LOOQR

Unlocking Digital Trust

Identity Verification & Digital Signing in Insurance

Compliance Playbook for Digital Insurance (2026 Edition)

Compliance Playbook for Digital Insurance

A practical guide to implementing regulator-ready digital onboarding and policy issuance across the EU

Regulatory Context

Digital transformation in insurance is no longer optional, yet regulatory requirements have not become any less stringent.

Supervisory authorities across Europe are increasing scrutiny over digital onboarding processes, particularly in areas such as identity assurance, AML compliance, and auditability.

Insurance companies should not simply implement digital processes; they must also be able to demonstrate, at any time, how compliance has been achieved.

Failure to comply with these provisions may result in:

- Regulatory findings during audits.
- Increased supervisory scrutiny.
- Remediation requirements or sanctions.

In this context, digital onboarding becomes a compliance-critical function, not just a customer experience improvement.

At the European level, several regulatory frameworks shape how digital identity and electronic transactions must be implemented:

- eIDAS Regulation - governing electronic signatures and trust services.
- AML Directives (AMLD5 / AMLD6) - defining customer identification requirements.
- eIDAS 2.0 - introducing the European Digital Identity Wallet.
- National supervisory regulations for insurance providers.

These frameworks increasingly promote secure digital identity mechanisms and legally valid electronic signatures as the foundation for trusted digital transactions.

What Insurers Must Implement

Insurers are required to implement identity verification processes that meet defined levels of assurance, depending on product risk and regulatory expectations.

Customer Identification

Collection of core identity data:

- Full name.
- Date of birth.
- Nationality.
- Identification document.
- Address.

Identity Verification

Insurance companies must ensure that the person interacting digitally is the rightful owner of the claimed identity.

Common mechanisms include:

- Identity document validation.
- Biometric verification.
- Video identification.
- Digital identity wallet authentication.
- Bank-based identity verification.

Modern onboarding platforms provide automated identity verification flows combined with regulatory-compliant identity proofing mechanisms.

AML Controls

Required controls include:

- Sanctions screening.
- Politically Exposed Person (PEP) screening.
- Risk profiling.

These checks must be embedded within the onboarding journey and remain fully auditable.

Risks of Weak Identity Verification

Weak identity verification processes expose insurers to significant operational and regulatory risks.

Identity Fraud

Fraudsters may:

- Purchase policies using stolen identities.
- Use synthetic identities.
- Exploit weak onboarding processes.

Regulatory Exposure

Regulators increasingly focus on the defensibility of onboarding processes.

The key question is no longer “Was identity verification performed?”, but rather “Can the insurer prove, with evidence, that identity verification was performed correctly?”

Operational & Reputational Risk

Consequences include:

- Financial loss.
- Operational disruption.
- Reputational damage.

Strong identity verification significantly reduces these risks.

Digital Onboarding Best Practices

Effective onboarding must balance compliance with user experience.

Mobile-First Design

- Automated document capture.
- Real-time verification.
- Seamless UX.

Multi-Layer Verification

- Document validation.
- Biometric matching.
- Device & behavioural analysis.
- External data verification.

Risk-Based Orchestration

Not all customers require the same level of verification.
Leading insurers adapt onboarding flows based on:

- Product risk.
- Customer profile.
- Jurisdiction.

Automation with Human Oversight

Systems must support:

- Manual review workflows.
- Escalation rules.
- Full audit logging.

Audit Evidence Requirements

Auditability is often the weakest point in digital onboarding implementations.
Many insurers can perform identity verification, but cannot reconstruct the process during an audit.

Supervisory authorities require proof that:

- Identity was verified.
- Correct procedures were followed.
- The signer matches the verified identity.

Typical evidence includes:

- Identity verification reports.
- Document validation logs.
- Biometric records.
- Device/IP data.
- Timestamped audit trails.
- Signature certificates.

Modern infrastructures generate tamper-proof evidence packages that can be securely stored and retrieved.

Digital Signatures and Legal Validity

Electronic signatures enable fully digital contract execution with legal validity.

Simple Electronic Signature (SES)

- Basic acceptance (e.g. click, draw).
- Legally valid but limited evidential strength.

Advanced Electronic Signature (AES)

- Must be uniquely linked to the signer.
- Identify the signer.
- Detect tampering.

Qualified Electronic Signature (QES)

- Uses qualified certificates.
- Issued by qualified trust service providers.
- Equivalent to handwritten signature under EU law.

The choice of signature level should align with:

- Risk exposure.
- Product type.
- Jurisdiction.

Increasingly, higher-assurance signatures are preferred in high-risk scenarios.

Reference Implementation Model

A compliant digital policy issuance architecture typically includes four layers:

1. Identity Verification Layer

- Remote identity verification.
- Document validation.
- Biometric verification.
- Optional agent-assisted flows.

2. Compliance Layer

- AML screening.
- Risk scoring.
- Eligibility checks.

3. Digital Signature Layer

- Signature orchestration.
- Certificate issuance.
- Signature validation.
- Evidence generation.

4. Evidence Vault

Secure storage of:

- Verification logs.
- Certificates.
- Document hashes.
- Timestamps.
- Audit reports.

In practice, insurers rely on specialised digital trust platforms to implement these capabilities in a scalable and compliant way.

For example:

- Identity verification and onboarding can be implemented via modular Platforms such as LOQR|brick.
- Digital signing workflows can be handled through solutions such as LOQR|sign.

These components can integrate into existing policy systems without requiring full infrastructure replacement.

Executes Before Journey Begins

CONTEXT INPUTS

- Product Risk Level
- Jurisdiction
- Distribution Channel
- Customer Indicators
- Contract Value

STAGE-LEVEL COMPLIANCE INSTRUCTIONS

- Identity Assurance Required
- AML Depth & EDD Threshold
- Signature Type (SES|AES| QES)
- Evidence Retention Obligation

1

Initiation & Legal Basis

Customer Onboarding

"Compliance begins at the first digital interaction."

- Lawful basis for data processing established and recorded.
- Product, jurisdiction, and channel captured - Risk Engine configured
- Session identity anchored: device, channel, timestamp.
- Consent scope documented, version-controlled and auditable.

GDPR Art. 6 | IDD Art. 20

Compliance Objective: Establishes the originating legal record that anchors all downstream compliance actions.

E1 - Legal Basis & Session Record

2
Know Your Customer
Identity Verification (KYC)

"Identity must be verified, and the verification must be proven."

- Identity confirmed to the required regulatory assurance level.
- Document authenticity verified, not just reviewed.
- Biometric match recorded with sufficient depth for examination.
- Assurance level formally assigned with documented rationale.

`AMLD5 Art. 13 | eIDAS LoA / eIDAS 2.0`

Compliance Objective: Fulfils Customer Due Diligence obligations. Produces a verification record that withstands regulatory examination.

E2 - Identity Assurance Record

3
Structured Risk Decision
AML Controls & Risk Scoring

"Risk decisions must be documented at the moment they are made."

- PEP and sanctions screening against live, versioned lists.
- Risk score calculated with documented rationale, not a black box.
- Enhanced Due Diligence formally triggered or formally waived.
- Every screening decision recorded as it was taken.

`AMLD5/6 Art. 18–24 | FATF Rec. 10, 12`

Compliance Objective: Implements a documented, risk-based approach. Decisions are traceable, not reconstructed after the fact.

E3 - Risk Decision Log

4
Legally Binding
Digital Policy Signing

"The contract must be enforceable, and the signing act must be provable."

- Signature type matched to risk profile - SES, AES, or QES.
- Signer identity cryptographically bound to the document.
- Signing intent and document review confirmed in the record.
- Qualified timestamp applied, non-repudiable, legally anchored.

`eIDAS Art. 25–32 | QES Legal Equivalence`

Compliance Objective: Satisfies legal validity requirements. Links the verified identity to the legal act under full audit conditions.

E4 - Signed Artifact & Certificate

5
The Regulator's View
Compliance Evidence Vault

"The regulator sees only what you can produce, not what you claim."

- Complete evidence bundle assembled from every prior stage.
- Tamper-evident sealing, any alteration is detectable.
- Retention enforced per jurisdiction - 5 to 10 years
- Structured export. available for supervisory examination on demand.

`AMLD5 Art. 40 | GDPR Art. 5`

Compliance Objective: Transforms continuous evidence into a defensible, regulator-ready record of the entire journey.

E5 - Full Chain of Custody

A regulator must be able to reconstruct what happened, why each decision was made, and who bore responsibility at any point in time. These five evidence nodes form a single, unbroken chain.

E1
Legal Basis
- Consent Record
- Version & Scope
- Session Metadata
- Channel Record
- Jurisdiction & Product Flag

E2
Identity Proof
- KYC Outcome
- Assurance Level
- Biometric Score
- Document Extract
- Verification Timestamp

E3
Risk Rationale
- Screening Results
- List Versions
- Risk Score & Model Rationale
- EDD decision or formal waiver

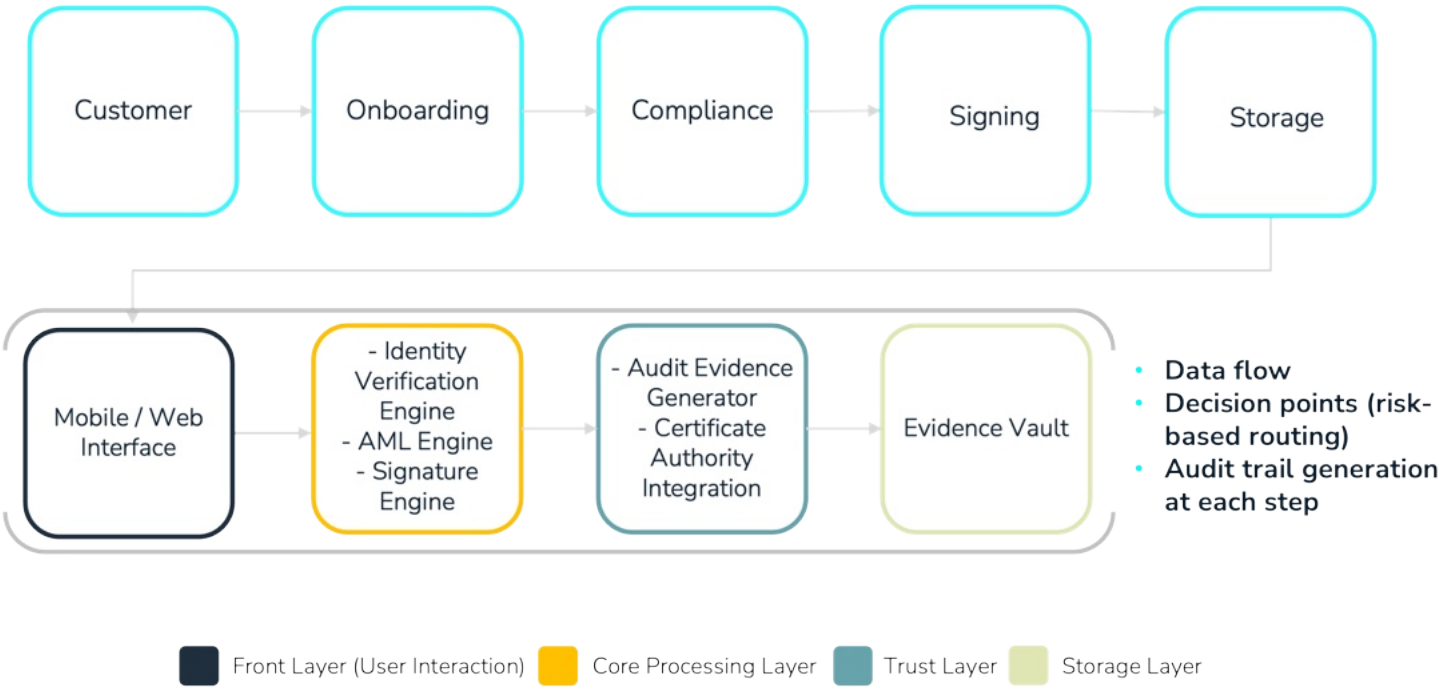
E4
Contract Record
- Signed Document
- Certificate Chain
- Signing Log
- Intent Confirmation
- QTSP-anchored Timestamp

E5
Custody Chain
- Consolidated Bundle (E1–E4)
- Immutable Access Log
- Retention Cert
- Regulatory export on demand

CRYPTOGRAPHICALLY SEALED · END-TO-END AUDIT CHAIN

- QTSP Timestamped
- Cryptographically Sealed
- Decision Rationale Captured
- Chain of Custody Maintained
- Jurisdiction-Compliant Retention
- Structured Regulatory Export

Visual Architecture



Conclusion

Digital policy issuance is becoming a core capability for insurers. Customers expect fully digital experiences, while regulators demand strong guarantees around identity, traceability and legal validity.

Insurers must implement systems capable of delivering:

- Strong identity verification.
- Legally valid digital signatures.
- Comprehensive audit evidence.

Failure to modernise these processes increases both operational inefficiencies and regulatory exposure.

By adopting a structured digital trust architecture, insurers can ensure compliance while improving efficiency and customer experience.

Solutions such as LOQR|brick and LOQR|sign provide modular building blocks that support this transformation.

LOQR

For more information, visit LOQR.COM

Or contact us at SALES@LOQR.COM

Unlocking Digital Trust