thalesgroup.com

THALES
Building a future we can all trust

SCA Training - A deep dive into Strong Customer Authentication

Banking & Payment Services

INTRODUCTION COURSES
Course reference: B10361

Strong Customer Authentication (SCA) becomes more and more important and evolves quickly:

- Regulation push (e.g. PSD2 mandating SCA)
- Security push
- New channels, new means of payment

Because our customers need to understand and identify user friendly authentication solutions, meeting the regulatory requirements, Thales propose an in depth dedicated training to help them understand the existing standards, the regulation and the impacts on usability, deployment or costs.

Objectives

During this session, you will get trained on:

- Authentication what for and how
- The main current techniques and their implementations How they integrate into the eco-systems
- How they integrate into the eco-systems

Key topics

- What is Strong Customer Authentication, what is it for
- Main standards
- Methods and use cases
- Biometrics in Authentication
- Risk Based authentication
- Authentication in the scope of PSD2
- Card schemes initiatives and rules
- The authentication delegated model
- Authorisation frameworks - ID Federation
- Identity proofing/KYC - The step before authentication

Who should attend

- Banks and other Financial Institution, Fintechs, payment organizations, local schemes, Retailers, Processors / Service Providers
- Managers or operationals: Marketing, Fraud prevention, Security, IT, Compliance

Deliverables

- Complete training manual

Pre-requisites

- This training does not require any specific technical skill
- This course is held in English. On customer request a session in French can be organized.

Duration:

- 2 days

Location:

- On-site at customer premises, or at one of the Thales training centers. Please contact us for more details.

Course fee:

- 1.400€ / attendee, minimum 4 attendees, Price does not include taxes nor travel expenses.

Course schedule

When performed at customer premises, the agenda is tailored to customer attendance profile. The standard agenda is provided below:

DAY 1: Basics, Standards, Techniques

Introduction

- What is Authentication for?
- Common threats in authentication
- What is Strong Customer Authentication
- Basics of cryptography and its use in authentication

Main standards

- The EMV standards
- The FIDO authentication standards
- OATH
- eIDAS

Methods and use cases

- Manual methods and non-manual methods
- Storing and transmitting the authentication elements
- Knowledge and inherence: server vs. client
- Some use cases examples

Biometrics in Authentication

- What it is, methods (morphological, Behavioral…)
- FRR/FAR
- Biometrics and data protection
- Biometric certification
- Who uses biometrics today?

DAY 2: Implementing SCA

Risk Based authentication

- Different approaches in Risk Management
- Risk management and authentication

Authentication in the scope of PSD2

- PSD2 and RTS basics
- The RTS requirements and exemptions
- Other regulations (AML, IFR, GDPR)
- SCA regulations outside of Europe

The authentication models

- Authentication models/journeys
- Redirect vs Decoupled vs Embedded vs Delegated authentication

Card schemes initiatives and rules

- The 3D-Secure authentication standard
- 3D-Secure mandates
- 3DS vs. DSRP

Authorisation frameworks - ID Federation

- Generic
- The role of IDP
- SAML, Oauth 2, Open ID Connect
- Non-government ID Federation implementations examples

Identity proofing/KYC - The step before authentication

For further information about registration, course schedule: please contact us via email to: bps_training@thalesgroup.com or visit our web site: https://www.thalesgroup.com/en/markets/digital-identity-and-security/banking-payment/consulting