STID ACADEMY

MIGRATION TO HIGH-SECURITY SYSTEMS

Course ID	**STID-ACD-SEC-09**
Duration	**2 days**
Format	**ILT / OST**
Certified Training	**Oui**
Languages	**FR / EN**

MASTER SECURE MIGRATION TO DESFIRE AND SSCPV2

Security threats continue to evolve, making it essential for organizations to migrate from legacy access control systems to advanced high-security infrastructures. The DESFire/SSCPv2 combination provides enhanced cryptographic protection, secure key management, and future-proof authentication mechanisms.
This advanced training is designed for integrators, administrators, and security managers seeking to seamlessly transition from outdated technologies to modern, secure architectures while minimizing downtime and operational risks.
Through a combination of theory, hands-on labs, and expert-led discussions, participants will acquire the skills to plan, execute, and optimize a high-security migration strategy tailored to their organizational needs.

PREREQUISITES

- A strong understanding of access control systems and cryptographic principles.
- Hands-on experience with RFID technologies, including DESFire, MIFARE®, or SSCP protocols.

AUDIENCE

This training is intended for security and access control professionals, including:

- Installers & Integrators
- Administrators & Security Managers
- System Architects & Technical Consultants involved in designing high-security infrastructures.
- Project Leaders & Risk Analysts managing security upgrades and regulatory requirements.

LEARNING OBJECTIVES

Master the fundamentals of DESFire and SSCPv2 technologies and their advantages over legacy systems.

Develop a secure migration roadmap, ensuring compliance with security best practices and minimizing system disruptions.

Manage cryptographic key generation and transfer, including encryption techniques (AES, 3-DES, HMAC) and key diversification.

Implement best practices for secure credential issuance and lifecycle management.

Configure and optimize SSCPv2 for end-to-end secure communications in access control environments.

Identify and mitigate potential risks associated with migrating critical security infrastructures.

MIGRATION TO HIGH-SECURITY SYSTEMS

DETAILED COURSE OUTLINE

INTRODUCTION TO SECURE MIGRATIONS

- Understanding the challenges involved in upgrading to high-security systems
- Comparison between existing systems and DESFire / SSCPv2 technologies
- Identifying challenges and risks in a migration project
- Overview of compliance requirements and industry regulations

MODULE 1: FUNDAMENTALS OF DESFIRE AND SSCPV2 SECURITY

- DESFire EV2 & EV3: Encryption models, authentication methods, and file structures.
- SSCPv2 architecture: End-to-end secure communication between cards, readers, and controllers.
- Advantages of SSCP over proprietary protocols (secure key management, encryption, mutual authentication).
- Understanding Secure Messaging & Secure Channel Protocols.

MODULE 2: CRYPTOGRAPHIC KEY MANAGEMENT & SECURE CREDENTIAL ISSUANCE

- Key diversification, encryption algorithms (AES-128, 3DES, HMAC-SHA1, CMAC).
- Secure key storage and best practices for cryptographic key rotation.
- Managing secure credential issuance in a migration scenario.
- Secure deployment of Virtual Credentials & Mobile IDs in high-security ecosystems.

MODULE 3: MIGRATION PLANNING AND DEPLOYMENT STRATEGY

- Step-by-step methodology for migrating from legacy systems to DESFire/SSCPv2.
- Defining a migration strategy: phased vs. full transition.
- Ensuring interoperability: Managing multi-technology environments.
- Case studies: Successful migrations from Wiegand, Prox, and MIFARE Classic to DESFire & SSCP.

MODULE 4: HANDS-ON LAB: SECURE SYSTEM MIGRATION

- Creating and testing secure DESFire card configurations.
- Implementing SSCPv2 authentication protocols in a real-world scenario.
- Encrypting and transferring credentials securely.
- Testing secure transactions, debugging issues, and optimizing security settings.

MODULE 5: RISK MITIGATION AND PERFORMANCE OPTIMIZATION

- Identifying and addressing potential security risks during migration.
- Ensuring minimal downtime and business continuity.
- Advanced troubleshooting & debugging secure communication failures.
- Optimizing performance in high-security infrastructures.

MODULE 6: CASE STUDIES, Q&A, AND FINAL ASSESSMENT

- Review of real-world migration projects and best practices.
- Q&A session with STid security experts.
- Final knowledge assessment and certification process.

CERTIFICATION

Certificate of Completion awarded upon successful completion.

LEARNING FORMAT

ILT (Instructor-Led Training):
Experience hands-on training at STid's headquarters, led by experts in a fully equipped environment. Benefit from live demonstrations, interactive exercises, and direct engagement with STid specialists for an optimal learning experience.

OST (On-Site Client Training):
Tailored training delivered at your site, adapted to your infrastructure, security needs, and equipment for a fully personalized learning experience.

SCHEDULE AND REGISTRATION

To check the schedule, pricing, or register for the course:

customer.training@stid.com

Learn more at:
www.stid.com

SMARTER SECURITY ANSWERS

Training Activity Number: 93 13 13328 13
STID-ACD-SEC-09 – March 2025