ISO 14443

An introduction to the contactless standard for smart cards and its relevance to customers

ISO 14443

Table of Contents

ISO 14443

An introduction to the contactless standard for smart cards and its relevance to customers

Introduction

Who is ISO?

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the international body for worldwide technical standardization. National organizations that are members of ISO or IEC participate in the development of International Standards through technical committees established to deal with particular fields of technical activity. *In this document we will refer to ISO standards when, in fact, they can technically be considered ISO/IEC standards.*

Each participating country can send several representatives to the committees, yet each country has only one vote in the Committee.[*]

Why is ISO Standardization Important?

Standardization under ISO or IEC specifications ensures the interoperability of various components produced worldwide by a number of manufacturers. Without such standards, each manufacturer would design products to its own internal specifications only, in essence creating an environment comprised of multiple proprietary systems. No component would be compatible with any competitor's components. For example, a stereo system produced by manufacturer A would not be able to read audio signals delivered by a CD player produced by manufacturer B. By meeting ISO standards, manufacturers offer their customers a choice in component selection, while ensuring compatibility with any other ISO-standard manufacturers' products.

What is ISO 14443?

ISO 14443 is a four-part international standard for contactless smart cards operating at 13.56 MHz in close proximity with a reader antenna. This ISO standard sets communication standards and transmission protocols between card and reader to create interoperability for contactless smart card products.

Customers these days *require* full compatibility with all 4 parts of ISO/IEC 14443 both in the readers (called *Proximity Coupling Device* or *PCD*) and in the cards (called *Proximity Integrated Circuit Cards* or *PICCs*).

[*] OTI has two representatives on the ISO 14443 committee, representing Israel.

PICCs are intended to operate within up to 10cm of the reader antenna at a frequency of 13.56 MHz. The 13.56 MHz frequency was chosen for various technical reasons (e.g. suitability for efficient proximity inductive coupling, compliance with EMC regulation (already allocated as ISM band), low absorption by human tissues and more).

Two main communication protocols are supported under the ISO 14443 standard series – Type A and Type B – which will be addressed further below. An attempt was made to include additional legacy systems as appendixes – Type C (Sony/Japan), Type D (OTI/Israel), Type E (Cubic/USA), and Type F (Legic/Switzerland) and Type G (China) – but they were not finally accepted as ISO-standard. ISO 14443 is supported by most contactless smart card providers to one level or another and is usually specified in the different RFP's who are looking for contactless smart cards. VISA and MasterCard have both announced that they are supporting ISO14443 in their relevant contactless specifications.

The specifications do not address operating systems residing on cards and readers, as they are proprietary to each vendor, similar to magnetic stripe terminal providers today. Vendors in the smart card industry also meet the ISO 7816 standard series relating to contact smart cards, which define commands, parameters and procedures as well. The ISO 14443 series define an "envelope protocol" that supports reliable, error-free data transmission with multiple cards, but do not define the contents of the data. ISO 14443 supports the exchange of standard ISO 7816 data packets, thus preserving the industry investment in contact smart cards by allowing almost transparent and painless application migration between contact to contactless environments.

ISO 14443 consists of the following parts, under the general title *Identification cards — Contactless integrated circuit(s) cards — Proximity cards:*

- Part 1: Physical characteristics
- Part 2: Radio frequency power and signal interface
- Part 3: Initialization and anticollision
- Part 4: Transmission protocols

Key features of ISO 14443:

- Operating frequency: 13.56 MHz
- Read/write range: up to 4 inches (10cm). Note: this figure is generally accepted but it is not stated in the standard.
- Speed: The ISO standard specifies a default speed of 106 Kbps, which is mandatory for anticollision stage. Higher communication such as 212 Kbps and higher are allowed as an option.
- Security:
    - Wired logic cards: authentication mechanisms are available.
    - Microprocessor cards: security mechanisms available in contact smart cards are also available for both ISO 14443 Type A and Type B (e.g., hardware memory firewalls, sensors, tamper resistance features). Also available are "secure messaging" and "cryptographic tokens" as described in the ISO 7816 standard series.

    - Crypto coprocessors, such as 3DES, ECC and RSA, can be used, but are not defined in the ISO standard.
    - The close proximity of the card to the reader helps limit unintended communication.
- Interoperability: Supported through full definition of commands in ISO 14443 Part 4, tested through ISO 10373-6, which will be discussed further below.

ISO 14443 – Part 1

Purpose:

ISO 14443-1 was published as an international standard on April 15, 2000. The standard defines the following:

- Card dimensions, referring to ISO 7810 standards for contact card size
- Surface quality for printing
- Mechanical resistance
- UV and X-ray resistance
- Sensitivity to surrounding magnetic fields

The standard also introduces the following specific terms:

- PICC: Proximity integrated circuit(s) card
- PCD: Proximity coupling device (the card reader or terminal)

Part 1 defines the size and physical characteristics of the card. It also lists several environmental stresses that the card must be capable of withstanding without permanent damage to the functionality:

- Ultra-violet light
- X-rays
- Dynamic bending and torsion stress
- Alternating magnetic and electric fields
- Static electricity and magnetic fields

These environmental requirements are intended to be met at the card level and depend on the construction of the card and on the antenna design. The operating temperature range of the card is specified in Part 1 as an ambient temperature range of 0°C to 50°C.

ISO 14443 – Part 2

Purpose:

ISO 14443-2 was published on July 1, 2001. This standard describes the characteristics of power transfer (based on inductive coupling) and communication between the PICC and PCD. Power is transferred to the card using a frequency-modulated field at 13.56 MHz +/- 7kHz.

Two different types of communication signal interfaces (bit modulation and coding) are specified: Type A and Type B. The bit protocol timings are defined and the default data transmission rate is defined at 106 kBaud.

Some abbreviations used in this standard are:

- ASK Amplitude shift keying
- BPSK Binary phase shift keying
- NRZ Non-return to zero

Part 2 defines the RF power and signal interface. Two signaling schemes, Type A and Type B, are defined in part 2. Both communication schemes are half duplex with a default 106 kbit per second data rate in each direction. Data transmitted from the card to the reader is achieved by utilizing load modulated with an 847.5 kHz subcarrier. The card is powered by the RF field and no battery is required.

Differences between Type A and Type B include the modulation of the magnetic field used for coupling, the bit and byte coding format and the anticollision method (i.e., how the cards and readers respond when more than one card responds at the same time to a reader's request for data).

Type A has an ASK of 100% Reader to Card modulation index, meaning that data is coded with short pauses in the transmission. During these pauses no power is transmitted to the card. This dictates special requirements to the chip in the card. Type A uses Modified Miller bit coding. Type B, however, has an ASK of 10% Reader to Card modulation index, meaning that data is coded with only minor reduction of its normal amplitude, enabling both card and reader to maintain power throughout the communication process. This provides major advantages compared with Type A. Type B uses NRZ bit coding.

For Card to Reader communication, Type A uses OOK Manchester bit coding technique and Type B uses BPSK bit coding, which is superior compared with the Type A technique.

ISO 14443 – Part 3

Purpose:

ISO 14443-3 was published as an international standard on February 1, 2001. This part of ISO 14443 describes:

- Polling for PICCs entering the field of a PCD (i.e., the terminal talks first).
- Byte format, command frames and timing.
- Request (REQ) and Answer To Request (ATQ) commands.
- Anticollision methods to detect and communicate with one particular card when several cards are presented to the same reader. Anticollision methods rely on a unique ID per card; however, depending on the communication type (A or B), the anticollision method is different.
    - Type A: Binary search method referring to the unique identifier (UID) of the card.
    - Type B: Slotted Aloha method with special slot markers.

Part 3 defines the initialization and anticollision protocols for Type A and Type B. The anticollision commands, responses, data frame, and timing are defined in Part 3.

The initialization and anticollision scheme is designed to permit the construction of readers capable of communication with several cards of the same type, powered simultaneously. Both card types wait silently in the field for a polling command. A multi-protocol reader would poll one type, complete any transactions with cards responding, and then poll for the other type and transact with them. It is not assumed that both types can be powered at the same time.

ISO 14443 – Part 4

Purpose:

ISO 14443-4 was published as an international standard on February 1, 2001. This standard specifies a half-duplex block transmission protocol (T = CL). Several protocol scenarios are included in Appendix B of this standard, showing how this common transmission protocol can be used. The standard also defines the transparent exchange of data, independent of the lower layers.

Part 4 defines the high-level data transmission protocols for Type A and Type B. The protocols described in Part 4 are optional elements of the standard; proximity cards may be designed with or without support for Part 4 protocols.

Part 4 deals mostly with the baud rate negotiation between the card and the reader, data encapsulation block format, chaining (breaking a long block into smaller ones) and error handling and recovery scenarios.

Status of ISO 14443

Several enhancements to ISO 14443 and the related testing standard are currently under discussion. These include:

- Increased transaction speed: ISO 14443 standard already cater for optional higher data rates of maximum theoretical speed of 847KBps. Type A, as is, is not suitable for such higher data rates so a mixed Type A and B scenario has been proposed and is debated by the ISO committee.

- Testing: With each published standard ISO must also publish a standard set of minimal test procedures that ensure the minimum accepted interoperability. For the ISO 14443 series, ISO is now developing ISO 10373 Part 6 that includes a set of test procedures. First version of ISO 10373-6 was published as an international standard on May 15,2001. Amendments 1,2 and 3 are expected to be finalized in the near future. Test tools start to come from companies excelling in test benches.

Why Should I Adopt ISO 14443?

The smart card industry is comprised of multiple vendors providing cards, readers, and related software, either as OEM components or as part of an integrated solution. Selecting products that meet ISO standards ensures that your smart card program will be interoperable with other ISO-standard systems, and any products that you may adopt in the future will seamlessly interact with your existing installation. You may purchase ISO-standard products from multiple vendors, rather than relying upon a single provider for proprietary products.

What Are The Technology Requirements To Fully Support ISO 14443?

While memory chips or ASICs can support most functions of ISO 14443, only a microprocessor can fully support all four parts, including Part 3, which refers to anti-collision measures required when more than one card is in a reader field; and Part 4, which specifies the protocols for high-level security required for secure transactions, including biometrics and financial information.

The 100% modulation index and the anti-collision requirements specified in Parts 2 and 3 require special hardware and memory on Type A PICCs so that it can be placed in an extremely low power consumption mode, while Type B cards do not need any special hardware circuitry to meet Parts 2 and 3 requirements.

Type B technology is supported by several chip manufacturers coming from multiple sources.

Companies who are looking to guarantee interoperability should require full compliance of ISO 14443 Parts 1-4.

Popular Misconceptions

<u>MIFARE = ISO 14443 Type A</u>:
MIFARE and ISO 14443 Type A are not the same. While MIFARE is often viewed as equivalent to or subset of ISO 14443 Type A, it is a proprietary encryption/conditional access protocol owned and licensed by Philips Semiconductors to multiple vendors of card ICs and reader ICs. All MIFARE readers must make use of a Philips special chip that handles these special security features.

Because MIFARE has been so predominantly used with products employing ISO 14443 Type A technology, it has mistakenly become synonymous with the standard. However ISO 14443 Type A is an open standard and does not require the use of this MIFARE encryption/conditional access scheme.

<u>Parts 1-3 are sufficient to meet ISO standards:</u>
While Part 4 is described as optional in the ISO standard specifications, it is required to ensure complete interoperability. All major customers require full four-part compatibility to ensure system support for cards coming from multiple vendors. A reader must support all parts to receive the ISO compatibility stamp (as well as both Type/A and Type/B).

<u>Microprocessors are cost-prohibitive</u>:
Advances in manufacturing capability have steadily lowered the price of smart card microprocessor-based chips, to the point where they approximate the cost of ASIC or memory cards in large quantities. Microprocessor chips are now becoming available

at affordable costs , thus the cost of a simple microprocessor based card should only be marginally more expensive (if at all) compared with an ASIC card,

Security is specified in ISO 14443:
While security is addressed in ISO 14443 where communication protocols are concerned, the security measures residing on the chip itself are not specified as it is part of the operating system, which is usually proprietary to each card manufacturer while remaining ISO-standard. The use of a microprocessor greatly enhances the security handling of the card in ways that are not possible with simple ASIC or memory logic at no significant cost increase.

Summary

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) established the ISO 14443 standard to ensure interoperability of proximity smart cards. ISO 14443 has four parts, which specify physical characteristics, radio frequency interface power and signal interface, initialization and anticollision, and transmission protocols. All four parts are required for full ISO interoperability, which is possible only on a microprocessor PICC. Two communication protocols are recognized by the ISO standard – Type A and Type B, based on how power is transmitted from the card to the reader and a few other differences. Prospective smart card customers should consider all of the specifications set forth in ISO 14443 when selecting a vendor. Customers can build a custom smart card solution using cards, readers, and software from a variety of vendors, as long as all products meet the ISO standard.

For additional information please contact:
Ohad Bashan
Email: ohad.bashan@otiamerica.com
Tel: +1-408-252-0333