B.X.6 Card parameters and features
Updated: 22.05.2026

Table of contents

1 Change log

Version	Change
22.05.2026	In section 3.1, CVM methods for CT, removed “Plaintext offline PIN”, “Signature if supported” and “No CVM if supported”
31.01.2023	Changed name of document to be more generic. Added section 2.4 and preface in 3 regarding virtual cards. Added header 2.2 for information on physical Visa/Dankort Changed version requirements (with italics): “EMV 2011 version 4.3 *with subsequent bulletins* and. The card must be approved by Visa according to minimum VIS 1.6.*3* (VISA Integrated Circuit Card Specification) and VCPS 2.2.*4*”
31.01.2022	Referenced version numbers of Visa and Mastercard chip specifications made “minimum” to allow for future versions. Changes to document formatting and headings. Added table of contents and change log.

	Parameters for Visa and Mastercard side of co-badged cards are not referred to as requirements, but as examples. Removed obsolete references to previously issued cards. Removed option to issue cards with old (short) keys. Consolidation of AUC-tables for Dankort, Visa/Dankort and Mastercard Dankort. Entire document translated to English. Language order changed to “da-en-sv-no” to match how current applications are configured.

2 General requirements

If the card is co-badged, then the Dankort application (AID) must not have a lower priority than the card’s other applications unless the cardholder specifically has requested this.

The Dankort application must not share data elements with other applications unless the Dankort rules in this document and the other payment network’s rules allow them to have the same value.

2.1 Physical Dankort

For a physical Dankort, one application with two interfaces (contact, CT, and contactless, CTL) must be implemented on the chip:

- Dankort application, A000000121 1010

2.2 Physical Visa/Dankort

For a physical Visa/Dankort, two applications, each with two interfaces (contact, CT and contactless, CTL), must be implemented on the chip:

- a Visa application, e.g. A000000003 1010
- a Dankort application, A000000121 4711

Solutions, where this is one application that can be used via the two AIDs, are allowed.

Data such as card number, transaction counter and offline accumulators of amount and transactions can be shared between the applications.

The chip must conform to EMV 2011 version 4.3 with subsequent bulletins. The card must be approved by Visa according to minimum VIS 1.6.3 (VISA Integrated Circuit Card Specification) and VCPS 2.2.4.

2.3 Physical Mastercard Dankort

For a physical Mastercard Dankort, two applications, each with two interfaces (contact, CT and contactless, CTL), must be implemented on the chip:

- a Mastercard application, e.g. A000000004 1010
- a Dankort application, A000000121 4713

The card numbers may be different for the two applications, e.g. 5019xxxx… for Dankort and 5xxxxxxx… for Mastercard.

Data such as card number, transaction counter and offline accumulators of amount and transactions can be shared between the applications.

The chip must conform to EMV 2011 version 4.3 (minimum). The card must be approved by Mastercard according to M/Chip Advance 1.2.x (minimum).

2.4 Virtual Dankort (all types)

For a virtual Dankort (a card virtualised to a mobile device using tokenisation) the following application must be used for the Dankort part, independently of whether the card is co-badged or not:

- a Dankort application, A000000121 4712

3 Card parameters

The following parameters are for physical cards only. Parameters for virtual cards are available in a separate document on request.

3.1 Functional chip requirements

Function	Implementation	Description
	Generation 4	
General chip setup		
Application Selection (CT)	PSE	
Application Selection (CTL)	PPSE	
Language list	da-en-sv-no	Default language preference. Issuer may choose another order.
Chip Application type	VIS 1.6.2 (min) / M/Chip Advance 1.2.x (min)	
Service Code	201	International usage, unrestricted
CVM methods: (only for CT)		
Priority 1	Online PIN if unatt. Cash / Fail	
Priority 2	Online PIN if Cashback / Go Next	
Priority 3	Enciphered offline PIN if Cashback. / Go next	
Priority 4	Plaintext offline PIN if Cashback / Fail	
Priority 5	Enciphered offline PIN if supported. / Go next	
Priority 6	Online PIN if supported / Fail CVM	

Function	Implementation	Description
	Generation 4	
CAM	DDA and CDA(CT) / fDDA(CTL)	Dankort and Visa/Dankort
	DDA and CDA(CT) / CDA(CTL)	Mastercard Dankort

Offline Risk Management		
Terminal Risk Management	For CT: The terminal executes Floor limit check and Random transaction selection. The card executes velocity checking. For CTL: The terminal executes Floor limit check and CVM limit check. The card executes velocity checking.	The card executes Card Risk Management. For CTL it is Upper Limit.
Currency table	DKK/EUR-SEK-NOK-GBP-USD	Visa/Dankort and Mastercard Dankort, known currencies
	DKK/DKK	Dankort, known currencies
Consecutive Transaction Counter Limit CTCL	0	Above this limit the card will try to send the transaction online
Consecutive Transaction Counter Upper Limit CTCUL	15	Above this limit the card will require the transaction to be sent online
Consecutive Transaction Counter International Limit CTCIL	0	Above this limit the card will try to send the transaction online (unknown currencies)
Consecutive Transaction International Upper Limit CTIUL	0	Above this limit the card will require the transaction to be sent online (unknown currencies)
Cumulative Total Transaction Amount Limit CTTAL	0	Above this limit the card will try to send the transaction online
Cumulative Total Transaction Amount Upper Limit CTTAUL	20.000	Above this limit the card will require the transaction to be sent online

Funktion	**Dankort and Visa/Dankort implementation**	**Note**
	Generation 4	
Accumulated amount limit - VLP Funds Limit	800	Card must go online (CTL) when the accumulated amount exceeds this limit
Offline PIN try limit	3	
PIN Action if above offline try limit	Go online / if not possible decline	
Issuer-to-Card script processing	Optional (CT)	

3.2 Dankort - Application Usage Control (AUC)

These card parameters tell the terminal which types of transactions the card may perform (code 1 = Yes, 0= No).

Service	**Dankort and Visa/Dankort**		**Mastercard Dankort**	
	CT	CTL	CT	CTL

Valid for domestic cash transactions	1	1	1	1
Valid for international cash transactions	1	1	1	1
Valid for domestic goods	1	n/a	1	1
Valid for international goods	1	n/a	1	1
Valid for domestic services	1	n/a	1	1
Valid for international services	1	n/a	1	1
Valid for ATMs	1	n/a	1	1
Valid for terminals other than ATMs	1	n/a	1	1
Domestic cashback allowed	1	1	1	1
International cashback allowed	1	1	1	1

3.3 Data elements in ARQC/AAC/TC

Input data for validation by the processing system.

Data elements in ARQC/AAC/TC	**Dankort and Visa/Dankort**		**Mastercard Dankort**	
	Data from terminal	Data from card	Data from terminal	Data from card
Amount, Authorised (numeric)	X		X	
Amount Other (numeric)	X		X	
Terminal Country Code	X		X	
Terminal Verification Results	X		X	
Transaction Currency Code	X		X	
Transaction Date	X		X	
Transaction Type	X		X	
Unpredictable Number	X		X	
Application Interchange Profile		X		X
Application Transaction Counter		X		X
Card Verification Results		X		X
Issuer Application Data		X		X
Last Online ATC		n/a		X

3.4 Issuer Action Codes (IAC)

Each condition (bit) has the following possible codes:

- Ignore Denial=0, Online =0, Default=0
- Try online Denial=0, Online =1, Default=0
- Require online Denial=0, Online =1, Default=1
- Decline Denial=1, Online =0, Default=0

Card Verification Results, CVR: Internal card register which stores information about a transaction risk assessment.

Issuer Action Codes, IAC: Card parameters that sets the issuer's preferences with regard to offline transactions and sending transactions online after the terminal has made risk assessment.

Card Verification Results (CVR)	Issuer Action Codes (IAC)	Note
	Generation 4	
Data Authentication was not performed	Require online	
ICC Data missing	Require online	
Card appears on terminal exception file	Require online	Terminals do not have exception files
DDA failed	Require online	Terminal could not determine card authenticity
CDA failed	Require online	Terminal could not determine card authenticity
Chip card and terminal have different application versions	Ignore	
Expired application	Require online	
Requested service not allowed for card product	Require online	
New card	Ignore	Card will automatically go online at first use
Transaction exceeds floor limit	Require online	
Lower consecutive offline limit exceeded	Ignore	
Upper consecutive offline limit exceeded	Ignore	
Transaction selected randomly for online processing	Try online	
Merchant forced transaction online	Try online	Determined by merchant as it is per merchant request
Default TDOL used	Ignore	Default TDOL not used
Issuer authentication was unsuccessful	Ignore	Not necessary since the card will request ARPC in CDOL2 ('9108') and will fail if the ARPC cannot be verified (with the exception of 8 x 00h which means that there was no ARPC from the host, which will cause an approved transaction since the card is configured for "partial grade").
Script processing failed before final Generate AC	Ignore	Script is no longer critical for current transaction
Script processing failed after final Generate AC	Ignore	Script is no longer critical for current transaction

3.5 Dankort Public Key

Dankort PROD	**CA_{PK} Index 3 - 1984 bit**
Key ID	SIGRSAP1.CADK.5019.P1984003
RID	A000000121

Service Identifier	10100000
CA Public Key Index	3
Expiration (YYMM)	1228
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