The ideal goal of every payment implementation is that it sets the right balance between security and convenience. An essential ingredient in the commerce value orchestration is the ability to authenticate consumers. Therefore, there’s an ongoing race to excel in the ability of authenticating customers, by deploying state-of-art solutions to enable this. This training explores the current demands for advanced authentication and enabling technologies, with special focus on mobile solutions and biometrics. It covers the most recent and upcoming frameworks in authentication, approaches for turning authentication into a product rather than just a checkpoint in the consumer journey and the business side of authentication. By becoming a reliable identification and authentication entity for consumers, payment institutions can leverage its position to become an online identity provider, increasing its relevance towards their customers and expanding their presence in the market beyond a financial service provider.

**WHAT YOU WILL LEARN**

- What is authentication and how it can be applied more efficiently
- Recent trends in authentication for mobile banking and payments
- Impacts of authentication in user experience
- Authentication as a service
- How to assess your authentication mechanisms and improve them

**KEY TOPICS**

- Identification and Validation – authentication for mobile payments
- Mobile, Biometrics and Wearable
- Authentication assurance frameworks
- Apple Pay, Samsung Pay, Android Pay
- Risk and context based authentication

**WHO SHOULD ATTEND?**

- Business analyst IT, system analyst, security analyst
- (Technical) Project manager, Product owners, project and process managers
- Solution architect
- Product Owners
- Security and Governance Officers
- Software engineer, quality assurance engineer
ADVANCED AUTHENTICATION IN BANKING & PAYMENTS

AGENDA

Authentication 101
- Fundamental authentication concepts (e.g. relying parties, identity, attribute, identifier, registration authority, trust frameworks)
- The "traditional" authentication landscape and common technologies
- Responsibilities in an authentication ecosystem

The business case for authentication
- Deriving value from customer ownership
- Is there a case for outsourcing risk (and data)? Is there a case for becoming an identity provider?
- The importance of authentication in value orchestration
- Regional requirements and opportunities e.g., PSD2, XS2A (Access to Account)

Harmonizing security and user experience
- The quest for seamless authentication
- When should I authenticate? And how should I authenticate?
- Strong authentication versus risk based authentication
- Benchmark of solutions available and technologies behind the scenes

Authentication assurance frameworks
- The importance of common frameworks in order to participate in identity & authentication ecosystems.
- The ISO 29115 and NIST 800-63-2 frameworks.
- The different phases: Enrollment, credential management and entity authentication
- The Levels of Assurance (LoA) classification
- Explaining concepts like "MultiFactor Software Cryptographic Tokens" in plain English!

Risk-based authentication
- Deep dive into risk-based and context-based authentication
- Risk profiling and scoring for assessing the needs for step-up authentication.
- Recent developments in the field: Behavioral analytics, device fingerprinting, threat detection, intelligence networks, etc.
Biometrics, Mobile & Wearables
• Focus on mobile as the de-facto authentication channel
• Trends in (active) wearable devices for authentication (e.g. heartbeat biometrics)
• Fundamentals of biometrics: learning from the basics to ensure trust in the solution until security, performance (FAR vs FRR), anti-spoofing and liveness detection. Benchmark of different mobile biometrics authentication methods.

Authentication and ID&V in Mobile Payments
• Relevant concepts of Identification and Verification (ID&V) required by tokenization services and payment schemes.
• Minimum requirements in order to support Apple, Samsung and Android Pay.
• Leveraging mobile banking app as authentication channel for Mobile Pay solutions.
• Lessons learned to improve your product.

Federated Authentication and Federated Identity
• Authentication and Identity as a Service
• The potential for federated login by financial and non-financial parties.
• The power of combining federated login with payment methods (e.g. login with Amazon and pay with Amazon, login with Google and pay with Google)
• Developments on technology and protocols (Open IDConnect, OAuth 2.0, etc)

3D Secure 2.0 and FIDO
• The FIDO mission to change the nature of online authentication.
• Where did 3D Secure (1.0) fail? What is expected to change with 3DS 2.0?
• Focus on mobile implementations of FIDO and 3DSecure 2.0.

Building an Advanced Authentication Strategy
• Combining all the pieces of the puzzle and getting ready for the future of authentication!
• Consolidating the learnings of the training into concrete recommendations for your authentication strategy.
• Revisiting, assessing and reformulating the authentication journey of your customers.

General information
Course duration: 1 day
Language: English
Location: Worldwide

Registration
Sign up on ul-ts.com/training