

Set up your Non-face-to-face Strong Authentication Project



Online Banking is strategic for banks, reducing drastically transaction costs in comparison to branches or ATM. With more than 230 million of users in 2006, online Banking meets a tremendous success among both the consumer and corporate market. However, banks and their customers are faced with an increasing online fraud (viruses, phishing, etc.) encouraged by the minimal security of static password for user authentication. For preventing this fraud, International Payment Schemes have a solution using an EMV card.

During this three-day workshop we will assist you in the definition of your business requirements to improve your current authentication procedure

Objectives

At the end of the training, you will:

- > Have an overview of the One Time Password implementation based on EMV card defined by MasterCard and Visa
- > Be able to make the most suitable choices for your implementation strategy related to your Strong Authentication Project
- > Evaluate the impact of support of the EMV OTP authentication method on your current IT infrastructure
- > Get concrete recommendations for your project and identify risks

Key topics

- > MasterCard Chip Authentication Program (CAP) specification
- > Visa Dynamic Passcode Authentication (DPA) implementation
- > Impacts and scenarios of migration

Who should attend

People involved in the smart card activity, online banking activity and financial transaction security:

- > Marketing managers
- > Technical project managers
- > Banking Project managers
- > Product managers
- > Security manager

Each session consists of

- > A complete course manual

Pre-requisites

- > Basic knowledge about smart cards.
- > This course is held in English. On customer request a session in French can be organized.

Duration: 3 days

Location: Customer premises

Course fee: € 5895¹

¹ Price does not include taxes nor travel & expenses for the consultant on-site.

Course schedule

Day 1 – Training for knowledge transfer

Business needs of security improvement for non-face-to-face transactions

General overview of EMV-based Authentication Method solution defined by International Payment Schemes

- Review of the options supported by EMV-based Authentication Method solution defined by International Payment Schemes
- EMV-based Authentication Method usage for improving security of E-Banking
- EMV-based Authentication Method usage for improving security of E-Commerce

Detailed analysis of the EMV-based Authentication Method algorithm

- Analysis of the algorithm defined in the MasterCard CAP specifications (reference document to the Visa DPA implementation)
- Review of the CAP/DPA parameters (IAF and IPB) involved in this algorithm

Impact analysis on Bank IT Infrastructure

- Analysis of the impacts on Card Issuance System
- Analysis of the impacts on Bank Authentication System for E-banking and E-Commerce

Conclusion

Day 2/3: Assistance in the definition of Bank Business Requirements

Introduction - Self-presentation by the participants (Bank)

- > Banking context: EMV migration status (Bank/country)
- > Payment System membership

Analysis of the Bank Environment and assistance in the definition of Bank Business Requirements

- > Online Banking Services
 - Presentation of the Online Banking Services provided
 - Current solutions used for Cardholder Authentication
 - Other types of business needs
- > E-Commerce transactions
 - Analysis if need of solution for improving security of e-Commerce transactions
- > Branch banking transactions
 - Analysis if need of solution for authenticating banking transaction parameters and authenticating the approval of the customer

At the end of the workshop, the Gemalto Consultant will provide the Bank with a report summarizing the information and decisions taken during the workshop related to the definition of the business requirement.

Note: In complement to this workshop the Gemalto Consultant may provide some addition consulting services for :

- > Migration Plan Definition
- > System Specifications Definition
 - Card Personalization Specifications
 - Definition of the CAP/DPA parameters
 - Validation using test cards
 - Delivery: CAP/DPA Personalization Specifications document
 - Online Banking System Upgrade Specifications
 - Specification of the Interface with Bank IT Infrastructure
 - Definition of the functions to support in the Home Banking System
 - Delivery: Online Banking System Upgrade Specifications document
 - Setup a demonstration for Proof of Concept

Related courses

EMV Business
Impacts
(B1001I)

Mastering EMV
Implementation
(B1002I)

EMV Migration
for Issuers
(B1003S)

Set up your Non-face-to-face
Strong Authentication Project
(B1023W)

For further information about registration, course schedule:
please contact us via email to: banking.training@gemalto.com
or visit our web site: <http://www.gemalto.com/>