand statement calling for the availability of standardised CAMARA network APIs to provide market coverage and cross-operator interoperability.
- **What this SoR does not include:** Proprietary implementation details, algorithms, thresholds, scoring logic, security tuning, protocols, user experience flows, product architecture, partner plans, commercial terms, pricing, or deployment commitments.

DEFINITIONS

- **Verified Existence Credential (VEC):** a privacy-preserving evidence concept indicating verified existence and continuity of a person or entity, assembled from minimal, consented signals. It is not citizenship determination, legal identity issuance or a replacement for national ID systems.
- **Relying party:** an organisation (for example a bank, mobile money operator, payment provider or humanitarian programme) that consumes network signals to make onboarding, recovery, transaction or risk decisions.
- **Network API provider:** a mobile network operator or aggregation platform exposing standardised network API capabilities through GSMA Open Gateway/CAMARA API interfaces.
- **Minimal signal:** an API output limited to a boolean result, an event timestamp and/or limited freshness metadata, without raw traces or unnecessary personal data.

MARKET DEMAND

Across multiple sectors, organisations need dependable identity and authorisation checks to onboard users safely, reduce fraud exposure and deliver digital services. At the same time, many markets have incomplete identity coverage or inconsistent verification pathways, creating exclusion for underserved populations and operational burden for providers.

Standardised network APIs and interoperable evidence requirements can reduce integration complexity, improve consistency across operators and enable scalable, privacy-preserving risk decisions. The requirements in this SoR are designed to support inclusion, fraud reduction, auditability and proportionate regulatory oversight.

ALIGNMENT WITH EXISTING FRAMEWORKS

The requirements in this SoR are designed to align with widely adopted principles and initiatives, including data protection principles such as those in the GDPR (lawfulness, purpose limitation, data minimisation), digital identity concepts emerging under eIDAS 2.0, FATF guidance on digital identity for customer due diligence, and the GSMA Open Gateway initiative and standardised CAMARA APIs.

This document does not claim compliance with, certification under, or endorsement by any of these frameworks or organisations; alignment is a design objective to be validated per deployment.

Any implementation of network APIs by relying parties must be based on a lawful basis under applicable data protection legislation and where required, freely given, specific, informed and explicit user consent. Data obtained via network APIs must be limited to what is strictly necessary and proportionate for the authorised purpose, and processed in accordance with applicable privacy, data protection, telecommunications and regulatory requirements. Such data must be used only as privacy-preserving supporting evidence within a risk-based verification framework and must not be abused, repurposed, disclosed or used for surveillance, profiling, discrimination, unauthorised tracking or any other unlawful, unethical or harmful purpose. Relying parties must maintain appropriate technical and organisational security measures, governance arrangements, accountability mechanisms and audit controls throughout the period of deployment and must comply with all applicable obligations regarding data subject rights, data retention, deletion and breach notification.

DEPLOYMENT SCOPE

This SoR calls for phased pilots and deployments in markets where identity coverage gaps, financial inclusion priorities and fraud-prevention needs are significant. Initial activities should be limited in scope and subject to appropriate governance, consent, data protection, security and operational controls.

PURPOSE

Digital finance and essential services increasingly depend on the ability to establish trusted identity and authorisation. In many regions, individuals and small entities may lack consistent access to official identification or verifiable authority checks, which can block access to payment accounts, remittances, benefits and digital workflows.

This SoR sets out the standardised network API capabilities needed to support a **Verified Existence Credential (VEC)** evidence concept. VEC evidence is described here as supporting evidence of verified existence and continuity.

ILLUSTRATIVE USE CASES

The following generic use cases illustrate where the capabilities demanded in this SoR create value. They are illustrative only and do not describe any specific product workflow.

- Account opening and tiered onboarding in markets with low official identity coverage.
- Account recovery and credential re-binding after loss of device or SIM.
- Remittance and payment onboarding, including step-up checks for higher-risk transactions.
- Humanitarian and NGO cash assistance programmes requiring inclusive, auditable beneficiary verification.
- Fraud and account takeover prevention for existing digital service users.

STANDARDS & TECHNOLOGY ORIGIN

This SoR is structured as a demand statement to accelerate interoperable deployment across the ecosystem. It is aligned with the principle of using standardised CAMARA network APIs interfaces and minimal outputs to enable cross-operator interoperability while preserving privacy and avoiding vendor lock-in.

CURRENT POLICY & REGULATORY ENVIRONMENT

1.1 Current regulatory environment

In many markets, identity verification and customer due diligence requirements are shaped by national regulations, sector-specific supervisory expectations and risk-based compliance frameworks. These conditions vary country by country and may affect whether alternative or supplementary evidence, such as VEC evidence, can be used by relying parties. VEC evidence is described in this SoR as supporting identity evidence of verified existence and continuity. It should not be treated as citizenship determination, legal identity issuance or a replacement for national ID systems. It may be used as a supervised, auditable pre-proofing layer to support tiered onboarding and, where permitted, acceleration of official processes.

1.2 Barriers affecting the adoption of Know Your Customer (KYC) network APIs

The adoption of KYC related network APIs may be influenced by jurisdiction specific legal and policy frameworks, regulatory expectations, operator data availability, and broader market conditions. Common barriers include limited or inconsistent KYC coverage for prepaid subscribers in some markets, variations in consent and lawful processing requirements, and differences in how identity data is collected, maintained and made available across mobile networks.

1.3 Importance and benefits of stronger identity credentials

Stronger, privacy-preserving identity credentials can support more reliable onboarding, account recovery, payment authorisation and fraud prevention. Where lawful and available, evidence categories may help relying parties improve confidence in user existence, continuity, device or SIM association, and the freshness of relevant risk signals while avoiding unnecessary disclosure of personal data.

NETWORK API REQUIREMENTS

2.1 Essential Open Gateway / CAMARA APIs requirements

> Mobile network operators and API providers are asked to expose the following standardised CAMARA API capabilities, where available and supported by applicable standards, lawful basis and consent requirements:
>
> **T-1** Number Verification API
>
> **T-2** Location Verification API
>
> **T-3** Device Roaming Status API

T-4 SIM Swap API

T-5 Device Swap API

T-6 Know Your Customer Tenure API

T-7 Know Your Customer Match API

2.2 Secondary priority Open Gateway / CAMARA APIs requirements

T-8 Know Your Customer Fill In API

T-9 Number Recycle API

T-10 Device Reachability Status API

EXPECTED IMPACT USING STANDARDISED NETWORK APIs

The benefits below are directional expectations. Any quantified impact claims should be supported by pilot evidence, production data or separately agreed evaluation criteria. When implemented lawfully and with appropriate safeguards, standardised network APIs can help identify legitimate users, detect suspicious changes in mobile identity context and reduce fraud in real time. Expected benefits include:

- Stronger real-time fraud detection and prevention.
- Improved trust and identity confidence.
- Reduced account takeover and impersonation risk.
- Lower operational burden for providers and relying parties.
- Improved financial inclusion for people who may lack conventional identity documentation.
- Cross-operator consistency that reduces integration complexity.
- Improved regulatory and audit readiness.
- Faster response to emerging fraud patterns.

CALL TO ACTION

WeVerify calls on mobile network operators to expose the essential standardised Open Gateway/CAMARA API capabilities listed in T-1 to T-7 and to express interest in interoperability discussions and pilot participation. Operators are also requested to indicate to WeVerify the status and roadmap for the secondary-priority capabilities listed in T-8 to T-10.

Timelines, Initial Pilots and Implementation: This SoR calls on mobile operators to support phased pilots in countries where identity coverage gaps and inclusion priorities are most acute. The sequencing below is indicative and non-binding, and does not constitute a deployment commitment by any party:

- **In 2026:** initial pilots focused on limited scope deployments with a small number of relying parties and participating network API providers in Mali and Sierra Leone.
- **Early 2027:** pilots expand to additional markets in West and East Africa.
- **Following successful pilots:** production deployment of network API capabilities, subject to separate commercial and service level agreements.

Comments, capability statements and expressions of interest are invited on an ongoing basis via info@weverify.com.

COLLABORATION AND NEXT STEPS

WeVerify welcomes collaboration through relevant industry and standards initiatives to help define and validate interoperable network API capabilities that address identity verification, fraud prevention and inclusion use cases.

As a next step, WeVerify is open to discussing pilot or proof-of-concept activities with mobile network operators, ecosystem partners, public authorities and relying parties to assess API applicability, implementation requirements, governance controls and measurable identity fraud prevention outcomes. Any such activity must be subject to separate written agreement, including appropriate confidentiality, data protection, security, intellectual property, commercial and operational terms.