consult hyperion
consulting by fime

Fime Academy

Payment Authentication Masterclass.

Explore in-depth payment authentication technology trends and considerations.

This comprehensive masterclass offers an in-depth exploration of the payment authentication landscape, covering key regulations, new technologies, and alternative payments. It presents strategic recommendations for best practices and key considerations for next-generation authentication.

By the end of the course, participants will be able to make better strategic decisions and build secure, compliant authentication solutions.

Objectives

- Understand the market landscape and dynamics.
- Explore key trends and their connections.
- Identify strategic focus areas for future evolution.
- Generate innovative ideas for unique differentiators.

Key topics

- State of payment authentication.
- Regulation landscape and emerging trend.
- Key industrial standards and initiatives.
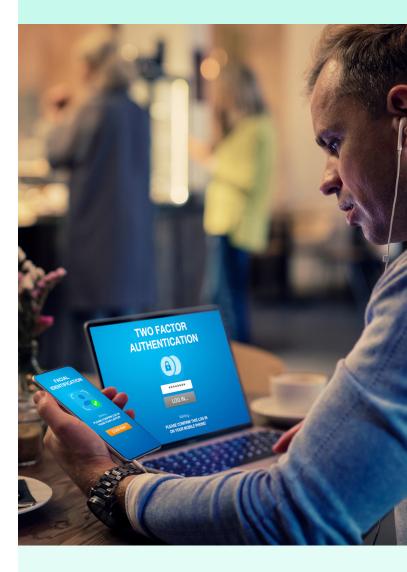- Recommended optimization practices.

Audience

Business leaders, decision makers, product / project managers, and solution developers across the payment ecosystem, specifically those from:

- Payment networks.
- Issuing banks.
- Payment Service Providers (PSPs).
- Digital wallet providers.

Price

For pricing or specific requests, please contact us directly.

Duration	Location	Language
1.5 days (onsite) or 4 online sessions (~2.5 hours each)	Customer premises Online delivery Available worldwide	English Local language options may be available.

Masterclass program

On site 1.5 days.

Day 1

M1. Introduction to authentication.

- Recap of main concepts and payment authentication definition.
- Overview of current market trends and challenges (fraud, cart abandonment, compliance).

M2. Regulatory landscape.

- Positioning of regulatory entities and protection mechanisms.
- Multifactor authentication, dynamic linking, verifier security requirements.
- Authentication factors, device binding, and data privacy.

M3. Authentication technologies.

- Digital identity, FIDO Passkey, behavioral biometrics
- Core principles and key use cases for payment ecosystem
- Emerging standards, compliance considerations, and best practices.

Day 2

M4. Authentication in alternative payments.

- Open banking, instant payments, ISO 20022.
- Central Bank Digital Currency authentication principles.

M5. Emerging threats.

- Sophisticated fraud types: authorized push payment fraud, quantum computing fraud, AI-powered fraud.
- Current countermeasures and prevention strategies.

M6. Consult Hyperion's perspective.

- Sharing Consult Hyperion's expert view on the main concerns for players in the ecosystem.
- Strategic themes: risk control, data privacy vs. user experience, biometrics and forward-looking trends.

Online 4 sessions.

Session 1 | 2.5 hours

1. Introduction to authentication.
1.1. Key trend.
1.2. Challenge.
1.3. Opportunity.

2. Regulatory landscape.
2.1. Authentication trends and regulations.

Session 2 | 2.5 hours

3. Authentication technologies.
3.1. FIDO Passkey.
3.2. Behavioral biometrics.

Session 3 | 2.5 hours

3.3. Digital Identity.
3.4. Synergies.

4. Alternative payments.
4.1. Account to Account (A2A).
4.2. CBDC.

Session 4 | 2.5 hours

5. Emerging threats and recommendations.
5.1. Authorized push payment (APP).
5.2. Quantum computing.
5.3. AI powered fraud.

6. Consult Hyperion's perspective.
6.1 Recommended practices.

Contact

fimeacademy@fime.com

Americas
fimeinsidesalesnalac@fime.com

APAC
fimeinsidesalesap@fime.com

China
fimeinsidesaleschina@fime.com

EMEA
fimeinsidesalesemea@fime.com

India
fimeinsidesalessa@fime.com

Japan
fimeinsidesalesjapan@fime.com

Korea
fimeinsidesaleskorea@fime.com

Making innovation possible.
Making the world work.

Consulting | Test Platforms | Testing Services