ATM Best Practices and great industry reference material available for all ATMIA Members!

ATMIA, the global non-profit trade association with over 5,000 members in more than 65 countries, has published these internationally benchmarked best practice manuals and industry reference material:

- Preventing ATM Malware, Black Box and Cyber-Attacks
- Branch Transformation Best Practices
- Recommendations on ATM User Interface
- ATM Replenishment in Europe Best Practices
- Risks of Maintaining Windows XP Platform for ATMs
- Cardless ATM Transactions Best Practices
- ATM Software Security Best Practices
- ATM Business Efficiency Best Practices
- ATM Cash Security Best Practices
- ATM Contactless Acceptance Best Practices
- ATM Integrated & Customer Experience Best Practices
- ATM Lifecycle Security Best Practices
- ATM Physical Key Management Best Practices
- ATM Physical Security Version 2 Best Practices
- Anti Skimming Best Practices
- CiT Best Practices - USA
- Corporate Governance Best Practices
- Dealing with Stained Banknotes Best Practices
- Decommissioning ATMs
- Developing & Deploying the ATM in a Multi-Channel Retail Banking Delivery System Best Practices
- End-to-End Encryption for ATMs
- Managing Anti Money Laundering at ATMs
- Mobile Device Banking Security
- Point of Sale Lifecycle Security
- Point of Sale Training Manual
- Preventing ATM Gas Explosive Attacks Best Practices
- Solutions for Preventing ATM Explosive Attacks
- Preventing Card Trapping Best Practices
- Preventing Cash Trapping Best Practices
- Preventing Insider Fraud Best Practices
- Protecting Personal Bank Accounts Best Practices
- Preventing Ram Raids Best Practices
- Skimming Prevention - Best Practices for Merchants
- Stored Value Products Best Practices

Brazilian Portuguese Translated Best Practices

Preventing ATM Gas Explosive Attacks Best Practices - Prevenção de Ataques a ATMs

Chinese Translated Best Practices

- Best Practises for ATM Physical Security Version 2 ATM 物理安全最佳实践方案（第二版）
- Best Practises for Anti Card Trapping 防止盗卡的最佳措施
- Best Practises for Anti-skimming 防止盗读的最佳措施
- Best Practices for End-to-End Encryption for ATMS ATMs端到端加密
- Best Practises for Multi-Channel Retail Banking Delivery System 在多渠道零售银行体系开发与布放ATM的最佳实践

French Translated Best Practices

- ATM Replenishment in Europe Best Practices - Meilleures Pratiques en Matiere de Chargement des gab en Europe
- Preventing ATM Gas Explosive Attacks Best Practices - Meilleures pratiques pour empêcher les attaques au gaz et à l'explosif des DAB

German Translated Best Practices

Preventing ATM Gas Explosive Attacks Best Practices - Praxisleitfaden zur Verhütung von Anschlägen mit Gas und Sprengstoff auf Geldautomaten

Portuguese Translated Best Practices

Preventing ATM Gas Explosive Attacks Best Practices - Prevenção de Ataques a ATMs

Spanish Translated Best Practices

- Preventing ATM Malware, Black Box and CyberAttacks - Mejores prácticas para prevenir ataques con malware, ataques de caja negra y ataques cibernéticos en cajeros automáticos
- Best Practices for ATM Integrated Payments Customer Experience - Sistema de Pagos Integrados en el ATM y Experiencia del Cliente
- Preventing ATM Gas Explosive Attacks Best Practices - Mejores prácticas para la prevención de ataques contra cajeros automáticos con gas y explosivos

Global Sponsors:

U.S. Regional Sponsors:

Asia Pacific Regional Sponsor and Latin America Regional Sponsor:

European Regional Sponsors:

Asia Regional Sponsors:

Canada Regional Sponsors:

www.atmia.com

ATM Contactless Payment Acceptance Best Practices

Overview
The term "contactless communications" describes a form of communication where data from one device passes to another device across a contactless interface, such as radio frequency (RF) transmission. In payments, contactless communication most often occurs when a customer positions his/her payment card within close proximity of a contactless reader integrated into the payment solution. This action is known colloquially as "tapping" or "waving" the card.

Contactless payments generally use passive contactless cards issued by a customer's financial institution or virtual cards stored within an NFC capable device, such as a mobile phone. These best practices show how to prevent attacks on contactless technology at ATMs.

Preventing Mobile Banking Fraud Best Practices

Overview
Due to the increasing popularity of mobile phones, and in particular smartphones and tablet computers which are capable of full internet access, mobile banking and related mobile commerce has become an important channel for the financial services industry, including the ATM industry. In a time when the ATM can be used to complete transactions begun on a mobile phone, and as cardless ATM transactions gradually replace ones initiated by plastic cards, this manual highlights security vulnerabilities associated with mobile phone banking applications and makes practical recommendations to reduce risks of future compromise.

Best Practices for ATM Integrated Payments and Customer Experience

Overview
This new guide provides principles and recommendations for evolving the ATM into a secure payments hub linked to established and emerging devices for accessing payments.

After surveying the range of payment methods available today, including cash, the new guide defines and discusses the main processes and transactions-for-value handled by an ATM, including withdrawals and deposits (of notes, coins and checks), inter-account transfers, media dispensing, promotional offers, and even purchases through an ATM. Each transaction type is analysed, accompanied by recommendations for optimizing these transactions.

Then the manual focuses on ways to make the customer's experience of each transaction type as secure, convenient and fast as possible, including for physically challenged cardholders. The critical success factors for increasing the migration to ATMs as the terminal evolves into a payments hub are outlined. Security and risk factors are then addressed in detail. Finally, an Appendix sums up all the terminology currently in use in the industry to describe this new payments environment.

End-to-End Encryption for ATMs

Overview
This document discusses the end-to-end encryption of communications between an ATM and its host.

An ATM encrypts a cardholder's PIN before sending it to a remote host for verification, but all other data sent to and from an ATM is generally unencrypted. The transmission of unprotected data may contravene industry standards and fail to meet society's expectations of privacy from ATMs and financial institutions.

As ATM traffic increasingly shifts from closed networks to the Internet, the scourge of cyber crime targeting cardholders, and individuals battling to keep their personal information private in an era of surveillance, the importance of encrypting ATM communications simply cannot be overstated.

A primary objective of this encryption is to prevent the disclosure of cardholder credentials, such as account numbers and card expiration dates, thereby complying with regulations and defending against fraudulent transactions. Broader objectives may be to thwart other classes of attack, such as identity theft, personal blackmail, and industrial espionage. Or viewed even more broadly, the encryption of ATM communications may help to uphold the basic human right to privacy.

Managing Anti Money Laundering at ATMs

Overview
Owing, in part, to the successful implementation of anti-money laundering strategies throughout international financial systems, money launderers must seek new methods to achieve their objective.

This manual sets out the typical process followed by money launderers and highlights potential vulnerabilities in ATM systems to this kind of fraud.

The ATMIA believes this document will assist its members in proactively adopting international security guidelines and anti-money laundering best practices at the ATM level to further strengthen our systems.