International Digital Asset Association (IDAA)

IDAA BRIEFING NOTE · No. 03 28 October 2026

Digital Identity Standards Map 2026–2028

Between September 2026 and December 2027, verified identity becomes regulated infrastructure for digital assets in the UK and the EU. This note maps the rules and the standards pipeline that will define it.

EXECUTIVE SUMMARY

Two dates now frame identity verification for crypto-asset firms. In the UK, the digital verification services (DVS) trust framework 1.0 certification scheme has been in force since 2 September 2026, and HM Treasury guidance says digital identity meets Regulation 28 of the Money Laundering Regulations only when a certified provider on the DVS register performs it.[3][4][5] In the EU, the AML Regulation (AMLR) applies to every obliged entity, including crypto-asset service providers, from 10 July 2027, with remote identification under eIDAS treated as equivalent to in-person checks at an appropriate assurance level.[1]

Between those dates, every member state must offer an EU Digital Identity (EUDI) Wallet by December 2026, and banks and other regulated sectors must accept it by around December 2027.[2] In parallel, ISO/TC 307 and CEN are drafting the standards for decentralized identity, trust anchors and DLT-based evidence that will define how a verified identity is recorded and trusted on a ledger.[7] Identity checks are moving from a vendor feature to certified, audited infrastructure, and firms that plan for both regimes now will avoid re-tendering their onboarding twice.

1. Why Identity Becomes Infrastructure

Until now, identity verification in crypto onboarding has been a procurement choice: each exchange or fintech picked a vendor, set its own thresholds and defended its choice to its supervisor. The rules arriving in 2026–2027 change that. In the UK, reliance on a digital check for AML purposes now depends on the provider holding a certificate from an accredited body. In the EU, a single directly applicable regulation replaces national transpositions, and the EUDI Wallet introduces a state-issued credential that regulated firms will have to accept.

The result is a shift from “which vendor do we trust?” to “which certified service, at which assurance level, producing which evidence?” That is a question that standards, not contracts, will answer.

2. Regulatory Timeline

Five rules decide what identity checks digital-asset firms must buy in the next 15 months.

Rule	What it asks of identity verification
EU AML Regulation (2024/1624)	Applies from 10 July 2027. Crypto-asset service providers are obliged entities. eIDAS-compliant remote identification at an appropriate assurance level counts as equivalent to in-person; existing customers are brought in over up to five years.[1]
AMLA technical standards on CDD	Draft published 9 February 2026; consultation closed 8 May 2026; final text due to the Commission by 10 July 2026. Sets how remote identification and wallet credentials are accepted at onboarding.[1]
eIDAS 2.0 and the EUDI Wallet	Every member state offers a certified wallet by December 2026; banking, financial services and other regulated sectors must accept it around December 2027.[2]
UK DVS trust framework 1.0	Final release 9 June 2026; certification scheme 1.0.1 in force from 2 September 2026. New providers certify only against 1.0; gamma (0.4) certificates remain valid until 1 December 2028.[3][4]
UK MLR Regulation 28 guidance	Since February 2026, digital identity satisfies Regulation 28 only when a certified provider on the DVS register performs it. At the time, 14 of 39 surveyed providers were certified.[5]

Two hard dates: UK certification from 2 Sep 2026, EU AMLR from 10 Jul 2027

Identity-verification milestones for digital-asset firms, EU and UK



Figure 1. Regulatory milestones for identity verification, EU and UK, 2026–2027. Sources: [1]–[5].

3. The UK: Certification as the Entry Ticket

The UK framework is the most concrete of the two regimes because it already has a working certification route. Conformity assessment bodies (CABs) must be approved by DCMS and accredited by UKAS, and they audit services under ISO/IEC 17065; only certificates from accredited CABs count for joining the DVS register.[4] The

framework recognises distinct roles: identity, attribute, orchestration, holder and component services; and under 1.0 a component service provider cannot hold another role at the same time.[3][6]

> **Why it matters**
>
> For document and biometric verification providers, certification is no longer optional for the UK regulated market: an uncertified check "cannot reliably be deemed suitable" for MLR identity verification.[5] With fewer than half of surveyed providers certified, early movers gain a procurement advantage with UK banks and crypto firms.

4. The EU: One Rulebook, One Wallet

The AMLR settles who is regulated and when; the AMLA technical standards will settle how remote identification is performed. The EUDI Wallet then adds a new kind of input: a government-issued credential that a firm verifies rather than a document it inspects. Firms will need to support both paths: document and biometric checks for customers without a wallet, and wallet credentials for those who have one, while producing an audit trail that satisfies the AMLR's ongoing monitoring obligations.[1][2]

> **Why it matters**
>
> Crypto-asset service providers licensed under MiCA will re-tender onboarding in 2026–2027. The winning set-up accepts EUDI credentials, mobile driving licences (ISO/IEC 18013-5) and physical documents through one flow, and keeps evidence that can be shown to a supervisor years later.

5. Standards Pipeline

ISO/TC 307 (Blockchain and distributed ledger technologies) and CEN/CENELEC JTC 19 are developing the standards that connect verified identity to ledgers. The UK national committee BSI DLT/1 publishes its work programme openly; the projects most relevant to identity are listed below.[7]

Project	Scope	Public status
ISO 23042	Reference architecture for DLT-based decentralized identity systems[8]	Drafting
ISO/WD 7603	Decentralized identifiers for legal entities, natural persons and assets on DLT, used with Verifiable Credentials[11]	Deleted (2023)
ISO/TS 26691	Trust anchor requirements for DLT-based decentralized identity systems[9]	Proposal
BS ISO 24876	Privacy protection when trust anchors are used in DLT-based identity management	Drafting

Project	Scope	Public status
PD CEN/TS 18474	Functional and interoperability requirements for Decentralized Identifiers (DID)	Drafting
CEN new work item	Trust anchors for decentralized identity management using trust services on an electronic ledger	Proposal
BS EN 18379	Requirements on processing personal data using blockchain and DLT	Drafting
PD ISO/PAS 26347	Interoperable protocol between digital wallets based on blockchain and DLT	Drafting
ISO 26692	Identification, collection, acquisition and preservation of DLT-based digital evidence[10]	Proposal

Statuses as listed in the public BSI DLT/1 work programme and public ISO project listings on 28 October 2026.[7]–[11] ISO/WD 7603 was deleted at ISO stage 20.98, effective 23 June 2023, and no longer appears on the ISO Projects portal. Third-party project listings can lag ISO's own registry; readers should verify current status directly with ISO or BSI DLT/1. No committee drafts are quoted.

> **Why it matters**
>
> The CEN work item on trust anchors using trust services on an electronic ledger is the clearest sign that the eIDAS trust-services model and blockchain identity standards are converging. Identity providers that align with eIDAS assurance levels today will find the DLT standards built on the same foundations.

6. What This Means for Market Participants

Participant	Priorities for 2026–2027
Identity-verification providers	Certify against UK DVS 1.0 in the right role; support EUDI Wallet and mDL credentials; document assurance levels in terms the AMLA standards use.
Crypto-asset service providers	Plan onboarding for the AMLR start on 10 July 2027; choose certified identity services; keep evidence that survives later supervisory review.
Banks serving crypto clients	Prepare to accept EUDI credentials around December 2027; rely on certified UK checks for MLR Regulation 28; ask crypto clients for portable, standardised evidence files.
Standards contributors	Comment on public drafts as they open, especially decentralized identity and trust anchors, where eIDAS and DLT work now overlap.

7. The Open Question: Substitute or Parallel Check?

None of the five rules in Section 2, and none of the ISO/CEN projects in Section 5, settle a question that will decide whether this pipeline delivers the efficiency gain it is designed to: once a credential has been verified at a given eIDAS assurance level, does that verification *substitute* for a firm's own re-identification of the holder, or does the firm keep running its legacy checks in parallel, “to be safe”?

The AMLR text treats eIDAS remote identification “at an appropriate assurance level” as equivalent to in-person verification, which, read plainly, means equivalent, not merely one more data point alongside a firm's existing biometric or liveness process.[1] If firms treat the EUDI Wallet as an additional input rather than a sufficient one, the market gains none of the cost or friction reduction the Wallet is designed to deliver, and the new regime simply adds a compliance cost on top of the existing one.

> **Why it matters**
>
> A credential verified at eIDAS “high” assurance already carries a cryptographically auditable trail back to a trust anchor (Section 5). Re-running a separate biometric or liveness check at the relying party's end duplicates work the issuing framework has already performed to a stated, regulated standard. The open question for the standards and supervisory community is whether a firm accepting such a credential should be expected to independently re-establish that the person presenting it is its rightful holder, or whether, once the credential itself verifies, that responsibility sits with the wallet issuer and the credential's custody chain, leaving the relying party's residual obligation to risk-based monitoring of the holder's activity rather than renewed identity-binding.
>
> A comparable dynamic is visible elsewhere in AML tooling: the Travel Rule has remained standard practice well past the point where some participants consider parts of it architecturally avoidable, because absent an explicit instruction to retire a control, operational prudence favours keeping it. The standards and supervisory bodies named in Section 5 are where this gets resolved one way or the other, and firms investing in onboarding now should track it as closely as the certification dates in Section 2.

Sources

[1] AU10TIX, “AMLA KYC technical standards: July 2026 deadline,” June 2026. https://www.au10tix.com/blog/amla-kyc-technical-standards-july-2026-deadline/

[2] FinTech Global, “eIDAS 2.0 deadlines loom: two tracks, one trust chain,” 13 July 2026. https://fintech.global/2026/07/13/eidas-2-0-deadlines-loom-two-tracks-one-trust-chain/

[3] GOV.UK, Enabling Digital Identity blog, “Final release of the 1.0 trust framework: what does it mean for you?”, 10 June 2026. https://enablingdigitalidentity.blog.gov.uk/2026/06/10/final-release-of-the-1-0-trust-framework-what-does-it-mean-for-you/

[4] GOV.UK, “Certification scheme for the UK digital verification services trust framework,” updated 21 September 2026. https://www.gov.uk/guidance/certification-scheme-for-the-uk-digital-identity-and-attributes-trust-framework

[5] Biometric Update, “UK guidance on digital ID for AML compliance answers and raises questions,” 27 February 2026. https://www.biometricupdate.com/202602/uk-guidance-on-digital-id-for-aml-compliance-answers-and-raises-questions

[6] Biometric Update, “BSI launches certification scheme for UK DIATF,” 4 September 2025. https://www.biometricupdate.com/202509/bsi-launches-certification-scheme-for-uk-diatf

[7] BSI Standards Development, DLT/1 Blockchain and Distributed Ledger Technology, public committee work programme, accessed 28 October 2026. https://standardsdevelopment.bsigroup.com/committees/50270820

[8] ISO, ISO/WD 23042, Reference architecture for DLT-based decentralized identity systems. https://www.iso.org/standard/87349.html

[9] ISO, ISO/TS 26691, Trust anchors requirements for DLT-based decentralized identity systems. https://www.iso.org/standard/94232.html

[10] ISO, ISO 26692, DLT-based digital evidence. https://www.iso.org/standard/94233.html

[11] ISO project listing, ISO/WD 7603, Decentralized Identity standard for the identification of subjects and objects, stage 20.98, “Project deleted,” effective 2023-06-23. https://isme.me/en/project/show/iso:proj:82842

This Briefing Note is prepared for informational purposes as part of IDAA's ongoing review of digital asset identity, AML and documentation practice. It is based on public sources only and does not represent the views of BSI, ISO or CEN. It does not constitute legal advice. IDAA, International Digital Asset Association, London, UK (Co. 17223770), idaa.uk