



ITSO

Customer Media Alternatives Conference
MIFARE Classic Customer Media Phase Out





Introduction:

- Message from the Chair: Neil Scales
- Morning Schedule:
 - Next: MIFARE Classic Customer Media Phase Out:
Introduction
Background to Phase Out
Security Aspects Summary
What Next? (Including Timescales)
 - 11:20 Introduction to Customer Media Alternatives:
 - CMD2 – Generic Micro-processor
 - CMD7 – MIFARE DESFire
 - CMD8 – Calypso
 - ‘Play your cards right’ – MVA Consultancy
 - Update from LASSeO
 - Questions & Answers, Panel Discussion

Introduction

- Afternoon Schedule
 - 12:45 Lunch + Exhibit commencement
 - 14:15 SmartCard Networking Forum
 - 15:00 Questions & Answers, Round-up
 - 15:30 Close



Background:

- There are currently approximately 10.8 million smart cards in circulation across the ITSO Environment
- MIFARE Classic Customer Media refers to MIFARE 1k & 4k media (known in the ITSO specification at CMD 1 & 3 respectively)
- MIFARE Classic Media constitutes the majority of all media in the ITSO Environment



Background:

- 11 January 2008: ITSO press release acknowledges alleged hacking into MIFARE Classic security system. ITSO security 'sits over and above' Classic media security.
- 12 March 2008: Researchers at the University of Nijmegen circulate press release and film highlighting a 'serious security flaw' in MIFARE Classic media.
- 4 November 2008: ITSO circulates press release stating intention to phase out Classic media by end of 2016, with no new media allowed after end of 2009.



Background:

- Statement welcomed by some of the membership:

TCA's who have responded have not appeared overly concerned....

It is quite reasonable for ITSO to respond to the changing security status of the Mifare customer media, by identifying a course of action leading to its ultimate withdrawal....

- Moving forward:

Today's information is provided by industry leading experts





What Next?

- The deadline for issuing either CMD1 or CMD4 is 31st December 2009. After this date, all customer media issued in the ITSO environment must be of an alternative CMD type.
- Neither CMD1 or CMD3 will be supported in the ITSO environment after 31st December 2016. This date has been selected to ensure all current Classic media is fully supported until its given expiry date.
- ITSO have set a parallel phase out timetable for CMD2 that fails to meet benchmark transaction limit of 600ms.





ITSO Security and Compliance

John Verity





The ITSO IFM Environment

The environment consists of;

- The Specification
- The Security Domain
- A method for showing compliance
- A Set of 'Business Rules' and a Registrar





The ITSO Security Domain

ITSO Security Domain is made up of:

- The ITSO Secure Application Module
- The ITSO Security Management System
- The ITSO Certification Service
- The ITSO Trust Model

The ITSO SAM (ISAM)

ITSO has an tamper resistant **ITSO Secure Application Module (ISAM)**, which resides in all ITSO-compliant point-of-service equipment and back offices.



ISAM



ITSO Security Management System

- Registers all Players, Shells, Products and Hot Lists
- Generates and holds Public and Secret Key pairs
- Distributes keys to AMS for onward distribution
- Provides a secure VPN to support Messages and Hot List distribution



The ITSO Trust Model

- Works alongside the Physical and Business Models
- And the ITSO Risk Matrix
- Verifies that ITSO uses current Best Practice in Security
- Identifies the Risks that ITSO does not address
 - Who is responsible for managing them
 - What Operators should do in mitigation
- Encourages Operators to prepare and abide by Codes of Practice



Risk Model v Trust Model

Risk:

Identify → Close → Control → Allow

Trust:

Recognise → Own → Accept → Mitigate



The Customer Media Trust

- Speed a limiting consideration
- Authentication more important than security for lower value products
- ITSO keys reside in Tamper-resistant POSTs, not Media
- Secure Messaging used where possible



Steps to Media Authentication

- Challenge
- Response
- Authenticate
- Share Private Security Key
- Diversify the key
- Message Authentication (MAC)





Symmetric Key Processes

Risk: 2 or more nodes could have generated and used keys

Mitigation: Each event notarised

Trust: All events are recorded and available for audit





ITSO Compliance Regime

- Identify and prioritise risk
- Communicate risk to all stakeholders
- Develop mitigating actions
- Build a Control Framework
- Confirm that valid Controls are in place



Responsibilities of ITSO Licensed Operator

- The Licensed Operator (and their AMS) should:
- Perform procedures to identify inappropriate or abnormal transactions or usage patterns
- Distinguish potential fraud from error
- Maintain professional scepticism
- Determine materiality and risk of fraud
- Report and Act





Potential Media Risks

- Relay Attack
- Replay Attack
- Replication (cloning)



ITSO Security and Compliance

John Verity

