



March 21, 2012

Markus Gagliardi
PayTec AG
Vogelsangstrasse 15,
CH-8307 Effretikon,

Switzerland

Re: *EMVCo Letter of Approval - Terminal Level 2*

EMV Application Kernel: PayTec EMV Kernel 1.2.0

Approval Number(s): 2-02255-1-1S-CET-0312-4.3.a
2-02255-1-1OS-CET-0312-4.3.a

The EMV Application Kernel has been tested on the following terminal

Terminal: **PT-A101**
PinPad: **n/a**
Operating System: **1OS = uTasker Version 1.3**

Report ID Session 1: **2PAYT_3-6207-01-04-11_CET - CETECOM ICT Services GmbH**

Approved Configurations:

Config	Vendor Config ID	Terminal	Checksum
1S		25	8DD736075868832D

Renewal Date: 21-Mar-2015

Dear Markus Gagliardi:

EMVCo, LLC ("EMVCo"), a Delaware limited liability company, has received your request for Level 2 terminal type approval for the EMV Application Kernel (hereafter referred to as Application) identified above. In connection with your request, we have reviewed all test file number(s) listed above.

After assessing such file(s), EMVCo has found reasonable evidence that the submitted samples of the above referenced Application Kernel sufficiently conform to EMV Integrated Circuit Card Specifications for Payment Systems, Version 4.3 of November 2011.

EMVCo hereby (a) grants your Application EMVCo Type Approval for Terminal Level 2, based on the requirements stated in the EMV 4.3 Specifications, and (b) agrees to include your Application Kernel in EMVCo's approved Application list.

EMVCo's grant to your Application Kernel is subject to and specifically incorporates (i) the General Terms and Conditions to the Letter of Approval enclosed as Exhibit A, and (ii) the Specific Terms and Conditions to the Letter of Approval attached hereto as Attachment 1. Because EMVCo's grant is subject to such limitations, including certain events of termination, you and any third parties should confirm that such approval is current and has not been terminated by referring to the list of approved Application Kernels published on the EMVCo website (www.emvco.com).

PayTec AG

This Letter of Approval is effective on dispatch from EMVCo.

EMVCo, LLC, a Delaware limited liability company

By:

Name: Arnaud du Chéné

Title: EMVCo Terminal Type Approval

Terminal Capabilities		Value Supported
Card Data Input Capability		
Manual Key Entry		No
Magnetic Stripe		Yes
IC with Contacts		Yes
CVM Capability		
Plaintext PIN for ICC Verification		Yes
Enciphered PIN for online Verification		No
Signature (Paper)		No
Enciphered PIN for offline Verification		Yes
No CVM Required		Yes
Security Capability		
Static Data Authentication and Dynamic Data Authentication		Yes
Card Capture		No
Combined Dynamic Data Authentication / Application Cryptogram Generation		No
Transaction Type Capability		
Cash		No
Goods		Yes
Services		Yes
Cash Back		No
Inquiry		No
Transfer		No
Payment		No
Administrative		No
Cash Deposit		No
Terminal Data Input Capability		
Does terminal have keypad		Yes
Numeric Keys		Yes
Alphabetic and Special Character Keys		No
Command Keys		Yes
Function Keys		No
Terminal Data Output Capability		
Print, Attendant (Mandatory for terminals supporting signature)		No
Print, Cardholder		Yes
Display, Attendant (Mandatory for Attended terminals)		No
Display Cardholder		Yes
Code Table 10		No
Code Table 9		No
Code Table 8		No
Code Table 7		No
Code Table 6		No
Code Table 5		No
Code Table 4		No
Code Table 3		No
Code Table 2		No
Code Table 1		No

Terminal Capabilities		Value Supported
Application Selection		
Support PSE selection Method		Yes
Support Cardholder Confirmation		Yes
Does Terminal have a preferred order of displaying applications		No
Does terminal perform partial AID selection		Yes
Does the terminal have multi language support		Yes
Does the terminal support the EMV Language Selection method		Yes
Does the terminal support the Common Character Set as defined in Annex B table 20 Book 4		Yes
Selectable Kernel Configurations		
Is your Multi-Configuration Kernel capable of dynamically selecting a configuration at the time of transaction based on 'triggers' as described in SU70?		No
Data Authentication		
What is the maximum supported Certificate Authority Public Key Size (Mandatory for terminals supporting Data Authentication with minimal support for 248 bytes)		248
What exponents does the terminal support (Mandatory for terminals supporting Data Authentication, 3 and $2^{16}+1$)		3 and $2^{16}+1$
During data authentication does the terminal check validity for revocation of Issuer Public Key Certificate		No
When supporting certificate revocation, what is the Certificate Revocation List format?		
Does the terminal contain a default DDOL (Mandatory for terminals supporting DDA)		Yes
Is operator action required when loading CA Public Key fails		No
CA Public Key verified with CA Public Key Check Sum		Yes
Cardholder Verification Method		
Terminal supports bypass PIN Entry		No
Terminal supports Subsequent bypass PIN Entry		No
Terminal supports Get Data for PIN Try Counter		Yes
Terminal supports Fail CVM		Yes
Are amounts known before CVM processing		Yes
Terminal Risk Management		
Floor Limit Checking (Mandatory for offline only terminals and offline terminals with online capability)		Yes
Random Transaction Selection (Mandatory for offline terminals with online capability, except when cardholder controlled)		Yes
Velocity Checking (Mandatory for offline only terminals and offline terminals with online capability)		Yes
Transaction Log		No
Exception File		Yes
Performance of Terminal Risk Management irrespective of AIP setting (expected behavior)		Yes

Terminal Capabilities		Value Supported
Terminal Action Analysis		
Does the terminal support Terminal Action Codes		Yes
Can the values of the Terminal Action Codes be changed		Yes
Can the Terminal Action Codes be deleted or disabled? If yes what are the default TAC values supported? (according to Book 3 Section 10.7)		Yes
	TAC Denial:	0000000000
	TAC Online:	0000000000
	TAC Default:	0000000000
Does Offline Only Terminal process Default Action Codes prior to First Generate AC		No
Does Offline Only Terminal process Default Action Codes after First Generate AC		No
Does Online Only Terminal skip processing TAC/IAC-Default and automatically request an AAC when unable to go online		No
Does Online Only Terminal process TAC/IAC-Default as normal when unable to go online		No
Device capable of detecting CDA failure before Terminal Action Analysis		No
Mode 1: Req. CDA on ARQC + Req. CDA on 2nd GenAC after approved Online authorization		No
Mode 2: Req. CDA on ARQC + No Req. CDA on 2nd GenAC after approved Online authorization		No
Mode 3: No Req. CDA on ARQC + No Req. CDA on 2nd GenAC after approved Online authorization		No
Mode 4: No Req. CDA on ARQC + Req. CDA on 2nd GenAC after approved Online authorization		No
Completion Processing		
Transaction Forced Online Capability		No
Transaction Forced Acceptance Capability		No
Does terminal Support advices		No
Does the terminal support Issuer initiated Voice Referrals		No
Does the terminal support Batch Data Capture		Yes
Does the terminal support Online Data Capture		No
Does the terminal support a Default TDOL		Yes
Exception Handling		
What is the POS Entry Mode value when IC cannot be read and the transaction falls back using Magstripe (Mandatory for attended terminals)		81
Miscellaneous		
Is the terminal equipped with a PIN Pad		Yes
Is the amount and PIN entered at the same keypad		No
Is the ICC/Magstripe Reader combined		Yes
If Combined ICC/Magstripe reader is supported, is Magstripe read first		No
Does the terminal support account type selection		No
Does the terminal support 'on fly' script processing (not recommended behavior)		No
Is the Issuer Script device limit greater than 128 bytes		No
If the Issuer Script device limit is greater than 128 bytes, what is the value supported		
Does the terminal support Internal Date Management		Yes

Attachment 1

Specific Terms and Conditions to the Letter of Approval

Restriction:

None