Release Notes

Viking Payment Terminals

Production Version 08.0.9 | Jan 2022

TETRA Test Version 0809 | Mock-up Test Version 8138

SMURR	AKANG	MADSA	Issued for Use
Originated	Checked	Approved	Remarks

Table of Contents

Section Page

1. INTRODUCTION

This release covers all terminal models. However, iWL251 GPRS/iWL252 (BT)/iWL220C/iCT250EG (using GPRS communication) are required to be upgraded to version 08.01 before upgrading to 08.09. This is as a result of some technical improvements.

The features and upgrades introduced in this release include:

- Swish QR functionality (Sweden)
- Single-tap improvements
- S-Group loyalty support enhanced (Finland)
- UI upgrade (including update of *Pay@Table 2.0* for Move/3500 terminals)
- VAS and Alternative Payment support
- German/Dutch text strings
- Return card type in GetCardInfo and LocalMode responses
- Support for the new Dankort Mastercard

The production release version is 08.0.9 and the TETRA test version is 0809.

For information on the availability of this release, please contact: techsupport@nets.eu. For further information on the terminal range, please consult the user guides/quick guides on the Nets website.

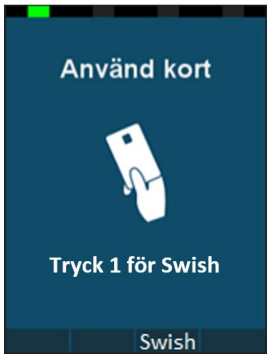
2. NEW FEATURES

This release brings Swish QR functionality to the Swedish market as a Value-Added Service (VAS), and improvements have been made to the UI using colours, including Pay@Table 2.0 for Move/3500. The OK button confirmation for single-tap contactless solutions has been removed, where amounts fall below the Cardholder Verification Method (CVM) limit. The release also includes S-Group functionality, which allows payment method benefits for loyalty cards within the S-Group chain in Finland.

2.1 SWISH QR

Swish QR will be available for both Android and iOS devices in Sweden. For Swedish payment terminals that are configured to support Swish QR, the Swish label will appear above the F3 button on the terminal screen. Swish allows the customer to use their Swish mobile app as a payment method by scanning the (Swish) QR code displayed on the terminal. Purchase and Reversal transactions are supported.

For Swish to function, the merchant is required to contact their bank to get an agreement for the product 'Swish Handel'. The service is activated in Nets internal systems when the merchant has made the order for the Swish QR feature *and* provided their Swish Handel agreement number.



If the terminal has multiple alternative payment methods activated (e.g. both Swish and Klarna), the MENU label will be displayed in the footer of the Awaiting Card screen (above the F3 button).

To be able to pay using Swish, the consumer can push 1. It is also possible to push F3. Then all the supported schemes will be listed in the terminal window.

Once the consumer has selected Swish, a QR code will be displayed on the terminal screen.

The consumer then opens the Swish app on their smartphone and scans the QR code. A receipt is printed. For integrated terminals, *Local Mode* is sent to the ECR as a normal card transaction.

2.1.1 Switching QR to Manual Entry

It is possible to trigger the terminal to accept manual key entry of a phone number. This is done by selecting *F3/Manuell* on the screen which displays the QR code. If manual key entry is selected, the consumer enters their mobile number into the terminal, before then approving the transaction in the Swish app. The receipt is then printed. For integrated terminals, *Local Mode* is sent to the ECR like a normal card transaction.

Transaction receipt:

STANDARD
StoreID: 30779896
Term: 63636304-636363
2021-07-19 08:33

Swish
Ref.: 341063636304000404
DC1
Session: 195
PP Ref.: 20130
AA Time: 2021-07-19 06:
34:10.365
AA Resp: PAID

PURCHASE
SEK 12,00
APPROVED

2.1.2 Limitations

Swish QR is not supported on monochrome or unattended terminals.

In case of refunds, once a refund has been initiated, the consumer must press F3 and choose Swish from the supported schemes displayed on the terminal. Following this, the Swish app will ask for the consumer's mobile number, before instructions are sent to their smartphone. The consumer is then asked to add (to the Swish app) the Reference Number which is printed on the receipt of the original transaction (Pp ref.nr.).

2.2 SINGLE-TAP IMPROVEMENTS

For amounts that fall below the CVM limit, the *OK* confirmation button is removed. The display of the feature varies between different countries and card schemes. In general, there are two ways to handle the single-tap.

- The *Tap Before Amount* legacy method, where a transaction is initiated with a placeholder amount. The cardholder taps on the screen when the amount is missing from the awaiting screen.
- The *Change Amount After Tap* method, where the transaction is initiated with the original amount. The pre-calculated amount is displayed on the screen and may change after the tap due to e.g. loyalty benefits.

2.2.1 Tap Before Amount

The amount confirmation screen has been removed for purchases (with a total amount) below CVM limits. This improved solution applies for transactions performed with Visa or MasterCard.

Due to requirements from other issuers (ie. Bankaxept), the amount confirmation screen will continue to be displayed for total amounts below CVM limits.

For transactions where the amount confirmation screen has been removed, the final amount will be displayed on the terminal screen when the transaction is sent to the Nets host (and on the final approved).

Additionally, support for mobile wallets has been added to the feature. The cardholder is able to perform single-tap transactions with their mobile wallet.

2.2.2 Change Amount After Tap

In this feature, the placeholder amount is replaced with the original amount during the transaction. To initiate a single-tap transaction, the ECR will send a VAS request with the original amount (and the transaction type) after all the goods are scanned. The amount and the transaction type are displayed on the *Present Card* screen. Once the card is read, the terminal will send the VAS response to the ECR. The ECR calculates the final amount (this amount may differ from the original amount). If the final amount is greater than original amount, the cardholder must confirm the amount by pressing the *OK* button on the terminal. For these transactions, it is the original amount that is used to determine the CVM method to be used.

In cases where the final amount is above the CVM limit - but where the terminal did not ask for the CVM because the original amount was below the limit - the terminal will prompt the cardholder to *Insert Card* or *Enter PIN* (this is based on the response from the host).

NOTE: For transactions in which the CVM is mandatory, e.g. Purchase + Cashback, the terminal will prompt for the CVM irrespective of the original amount.

Mobile wallets can be used for single-tap with the original amount.

The 26th bit of descriptive data sent to the PSP will have the below change highlighted in bold text:

Bit 26th Value	*Description*
0	Double-tap
1	Single-tap with placeholder amount
2	**Single-tap with original amount**

The below VAS requests may be used to initiate single-tap with the original amount:

JSON Request

Request	*Response*
{"cardinfo":{"ver":"1.04","issid":"?","loyaltyinfo2":"?","aid":"?","**amount**":"1200","txntype":"30"}}	{"cardinfo":{"ver":"1.04","issid":"30","aid":"D5780000021010","loyaltyinfo2":{"ver":"1.00","mid":"","mtype":"","issid":"0"}}}
Request	*Response*
{"cardinfo":{"ver":"1.04","alltags":"?","txntype":"33","**amount**":"10000","**cash**": "8000"}}	{"cardinfo":{"ver":"1.04","iccgrpid":"","pan":"34965181982","issid":"30","countrycode":"578","restrictions":"N","fee":"N","track2":"","tcc":"K__","bankagent":"","track3":"","loyaltyinfo":""}}

TLD Request

Request	*Response*
2000 US 0003 US 001 RS 2002 US 0003 US 001 RS 2001 US 0000 US RS 3017 US 0002 US 30 RS **3020 US 0008 US 00012500 RS**	2000000300120020003001200100080000004520030002002006000 21;20070019499401*****;30;-;-;
Request	*Response*
2000 US 0003 US 001 RS 2002 US 0003 US 001 RS 2001 US 0000 US RS 3017 US 0002 US 33 RS **3020 US 0008 US 00012500 RS 3021 US 0008 US 00001500 RS**	2000000300120020003001200100080000004520030002002006000 21;20070019499401*****;30;-;-;

DA Request

Request	*Response*
{"da":{"ver":"1.04","type":998,"action":3,"ra2t":{"ver":"1.0","query":[{"mode":4,"pin":1,"exclude":03,"**amount**":"1200","txntype":"30"}]}}}	{"da":{"ver":"1.0","type":998,"action":3,"status":"6:096"}}
Request	*Response*
{"da":{"ver":"1.04","type":998,"action":3,"ra2t":{"ver":"1.0","query":[{"mode":4,"pin":1,"exclude":03,"**amount**":"1200","**cash**": "800","txntype":"33"}]}}}	{"da":{"ver":"1.0","type":998,"action":3,"status":"6:096"}}

2.3 PRODUCT TYPE INFO - EMV CHIP CARDS

This allows the ECR to identify whether payment was done using Debit, Credit, Business, or some other type of card defined by the EMV specifications. Data is returned in responses if it exists in the chip data of the card. This is available for both contact and contactless.

Product type	*Description*
01	Debit Product
02	Credit Product
03	Commercial Product
04	Pre-Paid Product

2.3.1 Product Type

JSON Request

Request	*Response*
{"cardinfo":{"ver":"1.09","prodtype":"?"}}	{"cardinfo":{"ver":"1.09","prodtype":"01"}}

Local Mode

Result Data
LocalModeResultData:D04541333******1075;20210524101414;2;085;272830029939;;;;;;;79020100;790201;PPC MAP 07 v2 2;00;KC1;A0000000041010;0000808001;;05704;040101;0000000000;;;;Undefined;;;0;01

2.4 S-GROUP LOYALTY ENHANCEMENTS (FINLAND)

S-Group loyalty info is returned with the *GetCardInfo* and *LocalMode* reponses. This allows for recognizing the S-Group loyalty cards and further calculations of benefits available for applicable transactions (handled by an ECR).

The S-Group loyalty program allows payment benefits for certain types of transactions. The ECR calculates the amount by a defined rule, and – when the transaction type is Bonus - payment benefit info (maksutapaetu) can be sent in the “hostdata” field with TransferAmount. Further information is available in separate documentation.

2.4.1 Loyalty Information

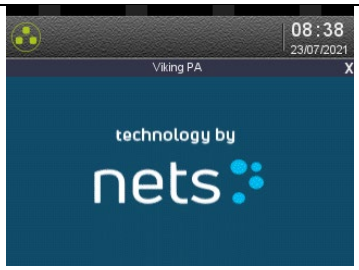
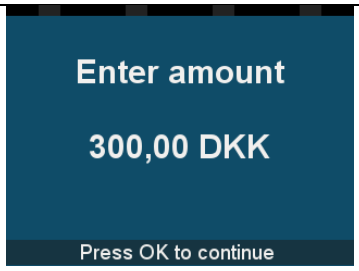
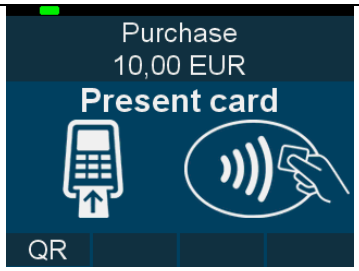
Local Mode

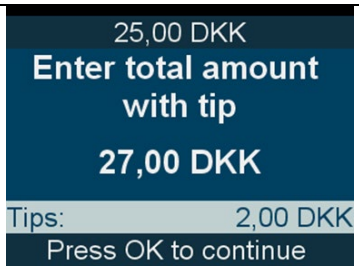
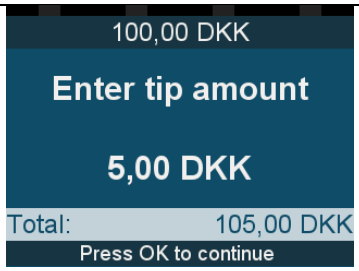
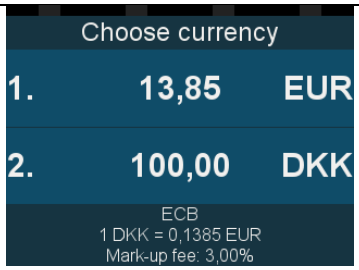
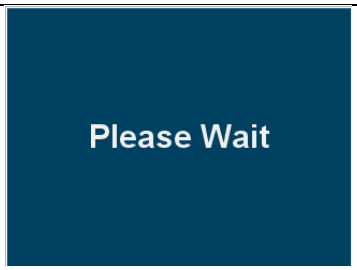
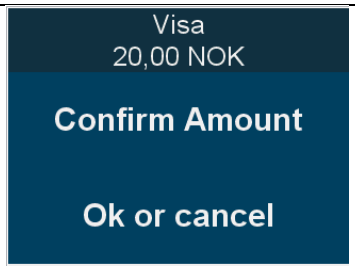
Result Data
LocalModeResultData: D 68621094******0003;20210524091623;1;091;269296318420;;00000001200;;;;;79020500;790205;UICS DEBIT;00;K@1;A000000333010101;0000000000;;00014;;0000000000;;;;Undefined;{"od":{"ver":"1.03","loyaltyinfo2":{"ver":"1.00","mid":"60040713416488124","mtype":"","issid":"12"}}};;4

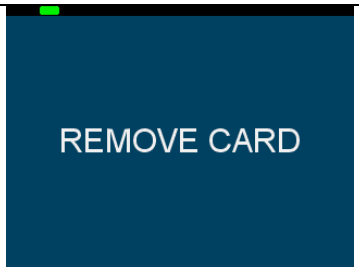
The same content shown above in optional data also applies for the GetCardInfo - JSON request/response.

2.5 USER INTERFACE (UI)

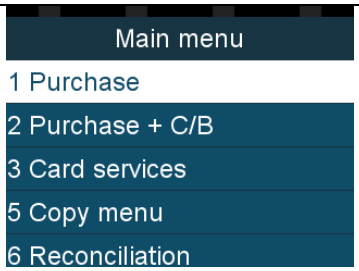
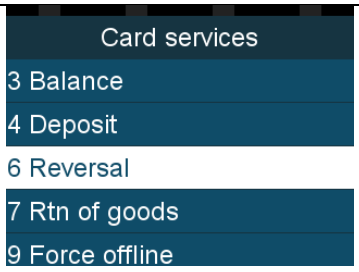
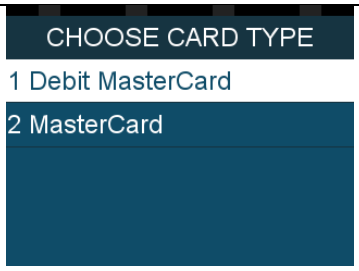
UI design improvements have been made to those terminal screens that are shown to the cardholder. This is the third stage for updating the Viking UI; making the screen texts more user-friendly and readable. The background has been converted from a black to blue theme with white text. Note: Monochrome and unattended terminals are not included in the scope for UI upgrades.

Idle screen with logo	
Enter Amount	
Present Card	

Tip – enter total amount	
Tip – enter tip amount	
DCC - select currency screen	
Enter PIN	
Please Wait	
Confirm Amount	

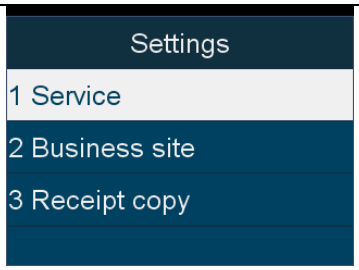
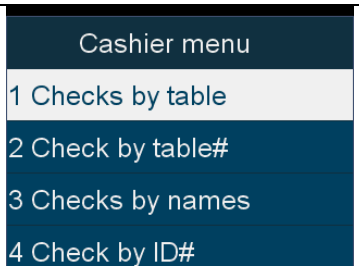
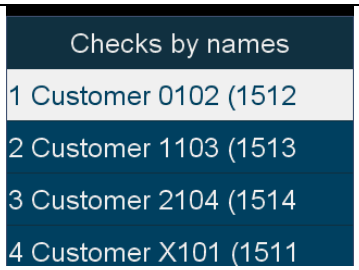
Approved	
Remove Card	

The terminal menu has been updated to reflect the new colour scheme, as shown below:

Main Menu	
Card Services Menu	
Application selection	

2.5.1 Pay@Table

Improvements to the UI for Pay@Table version 2.0 are shown below:

Settings Menu	
Cashier Menu	
Checks by Table Menu	
Checks by Names Menu	

2.6 VAS & Alternative Payment Support

The Viking application now supports offering Alternative Payment Method (APM) payments such as Vipps, Swish and Klarna for those terminals configured to support card-based, pre-purchase identification VAS services. When a VAS request is initiated, the option to start an APM transaction will also be made available on the *Awaiting Card* screen. Once an APM option is selected, the VAS request will bypass available values, and the terminal will continue to wait for further requests from the ECR (*Please Wait* screen); the merchant may now initiate a normal transaction or any other VAS request.

When initiating a normal transaction, the terminal will proceed based on the options selected during the VAS request. It will not prompt for the *Present Card* screen again.

However, if the transaction type sends in a transfer amount that does not match the transaction type mentioned in the VAS request, then the terminal will prompt for the card again.

The supported VAS requests and responses are shown below:

Card Info JSON

Request	*Response*
{ "cardinfo": { "ver": "1.00", "alltags": "?"},"o": {"ver": "1.00","merch": 733300}}	{"cardinfo":{"ver":"1.00","iccgrpid":"","pan":"0000000000000000","issid":"0","countrycode":"578","restrictions":"-","fee":"-","track2":"","tcc":"D__","bankagent":"","track3":"","loyaltyinfo":""}}

Card Info Top Level Domain (TLD)

Request	*Response*
3999 US 0000 US RS	3000000030010016000000000000000030020001030030003578300400001-30050001-30090000301100003D__30120000301300003014000030180000030190000

Graphic Command Interpreter (GCI)

Request	*Response*
2000 US 0003 US 001 RS 2002 US 0003 US 001 RS 2001 US 0000 US RS	2000000300120080003001200200030012001000020030002012004002 3Information Unavailable

DA Messages Prompting for Card

Request	*Response*
{"da": {"ver": "1.0","type": 998,"action": 3,"ra2t": {"ver": "1.0","query": [{"mode": 4,"pin": 1,"exclude": 30}]}}}	{"da":{"ver":"1.0","type":998,"action":3,"status":"2:001","statustext":"Information Unavailable"}}

3. COMPLIANCE

Support for online PIN in Finland and Iceland.

4. INCIDENTS RESOLVED

Serial numbers of up to 64 bytes can now be sent to the ECR via TLD 1010. Previously, only serial numbers up to 24 bytes were supported.

NB: If you have enabled TIDSupervision in BAXI settings, this change will update the serial number in the control file. There will be an error message for the ECR, and the interface is locked until the issue is manually resolved. To resolve it, you must follow the same actions that apply if a terminal was being replaced.

Previous incidents in version 08.0.6 are also resolved. The fixes are listed below:

- A controlled reboot every 24 hours will be implemented for Telium2 (T2) terminals with PCI 3/2 (same as exists on PCI 4 terminals).
- A treasure hold reboot (when memory goes below a treasure for available memory, the terminal will take a controlled reboot).
- API calls workaround to fix the previous memory leak.

4.1 MOVE/3500 WI-FI STABILITY

Complaints have been received regarding the stability of the Wi-Fi connection on Move3500 terminals. We found that the “Active Roaming” parameter in the terminal’s Wi-Fi settings must be disabled to achieve stable network connectivity, hence the problem is easily reproduced. We continue to investigate and follow the issues reported, but, until further notice, the “Active Roaming” setting should not be used.

Below are the correct configurations for terminal settings:

- Press the arrow down ↓ button below the display and select 4 – Wi-Fi settings. Swipe the Merchant Card to get access to the menu.
- Set the "Frequency Bands" to "auto" (Advanced Options – Frequency Bands – then select the "Auto" option, and press Enter or the 0 key).
- Set "Active Roaming" to "Off" (Advanced Options - Active Roaming - select "Off", then press Enter or 0 key).