

2008-11-17 131674903-08/111

**SKVFS 2009:y**  
**Cash registers**  
Published on  
xx month 2009  
Reprint

## **Code of Statutes of the National Tax Board**



ISSN 1652-1420

---

### **Regulations of the National Tax Board amending the regulations of the National Tax Board on control units for cash registers;**

adopted on xx month 2009.

The National Tax Board lays down the following based on Section 1 of the Act (2007:597) on cash registers with respect to the regulations of the National Tax Board (SKVFS 2008:y) on control units for cash registers<sup>1</sup>

Chapter 3 Section 6 and Chapter 11 Section 1 shall read as follows, 35 new paragraphs, Chapter 13 Section 11, Chapter 14 Sections 7-40, which read as follows, shall be introduced

immediately preceding Chapter 14 Sections 7, 11, 19 and Section 37, new intermediate headings which read as follows shall be introduced,

immediately preceding Chapter 14 Sections 18, 19, 29, and Section 34, new subheadings which read as follows shall be introduced.

The regulations shall thus read as follows from the day on which these regulations enter into force.

<sup>1</sup> The notification was made in accordance with Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations (OJ L 204, 21.7.1998, p. 37, Celex 398L0034), as amended by Directive 98/48/EC of the European Parliament and of the Council (OJ L 217, 5.8.1998, p. 18, Celex 398L0048).

## Chapter 1 Area of application

1. The regulations of the National Tax Board of Sweden on the requirements for cash registers (SKVFS 2008:x) contain provisions on requirements regarding cash registers as referred to in the Act (2007:592) on cash registers. The stipulations on the requirements imposed on cash registers state that a cash register must be connected to a control unit integrated in the system. These regulations include specific stipulations concerning the control unit.

## Chapter 2 Definitions

1. *Company* in these regulations means the party bearing the responsibility as per Section 2 of the Act (2007:592) on cash registers. *Registration* in these regulations means that sales and other day-to-day information have been handled with respect to a cash register so that the information can be included in the Z daily report.

2. *Control slip* and *log/journal memory* in these regulations have the same meaning as outlined in Section 7 of the Act (2007:592) on cash registers.

3. *Receipt data* in these regulations means information that is read from the cash register to a control unit.

4. *Receipt control data* in these regulations means that part of the receipt data that provides the basis for generating the control data and the control code.

5. *Control data* in these regulations means the receipt control data and internal data that is stored in a control unit. Only the National Tax Board shall have access to the control data in a control unit.

6. *Control code* in these regulations means the unique code identifying the cash register receipts.

7. *Receipt type Normal* in these regulations means the cash register receipt and return receipt as per Sections 8 and 2 of the National Tax Board regulation on the requirements imposed on cash registers (SKVFS 2008:x).

8. *Receipt type Copy* in these regulations means a cash register receipt and return receipt as per Sections 8 and 2 of the National Tax Board regulation on the requirements imposed on cash registers (SKVFS 2008:x).

9. *Receipt type Practice* in these regulations means a practice receipt as per Section 2 of the regulations of the National Tax Board on the requirements on cash registers (SKVFS 2008:x).

10. *Receipt type Profo* in these regulations means a pro forma (advance) receipt as per Section 2 of the National Tax Board

regulation concerning the requirements imposed on cash registers (SKVFS 2008:x).

**SKVFS 2009:y**

**11.** *Serial number* in these regulations means a unique number composed of 17 alphanumeric characters, which identify the control unit and its manufacturer. The first five characters shall uniquely identify the manufacturer. These shall be followed by twelve characters, which uniquely identify the control unit.

**12.** *Version number* in these regulations means the unique identification of the software version, and the said number changes each time the software changes.

*Revision number* in these regulations means the unique identification of the hardware version, and the said number changes each time the hardware changes.

**13.** *Manufacturer* in these regulations also refers to subcontractors to the manufacturer.

*Production environment* in these regulations refers to the entire process from the development of the control unit to the manufacturing of the control unit.

### **Chapter 3 General requirements on a control unit**

1. A control unit shall fulfil the requirements set out in these regulations.
2. A control unit shall include only the functions set out in these regulations. Additional functions may be included should they be necessary to ensure compliance with the requirements stated in these regulations.
3. Should an accessory/fitting or some other piece of equipment be connected to a cash register, this shall be done so that no changes are made to a control unit.
4. A control unit must be so constructed that it can remain functioning at the company's facilities at the same time that it transmits control data to the National Tax Board in the manner set out in Chapter 10.
5. A control unit must not write over or erase the control data. However, control data older than five years may be written over or erased. The same applies to the updating of the necessary parts of the internal data.
6. A control unit shall at least be provided with information on
  - model name
  - serial number and version number of the software
  - revision number of the hardware
  - name of the body that certified the control unit
  - designation of the certificate
  - regulations of the National Tax Board (SKVFS 2008:y) on

control units for cash registers.

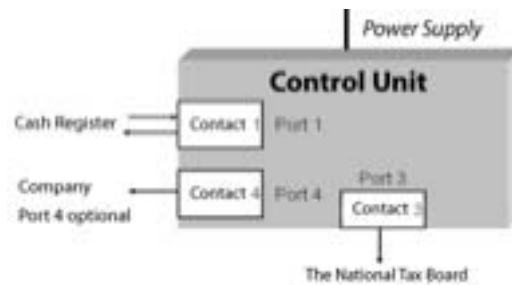
**SKVFS 2009:y**

## Chapter 4 Different types of control units

1. A control unit shall be of the type A, B or C as laid down in this chapter.

### *Type A control unit*

2. A type A control unit shall be provided with ports and contacts as shown in the following diagram.



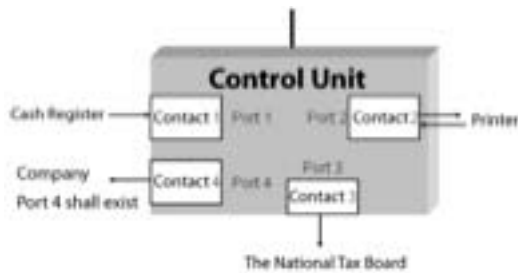
Power supply	
Control unit	
Cash register	
Company Port 4 optional	
Contact 1	
Port 1	
National Tax Board	

3. A type A control unit shall be able to receive receipt data from a cash register via Port 1. It then sends back a control code to the cash register via Port 1. It shall have a log memory that can be read via Port 4.

### *Type B control unit*

4. A control unit of type B shall have ports and contacts as shown in the following diagram.

**SKVFS 2009:y**

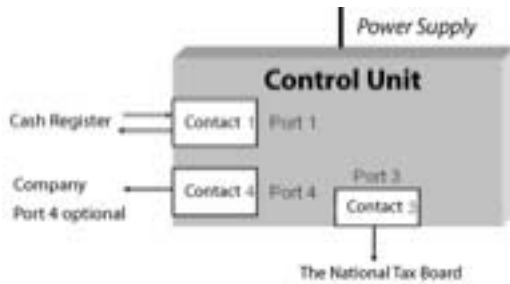


Power supply	
Control unit	
Cash register	
Company Port 4 shall exist	
Contact 1	
Port 1	
Printer	
National Tax Board	

5. A type B control unit shall be able to receive receipt data from a cash register via Port 1. It shall have a log memory that can be read via Port 4. Receipts are printed via Port 2.

*Type C control unit*

6. A type C control unit shall have ports and contacts as shown in the following diagram.



Power supply	
Control unit	
Cash register	
Company Port 4 optional	
Contact 1	
Port 1	
National Tax Board	

**SKVFS 2009:y** 7. A type C control unit shall be able to receive receipt data from more than one cash register. It shall also be able to receive receipt data from more than one of a company's registers as per Section 20 of the National Tax Board's Regulations (SKVFS 2008:x) on the requirements regarding cash registers.

8. A type C control unit shall receive receipt data via Port 1. It then sends back a control code to the respective cash register via Port 1. It shall have a log memory that can be read via Port 4.

## Chapter 5 Interface and clock

### *Logistical interface (ports)*

1. The ports of a control unit shall transmit data only as indicated in the following table and only in the stipulated direction.

Port	Interface to	Permitted data
Port 1	Cash register	Input: - Receipt data or other data needed to be printed out - Queries about printer status Output: - Printer status - Control code
Port 2	Printer	Input: - Printer status Output: - Receipt data incl. control code or other data needed to be printed out
Port 3	National Tax Board	Output: - Control data
Port 4	Company	Output: - Log memory

### *Port-specific functions*

2. Port 2 shall only be provided for type B control units.

### *Physical interface (contacts)*

3. The following applies to contacts.

Contact 1: Located in front of Port 1. To be used for power supply.

Contact 2: Located in front of Port 2.

Contact 3: Located in front of Port 3 and constructed for the Secure Digital (SD) type of standard, which serves as a data file storage facility under the FAT16 or FAT32 file system.

Contact 4: This is located in front of Port 4.

**SKVFS 2009:y**

4. A control unit shall be provided with communications protocol in which the data formats for Port 1, Port 2 and Port 4 are defined.

5. The installation of Port 1 and Port 2 need to be configured during production.

The configuration parameters, which need to be set in connection with the hardware solution (post-production), are speed, bits, stop-bits and parity along with printer settings and communications protocol.

#### *Power supply*

6. A control unit shall have its own power supply if no power supply can be arranged via the connected cash register.

#### *Clock*

7. A control unit shall have a real-time clock which shows the date and time of day according to standard Swedish time.

### **Chapter 6                      Receipt data provided by a cash register and generation of receipt control data**

1. A control unit shall receive and process receipt-specific data from the cash register.

2. A control unit shall interpret and process receipt data before presenting receipt control data.

3. The necessary internal data contained by a control unit shall be updated with respect to each record of receipt data that a control unit reads in.

4. The receipt control data shall comprise the following receipt data sections.

<b>Data</b>	<b>Description</b>	<b>Format</b>
Date and time	Date and time of the day as per the sale transaction Section 28c, SKVFS 2008:x	12 numerals, format YYYYMMDDhhmm
ID code	Company's corporate ID code or personal ID code as per Section 28a, SKVFS 2008:x	10 numerals
Cash register marking	Cash register marking as per Section 10, SKVFS 2008:z	At maximum 16 alphanumeric characters
Run number	Run number as per	At maximum 12 numerals

**SKVFS 2009:y**

	Section 28d, SKVFS 2008:x	
Receipt type	Depending on the receipt type, the following text is output: - Normal - Copy - Practice - Profo	At maximum 6 alphanumeric characters
Return amount	Absolute value of summed up amount of the return record on the receipt.	At maximum 14 characters incl. decimal point. *)
Sale amount	Amount for customer to pay, as per Section 28h, SKVFS 2008:x	At maximum 14 characters incl. decimal point. *)
VAT batch 1; VAT amount 1	First VAT batch as percentage; Amount of first VAT batch as per Section 28j, SKVFS 2008:x	<Percentage batch>;<Amount> Percentage batch: At maximum 5 characters incl. decimal point. *) Amount: At maximum 14 characters incl. decimal point. *) Field length: 20 characters incl. semicolon.
VAT batch 2; VAT amount 2	Second VAT batch as percentage; Amount of second VAT batch as per Section 28j, SKVFS 2008:x	<Percentage batch>;<Amount> Percentage batch: At maximum 5 characters incl. decimal point. *) Amount: At maximum 14 characters incl. decimal point. *) Field length: 20 characters incl. semicolon.
VAT batch 3; VAT amount 3	Third VAT batch as percentage; Amount of third VAT batch as per Section 28j, SKVFS 2008:x	<Percentage batch>;<Amount> Percentage batch: At maximum 5 characters incl. decimal point. *) Amount: At maximum 14 characters incl. decimal point. *) Field length: 20

		characters incl. semicolon.
VAT batch 4; VAT amount 4	Fourth VAT batch as percentage; Amount of fourth VAT batch as per Section 28j, SKVFS 2008:x	<Percentage batch>;<Amount> Percentage batch: At maximum 5 characters incl. decimal point. *) Amount: At maximum 14 characters incl. decimal point. *) Field length: 20 characters incl. semicolon.
*) Values always to accuracy of two decimal places.		

**SKVFS 2009:y**

5. Data shall be presented in ASCII format and right justified, and if necessary filled in with blanks (spaces) in order to use up the given field length.

## Chapter 7 Generation of the control code

1. A control unit shall generate a control code per receipt for the receipt types Normal and Copy. No control code shall be generated for the receipt types Practice and Profo.
2. A control unit shall use receipt control data as per Chapter 6, Section 4, as the basis for generating the control code.
3. The control code shall consist of two parts.
  - Part 1: Signature code, 32 characters
  - Part 2: Encryption code, 26 characters
 The point separating Part 1 and Part 2 shall be indicated by a semicolon (;).  
 The combined length shall comprise 59 characters.

### *Part 1: Signature code*

The signature code shall be formed as follows (1-2).

1. The receipt control data as per Chapter 6, Section 4 shall be signed using an algorithm as per Chapter 11, Section 6. The signature shall consist of 20 bytes.

2. The result shall be converted using base-32 encoding to create the signature code.

The signature code shall consist of 32 alphanumeric characters in ASCII format.

### *Part 2: Encryption code*

The encryption code shall be formed as follows (1-3).

**SKVFS 2009:y**

1. The basis for generating the encryption code shall consist of a 128-bit data record with the following fields:

<b>Field (bits)</b>	<b>Data</b>	<b>Calculation</b>
0-31 (length 32 bits)	32-bit whole number for total sale amount excl. VAT in thousands of Swedish crowns.	Calculator G (total sale amount) shall be reduced by Calculator H (total VAT). The result shall be rounded to the nearest thousand Swedish crowns and divided by 1000. If the result is negative, it shall be represented using a two's complement binary value.
32-47 (length 16 bits)	16-bit whole number containing the missing receipt calculator.	Value shown by Calculator B (number of missing receipts). If the value is greater than 65535, the field gets the value 65535.
48-95 (length 48 bits)	48-bit whole number containing the sale amount expressed in pennies.	Sale amount as per Section 4, Chapter 6 expressed in pennies from this receipt's receipt data. If the amount is negative, it shall be represented using a two's complement binary value.
96-127 (length 32 bits)	32-bit whole number containing the run number.	Run number as per Section 4, Chapter 6 from this receipt's receipt data. If the run number does not fit inside the 32 bits, the value of this field shall be 4294967295.

2. The basis for generating the encryption code (above table) shall be encrypted using the algorithm as per Chapter 11, Section 5.

3. The result shall be converted using base-32 encoding to create the encrypted control information.

The encryption code shall consist of 26 alphanumeric characters in ASCII format.

**SKVFS 2009:y****Chapter 8 Storage of internal data***Storage of internal data*

1. A control unit shall store internal data needed for creating control data and at least store the tasks stated in Sections 2 – 15.

*Calculators in a control unit*

2. A control unit shall include the following calculators.

Calculator A, transaction calculator.

Calculator B, calculator for the number of missing receipts.

Calculator C, calculator for the number of receipts of receipt type Normal.

Calculator D, calculator for the number of receipts of receipt type Copy.

Calculator E, calculator for the number of receipts of receipt type Practice.

Calculator F, calculator for the total of the amount to be returned.

Calculator G, calculator for the total of the sale amount.

Calculator H, calculator for the total of the VAT.

*Calculator A: Transaction calculator.*

3. Calculator A shall calculate on a continual basis the number of records of receipt data for receipt types Normal, Copy, Practice and Profo which are read into the control unit.

Calculator A shall begin with the value 1 for the first record and then increase the value by 1 for each new record.

*Calculator B: Calculator for the number of missing receipts.*

4. Calculator B calculates the number of run numbers missing/lacking receipts of receipt type Normal. The calculation shall take place as is described in the following.

– If the difference between the current run number and the previous run number is 1, this shall not be taken into account.

– If the difference between the current run number and the previous run number is zero, this shall be given the value 1.

– If the difference between the current run number and the previous run number is greater than 1, this shall be given the said value minus 1.

– If the difference between the current run number and the previous run number is less than zero, this shall be given the absolute value of the difference.

Calculator B shall begin with the value 0.

Calculator B shall not take into account the first receipt that is read.

**SKVFS 2009:y**

*Calculator C: Calculator for the number of receipts of receipt type Normal*

**5.** Calculator C shall calculate on a continual basis the number of records of receipt data for receipt type Normal, which are read into the control unit.

Calculator C shall begin with the value 1 for the first record of receipt data and then increase the value by 1 for each new record.

*Calculator D: Calculator for the number of receipts of receipt type Copy*

**6.** Calculator D shall calculate on a continual basis the number of records of receipt data for receipt type Copy, which are read into the control unit.

Calculator D shall begin with the value 1 for the first record of receipt data and then increase the value by 1 for each new record.

*Calculator E: Calculator for the number of receipts of receipt type Practice.*

**7.** Calculator E shall calculate on a continual basis the number of records of receipt data for receipt type Copy, which are read into the control unit.

Calculator E shall begin with the value 1 for the first record of receipt data and then increase the value by 1 for each new record.

*Calculator F: Calculator for the total of the amount to be returned*

**8.** Calculator F shall sum up on a continual basis the amount to be returned per receipt of receipt type Normal, which are read into the control unit.

Calculator F shall begin with the value 0.00 for the first record of receipt data, which is read into the control unit.

*Calculator G: Calculator for the total of the sale amount*

**9.** Calculator G shall sum up on a continual basis each record of receipt data for receipts of type Normal, which are read into the control unit.

Calculator G shall begin with the value 0.00 for the first record of receipt data, which is read into the control unit.

*Calculator H: Calculator for the total of the VAT*

**10.** Calculator H shall sum up on a continual basis the total of the VAT amount for each record of receipt data for receipts of type Normal, which are read into the control unit.

Calculator H shall begin with the value 0.00 for the first record of receipt data, which is read into the control unit.

*Further provisions concerning calculators***SKVFS 2009:y**

- 11.** The readings on Calculators A – H must not be reduced nor set to zero. This does not apply to the actions set out in Chapter 3, section 5.
- 12.** As regards control unit of type C as per Chapter 4, Section 6, Calculators A – H shall be required for each cash register from which the control unit receives receipt data.

*Further provisions concerning internal data*

- 13.** *The latest transaction calculators* containing the value of Calculator A (transaction calculator) with the time of day of the latest copying of control data to the National Tax Board being stored in the Control unit. This shall have the value 0 before the first copying.
- 14.** *Time stamp of the latest copying* shall be stored in the control unit and it shall contain notification of the time when the latest copying of control data was done. This shall have the value 0 before the first copying.
- 15.** The control unit's serial number shall be stored.

**Chapter 9 Encryption and storing of receipt control data**

- 1.** Receipt control data for receipt types Normal and Copy, along with the associated control code and the time stamp, shall be encrypted and stored. This forms the encrypted control data per receipt.
- 2.** Receipt control data shall be stored in the order that the data is received.
- 3.** For type C control units, per Chapter 4, Section 6, the receipt control data shall also be sorted per cash register.

*Encrypted control data per receipt*

- 4.** A control unit of type shall encrypt and store records of control data as shown in the following table.

<b>Data</b>	<b>Description</b>	<b>Format</b>
Date and time	Date and time of the day as per the sale transaction Section 28c, SKVFS 2008:x	12 numerals, format YYYYMMDDhhmm
ID code	Corporate identification code or personal ID code as per Section 28a, SKVFS 2008:x	10 numerals
Cash register	Cash register marking	At maximum 16

**SKVFS 2009:y**

marking	as per Section 10, SKVFS 2008:z	alphanumeric characters
Run number	Run number as per Section 28d, SKVFS 2008:x	At maximum 12 numerals
Receipt type	Depending on the receipt type, the following text is produced: - Normal - Copy - Practice - Profo	At maximum 6 alphanumeric characters
Return amount	Absolute value of summed up amount returned on the receipt.	At maximum 14 characters incl. decimal point. *)
Sale amount	Amount for customer to pay, as per Section 28h, SKVFS 2008:x	At maximum 14 characters incl. decimal point. *)

VAT batch 1; VAT amount 1	First VAT batch as percentage; Amount of first VAT batch as per Section 28j, SKVFS 2008:x	<Percentage batch>;<Amount> Percentage batch: At maximum 5 characters incl. decimal point. *) Amount: At maximum 14 characters incl. decimal point. *) Field length: 20 characters incl. semicolon.
VAT batch 2; VAT amount 2	Second VAT batch as percentage; Amount of second VAT batch as per Section 28j, SKVFS 2008:x	<Percentage batch>;<Amount> Percentage batch: At maximum 5 characters incl. decimal point. *) Amount: At maximum 14 characters incl. decimal point. *) Field length: 20 characters incl. semicolon.
VAT batch 3; VAT amount 3	Third VAT batch as percentage; Amount of third VAT batch as per Section 28j, SKVFS 2008:x	<Percentage batch>;<Amount> Percentage batch: At maximum 5 characters incl. decimal point. *) Amount: At maximum 14 characters incl. decimal point.

		*) Field length: 20 characters incl. semicolon.	<b>SKVFS 2009:y</b>
VAT batch 4; VAT amount 4	Fourth VAT batch as percentage; Amount of fourth VAT batch as per Section 28j, SKVFS 2008:x	<Percentage batch>;<Amount> Percentage batch: At maximum 5 characters incl. decimal point. *) Amount: At maximum 14 characters incl. decimal point. *) Field length: 20 characters incl. semicolon.	
Total sale amount	Calculator G (total of the sale amount).	14 characters incl. decimal point.	
Control code, Part 1	Signature code as per Chapter 7 for this receipt.	32 alphanumeric characters	
Control code, Part 2	Encryption code as per Chapter 7 for this receipt.	26 alphanumeric characters	
Time stamp	Point in time as per control unit's clock.	12 numerals, format YYYYMMDDhhmm	
*) Values always to accuracy of two decimal places.			

5. The data shall be presented in ASCII format and right justified, and possibly filled in with blanks (spaces) in order to use up the given field length.

*Encryption of control data*

6. Each record of control data shall be encrypted. Encryption shall be done using the algorithm as per Chapter 11, Section 5.

## **Chapter 10 Transmission of control data to the National Tax Board**

*Control data to the National Tax Board*

1. A control unit shall generate log files with the control data and copy these to an external memory via Port 3 when this port is activated.
2. A control unit shall create the log files Serial.Log, TransHdr.Log, and Trans.Log.

*Serial.Log*

**SKVFS 2009:y**

3. The log file Serial.Log shall be a text file and shall contain the following data.

Field	Description	Format
Control unit's ID	Serial No. of control unit in plain text	17 (5+12) alphanumeric characters

*TransHdr.Log*

4. The log file TransHdr.Log shall be a binary file containing an encrypted data record and a signature record.

5. As regards control unit of type C as per Chapter 4, Section 6, a log file TransHdr\_X.Log shall be created for each cash register where X is a run number beginning with the value 1 and increasing by 1 for each cash register.

6. TransHdr.Log shall have the following partial batches / partial records which form a record of fixed length.

Partial batch / Partial record	Content	Length
Encrypted data batch / data record	Encrypted data batch / data record as per Sections 7 – 10	176 bytes
Signature record	Signature of encrypted data record	20 bytes

*Encrypted data record*

7. An encrypted data record shall be made up of the following data.

Field	Description	Format
Control unit's ID	The control unit's serial number as per Ch. 11, Section 3.	17 alphanumeric characters
Cash register marking	Cash register marking as per Section 10, SKVFS 2008:z	16 alphanumeric characters
Time stamp for copying of control data	Point in time at the beginning of the copying.	12 numerals, format YYYYMMDDhhmm
Transaction calculator	Value of Calculator A (transaction calculator) at the beginning of the copying.	10 numerals
Missing receipt calculator	Value of Calculator B (number of missing	10 numerals

**SKVFS 2009:y**

	receipts) at the beginning of the copying.	
Number of receipts of the receipt type Normal	Value of Calculator C (number of receipts of the receipt type Normal) at the beginning of the copying.	10 numerals
Number of receipts of the receipt type Copy	Value of Calculator D (number of receipts of the receipt type Copy) at the beginning of the copying.	10 numerals
Number of receipts of the receipt type Practice	Value of Calculator E (number of receipts of the receipt type Practice) at the beginning of the copying.	10 numerals
Total returned amount	Value of Calculator F (total returned amount) at the beginning of the copying.	14 characters incl. decimal point. *)
Total sale amount	Value of Calculator G (total sale amount) at the beginning of the copying.	14 characters incl. decimal point. *)
Total VAT	Value of Calculator H (total VAT) at the beginning of the copying.	14 characters incl. decimal point. *)
Time stamp of latest copying	Value of <i>time stamp of latest copying</i> as per Chapter 8.	12 numerals, format YYYYMMDDhhmm
Transaction calculator's value at time of latest copying	Value of <i>latest transaction calculator</i> as per Chapter 8.	10 numerals
Number of records in Trans.Log	Number of records of control data contained in Trans.Log.	10 numerals
*) Values always to accuracy of two decimal places.		

8. The data shall be presented in ASCII format and right justified, and possibly filled in with blanks (spaces) in order to use up the given field length.

**9.** The data shall be encrypted using the algorithm as per Ch. 11, Section 5.

*Signature record*

**10.** The encrypted data record as per Section 9 shall be signed using an algorithm as per Ch 11, Section 6.

*Trans.Log*

**11.** The log file Trans.Log shall be a binary file containing an encrypted control data record and a signature record for each receipt stored in the control unit.

**12.** For each receipt stored in the control unit, Trans.Log shall have the following partial records, which form a record of fixed length.

<b>Partial records</b>	<b>Content</b>	<b>Length</b>
Encrypted control data record	Encrypted control data per receipt as per Ch. 9, Sections 4–6	256 bytes
Signature record	Signature of encrypted control data record	20 bytes

**13.** The records shall be arranged in the same order as they were when read into and stored in the control unit.

*Encrypted control data record*

**14.** The encrypted control data record shall be encrypted control data per receipt stored in the control unit.

*Signature record*

**15.** The signature record shall be encrypted control data record signed using the algorithm as per Chapter 11, Section 6.

**Chapter 11 Encryption**

**Individual encryption keys**

*Generation of individual encryption keys*

**1.** A currently valid principal key issued by the National Tax Board shall be used when generating individual encryption keys for each control unit.

The principal key of the National Tax Board may not be used for any other purpose than that indicated in the first paragraph.

**SKVFS 2009:y**

2. The following three individual encryption keys shall be generated.

1. Individual encryption key: Insert capital letter "K" at the end of the serial number.

Individual encryption key =  
HMAC-SHA256(<primary key>,<serial number>K)  
This shall be composed of 256 bits.

2. Individual initialisation vector: Insert capital letter "I" at the end of the serial number.

Individual initialisation vector =  
HMAC-SHA256(<primary key>,<serial number>I)  
Only the 128 least significant bits in the result shall be used.

3. Individual signature key: Insert capital letter "A" at the end of the serial number.

Individual signature key =  
HMAC-SHA256(<primary key>,<serial number>A)  
This shall be composed of 256 bits.

3. The serial number of each control unit shall be used.

The serial number shall have the following format:

Field	Format
Manufacturer's ID	5 alphanumeric characters.
Control unit's ID	12 alphanumeric characters.

4. The field shall be presented in ASCII format and right justified, and if necessary filled in with blanks (spaces) in order to use up the given field length.

#### **Encryption algorithm**

5. The symmetrical encryption algorithm AES-256 in CBC position shall be used for encrypting the data in the control unit.

The individual encryption key as per Section 2, Subsection 1, and the individual initialisation vector as per Section 2, Subsection 2, shall be used in the algorithm.

Encrypted data shall be entered using zeros (0) to reach the necessary length.

#### **Signature algorithm**

6. The algorithm HMAC-SHA1 shall be used for the signature function.

The individual signature key as per Section 2, Subsection 3 shall be used in the algorithm.

**SKVFS 2009:y**

## **Chapter 12 Requirements on security, performance capacity, reliability, and the operating environment.**

**SKVFS 2009:y**

### **Security**

#### *Protecting the security functions and security-critical data*

1. The individual encryption keys shall be stored so that the risk of them becoming compromised is minimised.
2. The individual encryption keys shall be stored in a memory that cannot be modified or read by unauthorised persons or read using an oscilloscope or other tool.
3. Internal data and control data shall be stored in a memory that cannot be modified or read by unauthorised persons.
4. Software shall be protected so that it cannot be modified, added to or read via a control unit.
5. Software for encryption and signing shall be located in a secure component constructed for that purpose.
6. Individual encryption keys, internal data and control data shall be stored in a non-transitory memory without any moving parts. The memory shall be such that it does not need electrical power for the stored data to be retained.

#### *Transportation and storage*

7. A control unit shall be such that it can be transported and stored without individual encryption keys or internal data being altered or corrupted.

#### *Enclosure protection and security sealing*

8. A control unit shall be such that it cannot be opened. The control unit's construction shall be such that physical access and attempts at access shall leave signs visible to the naked eye.
9. A control unit shall be sealed with security-sealing tape or the like, which shall withstand temperature conditions between  $-30^{\circ}\text{C}$  and  $+110^{\circ}\text{C}$ . If the security sealing is broken, a sign visible to the naked eye shall be left.
10. Contact 3 shall be sealed with security-sealing tape or the like, which shall withstand temperature conditions between  $-30^{\circ}\text{C}$  and  $+110^{\circ}\text{C}$ . If the security sealing is broken, a sign visible to the naked eye shall be left.

*Marking and identification*

11. The control unit's enclosure shall be marked with its serial number.

**Requirements concerning performance capacity and reliability**

*Continuous operation and performance capacity*

12. A control unit shall be such that it can complete the encrypting and saving/storage of control data even in the event of a power outage.

13. It shall be possible to store data for at least 7 years even if the control unit is without power supply.

14. A control unit's clock shall function for at least 7 years even if the control unit is without power supply.

15. A control unit shall have a service life of at least 7 years.

16. The memory used for storing control data shall have such a capacity that it can provide the storage functions for control data covering at least 5 years.

17. A control unit shall not delay the printing out of a cash register receipt such that it becomes apparent to the user or affects the user's workplace environment.

*User interface*

18. A control unit shall produce a signal as to whether it is functioning or not functioning.

19. A control unit shall produce a signal once the copying of control data to the external memory is completed.

A Control unit shall produce a signal if an error occurs during the copying function.

*Performance capacity clock*

20. A control unit's real-time clock shall not deviate more than  $\pm 5$  minutes per year at room temperature ( $+20^{\circ}\text{C}$ ).

*Physical durability*

21. A control unit shall at least fulfil the requirements of IEC 721-3-7, Section 7. It shall withstand a free fall of  $< 1\text{kg}$  in Category 7M2.

*Temperature***SKVFS 2009:y**

**22.** A control unit shall withstand the operating environment it is set for and at least withstand the temperature range of +5°C — +40°C.

*Air humidity*

**23.** A control unit shall withstand the operating environment it is set for and at least withstand the air humidity range of 10% — 85% without condensation causing damage to the unit.

*EMC (Electromagnetic Compatibility, immunity and emission)*

**24.** A control unit shall at least meet the immunity requirement set out in SS-EN 55024, immunity from electromagnetic disturbances. It shall at least be able to withstand the demagnetisation equipment used in the control unit's operating environment.

**25.** A control unit shall at least meet the emission requirement of Category B set out in SS-EN 55022, limit values with respect to radio disturbances.

*Electrical safety*

**26.** A control unit shall at least meet the electrical safety requirement set out in SS-EN 60 950-1.

**Operating environment**

**27.** A description shall be provided setting out the operating environment for a particular control unit. The description shall at least cover the specification stipulated by the requirements per Sections 20 – 26.

**Chapter 13 Manufacturing, testing and documentation****Manufacturing of the control unit***Installation of the clock*

**1.** A control unit's clock shall be set to Swedish standard time and the current date. The clock shall be set before it is connected to the control unit.

*Serial number and encryption key*

**2.** The serial number shall be stored in the control unit when not connected.

**3.** The individual encryption key shall be stored in the control unit when not connected.

**4.** The National Tax Board's primary key is not to be stored in the control unit.

#### *Compliance*

**5.** The manufactured control unit shall comply with a certified version of the product.

#### **Testing and testing documentation**

**6.** Each model of a control unit shall be validated as fulfilling the requirements of these regulations

The validation process shall consist of the following.

- Testing of the functions set out in Chapters 4–11 of these regulations.

- Testing to ensure compliance with the requirements concerning security, performance capacity, reliability and operating environment set out in Chapter 12 of these regulations.

**7.** Testing documentation shall be made available for validation purposes. Testing documentation shall include descriptions of the testing procedure and of the testing event and of the operating environment as per Chapter 12, Section 27. If so requested, this documentation must be provided to the National Tax Board.

#### **Documentation of the control unit**

**8.** Detailed documentation must be available on the control unit's software and hardware including functional descriptions and the operating environment.

If so requested, this documentation must be provided to the National Tax Board.

**9.** Documentation shall be available regarding instructions on how to install the control unit.

**10.** Documentation (user manual) shall be available regarding all of the control unit's functions. The user manual shall be available in Swedish or in English, and it must accompany the delivered control unit.

**11.** The manufacturer shall maintain a register of manufactured control units including information with respect to when they were

manufactured, serial number and the identity of the primary keys that were used. At the request of the National Tax Board, the manufacturer shall provide information from the register.

**SKVFS 2009:y**

## Chapter 14 Certification of a control unit

### Introductory provisions

1. The Act (2007:592) on cash registers, along with the Technical Conformity Assessment Act (1992:1119), states that a control unit shall be certified by a certification body accredited for this task by the Swedish Board for Accreditation and Conformity Assessment, SWEDAC. The certification body shall fulfil the requirements set out in SWEDAC's regulation concerning bodies operating product certification systems.

2. The basis for certification shall be provided by SS-EN 45011 General Requirements for Bodies Operating Product Certification Systems together with STAFS-2007:12<sup>2</sup> and STAFS 2007:21<sup>3</sup>.

3. All control unit models must be certified. The certification shall be performed by a certification body that has been accredited for that purpose as per the Technical Conformity Assessment Act (1992:1119).

4. Certification shall include testing of functions, security, performance capacity, reliability and operating environment, together with the requirements imposed on manufacturing as presented in these regulations. The document for interpreting the requirements imposed on the software shall be the document WELMEC 7.2. Similarly, the document WELMEC 2.2 may also be used. As regards interpreting of the risk level of WELMEC, the risk level of D shall be adhered to.

5. The specifications shall indicate the operating environments for which the various control units are set to operate in. At least one type of operating environment shall be presented. The certification shall be performed taking into account the model and the given operating environment.

<sup>2</sup> Regulation and general guideline of the Swedish Board for Accreditation and Conformity Assessment (SWEDAC) concerning accreditation of bodies certifying products.

<sup>3</sup> Regulation and general guideline of the Swedish Board for Accreditation and Conformity Assessment (SWEDAC) concerning accreditation of bodies certifying IT security.

6. Certification may also be performed by a certification body based in some other Member State of the European Union, in Turkey or in the European Economic Area, assuming that the body meets the requirements of the standard SS-EN 45011:1998 (ISO /IEC Guide 65:1996) and has been accredited for the task by an accreditation body meeting the requirements of the standard SS-EN ISO/IEC 17011:2005, or by an accreditation body based in a Member State of the European Union, in Turkey or in the European Economic Area which otherwise offers corresponding guarantees in matters involving technical and professional competence together with a guarantee of being an independent body.

### **Development and production of the control unit**

7. The manufacturer shall review the codes included in the control unit's software to ensure that the program's functionality complies with these regulations (code analysis). The code analysis shall be documented.

8. The manufacturer shall carry out a vulnerability analysis of the control unit. The vulnerability that is identified should be analysed and subject to an impact analysis. Necessary security measures should be taken to minimise vulnerability.

9. The manufacturer shall issue a comprehensive description (high-level description) and a detailed description (low-level description) to be used in the vulnerability analysis as per Section 8. The high-level description should contain a comprehensive description of how the control unit works as well as the operating environment and security functions thereof. The low-level description shall contain a detailed description of software, source code(s) and the mechanisms that perform the functions laid down in these regulations.

10. The manufacturer shall perform security testing to validate the measures implemented after completion of the vulnerability analysis. The measures should be tested to verify that the implemented security functions function in a reliable manner.

The manufacturer shall document completed security testing in the form of test cases and testing environment. Test results should be repeatable.

### **Evaluation**

11. For the assessment of security testing, the certification body shall use international standards or accepted regulatory specifications. The manufacturer's own methods for the assessment of security tests may be used if they provide at least the same level of assessment security.

12. The certification body's evaluation of safety functions shall comprise at least

- protection of individual encryption keys in the control unit
- protection of the control unit's software
- protection of control data.

**SKVFS 2009:y**

**13.** The certification body's analysis and testing of the control unit's security functions shall comprise at least

- that the individual encryption keys cannot be modified or read from the control unit
- that the control unit's software cannot be modified
- that the control data of the National Tax Board cannot be modified or erased.

**14.** The certification body shall verify that the following events are traceable

- if individual encryption keys in the control unit are erased
- if the control unit's software is erased
- if the control data of the National Tax Board has been modified or erased.

**15.** The certification body shall evaluate and assess the manufacturer's vulnerability analysis and security testing and if necessary carry out their own security testing. When necessary, the certification body shall carry out penetration tests to identify additional vulnerabilities of the control unit not covered by the manufacturer's vulnerability analysis.

**16.** The certification body shall carry out an evaluation (reference testing) of control units from the manufacturer's production environment at least once a year. Reference testing shall comprise at least the most critical functions in the control unit, as demonstrated experientially. The reference testing shall be fact-based and applied to a selection representative of the production.

**17.** The certification body shall evaluate and assess the manufacturer's code analysis. If necessary, the certification body shall carry out their own code analysis.

#### **Revision**

**18.** The certification body shall initially and at least once a year carry out a revision of the manufacturer's production environment. The revision shall be done on location.

#### **Production environment**

##### **Management system**

**19.** The manufacturer shall have documented routines in the form of production environment management systems corresponding to ISO 9001. The management system shall moreover correspond to the requirements laid down in Sections 20 – 36.

The management system shall be revised on a continual basis as to account for existent requirements and risks.

**20.** A risk analysis shall provide the basis for the manufacturer's management system. The manufacturer shall initially and at least once a year carry out a risk analysis. A risk analysis shall always be included as the basis for a modification of the production environment. A risk analysis does not need to be done if the modification to the production environment obviously does not change the threat scenario with respect to the production environment (security and quality).

**21.** A risk analysis should comprise

- handling/management of encryption keys
- the production process from development to manufacturing
- existent threats to information security
- protective measures necessary to establish appropriate protective measures for access linked to the production environment for control units.
  - Access refers to access critical to the quality and security of the control unit (reliability).

**22.** The manufacturer shall take those protective measures with respect to the production environment that per the risk analysis are deemed necessary to maintain appropriate protection for access linked to the control unit.

The manufacturer shall take necessary protection measures as well as measures to guard against remaining risks.

The manufacturer shall handle new and remaining risks by means of environmental scanning to the extent that such is necessary.

**23.** The manufacturer shall clearly define the distribution of responsibility for information security in their production environment as well as distribute said responsibility in terms of roles. In particular, the responsibilities for the handling of the management system, the primary key of the National Tax Board and individual encryption keys, shall be clearly defined. A risk profile shall be specified for each role.

**24.** The manufacturer shall ensure that defined roles are maintained by persons with sufficient competence and that are appropriate for their roles, who moreover understand their responsibility for the role that they have been assigned.

**25.** The manufacturer shall have routines in place for the management and reporting of security incidents and incident reporting in their production environment. The result of incident management should be used for the purposes of risk management.

**26.** Operationally critical data and systems for the development and manufacturing of control units shall be protected from unauthorised access by means of security authenticating and traceability on the individual level. The manufacturer shall ensure that each user's access options are limited. Access options should be based on authorisation, area of responsibility and assigned role.

As to ensure traceability, necessary information shall be collected and saved. The data collection of necessary information shall comprise at least the update of software and exchanging of the primary key. The information shall be stored in a secure manner and for as long as such is deemed necessary by the certification body.

**SKVFS 2009:y**

The manufacturer shall regularly analyse collected information with the aim of ensuring that no unauthorised access or unauthorised use of the data or system has occurred.

**27.** The manufacturer shall apply routines for modification management so as to ensure that manufactured control units comply with the control unit that was assessed during the certification process.

Routines shall be in place for modification management with respect to updating of the software in the control unit and updating of all operative software in the manufacturing process.

**28.** The manufacturer shall have routines for information security in the production environment. The effects of the routines shall be inspected by means of internal revisions. The appropriateness of the routines shall be gone over on a continual basis.

#### **Primary key of the National Tax Board**

**29.** The manufacturer shall handle the primary key of the National Tax Board in a secure manner throughout the service life of said key.

In their production environment, the manufacturer shall store and use the primary key of the National Tax Board in a manner that minimises the risk of it being corrupted (compromised).

**30.** The manufacturer shall ensure that all handling of the primary key of the National Tax Board is done in the presence of at least two employees of the manufacturer.

The manufacturer shall collect, and for the purpose of supervision, be able to provide the National Tax Board with information regarding unit level traceability, with respect to the handling of primary keys.

**31.** The manufacturer shall immediately inform the certification body and the National Tax Board if a primary key is suspected of or has determined to have been corrupted. The certification body and the National Tax Board shall also be informed of the reason for such. The corrupted primary key shall be immediately destroyed and may not be used to generate individual encryption keys.

**32.** Copying of the National Tax Board's primary key may only be done in the secure production environment and only to the extent that such is necessary. Copies of the primary key shall be handled like the original. Copies of the primary key necessary for storing and forwarding shall be destroyed immediately and in such a way that they cannot be recreated.

**33.** The manufacturer shall destroy the National Tax Board's primary key when it is no longer valid or if the National Tax Board requires the destruction of a primary key. When the manufacturing of control units is terminated, the manufacturer shall destroy all primary keys.

The destruction shall be carried out immediately and in such a way that the primary key cannot be recreated.

#### **Individual encryption keys**

**34.** The manufacturer shall generate and manage individual encryption keys in the production environment in such a manner that the risk of the keys being corrupted is minimised.

Individual encryption keys may not be copied or stored outside of the control unit after manufacturing of the control unit. Copies of the individual encryption keys that have been created for storing and forwarding or in the manufacturing process shall be destroyed immediately and in such a manner that they cannot be recreated.

**35.** The manufacturer shall immediately inform the certification body and the National Tax Board if an individual encryption key in a control unit that has left the manufacturer is suspected of or has been determined to have been corrupted. The certification body and the National Tax Board shall also be informed about the reason for such.

**36.** The manufacturer shall only generate individual encryption keys for control units that fulfil the requirements laid down in these regulations. Any other individual encryption keys shall be immediately destroyed by the manufacturer in a secure manner.

#### **Certificate**

**37.** A certificate may be valid for a maximum period of five years.

**38.** Before a control unit is supplied to the Swedish market, the manufacturer shall turn over information about the control unit's certificate designation to the National Tax Board.

**39.** The certification body shall revoke a certificate

- if the manufacturer has failed to comply with all provisions in these regulations
- if the manufacturer has corrupted the National Tax Board's primary key
- if the manufacturer has in any other way done something implying that the control unit would not be authorised for certification or would not be authorised in the event of a recertification.

The certification body shall also evaluate if additional measures should be taken with respect to the manufacturer

Upon the revoking of a certificate, the certification body shall immediately inform the National Tax Board about this withdrawal as well as the reason for such.

40. The certification body shall establish criteria regarding renewal of certification. The criteria shall comprise at least essential modifications to the control unit and essential modifications to the production environment.

**SKVFS 2009:y**

These regulations shall enter into force on xx month 2009.

On behalf of the National Tax Board

DIRECTOR-GENERAL

Head of Unit  
(Production Section, unit).