



Digital Identity and Biometric Systems

Course: eKYC, Liveness Detection and Identity Proofing



Digital Identity and Biometric Systems Course: eKYC, Liveness Detection and Identity Proofing

Introduction:

Digital identity and biometric systems, covering eKYC, liveness detection and identity proofing, is a 5-day course for digital ID enrolment, customer onboarding and biometric design staff, ending with an Identity Proofing and Biometric System Design Plan. Agencies and banks that enrol people without a defined assurance level, a tuned match threshold or tested liveness checks issue identities that are easy to obtain fraudulently or hard for genuine applicants to complete. Nominees run enrolment or verification processes and learn through case studies on match score data and onboarding journeys. CoreConcept Training Center delivers this digital identity and biometric systems course.

Course Objectives:

- Assign identity assurance levels IAL1, IAL2 or IAL3 to each service and specify the evidence strength and proofing type each level needs
- Design an enrolment process with biometric capture quality checks, failure-to-enrol handling and one-to-many de-duplication
- Set face and fingerprint match thresholds by reading FMR, FNMR and EER results against the fraud and convenience targets of a service
- Specify liveness detection requirements and read ISO/IEC 30107-3 presentation attack detection test reports using APCER and BPCER
- Build an eKYC onboarding journey that joins document validation, authoritative data matching, face comparison and customer due diligence
- Produce an Identity Proofing and Biometric System Design Plan with template protection, consent and data minimisation safeguards for a case organisation

Target Audience:

- Staff responsible for running citizen or resident enrolment centres and digital ID issuance processes
 - Staff responsible for remote customer onboarding and know-your-customer checks in banks and payment firms
 - Staff responsible for configuring and tuning face and fingerprint matching engines
 - Staff responsible for specifying, procuring or testing identity verification and liveness services
 - Staff responsible for privacy and data protection controls over biometric and identity records
-

Course Outline:

Day 1: Digital Identity Landscape and Proofing Baseline

- Digital Identity Life Stages From Enrolment to Credential Use
- Foundational eID Versus Functional Sector Identity Schemes Compared
- Biometric Modalities Face, Fingerprint and Iris Selection Factors
- Verification One-to-One Versus Identification One-to-Many Search
- Current Proofing Baseline Review of Channels and Evidence

Day 2: Identity Assurance Levels and Biometric Accuracy Metrics

- NIST SP 800-63A Resolution, Validation and Verification Steps
- IAL1, IAL2 and IAL3 Requirements Mapped to Services
- Evidence Strength Fair, Strong and Superior Classification Exercise
- FMR, FNMR and Equal Error Rate Interpretation Worksheet
- Failure-to-Enrol Rate and Capture Quality Score Analysis

Day 3: Enrolment, Matching and eKYC Onboarding in Operation

- Enrolment Station Workflow With Attended and Unattended Capture
- One-to-Many De-Duplication Search and Candidate List Adjudication
- Match Threshold Setting Using Score Distribution Charts
- Identity Document Validation Checks and Authoritative Register Matching
- eKYC Journey Mapping With Customer Due Diligence Checkpoints

Day 4: Liveness Testing, Template Privacy and Identity Wallets

- ISO/IEC 30107-3 Test Report Reading With APCER and BPCER
- Active Versus Passive Liveness Check Selection Criteria
- Mask, Replay and Video Injection Countermeasure Requirements
- Cancelable Biometrics and Template Protection Scheme Options
- Digital Identity Wallets With Selective Disclosure and Consent

Day 5: Case Study Work on the Identity Proofing and Biometric System Design Plan

- Case Organisation Brief With Mixed Branch and Remote Onboarding
 - Case Assurance Level Assignment and Evidence Requirements Table
 - Case Threshold and De-Duplication Settings From Sample Score Data
 - Case Liveness Specification and Supplier Test Evidence Checklist
 - Identity Proofing and Biometric System Design Plan Panel Review
-

Skills You Will Gain:

- Identity Assurance Level Mapping
- Biometric Enrolment Design
- Match Threshold Tuning
- De-Duplication Adjudication
- Presentation Attack Test Evaluation
- eKYC Journey Design
- Biometric Template Protection
- Identity Wallet Assessment

Why Attend This Course:

- Deliver an Identity Proofing and Biometric System Design Plan to the digital ID programme board or the onboarding risk committee for approval
- Decide which assurance level, proofing type and biometric threshold each service requires, backed by error rate evidence
- Avoid duplicate identities, high false rejection of genuine applicants and liveness services bought without independent test evidence
- Coach enrolment, onboarding and verification colleagues using the score analysis worksheets and supplier evidence checklist

Conclusion:

Back at work, the participant hands the Identity Proofing and Biometric System Design Plan to the digital ID programme board or the onboarding risk committee. They use it to approve assurance levels per service, the enrolment and de-duplication design, match thresholds and the liveness specification before suppliers are engaged or settings changed. After the first months of live operation, the unit should compare observed false rejections, failure-to-enrol cases, duplicate hits and fraud referrals with the plan, then adjust thresholds, capture guidance and evidence rules.

Frequently Asked Questions FAQ:

What should participants know before a digital identity and biometric systems course?

Participants should already work on enrolment, onboarding, identity verification or security design and understand basic identity documents and customer checks. No programming or statistics background is needed; error rates and score charts are explained through worked case data.

How does a digital identity and biometric systems course differ from an identity and access management course?

This course covers how a person is proven and enrolled in the first place: assurance levels, biometric capture, matching, liveness and eKYC. Identity and access management courses govern accounts, roles and permissions after an identity already exists.

Why do digital identity and biometric systems need tuned match thresholds?

A single threshold trades false matches against false non-matches. Set too low, impostors pass; set too high, genuine applicants are rejected and abandon onboarding. Each service needs a threshold chosen from measured score distributions and its own fraud tolerance.

What do participants take back from the digital identity and biometric systems course?

Each participant takes back an Identity Proofing and Biometric System Design Plan for a case organisation, with assurance level assignments, enrolment and de-duplication design, threshold settings, a liveness specification and template protection safeguards adaptable to their own service.
