INTERNATIONAL STANDARD

ISO 9564-4

First edition
2016-03-01

Financial services — Personal Identification Number (PIN) management and security —

Part 4: Requirements for PIN handling in eCommerce for Payment Transactions

Sercices financiers — Gestion et sécurité du numéro personnel d'identification (PIN) —

Partie 4: Exigences pour la manipulation PIN dans le commerce électronique pour les transactions de paiement

Reference number
ISO 9564-4:2016(E)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/TC 68, *Financial services*, Subcommittee SC 2, *Financial Services, security*.

ISO 9564 consists of the following parts, under the general title *Financial services — Personal Identification Number (PIN) management and security*:

— *Part 1: Basic principles and requirements for PINs in card-based systems*

— *Part 2: Approved algorithms for PIN encipherment*

— *Part 4: Requirements for PIN handling in eCommerce for Payment Transactions*

Introduction

The eCommerce environment is inherently high-risk. This is especially true for PIN-based transactions because if PIN security in this environment is deficient, there is a high probability, in some cases, that card and PIN data might be fraudulently captured and reused in the ATM, POS or eCommerce environments.

For conducting eCommerce transactions, cardholders use network access devices (NAD) of their choice. ISO 9564-1 prohibits PINs from being entered on NADs.

This part of ISO 9564 defines minimum security requirements and practices for acceptable devices used for the entry of the PINs in the eCommerce environment:

— devices that are compliant with ISO 9564-1 (i.e. PEDs);

— devices that are not compliant with ISO 9564-1 but are functionally secure devices for PIN entry (FSPED) for exclusive use with IC cards;

— devices that are not compliant with ISO 9564-1 but are IC cards with integrated keypad and display (ICCPED).

Financial services — Personal Identification Number (PIN) management and security —

Part 4: Requirements for PIN handling in eCommerce for Payment Transactions

1 Scope

This part of ISO 9564 provides requirements for the use of personal identification numbers (PIN) in eCommerce. The PINs in scope are the same cardholder PINs used as a means of cardholder verification in card-based financial transactions; notably, automated teller machine (ATM) systems, point-of-sale (POS) terminals, automated fuel dispensers, and vending machines.

It is applicable to financial card-originated transactions requiring verification of the PIN and to those organizations responsible for implementing techniques for the management of the PIN in eCommerce.

The provisions of this part of ISO 9564 are not intended to cover

— passwords, passcodes, pass phrases and other shared secrets used for customer authentication in online banking, telephone banking, digital wallets, mobile payment, etc.,

— management of cardholder PINs for use as a means of cardholder verification in retail banking systems in, notably, automated teller machine (ATM) systems, point-of-sale (POS) terminals, automated fuel dispensers, vending machines, banking kiosks and PIN selection/change systems, which are covered in ISO 9564-1,

— card proxies such as mobile phones or key fobs,

— approved algorithms for PIN encipherment, which are covered in ISO 9564-2,

— the protection of the PIN against loss or intentional misuse by the customer or authorized employees of the issuer,

— privacy of non-PIN transaction data,

— protection of transaction messages against alteration or substitution, e.g. an online authorization response,

— protection against replay of the transaction,

— functionality of devices used for PIN entry which is related to issuer functions other than PIN entry,

— specific key management techniques, and

— access to, and storage of, card data other than the PIN by applications such as wallets.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 9564-1, *Financial services — Personal Identification Number (PIN) management and security — Part 1: Basic principles and requirements for PINs in card-based systems*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
acquirer
institution, or its agent, that acquires from the card acceptor the financial data relating to the transaction and initiates such data into an interchange system

3.2
compromise
⟨cryptography⟩ breaching of confidentiality and/or integrity

3.3
contact IC reader
reader of an IC card that requires the insertion of the card into the contact IC reader to establish communication between the contact IC reader and the IC card through a physical connection

3.4
eCommerce
buying and selling of products or services over open networks

3.5
encipherment
transformation of intelligible data (plaintext) into an unintelligible form (ciphertext)

3.6
functionally secure PIN entry device
FSPED
device that communicates with a contact IC card for the purpose of using the PIN to generate an OTT offline, containing

— a contact IC reader,

— an integrated numeric keypad, and

— an alpha-numeric display

Note 1 to entry: An FSPED is not a PED in the sense of ISO 9564-1.

3.7
integrated circuit card
ICC
IC card
ID-1 card type, as specified in ISO/IEC 7816 (all parts) into which one or more integrated circuits have been inserted

3.8
integrated circuit card PIN entry device
ICCPED
ID-1 card type, as specified in ISO/IEC 7816 (all parts) into which one or more integrated circuits have been inserted, but which additionally is self-powered, has integrated keypad and display capabilities, for the purpose of using a PIN to generate an OTT offline

Note 1 to entry: Standards that describe these kinds of devices are under development (see Reference [8]).

Note 2 to entry: An ICCPED is not a PED in the sense of ISO 9564-1

3.9
issuer
institution holding the account identified by the primary account number (PAN)

Note 1 to entry: For this standard, references to an issuer may extend to an agent acting on the issuer's behalf, e.g. performing issuer functions such as card and PIN issuance, PIN verification and transaction authorization.

3.10
network access device
NAD
device capable of allowing access to public endpoints via an open network, e.g. personal computer, TV, mobile phone or even household appliances

Note 1 to entry: POS devices as defined in ISO 9564-1 with IP connectivity with access restricted to a limited number of acquirers are not NADs.

3.11
open network
communications network for public use

EXAMPLE Internet, mobile phone networks.

3.12
personal identification number
PIN
string of numeric digits established as a shared secret between the cardholder and the issuer, for subsequent use to validate authorized card usage

3.13
PIN entry device
PED
device, as specified in 9564-1, providing for the secure entry of PINs

3.14
primary account number
PAN
assigned number that identifies the card issuer and cardholder, composed of an issuer identification number, individual account identification and accompanying check digit, as defined in ISO/IEC 7812-1

3.15
one-time token
OTT
authentication data cryptographically generated by the IC card in response to PIN entry and optionally formatted (e.g. decimalized and/or truncated) by the FSPED

4 eCommerce model

In eCommerce, the cardholder and the merchant are not typically in the same location at the time of payment. eCommerce occurs in an open network environment and the cardholder uses a network access device (NAD) to perform an eCommerce transaction. In the open network environment, the NAD may initiate a transaction with any open-network-connected merchant. In eCommerce, the device into which the PIN is entered might not be under the control of the merchant or the merchant's acquirer.

For card payment transactions based on PIN, the eCommerce model introduces some fundamental changes with respect to the POS environment:

— the NAD may be a general purpose computing device connected to an open network and therefore cannot be considered secure;

— the NAD, which may include a numeric keypad, has not been manufactured in order to be compliant to the requirements of the payments industry;

— the NAD is not under the control of the merchant, issuer or the merchant's acquirer.

As a consequence, the NAD is not acceptable for PIN entry. Clause 5 specifies the requirements for the secure handling of PINs in the eCommerce environment.

5 PIN handling requirements

5.1 General

A PIN shall not be entered into a network access device (NAD), including, but not limited to, personal computers, mobile phones, etc.

Personal devices used for PIN entry in eCommerce shall be for the exclusive use of the cardholder. The use of public (shared) PIN entry devices is restricted to PEDs defined in 5.4 and 5.5.

5.2 Functionally secure PIN entry devices (FSPED)

Functionally secure PIN entry devices (FSPED) are limited functionality PIN entry devices that shall be approved by the issuer for use in conjunction with any of that issuer's IC cards for offline OTT generation.

FSPEDs that support software updates shall have a cryptographic relationship with the card issuer but the associated cryptographic keys shall not be used for PIN encipherment. The device shall only apply software updates that it has cryptographically authenticated and shall ensure that the software updates are applied in the correct order (an older update cannot be applied after a newer one has already been applied).

An FSPED shall contain a contact IC reader for communication with an IC card. The device shall also contain a keypad for PIN entry and a display screen.

Following entry of a PIN (which may be verified by the IC card), the FSPED interacts with the IC card to produce an OTT for subsequent verification by the issuer. The IC card generates a cryptographic value. This value may be used directly as the OTT or the FSPED may format this value to an OTT (e.g. by decimalization and/or truncation) that is convenient for a user to enter manually. The OTT is then either entered into or transferred to the NAD as part of the eCommerce transaction and sent to the issuer for verification. In addition to the PIN, solutions may require the entry of other transaction related data into the FSPED before an OTT can be generated. Such transaction related data may be manually entered or transmitted from the NAD to the FSPED. Such transaction details (e.g. amount) should be displayed on the FSPED for the cardholder to verify.

The FSPED shall make no cryptographic contribution to the value of the OTT. However, for example, the FSPED may encipher the PIN with an IC card public key for transport to the IC card.

Magnetic stripe-only cards have no processing capability (e.g. for PIN verification) and therefore cannot be used for OTT generation.

The cardholder should be instructed by the issuer to

— not use any FSPED from an untrusted source such as an Internet cafe, hotel business centre, etc.,

— remove the card from the FSPED after each use,

— physically protect the FSPED from unauthorized replacement or alteration, and

— cease to use the FSPED if it appears to be damaged.

NOTE The requirements in this subclause do not preclude the use of an ISO 9564-1 compliant PED for OTT generation. Whenever the term PED is used as a stand-alone term in this part of ISO 9564, an ISO 9564-1 compliant PED is understood.

FSPEDs shall comply with the following requirements:

a) unauthorized modifications to the device's functional characteristics cannot be made without physical penetration of the device;

b) the device has characteristics that make it likely that physical penetration results in visible damage detectable by the end-user;

c) the device shall not disclose the value of the PIN in any form except to the IC card. For example, it shall not provide visual or auditory signals that divulge the value of entered PIN digits;

d) the device shall only perform its designed functions;

e) the functionality implemented in the device shall have been approved by the issuer whose cardholder will use the device;

f) the device shall be a single device that includes the contact IC reader, processor, keypad, display, and memory;

g) the device shall immediately erase the entered PIN from all device memory once the PIN has been submitted to the IC card or enciphered for the transmission to the IC card;

h) after PIN entry, the OTT shall be displayed on the device unless automatically transferred to the NAD;

i) the device shall only apply software updates that it has cryptographically authenticated and shall ensure that the software updates are applied in the correct order (an older update cannot be applied after a newer one has already been applied);

j) the device shall not forward PIN verification commands which originate from outside the device.

5.3 Integrated circuit card PIN entry devices (ICCPED)

Integrated circuit card PIN entry devices (ICCPED) are self-powered IC cards which have integrated keypad and display capabilities. Following entry of a PIN, an ICCPED generates and displays an OTT. This OTT is then entered into the NAD as part of the eCommerce transaction and sent to the issuer for verification.

An ICCPED shall satisfy requirements a), b), d), e), g), and h) in 5.2 and the following requirements:

a) the ICCPED shall not disclose the value of the PIN in any form. For example, it shall not provide visual or auditory signals that divulge the value of entered PIN digits;

b) the ICCPED shall be a single device that includes the IC, processor, keypad, display, power supply, and memory in a single tamper-evident housing;

c) the ICCPED shall store the reference PIN only in the secure memory of the ICC part of the device and immediately erase the transaction PIN from all other memory once the PIN has been verified.

5.4 PIN entry devices with a keying relationship to an acquirer

This model can be seen as extending the existing point-of-sale environment to where the cardholder has a PED managed by an acquirer in a manner similar to PEDs in traditional point-of-sale environments.

Where there is a cryptographic keying relationship between the PED and an acquirer, the requirements of ISO 9564-1 shall apply. In addition, the following requirements shall be satisfied:

a) the PED shall authenticate itself to the acquirer for each transaction;

b) the PED shall authenticate each command from the acquirer;

c) these PEDs shall not support manual PAN entry.

These PEDs may use offline PIN verification for IC cards and may use online PIN verification for either magnetic stripe or IC cards. Acquirers that accept magnetic stripe online-PIN eCommerce transactions should authenticate the transaction origin or have some other means to mitigate fraudulent PIN guessing attacks.

5.5 PIN entry device with a keying relationship to an issuer

Where there is a cryptographic keying relationship between the PED and an issuer, the requirements of ISO 9564-1 shall apply. In addition, the following requirements shall be satisfied:

a) the PED shall authenticate itself to the issuer for each transaction;

b) the PED shall not forward PIN verification commands to the IC card, such that PIN exhaustion attacks are prevented;

c) the PED shall authenticate each command from the issuer. This mechanism would rely on issuer provided and managed devices. For an example, see Figure A.6;

d) these PEDs shall not support manual PAN entry.

Issuers that accept magnetic stripe online PIN verification messages should authenticate the transaction origin or have some other means to mitigate fraudulent PIN guessing attacks.

5.6 PED class summary

Table 1 summarizes the acceptable PED classes.

Table 1 — PIN entry device classes

PIN entry device class	FSPED	ICCPED	9564-1 PED
Reference	5.2	5.3	5.4 and 5.5
Connected to NAD at transaction time	Allowed	Allowed	Allowed
Use of IC card	Allowed	N/A	Allowed
Use of magnetic stripe card	Not Allowed	N/A	Allowed
Manual PAN entry on PIN entry device	Not Allowed	Not Allowed	Not allowed
PED authenticated at time of transaction	N/A	N/A	Mandatory
OTT generated offline	Yes	Yes	Optional
PIN verified online	No	No	Yes
OTT transferred automatically to NAD	Allowed	Allowed	Allowed
Device displays OTT for manual OTT entry into NAD	Allowed	Allowed	Allowed
Software upgrade	Allowed	Optional, by using a card script by the issuer	Optional

Annex A
(informative)

Example flows for PIN verification in eCommerce

A.1 General

This Annex illustrates various PIN-flow topologies:

— offline, where the PIN is processed locally by the cardholder's IC card

  — using an FSPED (see Figure A.1 or A.4) or ISO 9564-1 compliant PED (see Figure A.4) via an acquirer,

  — using an FSPED via an issuer (see Figure A.3), and

  — using an ICCPED (see Figure A.2);

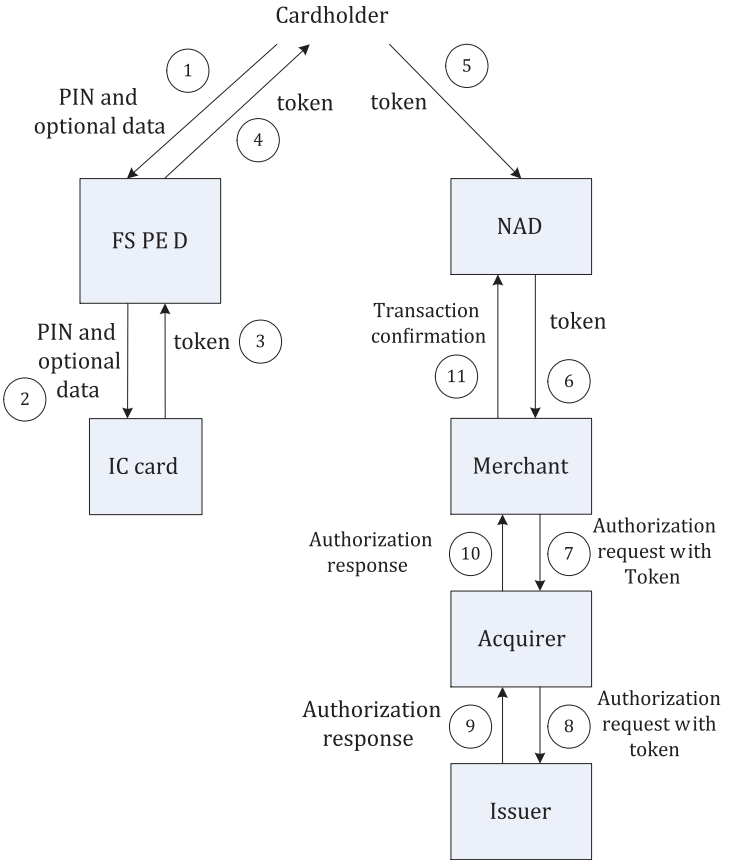
— online, where PIN is sent to the issuer for verification

  — where there is a cryptographic relationship between the PED and an acquirer (see Figure A.5), and

  — where there is a cryptographic relationship between the PED and the issuer (see Figure A.6).

A.2 PIN entry with OTT generation

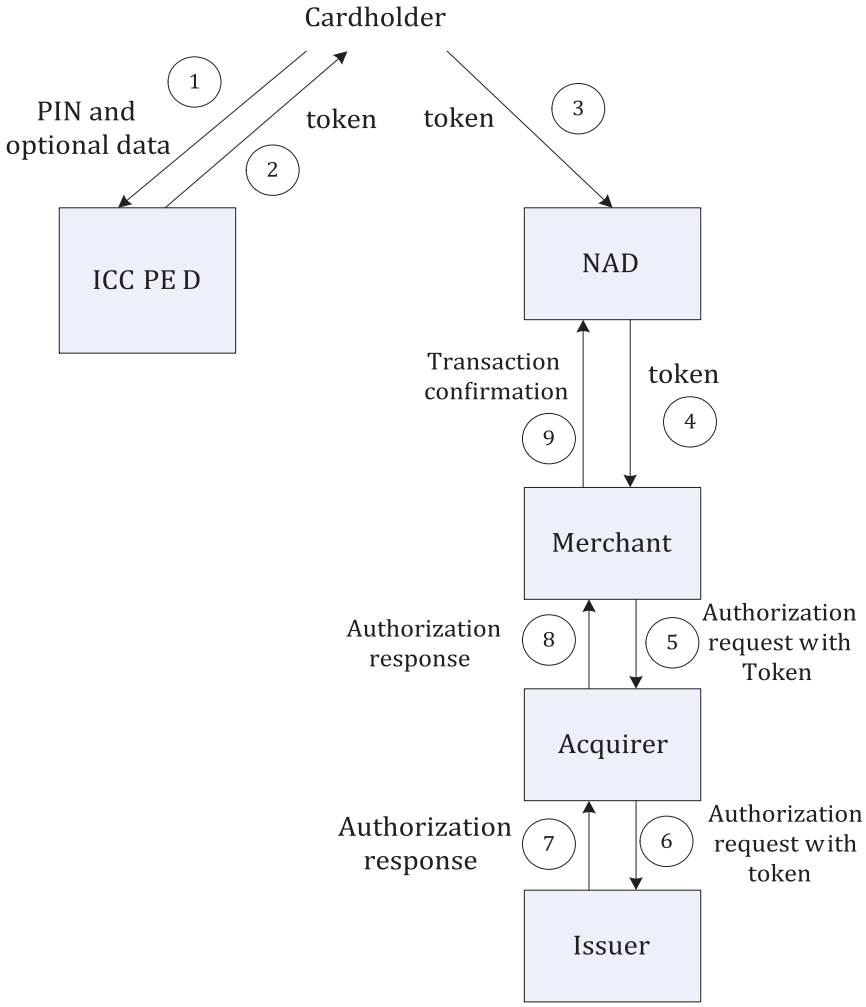
Figure A.1 shows a scenario where the cardholder's IC card is inserted into an FSPED, into which the PIN is then entered, and produces an OTT that the consumer enters into their NAD.



NOTE Optional data can include transaction amount and/or target account.

Figure A.1 — PIN entry with OTT generation (FSPED)

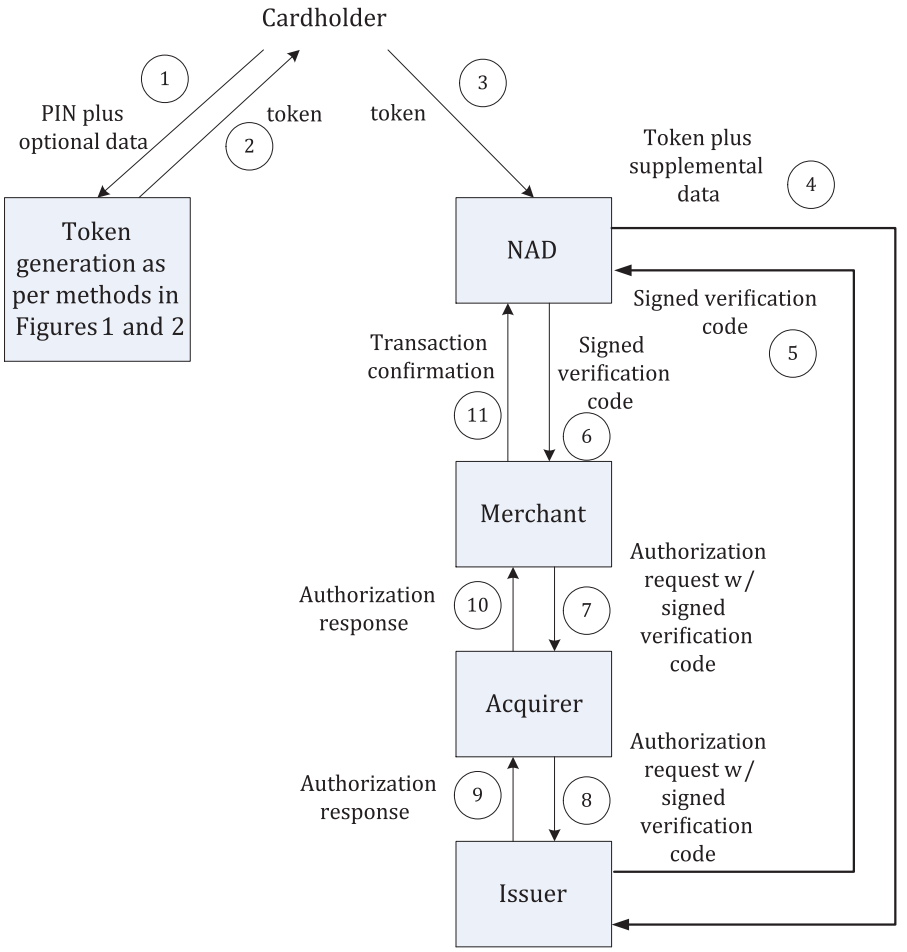
In this case, the IC card is inserted into an FSPED. The cardholder enters their PIN into the FSPED, the PIN is verified by the IC card, and the response is sent back to the FSPED, which displays an OTT (typically a string of digits) as a response for input as part of their eCommerce transaction. The OTT is transmitted to the merchant in the online session and the merchant proceeds with a payment transaction that uses the OTT received from the cardholder. This may be a two-step process where as the first step the OTT is sent to the issuer (via the acquirer) and when a confirmation comes back from the issuer, the second step is the authorization request or it could be a one-step process where the OTT is combined with the authorization request. Only the one-step process is represented in Figure A.1.



NOTE Optional data can include transaction amount and/or target account.

Figure A.2 — PIN entry with OTT generation (ICCPED)

The cardholder enters their PIN into the keypad of their ICCPED, the PIN is verified by the ICCPED, and the response OTT is displayed by the ICCPED for input as part of their eCommerce transaction. The OTT is transmitted to the merchant in the online session and the merchant proceeds with a payment transaction that uses the OTT received from the cardholder. This may be a two-step process where as the first step the OTT is sent via the acquirer to the issuer and when a confirmation comes back from the issuer, the second step is the authorization request or it could be a one-step process where the OTT is combined with the authorization request. Only the one-step process is represented in Figure A.2.



NOTE Optional data can include transaction amount and/or target account.

Figure A.3 — OTT generation with direct issuer OTT verification

This flow is similar to the flows shown in Figures A.1 and A.2, except that the OTT is sent directly from the cardholder's NAD to the issuer for verification. If the verification is successful, the issuer returns a signed verification code to the cardholder's NAD. This code is then presented to the merchant, who verifies the digital signature of the code and forwards it in the authorization request message through the acquirer to the issuer.

Note 3-D Secure can be mapped to this flow.

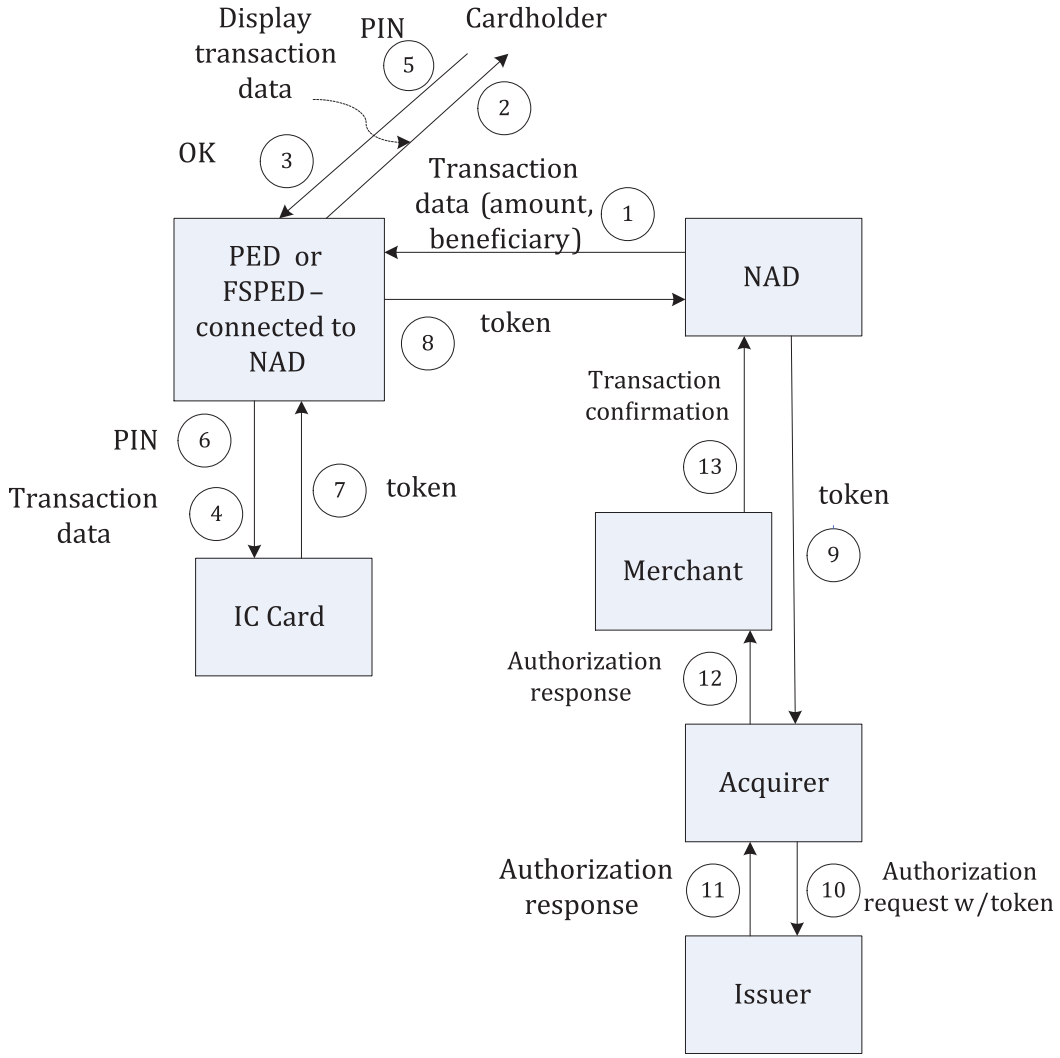


Figure A.4 — Cardholder verification with transaction data in OTT

In this case, the cardholder provides their PIN to the PED or FSPED. The PIN is cryptographically combined with transaction data such as amount and beneficiary to form an OTT (e.g. a MAC is created with an IC card specific key that the issuer can also derive). The issuer is then able to verify that the PIN was entered correctly by validating the OTT together with the transaction data.

There can be variations in this pattern in regards to how the PED or FSPED receives the transaction data from the NAD, as well as whether the PIN is entered before or after the transaction data has been transmitted from the NAD to the PED or FSPED. The arrow from the consumer to the NAD indicates the cardholder confirming the transaction data. Additionally, the IC card may generate a larger authentication value that the PED or FSPED truncates/formats to produce the OTT that is forwarded through the rest of the transaction.

A.3 Online PIN verification with an ISO 9564-1 compliant PIN entry device

Figure A.5 shows an example flow where an ISO 9564-1 compliant PED is used for PIN entry in an eCommerce setting.

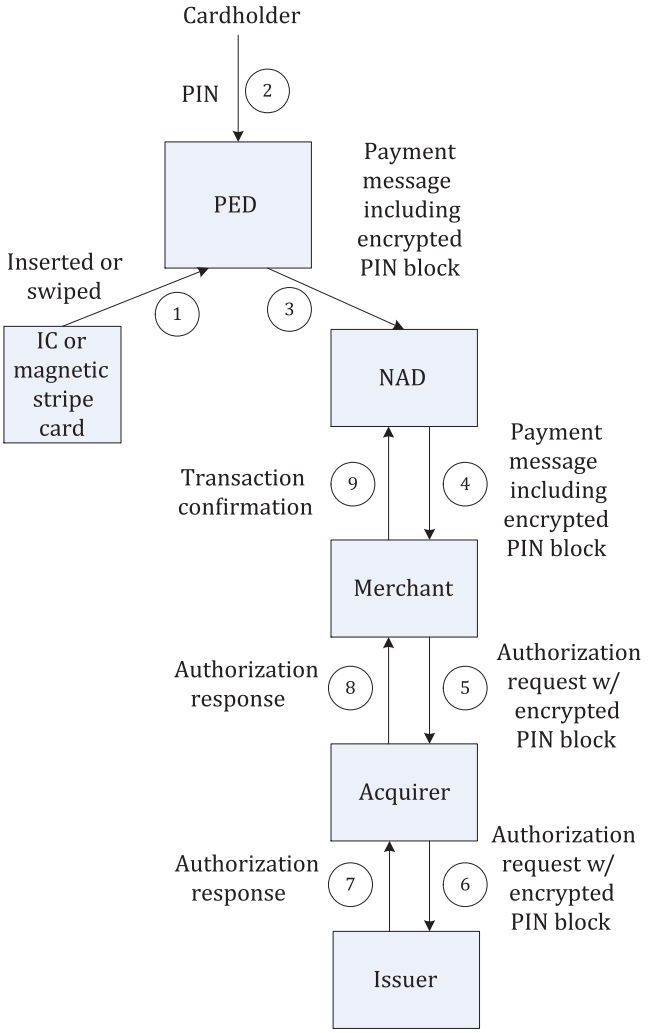
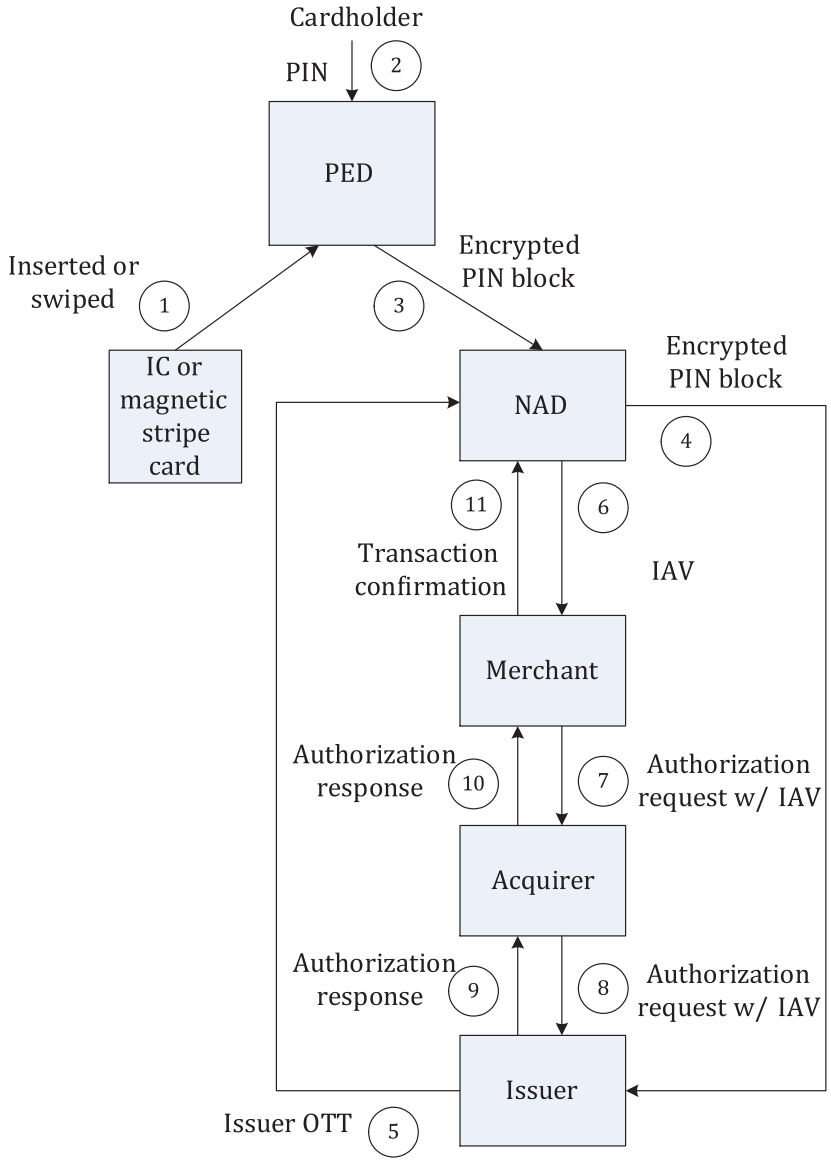


Figure A.5 — Online PIN verification with ISO 9564-1 compliant PED

After the NAD has initiated the payment transaction with the PED, the cardholder inserts or swipes their card into the PED, which is a private-use ISO 9564-1 compliant PED, connected in this case to the NAD. The NAD could be a personal device or at a public place. The cardholder enters their PIN and the PED creates an encrypted PIN block, which is sent from the PED to the NAD, from where it is forwarded to the online merchant that sends it via their acquirer to the card issuer as a conventional point-of-sale payment transaction with PIN. Once the authorization response comes back from the issuer, the merchant can make a decision and confirm or decline the transaction to the cardholder in the online session.

A.4 Online PIN verification with a direct keying relationship between PED and issuer

Figure A.6 shows an example flow where there is a direct keying relationship between an ISO 9564-1 compliant PED and the consumer's card issuer.



NOTE The encrypted PIN block travels from the NAD to the issuer directly when the issuer has a keying relationship with the PED.

Figure A.6 — Online PIN verification with a direct keying relationship between PED and issuer

After the NAD has initiated the payment transaction with the PED, the cardholder inserts or swipes their card and enters their PIN into the PED. The PED in this case has a direct relationship to the card issuer, meaning that the PED contains a cryptographic key known to the issuer. For this reason, when the NAD receives the encrypted PIN block from the PED, it can send it directly to the issuer. The issuer performs PIN verification and returns a confirmation that the PIN was correct, in the form of an issuer authentication value (IAV). This IAV is sent back to the merchant via the NAD. After receiving the IAV, the merchant makes a transaction decision and proceeds with a normal authorization request.

Bibliography

[1] ISO/IEC 7810:2003, *Identification cards — Physical characteristics*

[2] ISO/IEC 7811 (all parts), *Identification cards — Recording technique*

[3] ISO/IEC 7812-1, *Identification cards — Identification of issuers — Part 1: Numbering system*

[4] ISO/IEC 7812-2, *Identification cards — Identification of issuers — Part 2: Application and registration procedures*

[5] ISO/IEC 7813:2006, *Information technology — Identification cards — Financial transaction cards*

[6] ISO/IEC 7816-1:2011, *Identification cards — Integrated circuit cards — Part 1: Cards with contacts — Physical characteristics*

[7] ISO 13491-1, *Banking — Secure cryptographic devices (retail) — Part 1: Concepts, requirements and evaluation methods*

[8] ISO/IEC 18328-1, *Identification cards — ICC-managed devices — Part 1: General framework*

[9] ISO/IEC 18328-2, *Information technology — ICC-managed devices — Part 2: Physical characteristics and test methods for cards with devices*

[10] ISO/IEC 18328-3, *Identification card — ICC-managed devices — Part 3: Organization, security and commands for interchange*

ICS 35.240.40

Price based on 14 pages