Shufti

AMLR ISN'T JUST A COMPLIANCE PROJECT

IT'S AN IDENTITY DECISION

Building One Defensible Journey Across EIDs, Wallets, QES And Document Verification

WATCH WEBINAR HERE

www.shuftipro.com

OVERVIEW

Verification used to be a choice you made and a policy the regulator read. Under the AMLR, it becomes a decision you have to demonstrate.

The regulation replaces a patchwork of directives with one rulebook applying directly across the EU, supervised by AMLA and binding from 10 July 2027. Under the CDD RTS, government-backed electronic identification is the reference method for verifying a remote customer and anything else is an exception you have to evidence.

The panel's warning was simple: updating your policy will not be enough. What a auditor will ask for is the file behind the decision, and most firms are not building one yet.

DISCUSSION POINTS

This is an effectiveness review, not a policy update.

Oonagh van den Berg set the frame early. The AMLR tests whether your controls actually work, starting from the real risk in your book, clients, geographies, products, third parties and not from what the policy says. She was just as direct about who owns that.

"This is not the job of the compliance department. It's the responsibility of the risk owners within the organisation, and that goes right up to the board."

The burden of proof has moved, and it was deliberate.

Andrei Sribny traced the shift through the drafting history. Industry argued at the EBA consultation that firms shouldn't be pushed toward eIDAS routes if other methods met the guidelines. The EBA agreed the point was reasonable, but couldn't add the flexibility. AMLA held that line, leaving other methods as a conditional exception rather than a free choice.

"Until now, you chose a verification method and the regulator checked your policy. From July 2027, you justify the method itself and if it isn't an eIDAS route, the burden of proof is yours."

The wallet is not arriving on schedule, and that changes nothing about the deadline.

Clemens Brunner was blunt: the EUDI wallet isn't unevenly available today, it isn't available at all. Member states are meant to provide one from early 2027, and some haven't yet appointed anyone to build it. Counting infrastructure plus getting citizens actually onboarded, he put a realistic rollout at more than a year past that date.

"Some countries have not even defined the company who builds the wallet itself. And now we have August."

He also flagged a limit worth knowing before designing a flow around reusable identity: a qualified electronic signature carries only first and last name, so it cannot stand in for the full attribute set AML onboarding requires.

Multi-vendor is allowed. Disconnected evidence is the liability.

Neliswa Mncube's concern about multi-vendor stacks was evidence rather than compliance in principle. Four providers means four contracts, four retention policies and four formats of evidence, which stays invisible until a regulator asks about one customer file three years later.

"What should have been a regulatory inquiry becomes a project. Design a single chain, instead of designing to accumulate."

Two different problems, one deadline.

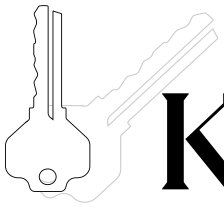
Sarah Adenaike drew the distinction. Large institutions struggle with legacy and coordination, untangling verification from old core systems across businesses, jurisdictions and vendors. Buildable, but slow, political and expensive. Smaller and newly in-scope firms have a clean slate technically, and are arguably better placed for it, provided they have the budget, the compliance depth and the engineering capacity, which many don't.

Gaming, betting, PSPs and crypto have no infrastructure to upgrade at all. The evidence trail gets built from zero, and at their volumes automation carries the full weight.

"It's not just about doing it right, it's being able to evidence what you've done. And when you get it wrong, it's not a compliance gap, it's a business-breaking one."

Challenges Discussed

- **Gap analysis is the wrong exercise.** The AMLR tests whether your framework works in practice. The policy is the last step, not the first.
- **The obligations live in the technical standards.** Firms preparing against the AMLR text alone are, in Andrei's words, "preparing for the wrong exam" and they will find out during an inspection.
- **Not all electronic IDs are equal.** Around 45% of countries have an eID, and, like corporate registries before them, they differ in reliability, assurance and legal status. Every firm needs a documented position on which schemes it will rely on, and an owner for that decision.
- **Siloed KYC stacks fail the evidence test.** Document verification, liveness, screening and trust services each doing their own job doesn't add up to one explainable journey one file you can hand a auditor.



KEY TAKEAWAYS

- **Build for the eIDAS default, and document why when you don't.** Alternatives are still allowed, but you carry the proof. Build the file as you go: the assessment, the reason, the safeguards.
- **Don't wait for the wallet.** Build now with the routes you have, in a way that lets you add the EUDI wallet later without starting over.
- **Design a single chain, not a stack.** Multi-vendor is permitted; disconnected evidence is the liability. Know what comes out as the end evidence before someone asks for it.
- **Pressure-test whether you can produce an audit trail.** Pull a sample onboarding decision and ask how you did it, when, and what data you relied on. Close that gap first.

ABOUT US

Shufti is a global identity verification platform built on fully owned technology, helping businesses strengthen onboarding, fraud prevention, and compliance at scale, without forcing a trade-off between security and growth.

- One platform, fully owned technology for greater control, flexibility, and consistency across the verification journey.
- Global coverage with real local depth, supporting 10,000+ document types across 220+ countries and in-house OCR across 150+ languages.
- Flexible deployment options, including local cloud and on-premises deployment, to support data residency, security, and enterprise compliance needs.

What We Deliver

- Customers can be verified through national eIDs, NFC chip reading, document capture with a liveness check, or qualified trust services. Each route carries a known assurance level, and new ones can be added without rebuilding what you already run.
- Qualified trust services delivered through our partnership with Evrotrust, designed from the outset as a single chain rather than a bolted-on integration: defined roles, one retention policy, and one end piece of evidence.
- A single evidence chain across the verification journey, so a customer file can be produced complete when a supervisor asks for it.
- Verified identities connected to proprietary global AML data and in-house name matching, for fewer false positives, higher pass rates, and a clear audit trail across the customer lifecycle.

JOIN THE SHUFTI COMMUNITY

Stay connected for expert insights, regulatory analysis, and practical guidance on compliance, AML, and digital identity.

Follow us. Learn with us. Grow with us.

Shufti on Website | Shufti on LinkedIn | Shufti on Twitter/X | Shufti on Facebook | Shufti on YouTube