

EMV

White Paper

Introduction

EMV is the key ATM and card payment issue facing banks today. As the deadline for migration to EMV draws closer, it is an issue that will require increasing attention and resources from both banks and the ATM specialists with whom they work.

EMV is a common specification published by EMVCo on behalf of Europay (now MasterCard Europe), Mastercard and VISA . Focused on payment applications (debit and credit cards), the EMV standard is based on smart card technology and provides a new dimension in card security.

EMV aims to:

- Set a worldwide, recognised and accepted standard for chip cards
- Ensure interoperability throughout all countries and all ATM Networks
- Reduce fraud from lost, stolen or counterfeited cards
- Reduce telecom & processing costs
- Add enhanced and new functionality that cannot be provided through existing magnetic stripe cards

EMV is already the recognised, worldwide standard for the implementation of ATM and POS networks based on chip card technologies.

Specification

EMV constitutes a base specification that defines all the technical characteristics for chip cards, ATM, POS and related software (SW) applications and represents the minimum needed to achieve cross border interoperability.

It is important to appreciate that EMV is not a specification for software but is, rather, a set of base principals by which applications can be developed and deployed. On its own, EMV is not sufficient to implement an ICC (Integrated Circuit Card) based credit or debit payment system. To implement such a system, it is necessary for banks, relevant national bodies or card schemes to add a further layer of specification on top of EMV.

Many of these further layers of specification already exist; such as UKIS in the UK, IMV in Canada, Telekurs in Switzerland, SIA in Italy and GIE- CB in France, which covers domestic transactions. The VISA card scheme has also issued the VSDC (Visa Smart Debit and Visa Smart Credit) specification and MasterCard the M/Chip application specifications, which cover international transactions.

These various application specifications – developed at local, regional and international level – are designed to operate in harmony.

In essence, EMV provides the basic ground rules onto which each card scheme, national or international network as

CONTENTS

Introduction	1
Specification	1
ICC Authentication	2
Cardholder Verification Methods	2
PIN Transport Inside the ATM	2
EMV Impacts on HW architecture	3
Impact on SW architecture	3
EMV Level 1 and Level 2 Certifications	3
EMV Level 1 Certification	3
EMV Level 2 Certification	3
Compliance with EMV Specification	3
Compliance with Card Scheme Specification	4
Integration into ATM Network	4
Diebold Hardware and the EMV migration	4
Card Readers:	4
Encrypted PIN Pad:	4
Diebold Software and the EMV migration	4
Glossary	5
EMV FAQ	5
EMV Getting Started	5
EMV Certifications	6
Cardholder's Verification Methods	8
Encryption	8
EMV Kernel	10
ICC Cards	10
Electronic Purse	11
Miscellaneous	11

well as individual banks can add their own applications, reflecting their specific priorities and customer requirements.

EMV started in 1996 with EMV 3.1.1, issued in May 98, while the current EMV base specification is based on EMV2000 V4.0, issued in Dec 2000. EMV 3.1.1 will remain valid for certification testing and approval until March 1st –2004. EMV 4.0 began to be used for certification testing and approval in January 2002.

The EMV specification addresses the following issues:

- Application Independent ICC to terminal Interface Requirements –
- Security & Key Management –
- Application Specification –
- Cardholder, Attendant, and Acquirer Interface Requirements –
- Cardholder Verification –
- ICC Authentication.

ICC Authentication

EMV anticipated the requirement to guarantee that the ICC card is not counterfeited and that the data is not deteriorated or falsified. These methods are based on RSA (Rivest, Shamir and Adleman - the inventors of the RSA cryptosystem) public key technology.

- The first method in place is the Static Data Authentication (SDA) working with EMV cards without RSA capabilities.
- The second method is Dynamic Data Authentication (DDA), which takes advantage of the RSA capabilities of EMV cards. In this authentication method, public and private keys are held and managed by the ICC chip itself.

Cardholder Verification Methods

There are three alternative cardholder verification methods specified by EMV:

1. On line PIN check with the PIN transmitted to the host and enciphered according to the payment system rules for verification at the host level. On Line PIN Check is used most for EMV solutions where there is a minimum requirement for hardware (HW) changes. PIN transports to host encryption algorithms in use today are either single Data Encryption Standard

(DES) or triple DES. It is important to stress that in parallel with EMV migration, major card schemes (VISA and MasterCard) are asking their member banks to adopt triple DES as the only encryption algorithm for on line PIN transport (1). Even if migration to triple DES occurs simultaneously to EMV migration, the two verification methods remain independent to each other.

2. Off line PIN check – in off line verification, the chip card emulates the security functions of the host. The PIN is passed to ICC in plaintext: the PIN check is made by the chip inside the Card, which receives the confirmed PIN in plain-text format via the terminal.
3. Off line PIN check – the PIN is RSA enciphered and passed to ICC: the PIN check is made by the chip in the card, which receives the confirmed PIN in RSA enciphered format(2) via the terminal.

It is up to the network as to which type of verification method they wish to implement. The decision is strongly influenced by the technology incorporated into the chip card being used.

Notes:

- (1) Cards Schemes are asking that Triple DES PIN encryption be made directly at the PIN Entry Point.
- (2) EMV specification allows RSA PIN encryption either in the EPP (Encrypted PIN Pad) or in the terminal Security Module, in case this is not integrated in the PIN Pad.

PIN Transport Inside the ATM

In the ATMs, the EPP (Encrypted Pin Pad) and the ICC card reader are not integrated in the same module: therefore, the PIN transport must follow the security rules to ensure that the PIN cannot be captured during transport between the two modules.

EMV specifies different ways of PIN transport within the ATM, depending on the cardholder verification methods used by the application software:

1. For on line PIN check, the PIN entry device (the EPP) must encipher the PIN. Either single DES or triple DES can be used, depending on the request of the

local ATM network authority. Migration to triple DES, if this has not yet occurred, must be planned for to ensure full compliance with the requirements of the card schemes. The triple DES mandate also specifies that the PIN is triple DES encrypted directly at the PIN entry point.

2. For off line PIN check – The PIN is passed to ICC in Plaintext, having been encrypted by the EPP at the PIN entry point and the ICC card reader must provide deciphering capabilities (DES onboard) to send the PIN in plain text to the ICC for verification.
3. For off line PIN check – the PIN is passed, RSA enciphered, to the ICC. EMV specifies that the PIN enciphering process will take place either in the EPP at the PIN entry point or in the terminal security module. In cases where the RSA encryption is handled by the terminal security module, the EPP will transmit the PIN, DES enciphered, to the terminal security module.

EMV Impacts on HW architecture

In order to support the new features introduced by EMV, as off-line PIN check methods, and authentication features, the ATM architecture must be able to transmit the enciphered PIN from the PIN pad to the card chip or the security module. In that way, some modules of the ATM are effected, such as:

- PIN Entry Device = EPP:
 - to support DES and Triple DES
 - to support RSA when no security module is present
 - to be tamper evident, and tamper resistant: any attempted break-in is revealed.
- ICC Reader:
 - to be EMV Lev 1 Compliant and Certified
 - to accept EMV cards (electrical compliance and contact position)
 - to be able to DES decipher the PIN for off-line check (DES onboard)
 - to be tamper evident
 - to manage the two communication protocols between the Reader and the

chip (called ICC transmission protocols T=0 and T=1)

- Security Module (if existing, not constituted by the EPP) to provide TDES and RSA capabilities

Impact on SW architecture

New application software must include EMV basic functionality to be EMV compliant and EMV Lev 2 Certified. It additionally needs to meet both the specific requirements for each country, as described in the local implementation specifications issued by each authority and meet the requirements of each card scheme.

EMV Level 1 and Level 2 Certifications

EMV foresees two steps of certification, usually called Level 1 and Level 2.

EMV Level 1 Certification

- This level ensures that the ATM can communicate with the ICC accurately and without damaging the ICC.
- Level 1 concerns the ICC reader only and is provided by ICC reader suppliers.
- Independent laboratories undertake certification: EMVco releases a Compliance Statement on the base of test report from the certification laboratory.

EMV Level 2 Certification

Level 2 Certification assures that the ATM terminal and the related SW applications are:

- Compliant with EMV specification
- Compliant with card scheme specification
- Correctly integrates into the ATM network

Compliance with EMV Specification

Compliance to EMV specification allows EMVco to issue the "EMVco Letter of Approval – Terminal Level 2".

Independent certification laboratories can certify the SW Application and will release related test reports. Upon receipt of positive test reports, EMVco releases the "EMVco Letter of Approval–Terminal Level 2", which is also posted on the EMVco web site.

VISA currently demands only the achievement of "EMVCo Letter of Approval – Terminal Level 2".

Compliance with Card Scheme Specification

In addition to compliance with EMV specification (in the form of the "EMVCo Letter of Approval – Terminal Level 2"), MasterCard also requires compliance with "MasterCard terminal Requirements". Compliance enables MasterCard to issue an "Approval of Supplier – ICC Terminal Level 2" statement.

Integration into ATM Network

MasterCard also requests that acquirers perform "end to end" certification to ensure the correct integration of the ATM terminal into ATM network.

Diebold Hardware and the EMV migration

Card Readers:

All the chip card readers provided by Diebold are EMV Lev 1 compliant and certified.

Diebold EMV Lev 1 card readers have been available since the introduction of the EMV. The majority of Diebold's installed base is already equipped with a Lev 1 card readers.

The oldest terminals have already been upgraded with EMV Lev 1 card readers.

Encrypted PIN Pad:

Diebold EPP4.0 supports all the principles (DES, Triple DES, RSA) demanded by the EMV specification. The EPP4.0 is a real TRSM (Tamper Resistant Security Module), certified by T-System (an independent certification laboratory in Germany) and matches and exceeds all the requirements of EMV in terms of tamper resistance and tamper evidence.

EPP4.0 is provided in all new Diebold terminals; older Diebold terminals not equipped with EPP4.0 can be easily upgraded with this module.

Diebold Software and the EMV migration

As there are numerous versions of EMV compliant application software running on Diebold units in different countries around the world, Diebold has developed a common software module, the Diebold EMV Kernel, that can be used as the basis for any new compliant application software.

The Diebold EMV Kernel, which operates in a Microsoft Windows environment, as used by Diebold, is designed not only to accommodate Diebold application software but also to the needs of customers or third parties developing their own solution.

The Diebold EMV Kernel is EMV Level 2 certified to version 4.0 of the EMVCo specifications. The related "EMVCo Letter of Approval – Terminal Level 2" has been released and posted on the EMVCo web site.

The Diebold EMV Kernel assures certification for application software built on the top of it.

However, this does not include certification in terms of the particular network environment, if this is required.

By integrating the EMV Kernel, Diebold Agilis® applications are ready to implement EMV-compliant solutions.

Glossary

ATM	Automatic Teller Machine
DAM	Data Authentication Module
DDA	Dynamic Data Authentication
DEM	Data Encryption Module
DES	Data Encryption Standard
DSA	Digital Signature Algorithm
EMV	Europay Mastercard Visa
EPP	Encrypted Pin Pad (is a PED with Encrypting features)
HHT	Hand Held Terminal
ICC	Integrated Circuit Card
OKD	Operator Keyboard Display
PED	PIN Entry Device
PIN	Personal Identification Number
POS	Point Of Sale
RSA	Rivest, Shamir and Adleman, the inventors of the RSA cryptosystem
SCD	System Control Device
SDA	Static Data Authentication
TDES	Triple DES (Data Encryption Standard)
TTU	Text Terminal Unit
T=0, T=1	Transmission Protocol to exchange commands and data with the ICC

EMV FAQ

EMV Getting Started

1. What is EMV?

EMV is a worldwide, well recognized and widely adopted standard on the use of Chip Cards and for creating an interoperable framework for credit, debit, cash-withdrawal and charge-back cards. This standard is defined by EMV specifications.

2. What does EMV mean?

EMV is the acronym of Europay, MasterCard and Visa.

3. What is the aim of EMV?

The aim of EMV is to create a recognized worldwide standard ruling chip cards for financial environments, their use and their Applications.

EMV is today the standard de facto for chip cards.

Advantage for Vendors: Vendors can introduce a reference specification with confidence of its global acceptance that allows Vendors to develop solutions that can be widely deployed.

Advantage for Card Users: EMV provides the possibility of using their Chip Cards in different ATM and POS terminals, on different ATM Networks and in different Countries.

4. What is EMVCo?

Created in February 1999 by Europay International, MasterCard International and VISA International, the role of EMVCo is to manage, maintain and enhance the EMV Integrated Circuit Card specifications for Payment Systems as technology advances and the implementation of chip card programs become more prevalent. The formation of EMVCo ensures that single terminal

and card approval processes are performed at a level that will allow cross payment system interoperability through compliance with the EMV specifications.

For more information, visit the EMVCo web site located at: <http://www.emvco.com/>.

5. What standards existed before EMV?

Other standards for the use of the Chip Cards and for Electronic Purses have been introduced locally: the lack of interoperability has prevented the global acceptance of these standards.

6. Why is EMV so important?

Because EMV is the first standard proposed by the major Credit Card issuers. The wide acceptance of this standard justifies the related investments.

7. To what extent is the EMV Standard accepted?

EMV is recognized as a global Standard and is widely accepted in the financial services industry.

8. What does EMV mandate?

EMV provides rules for:

- The terminal modules involved in the technology (see Q#9)
- The terminal Security Architecture
- The protection of the PIN and other security data, both inside the terminal and when transmitted outside the terminal to the Host
- The application software running the terminals

Both ATM and POS terminals are addressed by the EMV standard.

9. What are the ATM components affected by EMV?

EMV affects the following ATM components:

- The PIN Entry Device (PED) or the EPP
- The Security Module (if not integrated with the PIN Pad)
- The Card Reader
- The Application Software running the terminal

10. Why is EMV described as a "Base Specification"?

EMV proposes a series of security principles and operation modalities (i.e. how to perform the PIN Check).

The Network Authority and ICC Card Issuer decide the operation modality and the EMV specified principles to adopt on the network.

Additional specifications Issued by Cards Schemes rule the International Transactions.

11. What is the base recommendation of EMV?

The EMV base recommendation, which is already accepted and adopted by all Networks, is the use of Lev 1 Certified Cards Readers.

This means that no matter what type of implementation scheme is chosen within a territory, an EMV Lev1 Card Reader is mandated.

12. Is the EMV Specification enough for defining all the needs for an EMV Project?

No: the implementation of an EMV project is only possible through local network specifications and/or card scheme additional specification that complete the EMV base specification.

13. Who issues the local specifications?

The ATM network authority or the Central Bank institution (those that oversee the ATM network) is responsible for issuing local specification.

EMV Certifications

14. Which types of certification have to be achieved by an ATM before it can be considered EMV compliant?

Two certifications are needed:

- EMV Level 1
- EMV Level 2

15. What is EMV Level 1 for?

EMV Level 1 certification aims at assuring both the compatibility and the correctness of the communication between the ATM ICC card reader and the chip card for: electrical

compliance, contact position, DES deciphering capabilities (DES onboard) and support of transmission protocols T=0 and T=1.

16. What system module is involved in EMV Lev 1?

Only the ICC reader is involved.

17. Who is responsible to achieve Lev 1?

The card reader manufacturer is responsible for achieving Level 1 Certification.

18. Do Diebold ICC readers have Lev 1 Certification?

Yes, all Diebold's current ICC reader's are Level 1 compliant and certified. A list of approved ICC readers is available on <http://www.emvco.com/>. (Select Type Approval and then Level 1 Approved Interface Modules to view the current list).

19. Who has certified our Cards Readers?

The certification testing is performed by one of the independent laboratories accredited by EMVCo. EMVCo issues the approval statement.

20. To whom Level 1 is released?

Level 1 is released to the ICC readers manufacturers.

21. Why Level 1 is so important?

- Level 1 is important as it is always needed in an EMV compliant terminal.

22. What is EMV Level 2 for?

EMV Level 2 aims assuring that the ATM behavior is in full compliance with EMV prescriptions.

EMV Lev 2 assures interoperability between cards and terminals.

EMV Lev 2 certification checks compliance with (depending on the card scheme for which compliance is needed):

- EMV specification
- card scheme terminal specification

In addition an End-to-End integration (into the ATM Network) is needed (depending on the card scheme for which compliance is needed)

23. What Terminal components are involved in EMV Level 2?

The PIN Pad and/or EPP, the ICC Reader, the Security Module (if any) and the SW (Basic and Application) are involved.

24. Who is responsible for achieving Level 2?

The ATM Vendor is responsible for achieving the "EMVCo Letter of Approval – Terminal Level 2".

The Acquirer is responsible for achieving the "Approval of Supplier – ICC Terminal Level 2" demanded by MasterCard.

25. What does the "EMVCo Letter of Approval – Terminal Level 2" assure?

The "EMVCo Letter of Approval – terminal Level 2" assures compliance with the EMV specification.

26. What does the "Approval of Supplier – ICC Terminal Level 2" assures?

The "Approval of Supplier – ICC terminal Level 2" assures compliance with MasterCard terminal Requirements.

27. Diebold has Level 2 Certifications?

Yes. See the EMVCo website (<http://www.emvco.com/>). (Select Type Approval and then Level 2 Approved Kernels to view the current list.)

Diebold has achieved "Approval of Supplier –Terminal Level 2" for both SW Applications and for the Diebold EMV Kernel.

28. How is Level 2 Certification performed?

Tests are carried out by EMVCo accredited certification laboratories. Final EMVCo "Approval Letters" and MasterCard "Approval of Supplier Letters" are issued on reception of test reports provided by the certification laboratories.

29. What are the accredited Laboratories?

Accredited Laboratories are independent testing organizations that have been accredited by EMVCo to perform EMV Level 1 and/or Level 2 Certifications. The list of accredited labs is available on

<http://www.emvco.com/>. (Select Type Approval and then Laboratories to view the current list.)

30. Has Diebold an ATM Application Kernel EMV Lev 2 certified?

Yes. The Diebold EMV Kernel for Microsoft Windows has been Level 2 approved to version 4.00 of the EMV specifications. Other Diebold applications are approved to version 3.11. Refer to the EMVCo website (<http://www.emvco.com>) for the current list.

Cardholder's Verification Methods

31. What is a Cardholder's Verification?

It is a check made on cardholder's personal secret data (the PIN = Personal Identification Number) entered in the terminal by the cardholder, to verify the identity of the cardholder.

This verification is carried out with mathematical operations made on the PIN.

These operations are known as "PIN check".

32. Do different methods exist for Cardholder Verification?

Cardholder Verification can be performed either on-line by a host computer or off-line by the ICC chip itself.

33. What is an On-Line Cardholder's Verification?

An on-line cardholder's verification is done by a remote host computer that receives the PIN of the cardholder for processing and verification.

34. What is an Off-Line Cardholder's Verification?

An off-line cardholder's verification is done within the ATM, without the need of host processing.

EMV specifies that off-line cardholder's verification is performed by the ICC.

35. What is the advantage of Off-Line Cardholder's verification?

Cardholder verification does not need any communication with a host computer. It can work in an off-line environment and reduces telecommunication and processing times and costs.

36. What is a Data Authentication?

It is an operation that verifies the authenticity of data contained in the ICC Card, through defined security rules.

The authenticity of this data grants the authenticity of the card.

Encryption

37. What is an Encryption Algorithm?

It's a mathematical operation that, starting from an input data, generates an output data (different from the input) which value is depending on the enciphering key.

38. What are encryption algorithms for?

Encryption algorithms aim to protect critical data when they have to be transported from one module to another one inside a terminal (i.e.: an ATM) or to an external location (i.e.: a host computer).

Enciphered data (i.e.: the PIN – Personal Identification Number) are no longer in clear form, but appears in a form that is not understandable without having the encryption key.

Deciphering algorithm, applied with the correct key to the enciphered data, recovers the data in the original clear form.

Illegal tampering with the enciphered data does not allow retrieving the original data.

39. Which are the Encryption Algorithms referred by EMV?

EMV makes reference to both DES and RSA encryption technologies.

40. What is DES?

DES is an enciphering method based on a 64-bit key.

41. Is DES secure enough?

DES has been used extensively in the past as enciphering method in Financial Environments.

It's still used into ATMs for protecting the transport of critical data.

Currently DES is being taken over by Triple DES.

42. What is Triple DES, also called TDES or 3DES?

TDES is a data enciphering method using a DES Algorithm three times and based on a 128-bit key (also called a double length key). Protection of the data is much more robust than the one made with single DES.

The operation of Triple DES encryption is as follows:

- The 128 bit DES key is divided into 2 – 64 bit key halves (left half and right half)
- The data to be encrypted (typically PIN data) is first encrypted in the left half of the key
- The result of the first encryption is then decrypted in the right half of the key
- The result of the decryption is then encrypted in the left half of the key
- Since there are 3 cryptographic operations on the data, this is called 'triple DES' encryption

43. What is RSA?

RSA is a data enciphering and signing method based on asymmetrical algorithms using public and private 128-bit keys.

44. What are the differences between DES and RSA?

There are two types of enciphering method: secret-key method and public-key method.

In secret-key cryptography, also referred to as symmetrical cryptography, the same key is used for both encryption and decryption. The most popular secret-key enciphering method in use today is the DES.

DES is a symmetrical algorithm, that is, the encryption and the decryption keys are the same.

The DES encryption system involves precaution in the transport of the encryption key, since this has to be treated as secret: if the key is known, encrypted data can be recovered.

RSA is an asymmetrical algorithm with the key for encryption (Public Key) different from the one for decryption (Private Key).

No precaution is needed for the transport of the "Public Key".

45. What does Public Key and Private Key mean?

In an asymmetrical method, the Public Key is made public while the private key remains secret.

46. Why do you need a Public Key and a Private Key?

These are the keys used in an asymmetrical algorithm like as RSA.

Encryption keys are Public Keys, while deciphering keys are Private Keys.

Only the owner of the Private Key can decipher data sent.

The advantage of this approach is that no precaution is needed in the transport of the Public Key, since they are public and usually available in key directories.

A digital signature is instead made through the Private Key, and has to be verified with the Public Key.

Only the original owner of the key can produce a digital signature that anyone can verify through the Public Key.

47. What is a DSA digital signature?

It is a result of a mathematical operation performed on data with a Private Key.

48. What is a digital signature for?

The DSA digital signature enables the authenticity of the original data to be checked, (and/or the support that contains this data, i.e.: the ICC) when deciphered with the related Public Key.

The digital signature is used to prevent data alteration or modification and guarantees the origin of the data.

49. How is RSA enciphering performed?

RSA enciphering is performed with the Public Key; only the owner of the related Private Key is able to recover the data in clear form.

50. Why has RSA been introduced?

RSA assures a more powerful and resistant algorithm than DES.

In addition it allows data authentication.

Public Key distribution and transmission does not require any precaution (opposite to DES, where the Key is secret).

The RSA Key Schema allows easy management of authentication procedures.

51. Why must the PIN be protected?

The PIN must be protected since it constitutes one of the elements of the cardholder's identity, and it would be required by any criminal elements wishing to run a fraudulent transaction.

An unprotected or disclosed PIN makes it easier to perform a fraudulent transaction.

52. When is the PIN protected?

The PIN is protected both inside and outside the ATM.

It is protected inside the ATM by enciphering after the customer has entered their PIN.

It is also protected by enciphering when it is transmitted outside the ATM to the host computer for remote PIN on-line checking.

EMV Kernel

53. What is an EMV Kernel?

An EMV Kernel is a SW module that performs EMV functions and operations and supports an ATM software application.

54. Why has Diebold developed an EMV Kernel?

The aim of the EMV Kernel is to gather all the EMV functions into a software module. These functions have been EMV Level 2 certified once and this ensures the same certification for application's software implemented on top of the Kernel.

Instead of developing EMV functions in each application's software, Diebold will reuse the Diebold EMV Kernel with consequent efficiency in both the software development effort and certification costs.

55. Is the Diebold EMV Kernel Level 2 certified?

The Diebold EMV Kernel has been EMV Level 2 certified by EMVCo.

The Diebold EMV Kernel can be integrated into different software applications. The advantage of the Diebold EMV Kernel approach is that no additional certification

(for compliance with EMV Spec) is required for the integrated SW application.

The EMV Kernel for Windows was EMV level 2 certified and approved in Q4, 2002 and is developed with the EMV2000 V4.0 specification.

56. In which environments will the EMV Kernel be available?

The Diebold EMV Kernel is currently available in Microsoft Windows environments.

57. Will Diebold provide a "turn key package" to address third party SW houses and countries covered by distributors?

Yes, the Diebold EMV Kernel will be provided as a "turn key package" dedicated to third parties, countries and banks developing their own software solution on Diebold hardware.

ICC Cards

58. What is a Chip Card?

It is a plastic card that contains an electronic chip with memory and processing capabilities.

It is different from memory cards, which do not have any processing capabilities.

59. Do different types of chip cards exist?

Chip cards may be either contact or contactless.

The ones currently considered by EMV are contact chip cards.

60. What does ICC mean?

ICC is the acronym for "Integrated Circuit Card", and is the synonym of chip card.

61. How many types of Contact Chip Cards exist?

It is possible to divide contact chip cards into two categories:

- ISO 7816-1 fig 1 chip cards
- CP8 cards (in use only in France and planned to be withdrawn from banking sector)

62. What is the difference between the two cards?

The two cards may be easily distinguished by the different position of the contact pads.

63. How does the Chip Card communicate with the ATMs?

The contacts on the cards (small gold plated pads) are the electrical interface for the ICC card that is interfaced via the ATM through the ICC reader.

At the software level, the ATM communicates with the ICC with one of two protocol types (selected by the ICC card) called T=0 and T=1 to exchange data and to send commands to the chip.

64. Why using Chip cards?

Chip cards aim to both:

- Increase the level of security of the card
- Enhance the features of the card

65. How do Chip Cards increase the security?

Duplication of magnetic cards is relatively easy: related duplication equipment may be easily obtained at low cost. The technology relating to the duplication of ICC cards is much more sophisticated and expensive, therefore the threshold to prevent fraudulent duplication is much higher than that for magnetic cards.

66. How do Chip Cards enhance functionality?

With memory and processing capabilities, a chip card is able to load and execute new applications in the banking arena, such as Electronic Purse or, other new applications such as loyalty programs.

Electronic Purse

67. What is an Electronic Purse?

Electronic purses are software applications that store monetary value directly on a payment card. The value stored in the purses can be used for making purchases at shops, pay phones, and vending machines or on-line.

This payment method is alternative to cash, debit cards and credit cards.

The use of ICC as media for supporting Electronic Purse transactions constitutes a valid application taking advantage of the intrinsic security of the ICC.

68. What is the difference between and Electronic Purse and a phone card?

The difference with a standard phone card is that the Electronic Purse stores true virtual money and not call units purchased with cash or through electronic payment. The value of money stored on the Electronic Purse is part of money supply.

The Money is transferred from the account of the cardholder to the ICC and then deducted from the stored amount during transaction when it is transferred to the vendor.

69. Does EMV specify Electronic Purses?

No. There is another specification for an interoperable Electronic Purse that is known as CEPS (Common Electronic Purse specification). EMV and CEPS can be implemented on the same smart card.

Miscellaneous

70. NCR says it achieved EMV Level 1 approval in February 1999 and now is the first ATM manufacturer to support end-to-end smart card transactions. How does Diebold respond to this?

Diebold achieved EMV Level 1 approval on February 22nd, 1999 with the Omron ICC card reader.

Diebold has been providing its customers, mainly in EMEA countries, with solutions based on smart cards for many years for a wide range of purposes.

71. Does Diebold communicate enough with the SW vendors (PIX program) in order to give them our EMV specs with our protocol messages (i.e.: D912...)?

As we work toward updating and enhancing our solutions to meet market requirements, we also work closely with other solution providers, such as ACI, whose involvement is a critical piece of the retail banking delivery infrastructure. Some of our competitors have released specifications without actually having completed any development or testing. Diebold has taken another approach by providing ACI with our draft specifications for an EMV compliant application. We have developed an alpha VSDC application based

on the draft specification and worked with Visa International initially and then EMVCo to have it certified. It is now released and operating at Co-op Bank in the UK.

72. What is an EPP4?

An EPP4 is a secure module of the ATM bringing together both the Pin Pad Keyboard and Enciphering module and providing the capabilities (DES, RSA) needed in EMV Level 2.

73. In which case, is an EPP4 mandatory?

EPP4 provides DES, TDES and RSA capabilities. It is actually mandatory when the PIN has to be triple DES encrypted in the PIN entry devices, as demanded today by card schemes. EMV features require the use of EPP4.0.

74. Is EMV mandatory for my ATM fleet?

EMV cards will replace progressively current non-EMV chip cards or magnetic cards. At the end of this migration, EMV implementation will be mandatory to accept EMV cards.

75. When will EMV be mandatory?

Full implementation of EMV cards depends on the country and on the network authority involved.

76. Can Diebold ATMs support EMV Application Software?

Diebold ATMs are either already EMV compliant or can be easily upgraded. A wide range of upgrading kit and replacement kit is available allowing your ATMs to meet EMV standards.

77. Which parts of the ATM require an upgrade?

Modules involved in EMV are the ICC card reader, EPP and, if relevant, the security module. As most EMV application software is Windows NT or Windows 2000 based, the PC can require either upgrading or replacing.

78. What kind of EMV upgrade kit is or will be proposed by Diebold?

There is a wide range of upgrade kits or replacement kits for ICC card readers, EPP keyboards and security modules to ensure your ATM is EMV compliant, depending on the EMV requirements in your country and the type of ATM installed.

Diebold, Incorporated
Post Office Box 3077
Dept. 9-B-16
North Canton, Ohio
44720-8077

DIEBOLD

We won't rest.

©Diebold, Incorporated 2003
All rights reserved. Litho in U.S.A.
10.03