



Scheme Description and Approvals List

UK Card Payment Terminal Approval Scheme

UKTAS team

23 April 2024

TABLE OF CONTENTS

1	Introduction.....	3
2	Approval requirements.....	3
2.1	General description	3
2.2	Security evaluation of payment terminals	3
2.3	Evaluation of payment applications	3
2.4	Accessibility	4
2.4.1	General	4
2.4.2	Traditional PIN entry keypads.....	4
2.4.3	Touchscreen PIN entry and legibility of the display.....	6
2.5	Additional requirements and recommendations.....	6
3	Lists of approvals.....	7
3.1	General points about approvals.....	7
3.2	Approvals since the start of Common.SECC	8
3.3	Payment Application approvals	10
3.4	Approvals prior to Common.SECC	10
4	Further information	13

1 Introduction

This paper provides an overview of approval requirements relating to the security and usability of card payment terminals, and gives a list of approved devices.

Section 2 outlines the approval requirements. Note that they do not cover all topics that will need to be addressed before deployment, including compliance with scheme rules, national laws and regulations. It also gives some additional recommendations that are not approval requirements.

Section 3 lists currently approved devices.

Section 4 gives sources of further information.

The latest amendment is to recommend that non-touchscreen devices support an accessibility mode in which payment messages are spoken as well as displayed, and to indicate devices that provide this. Reference to PIN shielding has been removed.

2 Approval requirements

2.1 General description

Device approvals are based on devices as supplied to the laboratory for security evaluation, and where appropriate to the RNIB for accessibility and usability testing. Payment applications can also be checked for security. Security approvals relate to protection against external attack. If the software in a device approved by the RNIB is subsequently changed, the approval may be invalidated if the customer interface is impacted as a result.

It is essential that devices are accessible to a wide range of users, including people with limited or no sight. It is therefore important that touchscreen PIN entry devices have clear visual design and an accessibility mode to activate speech, and that keys on physical PIN pads can be easily felt and distinguished from each other by touch and sight. See section 2.4 for more details on accessibility.

2.2 Security evaluation of payment terminals

The UK requires that terminals are evaluated using the Common Criteria methodology and receive a successful Common Criteria evaluation as described at <https://common-secc.org>.

2.3 Evaluation of payment applications

Payment terminal security evaluations relate to the platform, and not to applications that run on it. When a device is evaluated it must include a payment application, but a different application may subsequently be loaded into the device before it is deployed. Common.SECC allows for payment applications to be evaluated and certified. The certification process for payment applications can be found in the Common.SECC website at <https://common-secc.org>, and certified applications are listed there and also in section 3.3 below. Payment application certification is optional in the UK but is strongly recommended. With software-only products, the security-relevant parts of the payment application (particularly the state machine and control of user prompts) are treated as part of the platform.

2.4 Accessibility

2.4.1 General

The UK requires there to be a common look-and-feel to the cardholder interface on card payment terminals, to ensure that they are as easy to use as possible.

In addition, devices should be usable by people with disabilities. Only certain aspects of this are addressed as part of UK approvals, and it is for acquirers, schemes, merchants and others to ensure that accessibility and usability is achieved in other respects. These requirements and recommendations address support for those with impaired vision through the design of the cardholder interface.

The topics addressed here are the layout of the PIN entry keypad, the use of touchscreens for cardholder input, the legibility of touchscreen information, and feedback from PIN entry.

2.4.2 Traditional PIN entry keypads

This section refers to 'traditional' mechanical keypads with individual physical keys that can be pressed and give tactile feedback, as opposed to virtual keys on a touchscreen.

The layout of the numeric (0-9) keys must be as shown in figure 1. This layout is compatible with the layout shown in ISO 9564-1.

In addition to the numeric keys, there must also be a Cancel key coloured or marked with a bold red, and an Enter key coloured or marked in a bold green. There may also be a Clear key, which if present must be coloured or marked a bold yellow. Pressing 'Enter' completes PIN entry, and pressing 'Cancel' terminates the transaction. The Clear key either erases all the characters previously entered, or (preferably) just the last one entered. Unless the whole key is coloured red (Cancel key), yellow (Clear key) or green (Enter key), the control keys must be marked as follows: "X" or "Cancel" for the Cancel key, either "<" or "|" or "<" or "Clear" for the Clear key, and "O", "OK", "Enter" or a tick (✓) for the Enter key.

The numbers on the number keys, and the names or symbols on the control keys, must contrast well with the background. A good contrast is for example white text on black keys, or a black symbol on a yellow key. Ideally the keys themselves should also contrast well with the surrounding area (e.g. black keys with white numbers on a light grey background is a good contrast).

Numbers on PIN pad keys must be a minimum of 5 mm in height. The numbers must not touch the edges of the key. Text should be in a large font size, a minimum of 5 mm in height for capital letters. The Font type must be sans serif, and should ideally use upper- and lower-case letters for key names (e.g. Enter, Clear or Cancel, and not ENTER, CLEAR or CANCEL). Many partially sighted people will read using the shape of the word to identify it especially if they are expecting to see a particular word (as would be the case for Enter, Cancel and Clear). A larger font in a combination of upper and lower case is easier to read than words in all upper case.

There must be a tactile identifier (e.g. a raised spot or textured surface) on the number 5 key, to assist the visually impaired. This will signify the central key from which all digits may be deduced. Control keys must have raised tactile markings: X for Cancel, < or | for Clear, and O for Enter. These should be as large as is reasonably possible on the buttons.

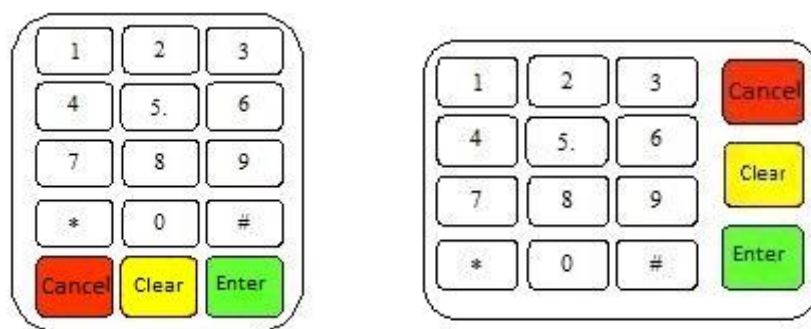


Figure 1 - PIN Pad Layouts as defined for Chip&PIN

Figure 1 shows the keypad layout requirements as specified for the original UK 'Chip & PIN' project. Some principles of this layout remain as requirements, others are more optional.

The layout of the Cancel, Clear and Enter key must be horizontal at the bottom of the keypad, or vertical in a column down the right-hand side of the keypad. The horizontal layout must have the Cancel key on the left, the optional Clear key in the middle, and the Enter key on the right. The vertical layout must have the Cancel key at the top, the optional Clear key in the middle, and the Enter key at the bottom. In all cases, the Enter key will be at the bottom right-hand-side of the keypad.

The star (*) and hash (#) keys shown in figure 1 to the left and right of the zero are optional. They can be included to give the keypad the familiar layout of the telephone keypad but if they are inoperative then they could be removed to simplify the layout of the PIN Pad. If they are functional, then their use must be defined.

Conformance with British standard BS EN 1332-3 (Key pads) is recommended. In particular, this requires that key centres are at least 12mm apart, the gap between keys is at least 3mm, and the tactile indicator on the '5' key is at least 0.7mm high.

Standardisation of the layout is not only aimed at helping those with visual impairment, but at all customers, since a common style of interface is important in achieving usability for everyone.

Keys should be easily found and distinguished from each other by touch, so that a blind person can easily navigate the keypad. This relates to markings on control keys, how big a gap there is between keys, how much they are raised above the underlying surface, and/or whether there are tactile areas to indicate the edges of keys.

All new devices that support PIN entry on traditional keypads are checked to determine if there are any concerns with regards to the accessibility of the devices for blind and partially sighted customers. In some cases RNIB may be involved, and then their approval will be required for a UK approval. Checking may be brief and based on images provided, but in some cases RNIB may wish to inspect a sample of the device and if necessary carry out usability testing.

Adequate positive feedback is required to indicate that a PIN digit has been received, and also indicating the number of digits received so far. This must be both acoustic (to assist blind people) and visual (to assist deaf people). There may also be additional haptic (vibrate) feedback, to help people with both sight and hearing impairment. The feedback must not identify which digits were pressed.

2.4.3 Touchscreen PIN entry and legibility of the display

Where physical keys are replaced by 'soft' keys on a touchscreen, there are additional accessibility and usability requirements that apply, and UK approval of touch screen PIN entry devices is dependent on RNIB giving its approval that the PIN entry function and the cardholder interface are suitable for blind and partially sighted people.

The separate paper 'Touchscreen Accessibility'¹ provides specific requirements and recommendations for touchscreens. The recommendations in that paper apply to all devices in terms of the legibility of payment transaction information and spoken messages for people who are unable to see the screen.

It is important to note that touchscreen PIN entry, and the use of touchscreens generally, are considerably less accessible than mechanical keypads for many users, particularly for blind users but also for others. Physical keys, with tactile markings where appropriate, are significantly more accessible. The methods we have developed for touchscreen use are aimed at making touchscreens more accessible, but they do not make their use easy. They also rely heavily on there being adequate merchant training material provided by the vendor, and merchants being trained in their use and in advising the customer. All touchscreen approvals are conditional on this, so that merchants can comply with equalities legislation and provide accessible products and services. Unattended devices are more difficult, since there is no attendant to assist the customer. In this case, the device must be able to guide the customer through audio output, or merchants must provide alternative ways for payment to be made. Where touchscreen payment terminals are built into kiosks and vending machines, the whole device must be accessible including the selection of goods and services.

While physical keys are preferred over touchscreens, even better accessibility can be available by adding audio output to devices with physical keys.

Where possible it is strongly recommended that merchants with touchscreen devices installed provide an alternative method of payment via a terminal with a mechanical keypad.

2.5 Additional requirements and recommendations

UK Finance strongly recommends that terminals are suitable in all respects for use by disabled people. As part of that, vendors are encouraged to work with RNIB and others to ensure that the needs of all disabled people can be met, including merchant staff.

UK approvals relate to card payment devices, which may themselves be components of other products such as vending machines. If the payment device is a touchscreen device that is intended as a component of a self-service machine, the vendor will be expected to provide implementation guidelines that incorporate the need for the touchscreen accessibility mode to be activated when the self-service machine is itself in accessible mode, and to advise and guide vendors on the implementation so that the accessibility mode is available as required. While beyond the scope of the scheme, and out of scope of this paper, all parties are urged to ensure that self-service machines are fully accessible.

¹ 'Touchscreen Accessibility' at <https://www.ukfinance.org.uk/policy-and-guidance/guidance/card-terminal-security-and-accessibility>

Company number: 10250295.

Registered address: UK Finance Limited, 1 Angel Court, London, EC2R 7HJ

It is strongly recommended that all devices, including non-touchscreen devices, support an accessibility mode in which payment-related messages are spoken as well as displayed. As a minimum it is recommended that the following information is spoken:

- The amount
- Any instructions (e.g. where to insert the card, the layout of the number pad, etc), but these instructions should be interrupted when the customer inserts their card, to speed up the process for people who are familiar with the device
- Any messages (e.g. Enter PIN, Payment approved/cancelled/declined)
- If the device supports PIN entry, how many digits have been entered (e.g. “first digit entered”), and if digits have been deleted.

3 Lists of approvals

3.1 General points about approvals

Approvals are for specific product configurations. Some of the approvals are conditional, and some are of components rather than fully functional terminals. Conditions may include restriction to specific uses, and even to a specific merchant. For further details of each approval please contact the vendor. Limited waivers for pilot implementations are not listed.

Approvals are not a guarantee of security, accessibility or usability. They are based on evaluations by approved laboratories and other external organisations against sets of agreed requirements, and are only valid on the day they are performed. Security evaluations and approvals do not address functionality, and do not cover the payment application unless otherwise stated. They focus on protection against external attack. Accessibility assessments are based on devices as presented to RNIB, and might be invalidated if the terminal is subsequently modified. Not all aspects of accessibility are addressed, such as suitability for wheelchair users or people with dexterity issues. Accessibility may be impacted by the way in which a device is deployed.

The approval dates shown in the lists below do not necessarily indicate that a device has become too old to be deployed, since some devices may remain secure for many years. However, the 3-year and 6-year certificate renewal periods for Common.SECC certificates indicate the need for periodic reviews, and UK Finance requires that approvals are refreshed with a reassessment at least every 6 years. **Devices that have not been reassessed for security and accessibility for 6 years are shown in red in the tables below.**

Vendor and device names shown are those that were used when the device was approved. Absence of a device from the lists does not necessarily mean that it is not approved, since vendor and device names may change. If a device is registered with Common.SECC as having more than one vendor / device name, then each vendor / device name will be listed here.

3.2 Approvals since the start of Common.SECC

The list below identifies all the card payment terminals approved in the UK since security evaluations started to be performed under the Common-SECC consortium.

The "Ver" column indicates a version identifier to be appended to the device name where it is necessary to distinguish between two different devices with the same marketing name.

The "Security Approval" column includes the original approval year and (where applicable) the year when a subsequent full reassessment was most recently performed and certified as part of the Common.SECC maintenance and surveillance process.

In the "Accessibility Approval" column, approvals by RNIB are indicated by a year number. They apply to all touchscreen PIN entry devices, and also to some devices with mechanical keypads. Most devices with mechanical PIN entry keypads have been approved by UK Finance on the basis of images of the device and the presence of adequate tactile and visual features, and these are marked "Y". Devices that do not support PIN entry are also marked "Y". Devices having a touchscreen for PIN entry are marked with a "T". Devices having a mechanical PIN entry keypad that also provide audio output are marked with an "A".

Vendor	Device	Ver	Security Approval	Accessibility Approval
BBPOS	WisePad 2		2018	Y
BBPOS	WisePad 2 Plus		2018	Y
BBPOS	WisePad 3		2020, 2023	Y
BBPOS	WisePad 3S		2020	Y
BBPOS	WisePad 3	2	2022	Y
BBPOS	WisePad 3S	2	2022	Y
Castles	MP200		2017, 2019	Y
Castles	SATURN1000 Version 2		2023	2023 T
Castles	S1P		2023	Y
Castles	S2L		2023	Y
Castles	VEGA3000		2017	Y
Castles	V3P3		2023	Y
Castles	V3CT3		2023	Y
Datecs	BluePad-50 v2		2019, 2022	Y
Datecs	BluePad-55		2018, 2021	Y
Datecs	BluePad-55 v2		2020, 2023	Y
Datecs	BluePad-500		2018	Y
Datecs	BluePad-5000 v2		2019, 2022	Y
Datecs	Card Reader One		2017, 2020	Y
Datecs	Card Reader One v1		2020, 2023	Y
Datecs	PD20-1		2021	Y
Datecs	Zettle Terminal		2021	2022 T
FEIG	cVEND PIN + SHCR 862 SR		2019, 2023	Y
FEIG	cVEND PIN		2023	Y
FEIG	cVEND plug		2023	Y
Fiserv	Clover Flex C400, C401E and C403		2017, 2019	2019 T
Fiserv	Clover Mini C302E / C303E / C503E		2018, 2019	2019 T

Vendor	Device	Ver	Security Approval	Accessibility Approval
Gilbarco	Flexpay Horizon-2		2020	Y
Ingenico	AXIUM D7		2018, 2019	Y
Ingenico	AXIUM DX4000		2023, 2024	2023 T
Ingenico	AXIUM DX8000-5		2022, 2024	2022 T
Ingenico	AXIUM RX5000		2024	Y
Ingenico	AXIUM RX7000		2024	Y
Ingenico	Desk/3200		2017, 2021	Y
Ingenico	Desk/3500		2017, 2021	Y
Ingenico	Desk/5000		2016, 2023	Y
Ingenico	iPP3xx		2017, 2020	Y
Ingenico	iSMP4		2017, 2020	Y
Ingenico	iUP250 with iUR250		2017, 2020	Y
Ingenico	Lane/3000 and Desk/1500		2018, 2020	Y
Ingenico	Lane/3600 and Desk/1700		2023	Y
Ingenico	Lane/5000		2017, 2021	Y
Ingenico	Lane/5000 LE		2023	Y
Ingenico	Lane/7000		2018	Y
Ingenico	Link/2500		2017, 2023	Y
Ingenico	Move/3500		2016, 2023	Y
Ingenico	Move/5000		2016, 2023	Y
Ingenico	RoamData Moby8500		2017	Y
Ingenico	Self/2000		2023	Y - contactless
Ingenico	Self/4000		2020	Y
Ingenico	Self/7000 and Self/8000		2022	Y
Invenco	G6-300		2020, 2023	Y
Miura	M010		2019, 2022	Y
Miura	M020		2018, 2023	Y
NEXGO	N86		2022	2023 T
PAX	A30		2020, 2023	Y
PAX	A35		2021	Y
PAX	A50		2021, 2023	2021 T
PAX	A77		2020	2021 T
PAX	A77	2023	2023	2021 T
PAX	A80		2020, 2023	Y
PAX	A920		2020, 2022	2020 T
PAX	A920Pro		2021, 2023	2021 T
PAX	D135 MSR		2023	Y - no PIN
PAX	IM10		2020	Y
PAX	IM15		2022	Y
PAX	IM30		2021, 2022	2021 T
PAX	IM30	2023	2023	2023 T
PAX	IM300/IM500/IM700		2018, 2021	Y
PAX	IM700		2022	Y
PAX	Q20 and Q20 U		2020	2021 T
PAX	Q25		2020, 2023	Y
PAX	Q30		2018, 2021, 2023	Y
Poynt	Poynt 5 and Poynt Smart Terminal V2.0		2019	2019 T
Poynt	Smart Terminal V3.0		2023	2022 T
Quest	UT430		2019	Y
SUNMI	T5810 (P2 Mini)		2023	2023 T

Vendor	Device	Ver	Security Approval	Accessibility Approval
SUNMI	T6800		2022	2022 T
SUNMI	T6920		2022	2022 T
SUNMI	T6A10 (P2 Smartpad)		2023	2023 A
Verifone	Carbon Mobile 5		2021	2021 T
Verifone	e235		2023	Y
Verifone	e280		2018, 2020	2021 T
Verifone	e285		2017, 2020	Y
Verifone	M400		2017	Y
Verifone	M400	2	2018, 2021	Y
Verifone	M425/M450		2024	Y
Verifone	P400		2016, 2022, 2023	Y
Verifone	P630		2022	Y
Verifone	T650p		2021	2021 T
Verifone	UX410		2017	Y
Verifone	V200c		2016, 2020	Y
Verifone	V200c	2	2018, 2022	Y
Verifone	V200t – V205c		2017	Y
Verifone	V210		2022	Y
Verifone	V240m		2017	Y
Verifone	V400c		2018, 2022	Y
Verifone	V400m		2017	Y
Verifone	V400m	2	2018, 2023	Y
Verifone	Vx690		2017, 2021	Y
Verifone	X10 Carbon		2017, 2018	2021 T
Worldline	Valina		2018, 2022	2020 T
XAC	xCL_AT-150		2021	Y
XAC	xCL_AT-150 R		2021	Y
XAC	xCL_AT-170		2021	Y
XAC	xCL_AT-170 R		2021	Y
XAC	xCL_RP-10		2020	Y

3.3 Payment Application approvals

Payment applications certified under Common.SECC are automatically approved for use in the UK. The following table shows currently approved payment applications.

Vendor	Application	Ver	Approval
Fiserv	Clover nexo Payment Application 1, software version 1.0-7595		2021
Fiserv	Clover nexo Payment Application 2, software version 1.0-7856		2021

3.4 Approvals prior to Common.SECC

The list below identifies card payment terminal approvals where the security evaluation was not performed under the Common-SECC consortium.

Vendor	Device	Security Approval
Bluebird	BIP 1300	2010
Bluebird	Vx675 Wi-Fi	2015
CCV	OPM-C60 + SCR + COR	2017
CCV	OPP-C60 + SCR + COR	2017
CCV	Motion Parking Solution	2017
Datecs	Bluepad 50 aka BP50	2014
Datecs	Bluepad 5000	2016
Fiserv (First Data)	FD-40	2014
Fujitsu	B-PAD	2006
Gilbarco	Modulo M2 Motorizzato	2012
Gilbarco	Modulo M3 Motorizzato	2013
HTEC	Hydra OPT	2008
ICP	BIA D-HP	2014
ICP	BIA-O with CR700 O-HP reader	2015
ICP	CP500	2014
Ingenico	CAD30 – UPP	2010
Ingenico	CAD30 – UxR	2010
Ingenico	EFT930 C'less, inc EFT930G, EFT930B	2009
Ingenico	EFT930, inc EFT930B, EFT930G, EFT930S	2009
Ingenico	i3070	2008
Ingenico	i3070 contactless	2009
Ingenico	i3300	2005
Ingenico	i3380	2007
Ingenico	i5100	2007
Ingenico	i7780	2007
Ingenico	i7810	2007
Ingenico	i7910	2007
Ingenico	i9500	2011
Ingenico	iCMP PED	2013
Ingenico	ICT 220	2009
Ingenico	ICT 250	2009
Ingenico	IPA280	2010
Ingenico	IPP 320 / 350 MD	2010
Ingenico	ISC350	2012
Ingenico	iSMP	2011
Ingenico	IWL 220 PED	2011
Ingenico	IWL 250	2011
Ingenico	iWL280	2013
Ingenico	ML30 Series	2010
Ingenico	P30 Series including P30 and P30 Contactless	2010
Ingenico	UN250	2012
Invenco	G6-OPT	2016
Itos	Mped – 400	2011
ITWell	C200M	2009
Miura Systems	M Series	2011
Miura Systems	M007	2014
Miura Systems	M010	2014
Miura Systems	Miura Shuttle	2012
Motorola	DCR7x00 – 200R	2009
PAX	S300	2014
PAX	S800	2014

Vendor	Device	Security Approval
PAX	S900	2014
Secure Electrans	HomePay HP 100 Series	2013
Spire Payments	Artema Hybrid	2007
Spire Payments	Artema Modular	2009
Spire Payments	M4200 series	2008
Spire Payments	MPT600 Series	2011
Spire Payments	Paycell POSMate 210	2011
Spire Payments	Paycell POSMate 211	2011
Spire Payments	S9PCI	2009
Spire Payments	SPc5 Counter-top	2016
Spire Payments	SPg7 Handheld	2016
Spire Payments	Spire SPc50	2014
Spire Payments	Spire SPp10	2014
Spire Payments	Spire SPp30	2014
Spire Payments	Spire SPw60 Dock	2014
Spire Payments	Spire SPw70	2014
Spire Payments	SPm2	2016
Spire Payments	T4200 Series	2008
Tokheim	Crypto VGA	2008
Tokheim	Crypto VGA 2.0	2012
Verifone	Artema Hybrid	2007
Verifone	Artema Modular	2009
Verifone	e210 Series - Previously Vx600	2011
Verifone	e265	2016
Verifone	e355	2016
Verifone	e315M	2015
Verifone	FOPT	2007
Verifone	M2100	2007
Verifone	Magic 1100	2005
Verifone	Magic 3 – C	2008
Verifone	Magic 3 – M and W	2008
Verifone	Magic 3 – P	2008
Verifone	Magic 3 – R	2008
Verifone	Magic 3 – X	2008
Verifone	Magic 5100	2005
Verifone	Magic X1000	2005
Verifone	Magic X1000 – 5100	2007
Verifone	MagIC X1000 DECT	2007
Verifone	OP3100	2008
Verifone	Optimum M4200 series	2008
Verifone	Optimum P2100 PCI	2009
Verifone	Optimum T4200 series	2008
Verifone	S9PCI	2009
Verifone	SC5000	2008
Verifone	SCR710	2011
Verifone	Secura SIM-IC	2007
Verifone	Secura Version 1.0	2006
Verifone	SIMIC/SIMIH	2008
Verifone	SIMMH/SIMMC	2008
Verifone	T2100	2007
Verifone	Ux300	2016

Vendor	Device	Security Approval
Verifone	VX510 Series including VX510	2007
Verifone	VX510 GPRS	2009
Verifone	VX520	2011
Verifone	VX570	2007
Verifone	Vx600	2016
Verifone	VX610	2008
Verifone	VX670 Series including VX670	2007
Verifone	VX670 ER	2009
Verifone	Vx675	2012
Verifone	VX680	2011
Verifone	VX700 in conjunction with SCR710	2011
Verifone	VX810	2008
Verifone	VX820	2011
Verifone	Xplorer Version 1.0	2005
Worldline	XENTA	2009
Worldline	XENTEO	2008
Worldline	XENTEO ECO	2014
Worldline	YOMANI	2010
Worldline	YOMANI XR-ML	2014
Worldline	YOMOVA	2016
Worldline	YOXIMO	2014
Zakus	8006L2	2016
Zakus	FD130 (FD130 with FD35GT PED)	2013, 2014
Zakus	xAPT-103	2013
Zakus	xAPT-103P	2014
Zakus	xUPT-303+P90	2015

4 Further information

The latest version of this paper, the paper on touchscreen accessibility, and contact details for vendors, can be found at <https://www.ukfinance.org.uk/policy-and-guidance/guidance/card-terminal-security-and-accessibility>.

Contact email addresses:

- UK Finance terminal approval scheme: uktas@ukfinance.org.uk
- RNIB User Experience Team: nppd@rnib.org.uk
- Common.SECC: common-secc@ukfinance.org.uk

---o0o---