D.X.1 Terminal parameters and features

Updated: 22.05.2026

This appendix specifies how the terminal should handle the Dankort application on the card, e.g. on a Visa/Dankort or a Mastercard Dankort. The handling of Visa and Mastercard applications is out of scope of this document. Please refer to the scheme rules from Visa and Mastercard.

Table of contents

1 Revision history

Version	Section	Change
22.05.2026	2.4	Added section with requirements concerning deferred authorization
	3	Obsolete section on magnetic stripe transactions removed
14.10.2025	2.1.2 + 5.1.1-2	Obsolete keys removed
	5.3	Added requirements concerning quasi-cash
16.05.2025	7.1	Clarify that overriding the choice must be done according to the description in 7.2
31.01.2025	2.3	Reorganized to remove redundancies
	2.3.5	Requirements for Late Amount Transactions changed and more detail added
	7	Added that requirements for contactless application selection don't apply to ATM
	7.2	Changed step 3 in table
31.05.2024	7.2	Heading changed (requirements are only for contactless). Cleanup empty row in table 7.2.
	7.1	Extended to also cover contact transactions
31.01.2024	7	Removed "in effect" date, since date is passed
	7.2	Added a single tap alternative method of offering cardholder application selection
31.08.2023	2.1.1	Update of table with listing of device types and AIDs
	3 and 4	BIN lists replaced with a reference to BIN lists on the TRG portal
	3.1	Added that Mastercard Dankort cannot be used for Dankort magstripe transactions
28.04.2023	2.1.2 and 5.1.2	Prod key with idx 1 removed (expired). Expiry for key with idx 2 changed 2023-12-31 -> 2024-12-31, and key with idx 3 changed 2030-12-31 -> 2031-12-31.
	6.1	Removed paragraph regarding double tap for mobile payments, not relevant any more.
31.01.2023	2.1.1 and 2.2.x	AID x4712 also used by single badge Dankort and for cards (i.e. non-mobile). Added section 2.2.2 with parameters for this AID.
	2.3.2	Added application version (03 00)
	6.1	Removed table 1 in section 6.1 (specific to ISO and is documented in that spec), incl. references
	7	Added new section with requirements for contactless application selection
31.03.2022	2.3.2	TAC – Denial, TAC – Online and TAC – Default for AID 4712 were incorrectly specified. Corrected values are set to match other AIDs.
31.01.2022		Add revision history Add table of contents Modify introductory text

		Correct "CA Public Key Check Sum" for test key with index 6
		Remove section in "Strong Customer Authentication (SCA) Request" about "new SCA rules" (the rules are no longer new) Remove "Action when cashback" and "Action when manual cash" from contact (special rules no longer relevant)

2 Chip-based Transactions

2.1 Common Data for Contact and Contactless Transactions

2.1.1 Application Identifiers (AIDs)

A terminal accepting contact and contactless chip transactions for Dankort must support the following AIDs:

- A000000121 1010
- A000000121 4711
- A000000121 4712
- A000000121 4713

Device type	Interface	Card Product		
		Dankort	Visa/Dankort	Mastercard Dankort
Physical card	Contact and Contactless	A000000121 1010 A000000121 4712	A000000121 4711 A000000121 4712	A000000121 4713
Mobile	Contactless	A000000121 4712	A000000121 4712	A000000121 4712

Parameters and functionality defined per AID is given below.

2.1.2 Certification Authority Public Keys (CA Public Keys)

An offline-capable terminal must support the following CA Public Keys:

Environment	CA_{PK} Index	Key length	Expiry Date	Remarks
TEST	6	1984	Expiration of CA Public Keys not enforced in the TEST environment	
PROD	3	1986	2031-12-31	May be extended

Key values are listed in section 4.

2.2 Contact Transactions

2.2.1 Miscellaneous (AID = A000000121 1010 and A000000121 4711)

AID	Parameter	Value	Remarks
A000000121 1010 -OR- A000000121 4711	General		
	Application Version	00 8C (or higher)	140 decimal (VIS 1.4.0)
	Default DDOL	9F3704	
	Terminal Action Codes		
	TAC – Denial	00 10 00 00 00	See section 4.2

	TAC – Online	FC 40 BC F8 00	
	TAC - Default	FC 40 A4 A8 00	
	Limits		
	Floor Limit	DKK 0.00	
	Transaction limit	DKK 100,000.00	
	Random Transaction Selection		
	Threshold Value for Biased Random	DKK 0.00	
	Target Percentage for Random Selection	0	
	Maximum Target Percentage for Random Selection	0	
	Special Transactions		
	Action when fallback	Online	

2.2.2 Miscellaneous (AID = A000000121 4712)

AID	Parameter	Value	Remarks
A000000121 4712	General		
	Application Version	03 00	
	Default DDOL	9F3704	
	Terminal Action Codes		
	TAC – Denial	00 10 00 00 00	See section 4.2
	TAC – Online	FC 40 BC F8 00	
	TAC - Default	FC 40 A4 A8 00	
	Limits		
	Floor Limit	DKK 0.00	
	Transaction limit	DKK 100,000.00	
	Random Transaction Selection		
	Threshold Value for Biased Random	DKK 0.00	
	Target Percentage for Random Selection	0	
	Maximum Target Percentage for Random Selection	0	
	Special Transactions		
	Action when fallback	Online	

2.2.3 Miscellaneous (AID = A000000121 4713)

AID	Parameter	Value	Remarks
A000000121 4713	General		
	Application Version	00 02	
	Default DDOL	9F3704	
	Terminal Action Codes		
	TAC – Denial	00 10 00 00 00	See section 4.2
	TAC – Online	FC 40 BC F8 00	
	TAC - Default	FC 40 A4 A8 00	
	Limits		
	Floor Limit	DKK 0.00	
	Transaction limit	DKK 100,000.00	
	Random Transaction Selection		
	Threshold Value for Biased Random	DKK 0.00	
	Target Percentage for Random Selection	0	
	Maximum Target Per-centage for Random Selection	0	
	Special Transactions		
	Action when fallback	Online	

2.3 Contactless Transactions

2.3.1 AID A000000121 1010 and A000000121 4711

AID	**Parameter**	**Value**	**Remarks**
A000000121 1010 and A000000121 4711	Application Version	00 8C (or higher)	140 decimal (VIS 1.4.0)
	Default Kernel ID	03	
	Default TTQ	36 20 40 00	Certain positions depend on the actual terminal type

2.3.2 AID A000000121 4712

AID	**Parameter**	**Value**	**Remarks**
A000000121 4712	Application Version	03 00	
	Default Kernel ID	05	
	TAC – Denial	00 10 00 00 00	See section 4.2
	TAC – Online	FC 40 BC F8 00	
	TAC - Default	FC 40 A4 A8 00	

2.3.3 AID A000000121 4713

AID	Parameter	Value	Remarks
A000000121 4713	Application Version	00 02	
	Default Kernel ID	02	
	TAC – Denial	00 10 00 00 00	See section 4.2
	TAC – Online	FC 40 BC F8 00	
	TAC - Default	FC 40 A4 A8 00	

2.3.4 Amount limits

Parameter	Value	Remarks
Floor Limit	DKK 0.00	
CVM Limit	DKK 350.00	
Transaction limit	DKK 100,000.00	

2.3.5 Late Amount Transactions

The table below outlines requirements in use cases where the amount is adjusted during the payment.

Use case	Required action	Remarks
The final authorization amount is less than the original amount displayed to the cardholder	Online	Amount confirmation optional
The final authorization amount is greater than the original amount displayed to the cardholder	Final amount below CVM limit or CVM exempted: Online + Confirm Final amount above CVM limit and CVM not exempted: Online + CVM	
The final authorization amount is different than the original amount, but an original amount was not displayed to the cardholder	Final amount below CVM limit or CVM exempted: Online Final amount above CVM limit and CVM not exempted: Online + CVM	

2.4 Deferred authorization

Terminals that lose connectivity are permitted to defer authorizations for a period of up to 7 days. The terminal must at reasonable intervals automatically check if connectivity can be reestablished. Deferred authorizations must be flagged according to Nets interface specifications.

3 Dankort BIN lists

Dankort BIN lists are available on Nets TRG Portal. To obtain access to the portal, contact trg-portal@nets.eu. The portal will automatically send notifications on updates. Consider registering with a department email, so that notifications are not disrupted by staff changes.

4 Detailed Data Elements

4.1 CA Public Keys

4.1.1 CA Public Keys – TEST Environment

Dankort TEST	CA_{PK} Index 06 – 1984 bit
RID	A000000121
CA Public Key Index	06
CA Public Key Modulus	C5 C3 E0 0F E0 96 D3 96 16 E2 CB 39 E9 DB E4 59 FF F1 DF F1 A3 33 DD 37 4B 3F D2 35 1D 49 77 32 8B 8B 14 F1 13 EC B0 65 04 0A 2A CC 28 F2 C4 D1 95 0D 11 4C 4F C3 59 0E C2 F9 33 CE 5C 35 09 AC 0D C7 B2 3F 90 9F C6 38 FA B3 A1 18 3B A6 B7 FD EC 73 14 24 77 D5 3E 42 23 3C 35 D8 2B F7 A4 B5 34 12 E2 50 CF 40 00 28 CB 0F A3 C8 EF E5 E7 3E 46 56 D1 D6 B6 97 E8 C7 B8 05 11 23 56 C3 B4 74 B1 E4 BD 1F 61 4F 03 66 96 84 2A AD C1 51 E3 D5 74 36 47 74 90 23 A3 D8 CF 31 67 6B 2F A1 D4 E0 12 27 E9 4B 7B 92 6C 50 67 36 BD 2A 36 60 48 B1 6E 8D 9B F6 CC 10 CD 03 E1 8B D7 BD CD D0 EC E8 79 38 AD 52 86 28 A9 4F 15 CD 22 F5 37 C1 13 CA 86 6C 19 91 6D 06 4F 2F 4C 3F 62 33 F4 5A 47 D1 5A 55 A6 8F 33 63 22 5E 9D 25 E9 CB 31 D6 43 98 DE BC 16 27 1B 4F 78 E7
CA Public Key Exponent	3
CA Public Key Check Sum (SHA-1 Hash)	BE 32 F4 25 B7 10 78 B7 D3 2D 54 AF CD 02 67 79 14 BC 43 46

4.1.2 CA Public Keys – PRODUCTION Environment

Dankort PROD	CA_{PK} Index 3 - 1984 bit
RID	A000000121
CA Public Key Index	3
CA Public Key Modulus	B8 26 DC A2 1E 3F 79 1D D8 A1 62 AC 1B 55 14 31 38 2A C1 BB C1 B0 15 B4 30 8C 2A A6 D5 4E 66 BC 38 5E DD C8 D5 B8 7F 08 0C 56 2F 8D 2D 8F DB 13 EA 16 8F EE 1A 7A E0 23 4B C4 CC 10 53 5B 81 FF 68 97 4A 9D 12 CA C2 AE 64 AB 8C EF F1 DD FB 44 3A F4 31 AC E3 DB B8 17 E4 59 52 47 29 87 87 23 9C DF 5B E4 1E AB A4 7D C2 65 A9 DD 56 63 0C F6 E3 EA 4A 8C C3 9D A3 84 A7 73 47 36 BB 97 C7 0F 7E 9A D8 FA 35 36 4E 99 F9 71 E7 D9 5C 49 1C A2 7C CC E8 1A A8 DD ED 01 14 02 B1 4F 66 45 A7 52 8F CE 55 69 4E 1C 63 59 BE 66 CC 73 04 7C EF 53 C9 E7 B5 29 D5 37 BD 42 E3 E7 02 8D 9B 68 8B 59

	26 97 6E 4F FA DF 26 BA E1 CA 50 21 FA 40 F7 DD 02 38 7D F0 2E D6 8C B0 07 40 DA 3B DC CC F5 48 72 E6 E4 3D 24 60 EC 56 34 1F FC F3 07 63 A8 C7 AD C7 77 C9 BB 77 19 55
CA Public Key Exponent	3
CA Public Key Check Sum (SHA-1 Hash)	CE EA 8B 63 58 5F 25 60 00 91 F5 D8 F1 22 A1 71 9F F0 B1 32

4.2 Dankort Terminal Action Codes (TAC)

Byte	Bit	Meaning	TAC-Denial	TAC-Online	TAC-Default
1	8	Offline data authentication was not performed	0	1	1
	7	Offline static data authentication (SDA) failed	0	1	1
	6	ICC data missing	0	1	1
	5	Card appears on terminal exception file	0	1	1
	4	Offline dynamic data authentication (DDA) failed	0	1	1
	3	Combined DDA/AC Generation (CDA) failed	0	1	1
	2	Static data authentication (SDA) selected	0	0	0
	1	RFU	0	0	0
2	8	ICC and terminal have different application versions	0	0	0
	7	Expired application	0	1	1
	6	Application not yet effective	0	0	0
	5	Requested service not allowed for card product	1	0	0
	4	New card	0	0	0
	3…1	RFU	0	0	0
3	8	Cardholder verification was not successful	0	1	1
	7	Unrecognized CVM	0	0	0
	6	PIN Try Limit exceeded	0	1	1
	5	PIN entry req. and PIN pad not present or not working	0	1	0
	4	PIN entry req., PIN pad present, but PIN was not entered	0	1	0
	3	Online PIN entered	0	1	1
	2…1	RFU	0	0	0
4	8	Transaction exceeds floor limit	0	1	1
	7	Lower consecutive offline limit exceeded	0	1	0
	6	Upper consecutive offline limit exceeded	0	1	1
	5	Transaction selected randomly for online processing	0	1	0

Byte	Bit	Meaning	TAC-Denial	TAC-Online	TAC-Default
	4	Merchant forced transaction online	0	1	1
	3…1	RFU	0	0	0
5	8	Default TDOL used	0	0	0
	7	Issuer authentication was unsuccessful	0	0	0
	6	Script processing failed before final GENERATE AC	0	0	0
	5	Script processing failed after final GENERATE AC	0	0	0
	4…1	RFU	0	0	0

4.3 Quasi Cash

For quasi cash transactions, transaction type 0 should be used, except if it is contact mode and the card is AID 4711 (Visa). The same transaction type should be used both towards the card and the chip data (tag 9A) sent in the authorization.

Note that quasi cash transactions cannot be noCVM.

5 Strong Customer Authentication (SCA) Request

5.1 General

Whether SCA is required or not for an online No CVM transaction is handled by the Nets host for physical cards and in the mobile device for wallets/apps.

If SCA is required, the terminal will (as usual) send an online No CVM Request to the Nets host. The host will return a specific code (Action Code) to the terminal/merchant i.e. SCA is required and this request is therefore declined by the host. A subsequent second request (with PIN) shall then be created using the existing transaction data (including PIN data etc.) according to the SCA requirements.

This will give the following changes in the payment flow:

For CAT terminals without PIN-pad, the terminal must:

- Abort the transaction and start a new transaction – and
- Prompt the customer to use another interface

For CAT-terminals with PIN-pad, the terminal must:

- Prompt the customer to enter PIN and
- Continue the transaction using the existing transaction data from the first transaction, meaning – the card must not be activated again (no new tap or use of the contact interface) and no re-entry of transaction amount is required.
- The existing data from the first transaction are resend to the host with the exception that this transaction is marked as a PIN transaction and includes PIN-data.

For merchant operated terminals (with PIN-pad), the terminal must:

- Prompt the customer to enter PIN and
- Continue the transaction using the existing transaction data from the first transaction, meaning – the card must not be activated again (no new tap or use of the contact interface) and no re-entry of transaction amount is required.
- The existing data from the first transaction are resend to the host with the exception that this transaction is marked as a PIN transaction and includes PIN-data.

For transactions based on use of wallet/apps there are no changes to the payment flow.

The specific impact on contactless transactions is that contactless PIN-retry is possible. In case of an incorrect online PIN during a contactless transaction, the customer is prompted to enter the PIN again (without starting a new transaction and presenting the contactless card again).

For Dankort contactless transactions, the issuer host checks the accumulated amount for No CVM transactions. When the accumulated amount limit is exceeded, the issuer host declines the transaction and sends a response code/Action Code requesting Strong Customer Authentication.

NOTE: The host may, in the future, maintain other counters/conditions that may inhibit/initiate Strong Customer Authentication.

Dankort supports a One-Tap SCA solution. It means that when the host declines the contactless card transaction as described above, the customer shall be prompted on the terminal display to enter the PIN. It shall in general *not* be necessary to present the card again and the same request data shall be resent, except for following updated fields:

- DE11: System Trace Audit Number (STAN)
- DE37: Retrieval Reference Number

and with the following data added to the request:

- DE52: PIN data present

5.2 Terminal Capabilities Indicator

A data element shall be conveyed to the host in *all* contactless requests (Purchase and Original Authorisations) indicating whether Strong Customer Authentication is supported or not for this terminal.

The internal ISO 8583 format will be as follow:

Terminal Capabilities Indicator

Purpose: Used to indicate the host whether the terminal supports e.g. SCA or not.

Format: b1 (1 byte).

Contents: See Table 1.

Remarks: The Terminal Capabilities Indicator may indicate "SCA not supported by the terminal" if the terminal does not support a PIN Entry Device. If the Terminal Capabilities Indicator is not present (e.g. for old terminals), it is interpreted by the host as "SCA not supported by the terminal". Tag C# is defined for this data element. Example: C# 0001 01.

Table 1 – Terminal Capabilities Indicator

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
-	-	-	-	-	-	-	x	Strong Customer Authentication (SCA):
-	-	-	-	-	-	-	0	- SCA *not* supported by the terminal
-	-	-	-	-	-	-	1	- SCA supported by the terminal
x	x	x	x	x	x	x	-	RFU
NOTE:								

5.3 SCA - Exceptions

Payment Service Providers shall be allowed *not* to apply to SCA for transport fares and parking fees. The host will differentiate using the Merchant Category Code (MCC).

6 Application selection for co-badged cards

EU regulation requires that cardholders with co-badged cards have the option of selecting which application is used. The regulation also allows merchants to configure preferred payment networks (referred to as "Merchant preferred").

The below requirements do not apply to ATMs.

6.1 Merchant preferred

Irrespective of interface (contact or contactless), the terminal must allow the merchant to configure either "Dankort" as preferred, or "Domestic methods" or similar general term. Setting either must mean that the terminal selects one of the Dankort AIDs, unless the cardholder chooses to override the choice by the method described in 6.2.

6.2 Contactless cardholder selection

The terminal must offer the cardholder a way of enabling application selection mode prior to tapping the card. This could, for instance, be by pressing the yellow button on the terminal.

What the terminal must do after the card is tapped depends on whether application selection mode is enabled:

Application selection mode	Step	Action
Disabled	1	The cardholder taps card.
	2	The terminal must select merchant preferred application if set. If not set, the terminal selects application according to EMV rules.
Enabled	1	The terminal displays a list of payment networks that the merchant accepts. *OR* The cardholder taps card. The terminal displays a list of the applications on the card (using application labels, if available from the card).
	2	The cardholder selects an application/network.
	3	The terminal uses the selected application/network. The terminal may ask the cardholder to tap if there was no tap in step 1, or if the terminal has not prepared all necessary transaction data (e.g. cryptogram) during the step 1 tap.