PAX Remote Key Injection

4-21-2025

V1.14

Preface

The Programs (which include both the software and documentation) contain proprietary information; they are provided under a license agreement containing restrictions on use and disclosure and are also protected by copyright, patent, and other intellectual and industrial property laws. Reverse engineering, disassembly, or decompile of the Programs, except to the extent required to obtain interoperability with other independently created software or as specified by law, is prohibited.

This document is provided for informational purposes only. All features and specifications are subject to change without notice. If there are any problems in the documentation, please report them to PAX in writing. This document is not warranted to be error-free. Except as may be expressly permitted in the license agreement for these Programs, no part of these Programs may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose.

Security Notice: No part of this publication may be copied, distributed, stored in a retrieval system, translated into any human or computer language, transmitted, in any form or by any means, without the prior written consent of PAX Technology, Inc.

PAX is a registered trademark of PAX Technology Limited in China and/or other countries. All other trademarks or brand names are the properties of their respective holders. PAXBiz, PAXSTORE, POSDK, The PAX Portfolio Manager and/or other PAX products referenced herein are either trademarks or registered trademarks of PAX Technology, Inc. or its Affiliates. Other product and company names mentioned herein may be trademarks of their respective owners.

The *Bluetooth*® word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. and any use of such marks by PAX Technology, Inc. is under license. Other trademarks and trade names are those of their respective owners.

EMV® is a registered trademark in the U.S. and other countries and an unregistered trademark elsewhere. The EMV trademark is owned by EMVCo, LLC.

Android is a trademark of Google LLC.

Technical Support

If there is a problem while installing, registering or operating this product, please make sure to review the documentation. If unable to resolve the issue, please contact PAX.

Monday-Friday 9:00 AM to 1:00 AM
Saturday 9:00 AM to 5:00 PM
Sunday Closed

The level of access to this Service is by the support plan arrangements made between PAX and the Organization. Please consult this support plan for further information about entitlements, including the hours when telephone support is available.

Technical Support Contact Information

Phone: (877) 859-0099
Email: support@pax.us
URL: www.pax.us

Revision History

Version	Page(s)	Description	Approved By	Approval Date	Published Date
v1.0	22	Initial draft	Li Yuan	06/26/2018	06/26/2018
v1.01	22	1. Made various grammar changes throughout document. 2. Changed version to 7/11/ 2018 v1.01. 3. Updated Cover Page Layout 4. Added Preface 5. Added Disclaimer 6. Updated Table of Contents 7. Added Error Message Table 8. Added document status as DRAFT 9. Added DRAFT watermark 10. Updated the version format 11. Updated the Revision History table format	Clif Euler	07/11/2018	07/11/2018
v1.02	22	1. Added “Please contact PAX customer support for serial number registration.” In three locations in the document. 2. Changed the version to 7-12-2018 v1.02	Clif Euler	07-12-2018	07-12-2018
v1.03	22	1. Update RKI Server IP Address 2. First release	Li Yuan	08-13-2018	08-13-2018
v1.04	22	1. Add RKI instruction for E500	Li Yuan	08-27-2018	08-27-2018
v1.05	22	1. Updated RKI support terminal type	Qin Yang	03/27/2019	03/27/2019
v1.06	22	1. Updated RKI support terminal type	Qin Yang	06/07/2019	06/07/2019

Version	Page(s)	Description	Approved By	Approval Date	Published Date
v1.07	22	1. Add check OS version 2. Update Monitor download key & check key info process 3. Update Prolin check key info	Qin Yang	06/07/2019	06/07/2019
v1.08	22	1. Add the S80/S500 basic application version of supporting RKI	Qin Yang	06/07/2019	06/07/2019
v1.09	22	1. Update Prolin Remote Key injection steps 2. Delete Version number in Preface	Xuefei Meng	08/22/2019	08/22/2019
v1.10	22	1. Added RKI instruction for External PINPAD 2. Added RKI instruction for S80-SP30 3. Added RKI instruction for S500-SP20V4 or S80-SP20V4 4. Added RKI Server information for SP20V4 OS Version Check 5. Update The Operating System version of support RKI	Xuefei Meng	10/15/2019	10/15/2019
v1.11	22	1. Updated RKI support terminal type 2. Updated Prolin OS RKI Download Menu steps.	Xuefei Meng	10/30/2019	10/30/2019
v1.12	22	1. Update “The Operating System version of support RKI” of A80	Xuefei Meng	11/08/2019	11/08/2019
v1.13	34	Updated the document with new sections accordingly.	Caroline Percy	10/17/2024	10/21/2024
V1.14	31	1. Added images for S300 (Monitor plus OS) 2. Added RKI instruction for A80-Q25 3. Added Error Message/ Code Definition 4. Updated “The Operating System version of support RKI”	Mezohn Owens	4/18/2025	4/18/2025

Table of Contents

1. Operation Environment

1.1 RKI Server Information

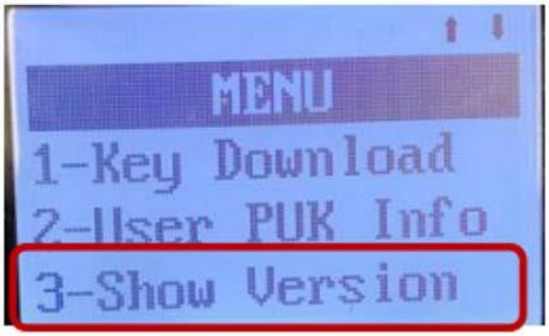
URL	https://rki.pax.us
IP Address	173.224.73.190
Remote Key Injection Port	33519

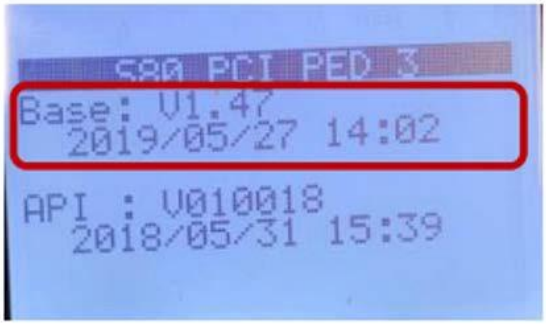
1.2 RKI Operating System Requirements

1.2.1 Monitor Plus OS Version Check

For more information on RKI Operating System Requirements, **please see the Appendix: The Operating System version of support- RKI.**

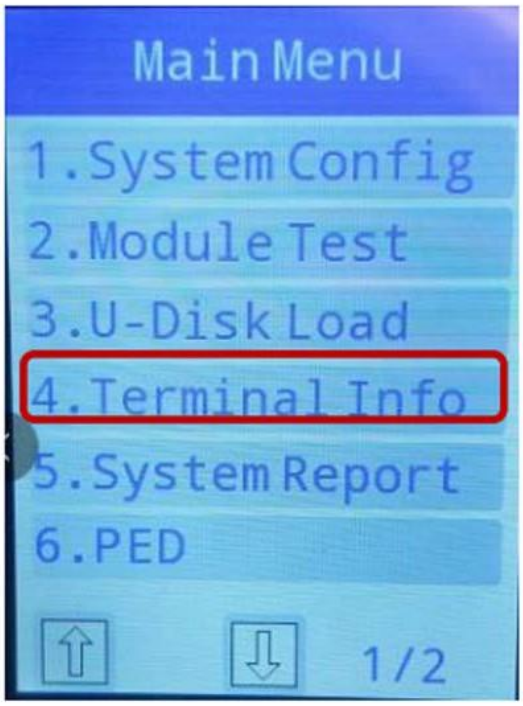
1. Power cycle the terminal.
2. During the self-test, press the [**MENU**] button.
3. On the main menu, select [**Show Version**]. Then, select the [▼ **button**], the [**Base version**] will appear.

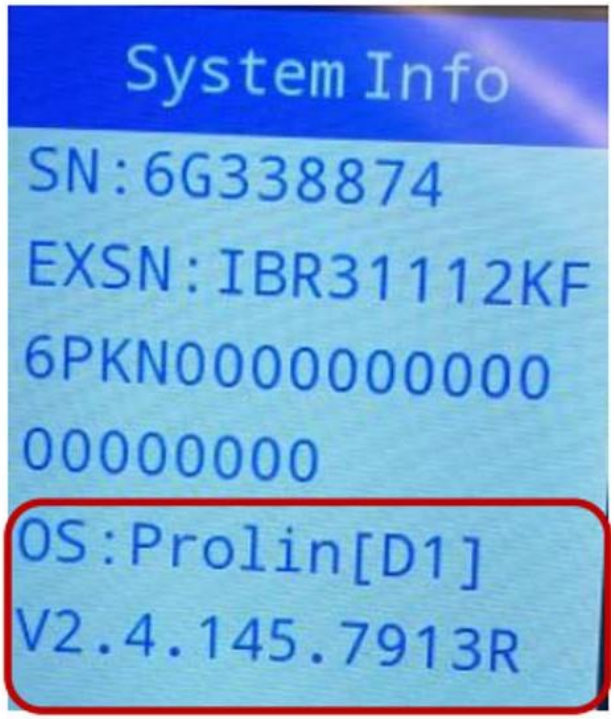




1.2.2 Prolin OS Version Check

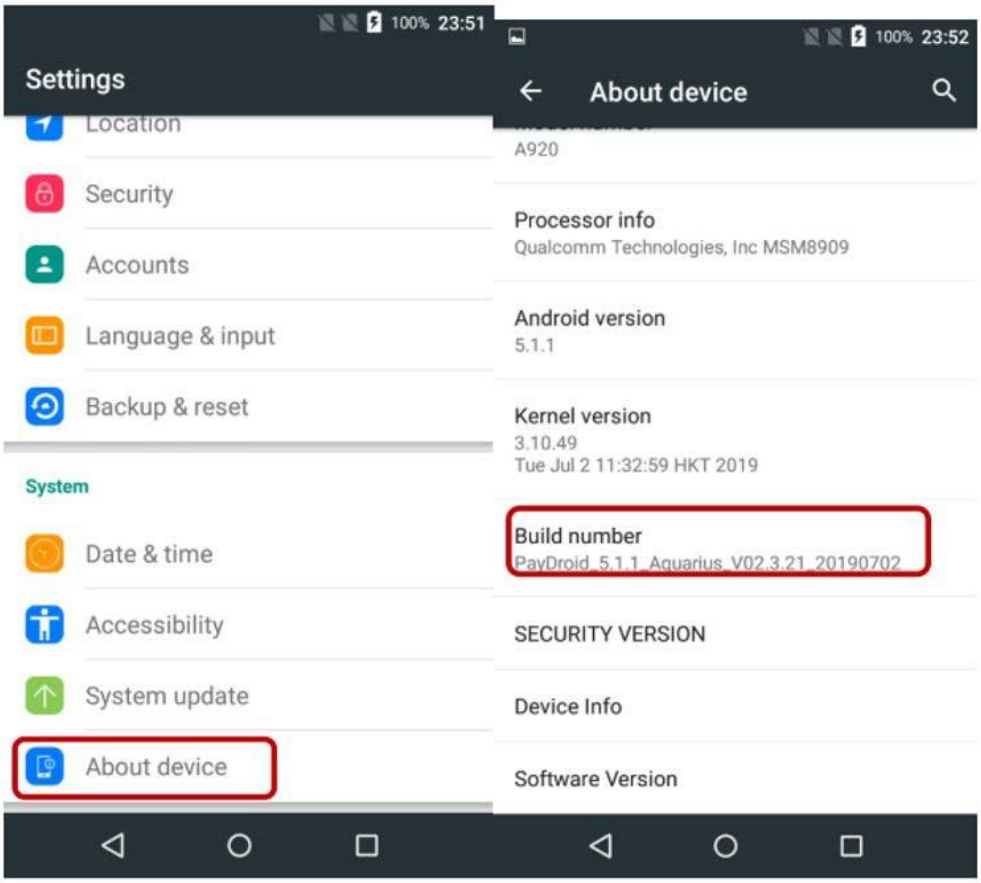
1. Power cycle the terminal.
2. During the self-test, press the [**#2**] button until the Menu screen appears.
3. On the [**Main Menu**], select [**4.Terminal Info**]. Then, check the [**OS version**].





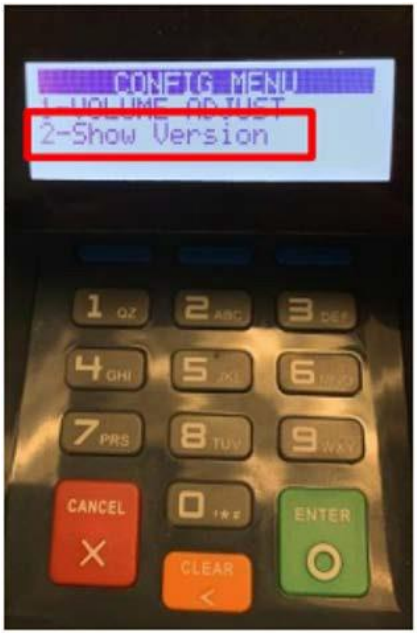
1.2.3 ANDROID OS VERSION CHECK

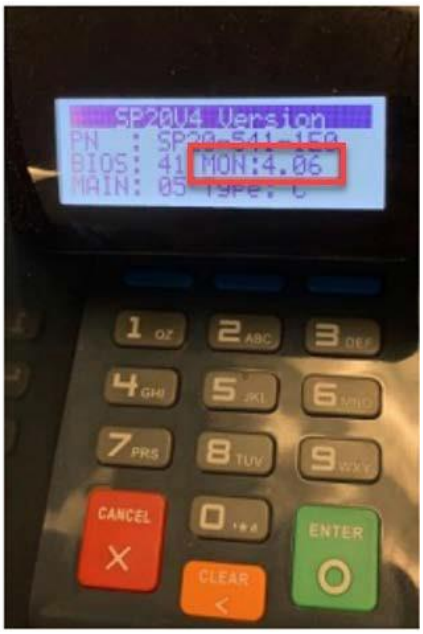
1. Power cycle the terminal.
2. Select [**Settings**], [**About device**], the [**Build number**] will appear.



1.2.4 SP20V4 OS Version Check

1. Power cycle the terminal.
2. Press the [**ENTER**] button. The [**CONFIG MENU**] will appear.
3. Press the [**PINPAD ▼ button**] twice.
4. Under the **[CONFIG MENU]**, select [**2. Show Version**].
5. Press the [**PINPAD ▼ button**].
6. In the [**SP20V4 Version menu**], view [**OS Version MON: 4.05 or above**].





2. Remote Key Injection

2.1 Monitor Plus OS Terminal

If the base version is V1.33 – V1.46, the Monitor Plus OS menu does not provide the Certificate Info or Key Injection selection. Those operations are implemented on the BroadPOS basic application level, except for terminal **S300**. For S300, those operations are implemented on the BroadPOS Application level.

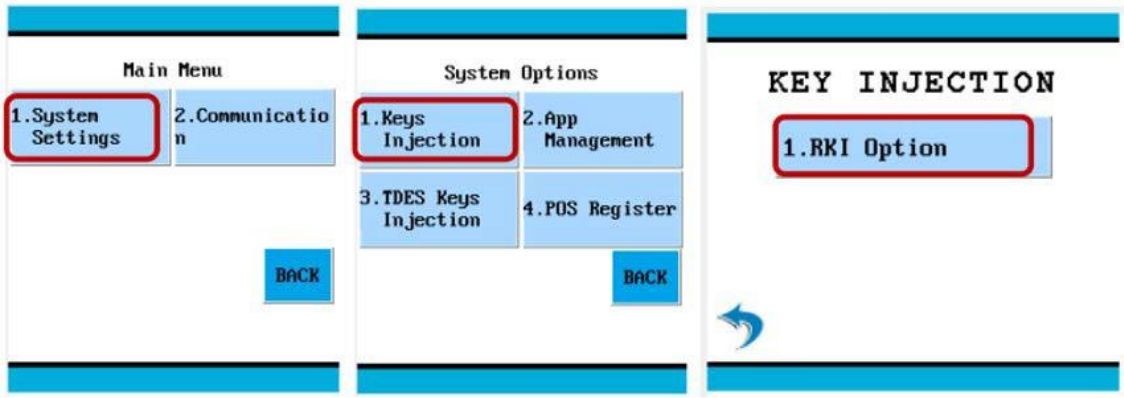
2.1.1 BroadPOS Basic Application or BroadPOS Application

Terminal Mode	Basic Application Version Of Supporting RKI
S80	BasicSystem_S80_V1.00.12_20190614
S500	BasicSystem_S500_V1.00.3_20190614

a. RKI Option Menu

On the [**Main Menu**] select [**System Settings**], [**Keys Injection**], [**RKI Option**].

Below are the screen shots for the PAX S300.

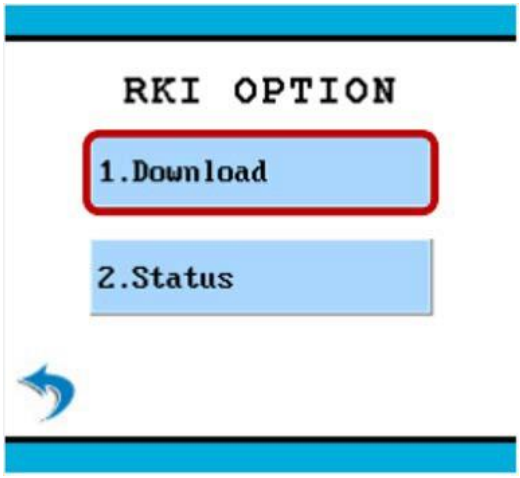


b. Check CA & Remote Key Injection

Before initiating the Remote Key Injection, please make sure the terminal serial number has been registered into the RKI server. Please contact PAX Customer Support Department for serial number registration.

For more information on serial number registration, please contact PAX Support at (support@pax.us).

Select [**RKI Option**]. Then, select [**Download**]. After the Remote Key Injection is successful, the [**Download Success**] message will appear on the screen. If the CA key has not been installed in the terminal, the terminal will display an error message [**PUK Missing**].

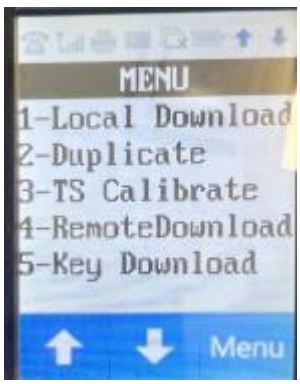


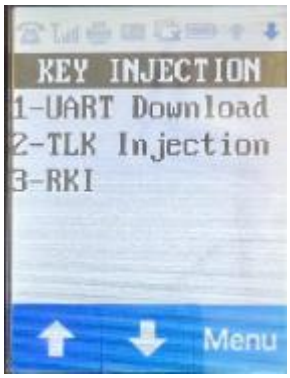
2.1.2 Monitor Plus OS (Base version V1.47 or above)

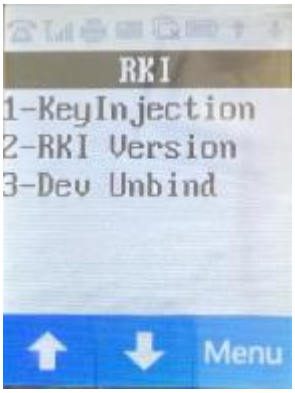
a. RKI Download Menu

1. Power cycle the terminal.
2. During the self-test, press the [**MENU**] button.
3. Select the [**button**]
4. Select [**1. Key Download**].

Below is a screen shot for the PAX S300.





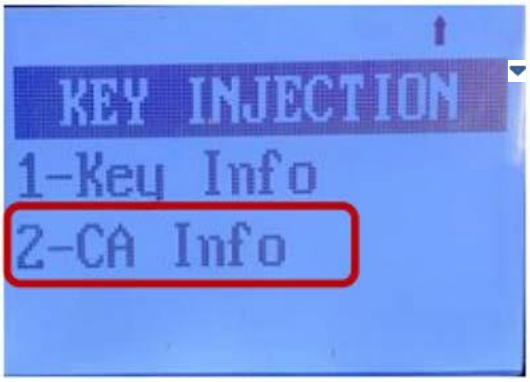


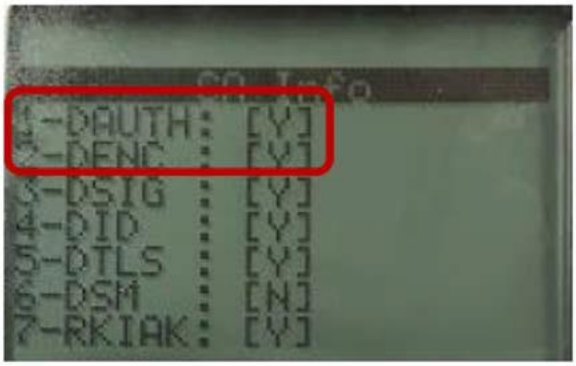
b. Check CA

Under the [**Key Injection**] menu, select the [down arrow **button**]. Then select, [**2-CA info**]. Verify both

[**1. DAUTH Cert**] and [**2. DENC Cert**] has certificates.
For more information on certificates, please contact PAX Support at (support@pax.us).

The body should contain the main content of the document, divided into logical sections and subsections with clear headings and subheadings. Visuals such as tables, lists, diagrams, screenshots or code snippets can be used to illustrate points and provide examples.



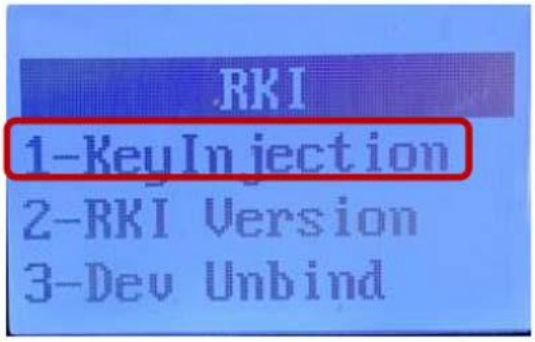


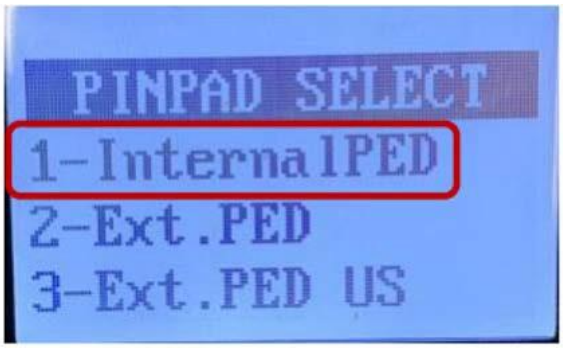
c. Remote Key Injection

Before initiating the Remote Key Injection, please make sure the terminal serial number has been registered into the RKI server.

Under the [**Key Injection**] menu, select [**3.RKI**], [**Key Injection**]. Then, select [**1. Internal PED**], press the communication method, e.g. [**1. TCP**]. Enter [**rki.pax.us**] under [**Remote IP**]- enter [**33519**] under [**Remote Port**] press [**1**] to enable.

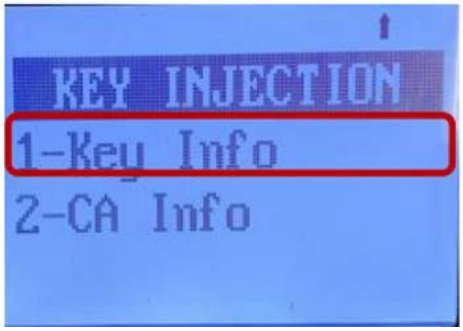
All Rights Reserved Page 5DHCP. After the remote key injection has successfully downloaded, the [**Download Success**] message will appear.





d. Check key information

Under the [**Key Injection**] menu, select [**button**], then select [**1-Key Info**].



2.2 Prolin OS Terminal

2.2.1 PROLIN OS

a. RKI Download Menu

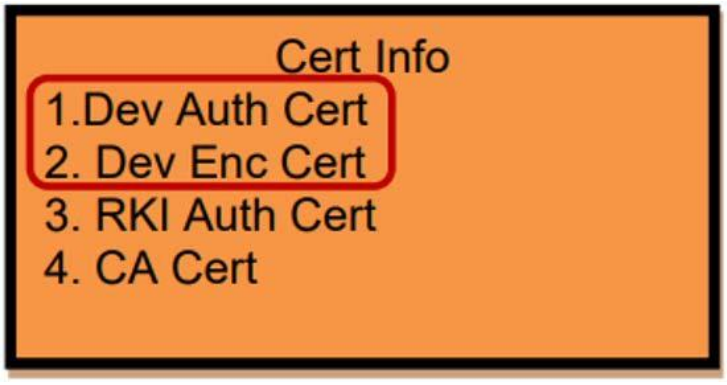
1. Power cycle the terminal.
2. During the self-test: If the terminal has a physical keyboard, press the [**# 2**] button until the [**Main Menu**] appears.

If the terminal does not have a physical keyboard, press the touch screen until the [**Main Menu**] appears.

3. Under the [**TM Test**]menu, select [**6. PED**].

b. Check CA

Under the [**PED**] menu, choose [**3. Cert Info**], verify both [**1. Dev Auth Cert**] and [**2. Dev Enc Cert**] has certificates.
For more information on certificates, please contact PAX Support at (support@pax.us).



c. Remote Key Injection

Before starting the Remote Key Injection, please make sure the terminal serial number has been registered into RKI server.

Under the [**PED**] menu, select [**1. RKI**], [**1. Internal PED**], then select the communication method.

If users select [**TCP**], follow the steps listed below:

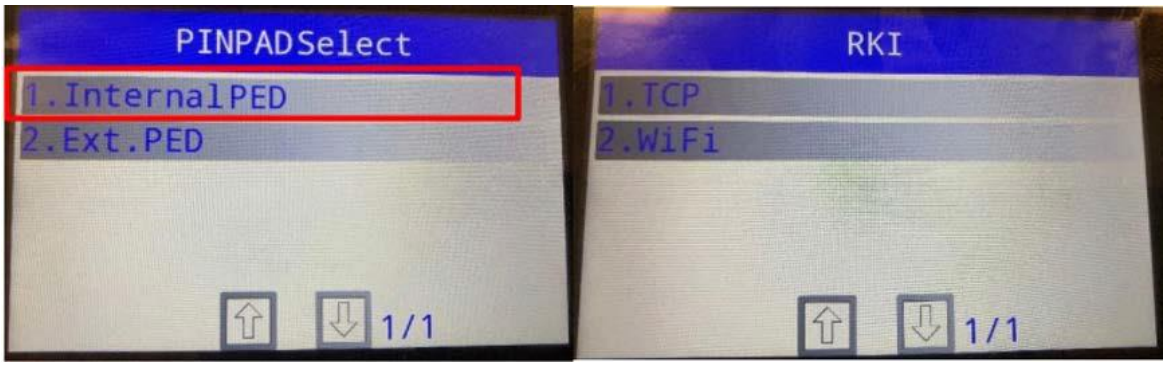
Select [**TCP**], enter [**rki.pax.us**]. Under [**Remote IP**], enter [**33519**], under [**Remote Port**] press [**1.Yes**] to enable DHCP.

If users select [**Wi-Fi**], follow the steps listed below:

Important Note: Before completing the RKI steps, the IP address should go through Wi-Fi.

Select [**Wi-Fi**], enter [**rki.pax.us**]. Under [**Remote IP**], enter [**33519**], under [**Remote Port**] press [**1.Yes**] to enable DHCP. Select [**Wi-Fi**], enter the [**Wi-Fi**] Password.

After the Remote Key Injection is successfully downloaded, the terminal will display a [**Download Success**] message.



P.S: Get IP address through Wi-Fi

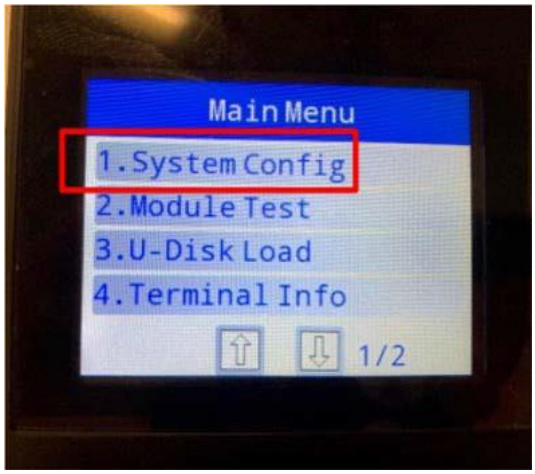
When selecting Wi-Fi as communication method to Remote Key Injection, please follow the steps listed below before Remote Key Injection (e.g. D190/D195/IM20/D220):

1. Power cycle the terminal.
2. During the self-test:

If the terminal has a physical keyboard, press the [**2**] button until the [**Main Menu**] appears.

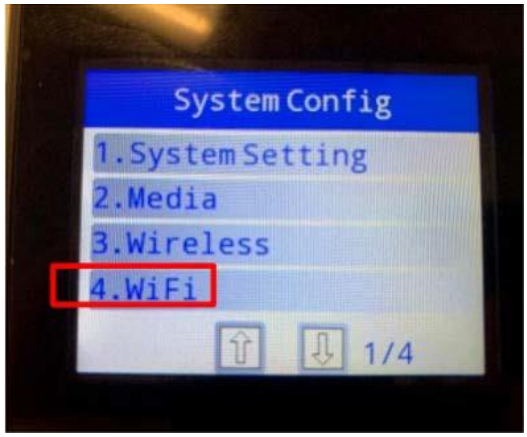
If the terminal does not have a physical keyboard, touch the screen until the [**Main Menu**] appears.

3. Select [**1. System Config**]



3. Enter password:123456

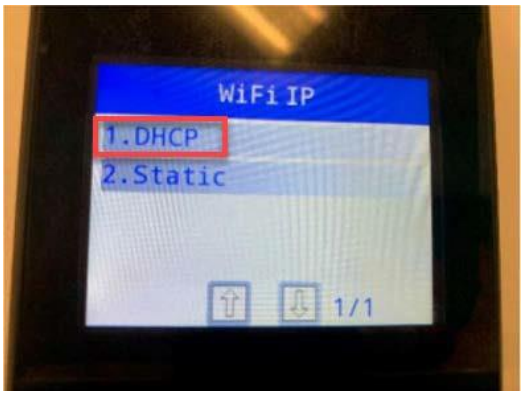
4. Select [**4. Wi-Fi**]

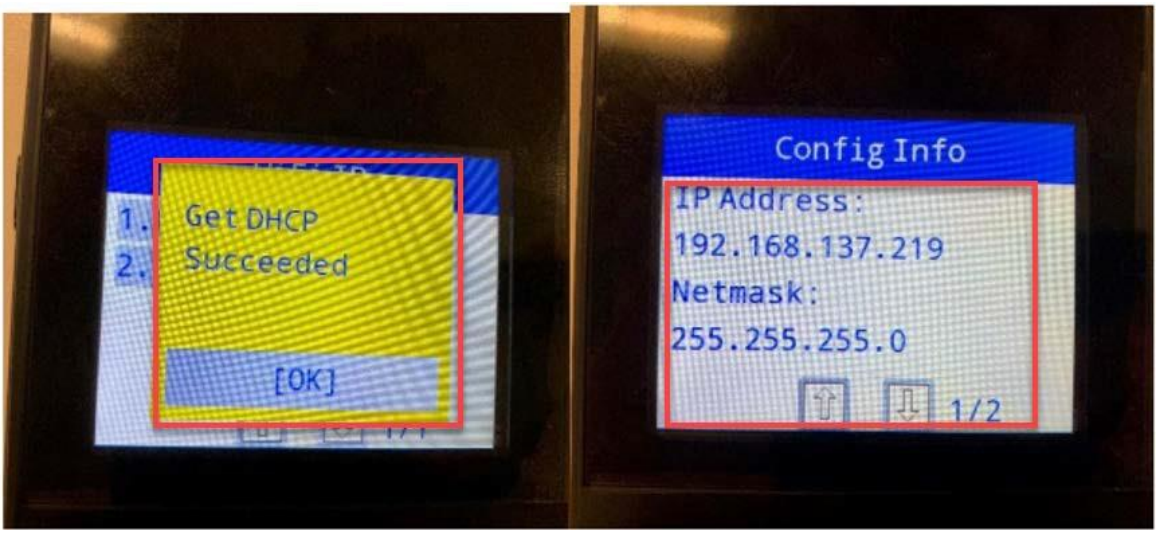


5. Select [**1. AutoSet**]

6. Pick your network and input the password. After entering the password, the device will display a [**connect success**] message. Then, navigate to [**Wi-Fi IP**].

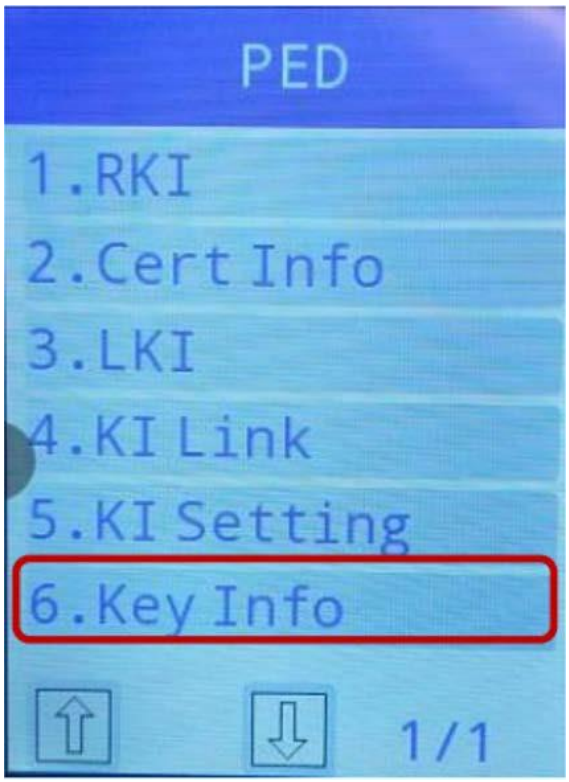
7. Select [**1. DHCP**], then, view the [**IP Address from the network**].





d. Check key information

1. Under the [**PED**] menu, select [**6.key Info**]



2.2.2 BroadPOS Application (currently not supported on Prolin)

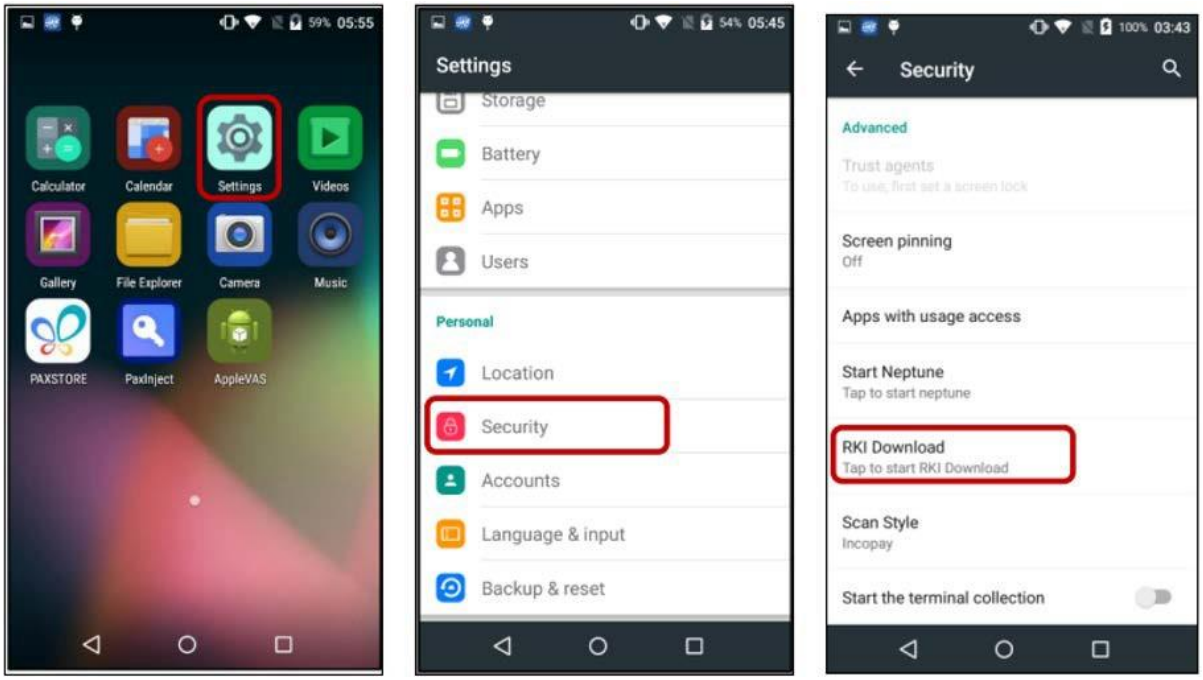
The RKI BroadPOS Application-level operation is the same as Monitor Plus OS Terminal (see 2.1.2BroadPOS Application).

2.3 Android Terminal

2.3.1 Android OS

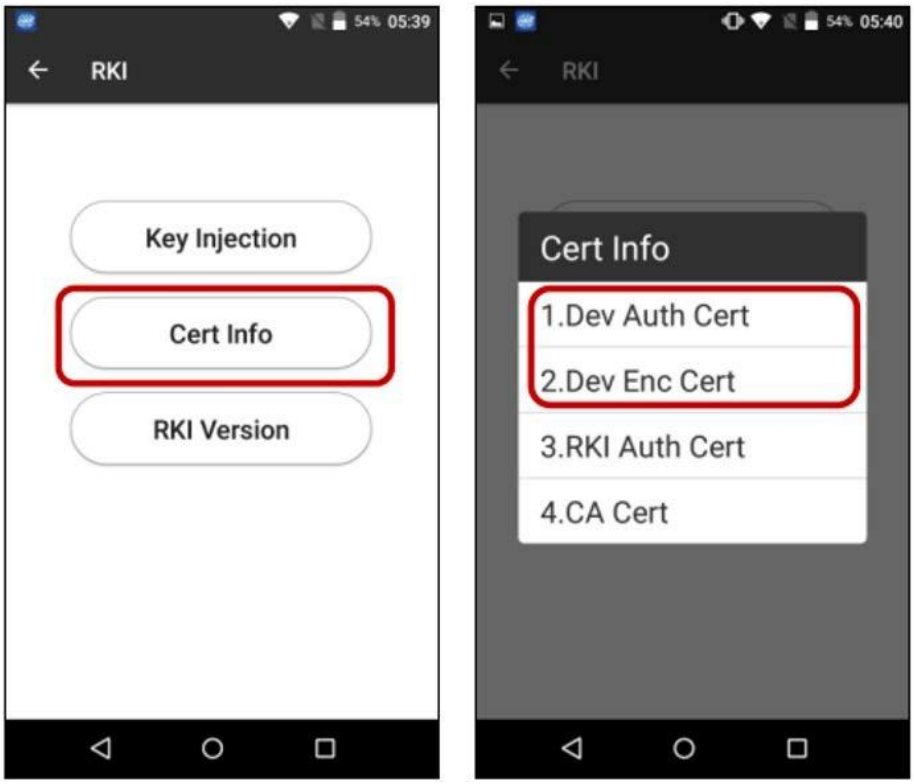
a. RKI Download Menu

1. Select [**Settings**], [**Security**], [**RKI Download**]



b. Check CA

1. Under the [**RKI**] menu, select [**Cert Info**]. Select both [**1. Dev Auth Cert**] and [**2. Dev Enc Cert**] has certificates.



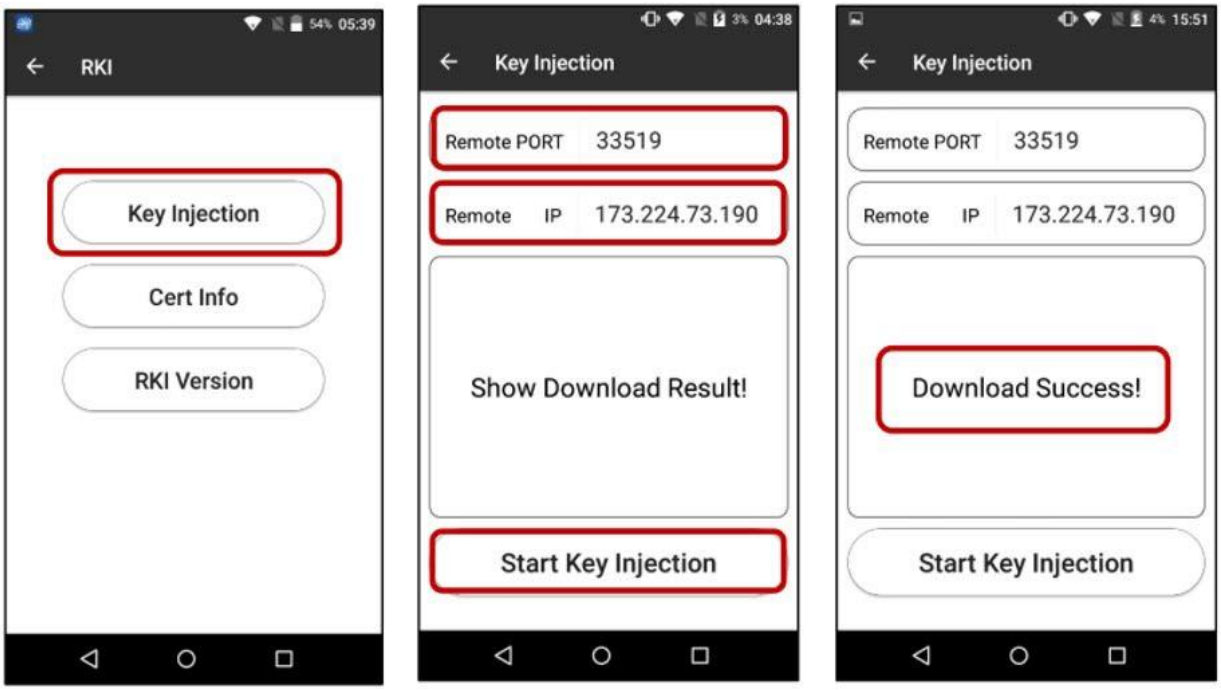
c. Remote Key Injection

Before initiating the Remote Key Injection, please make sure the terminal serial number has been registered into the RKI server.

For serial number registration please contact PAX Customer Support at support@pax.us.

1. Under the [**RKI**] menu, select [**Key Injection**]. The default Remote Port is [**33519**], default Remote IP is [**rki.pax.us**]. If the builder number is equal or above V02.3.14, press [**Start Key Injection**].

2. Enter [**173.224.73.190**] in Remote IP then, press [**Start Key Injection**]. After a successful Remote Key Injection, a [**Download Success**] message will appear.



2.3.2 BroadPOS Application (currently not supported on Android)

The RKI BroadPOS Application-level operation is same as Monitor Plus OS Terminal (see 2.1.2 BroadPOS Application).

2.4 E500-Q20

2.4.1 Q20

Before starting Remote Key Injection, make sure Q20 is in idle screen.

2.4.2 E500

a. PDM Version

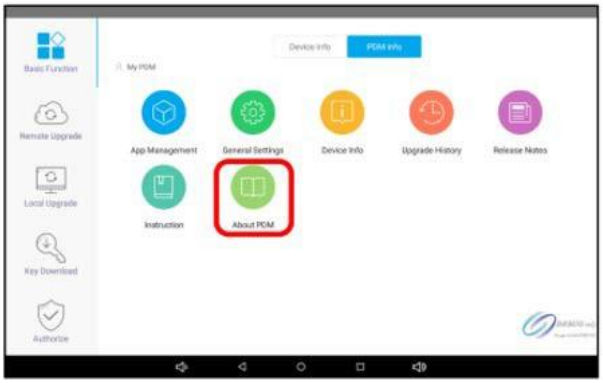
The minimum version of PDM that supports RKI is V2.00.00.

Steps for PDM version:

Select [**PDM**], [**PDM Info**]. Under Basic Function, select [**About PDM**]

1. Select [**PDM**], [**PDM Info**]. Under Basic Function, select [**About PDM**]



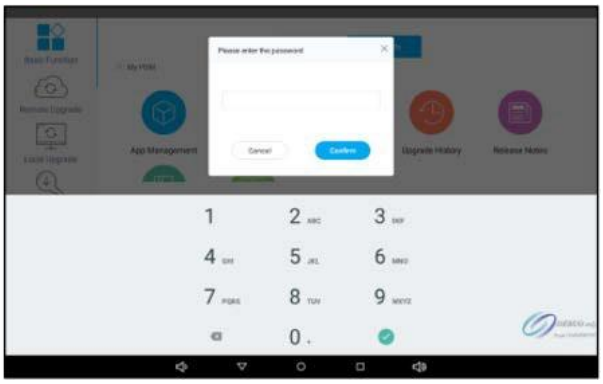


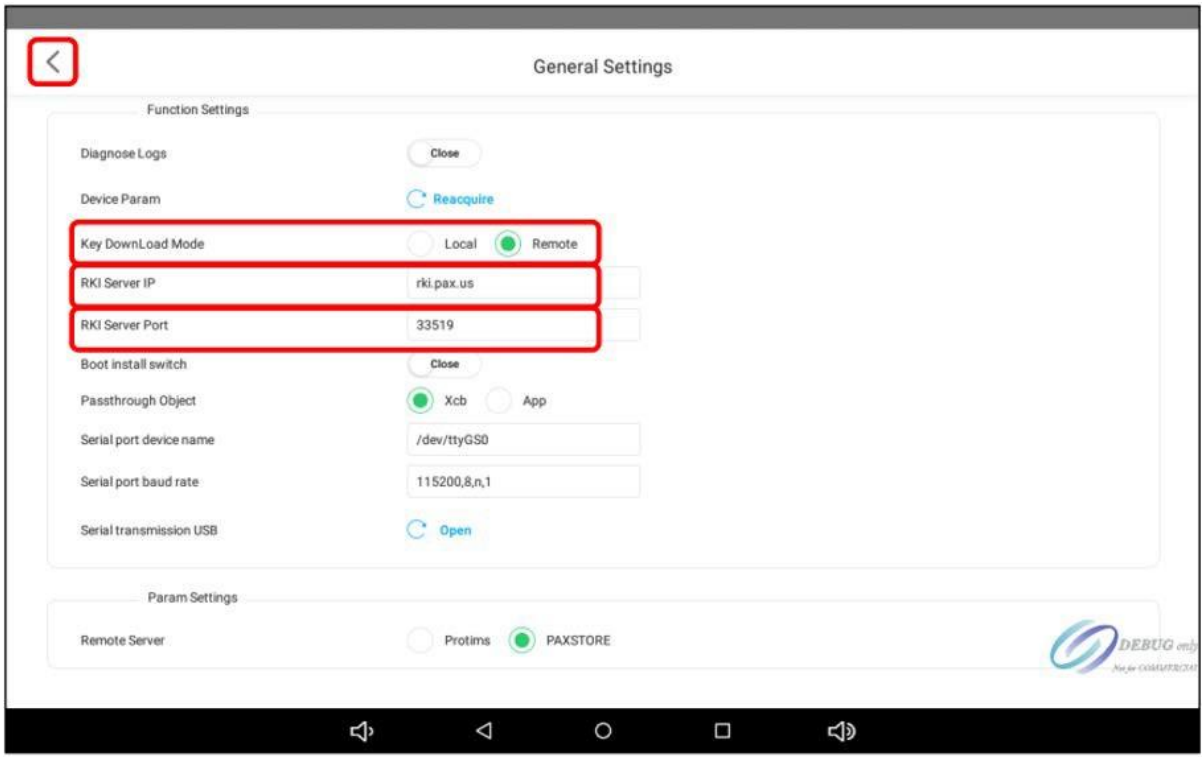

b. Remote Key Download Setting

1. Select [**PDM Info**], [**Basic Function**], [**General Settings**], and enter the password. (The default password is "**9876**").

2. Under [**General Settings**], select [**Remote**] under the Key Download Mode, enter [**rki.pax.us**] in RKI Server IP, enter "**33519**" in RKI Server Port. To navigate to the previous menu, press the [**"<" button**].


Basic Function
Remote Upgrade
Local Upgrade
Key Download
Authorize
Device Info
PDM Info
My PDM
App Management
General Settings
Device Info
Upgrade History
Release Notes
Instruction
About PDM

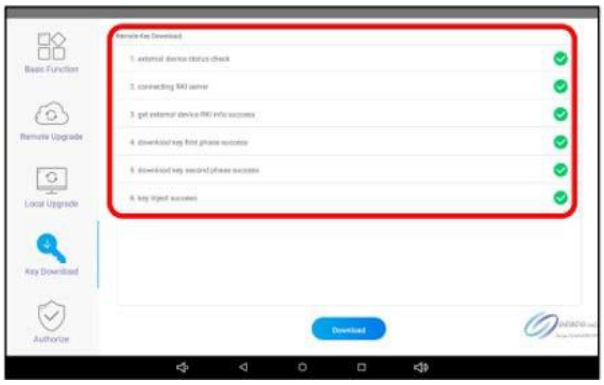

Please enter the password
Cancel
Confirm
App Management
Upgrade History
Release Notes
1
2
3
4
5
6
7
8
9
0


General Settings
Function Settings
Diagnose Logs
Close
Device Param
Reacquire
Key DownLoad Mode
Local
Remote
RKI Server IP
rki.pax.us
RKI Server Port
33519
Boot install switch
Close
Passthrough Object
Xcb
App
Serial port device name
/dev/ttyGS0
Serial port baud rate
115200,8,n,1
Serial transmission USB
Open
Param Settings
Remote Server
Protims
PAXSTORE
DEBUG

c. Remote Key Injection

Before initiating the Remote Key Injection, please make sure the terminal serial number has been registered into the RKI server.

1. Select [**Key Download**]. Under the [**Main Menu**], press [**Download**]. After a successful remote key injection, a [**Key Injection Success**] message will appear.

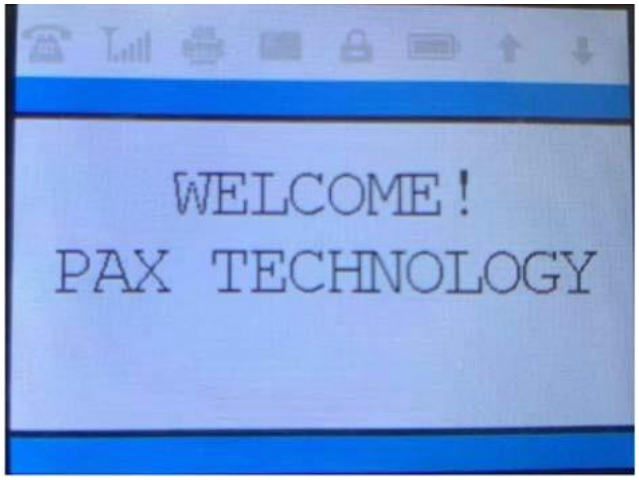



2.5 External PINPAD

2.5.1 S80-SP30

a. SP30

1. To connect the terminal with S80, use the PINPAD cable.
2. Before starting the Remote Key Injection, make sure the terminal is in idle screen.



3. Before initiating the Remote Key Injection, please make sure the terminal serial number has been registered into the RKI server.

b. S80

a) Monitor Version

Monitor Base version V1.47 or above

b) RKI Download Menu

1. Power cycle the terminal.
2. During the self-test, press the [**MENU**] button.
3. In the menu, select [▼ **button**].
4. Select [**1. Key Download**].

c) Remote Key Injection

1. Under the [**Key Injection**] menu, select [**3.RKI**], [**Key Injection**], [**3. Ext. PED US**], [**1-PINPAD**]. Select baud rate, "1-1200" or "6-115200." Select the attribute,"1-7,e,1."
2. Click the communication method, e.g., [**1 TCP**], enter [**rki.pax.us**].
3. Under [**Remote IP**], enter [**33519**], press [**1**] to enable DHCP. The SP30 display "1200(BPS)" or "115200(BPS)." After the remote key injection has successfully downloaded, S80 will display a [**Download Success**] message.

Important Note: If the CA key has not been installed in SP30, S80 will display an error message [**Read PUK Err**]

2.5.2 S500-SP20V4 OR S80-SP20V4

a. SP20V4

a) OS Version

OS version 4.05 or above

b) RKI Download Menu

1. To connect the terminal with S500, use the PINPAD cable.
2. Before starting Remote Key Injection, make sure the terminal is in idle screen.

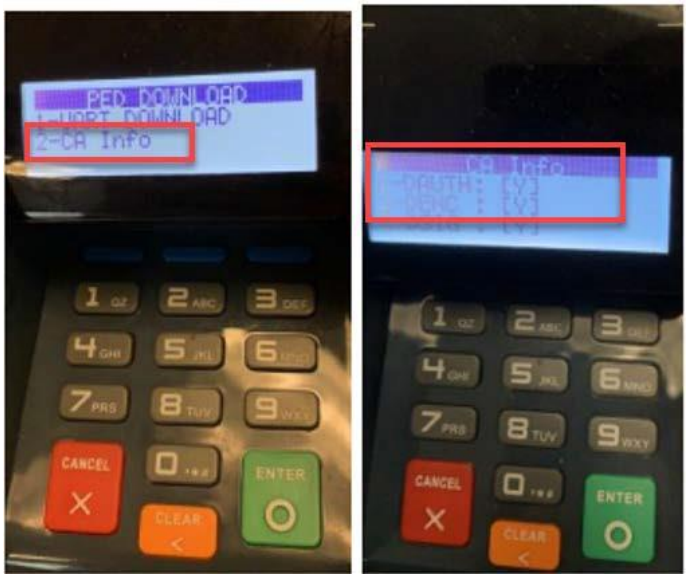
3. Before initiating the Remote Key Injection, please make sure the terminal serial number has been registered into the RKI server.

c) Check CA (OS version 4.06 or above)

1. Power cycle the terminal.
2. Press the [**ENTER**] button until the [**Config Menu**] appears.
3. Press the [**PINPAD ▼ button**].

4. Under the [**Config Menu**], select [**1. PED DOWNLOAD**].
5. In the [**PED DOWNLOAD**] menu, select [**2. CA Info**] verify both [**1. DAUTH**] and [**2. DENC**] has certificates.

For more information on certificates, please contact PAX Support at (support@pax.us).



b. S500 or S80

a) Monitor Version

Monitor Base version V1.47 or above

b) RKI Download Menu

1. Power cycle the terminal.
2. During the self-test, hold the [**MENU**] button.
3. Under the [**MENU**], select the [▼ **button**].
4. Select [**1. Key Download**]

c) Remote Key Injection

1. Under the [**Key Injection**] menu, select [**3.RKI**], [**Key Injection**],[**3. Ext. PED US**], [**1-PINPAD**]. Select the baud rate, “1-1200” or “6-115200.” Select the attribute, ”1-7,e,1”.
2. Click the communication method, e.g. [**1. TCP**], enter [**rki.pax.us**]. Under [**Remote IP**], enter [**33519**], press [**1**] to enable DHCP. The SP20V4 display “1200(BPS)” or ”115200(BPS).” After the remote key injection has successfully downloaded, S500 or S80 will display a [**Download Success**] message.

P.S: If the CA key has not been installed in SP20V4, S500 or S80 an error message [Read PUK Err] will appear.

2.5.3 A80-Q25

a. Q25

a) OS Version

OS version xx or above

b) RKI Download Menu

1. To connect the terminal with A80, use the PINPAD cable
2. Before starting Remote Key Injection, make sure the terminal is in idle screen.
3. Before initiating the Remote Key Injection, please make sure the terminal serial number has been registered into the RKI server.

b. A80

a) Monitor Version

Monitor Base version V1.47 or above

b) RKI Download Menu

1. Power cycle the terminal.
2. Select the Settings application
3. Scroll down and select [**Security**]
4. Select [**RKI Download**]

c) Remote Key Injection

1. In RKI download menu, select [**Ext.PED US**]
2. Select communication type with [**PINPAD**]
3. Choose baud rate with “115200,7,e,1” or “1200,7,e,1”
4. Set Remote Port to 33519, set Remote IP to “rki.pax.us”.

3. Error Message/Code Definition

Code	Message	Comment
102	Connect Err	Please check your network setups and connections. Please change to a more stable network and test again. Please contact PAX if nothing is wrong with your network.
301	Init Err- Router Err	
304	Init Err- Ethernet Init Err	
602	Comm Para Err	
603	Comm Para Err	
1301	Init Err - Wifi	
1304	Connect Err - Wifi	
1201	SSL Connect Er	Please check your network setups and connections. Please check whether the terminal has enabled the network whitelist, and whether the firewall has been enabled to restrict network ports when connecting to the network. Try connecting to a different network such as a Wi-Fi or mobile hotspot and try again. Please contact PAX if nothing is wrong with your network.
1412	Read Auth PUK Err	Please check the "DEV Auth Cert" and "Dev Enc Cert" information in the terminal. Please contact PAX to inject certificates (maintenance repair is needed) if certificates are missing.
1413	Read Device PUK Err	
1419	Generate Terminal Auth Data Err	
1420	Get Terminal Auth Data Err	
1421	Read Cert Err	
349	Terminal Cert Err	Terminal cert is failing to detect. Please use PPN to tamper the device and re-inject the certs.
1803	RKI Server IP or URL Err	Check the IP you entered is correct. The URL is not supported. Update the firmware to the latest version and the RKI client version to 2.03.03
1804	RKI Server Port Err	Check the port you entered is correct
1813	Get External Device ID Err	Please check whether the communication mode between the primary device and the extended device is selected correctly. Please contact PAX

4. Appendix: The Operating System version of support RKI Monitor

Terminal Mode	Base Version of support CFCA	Base Version of support CFCA+PAXCA
S80	V1.34_201703-V1.55_20210617	V1.56_20220406
S90	V1.34_201703-V1.55_20210617	V1.56_20220406
S300	prolin-2.4.145.7913R	V1.47
S500	V1.33-V1.46	V1.47 or above
S800		prolin-2.4.145.7913R
S900		prolin-2.4.145.7913R
D210		
D200		prolin-2.4.145.7913R

Prolin

Terminal Mode	Base Version of support CFCA	Base Version of support CFCA+PAXCA
D200(Prolin 2.4)		prolin-2.4.145.7913R
S300		V1.47 or above
S800	2.4.74-2.4.141	2.4.145 or above
S500		V1.47 or above
S900		prolin-2.4.145.7913R
S920		prolin-2.4.145.7913R
PX5		prolin-phoenix-2.5.31.7913R
PX7	2.5.6-2.5.27	N/A
S920(Prolin 2.5)		prolin-2.4.145.7913R
D220(Prolin 2.6)	prolin-cygnus-2.6.5.519R - prolin-cygnus-2.6.57.7702R	prolin-cygnus-2.6.59.7882R
Q30	2.6.5-2.6.58	2.6.59 or above
Q80	2.6.5-2.6.58	2.6.59 or above
Q90	prolin-cygnus-2.6.5.519R - prolin-cygnus-2.6.57.7702R	prolin-cygnus-2.6.59.7882R
IM300	prolin-cygnus-2.6.5.519R - prolin-cygnus-2.6.57.7702R	prolin-cygnus-2.6.59.7882R
D190	prolin-cygnus-2.6.5.519R - prolin-cygnus-2.6.57.7702R	prolin-pelican-2.7.43.7882R
D195	2.7.1-2.7.42	2.7.43 or above
Q20(Network available)	2.7.1-2.7.42	2.7.43 or above
Sp200(Network available)	prolin-cygnus-2.6.5.519R - prolin-cygnus-2.6.57.7702R	prolin-pelican-2.7.43.7882R
IM20	prolin-cygnus-2.6.5.519R - prolin-cygnus-2.6.57.7702R	prolin-pelican-2.7.43.7882R

Paydroid

Terminal Mode	Base Version of support CFCA	Base Version of support CFCA+PAXCA
A920(5.1)	5.1.1_Aquarius_V02.3.06-5.11_ Aquarius_V02.3.19	5.1.1_Aquarius_ V02.3.20 or above
A920(7.1)	7.1.1_Aquarius_V02.5.00-7.1.2_ Aquarius_V02.5.02	N/A
A930	7.1.1_Virgo_V04.3.02-7.1.1_Virgo_V04.3.06	N/A
A910	6.0_Leo_v07.1.03-6.0_Leo_v07.1.05	N/A
A60	6.0_Leo_v07.1.03-6.0_Leo_v07.1.04	6.0_Leo_v07.1.06_OTA
A80	V05_1.03-V05.1.07	6.0.1_Taurus_V05.1.09
PX7A	V05_1.03-V05.1.07	N/A

External PINPAD

Terminal Mode	Base Version of support CFCA	Base Version of support CFCA+PAXCA
SP30	Base Version: V1.33-V1.46	V1.47 or above
SP20V4		4.05 or above
Q25	prolin-pelican-2.7.6.624 - prolin-pelican-2.7.134.11327	prolin-pelican-2.7.167.12546R

PAX Customer Support

For questions or help with the terminal installation please contact your service provider or PAX customer support.

PAX Technology Inc.
8775 Baypine Road
Jacksonville, FL 32256

support@pax.us
(877) 859-0099
www.pax.us

PAX Technology, Inc. is not responsible for the content, quality, accuracy, or completeness of any information or materials contained on these pages. PAX Technology, Inc. does not endorse any content, viewpoints, products, or services contained on these pages and shall not be held liable for any losses caused by reliance on the accuracy, reliability, or timeliness of such information. Any person or entity that relies on any information obtained from these pages does so at his/her own risk.