N58 Security Policy

V 1.0.4

NEW POS TECHNOLOGY LIMITED

www.newpostech.com
<table>
<thead>
<tr>
<th>Date</th>
<th>Revision Level</th>
<th>Description</th>
<th>Modified by</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015-08-08</td>
<td>1.0.0</td>
<td>Original Issue</td>
<td>Alex Chen</td>
</tr>
<tr>
<td>2015-12-04</td>
<td>1.0.1</td>
<td>Add and fix up some mistake in section 5.4/5.6/7/8/4.7/5.2/5.3/5.5.</td>
<td>Ryan Huang</td>
</tr>
<tr>
<td>2015-12-19</td>
<td>1.0.2</td>
<td>Remove the references and add some information.</td>
<td>Alex Chen</td>
</tr>
<tr>
<td>2016-04-19</td>
<td>1.0.3</td>
<td>Improve and add some information</td>
<td>Jiang Li</td>
</tr>
<tr>
<td>2016-05-21</td>
<td>1.0.4</td>
<td>Update the firmware version to V1.0.5 Update the section of Software develop</td>
<td>Alex Chen</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Guidance</td>
<td></td>
</tr>
</tbody>
</table>
# Table of Contents

1 Purpose ..................................................................................................................... 4  
2 References ............................................................................................................... 4  
3 Device Identification And Inspection ...................................................................... 5  
   3.1 Device Functions ................................................................................................. 5  
   3.2 Appearance ......................................................................................................... 5  
   3.4 Identification ...................................................................................................... 6  
   3.5 H/W specification ............................................................................................... 7  
4 Security Guidance ..................................................................................................... 9  
   4.1 Environmental Requirements ........................................................................... 9  
   4.2 Self-Test ............................................................................................................. 9  
   4.3 Periodic Security Inspection ............................................................................. 10  
   4.4 Change Default Values ..................................................................................... 10  
   4.5 Installation Guidance ....................................................................................... 11  
   4.6 Configuration Setting ....................................................................................... 11  
   4.7 Sensitive Roles .................................................................................................. 11  
   4.8 Update/Download ............................................................................................. 12  
   4.9 Software develop Guidance ............................................................................. 12  
      4.9.1 The development process ........................................................................ 12  
      4.9.2 SRED applications development ........................................................... 13  
      4.9.3 Bluetooth security guidance ....................................................................... 13  
5 Key Management ...................................................................................................... 15  
   5.1 Key Management systems ................................................................................. 15  
   5.2 Key Loading ....................................................................................................... 15  
   5.3 Key Replacement .............................................................................................. 16  
   5.4 Key Table .......................................................................................................... 16  
   5.5 Signature and Verification ................................................................................. 17  
   5.6 Key removal ........................................................................................................ 17 
6 Device Maintenance .................................................................................................. 18  
7 Vulnerability Detection and Follow-up Action ......................................................... 19  
8. Tamper Detection and Response ............................................................................ 20  
   8.1 Tamper Trigger Events ..................................................................................... 20  
   8.2 Tamper Response .............................................................................................. 20
1 Purpose

This document is to describe a security policy which addresses the proper use of N58 in a secure fashion, including information on key-management responsibilities, administrative responsibilities, device functionality, identification and environmental requirements.

Any unapproved using of N58 will result in an incompliant with PCI PTS POI security requirement.

2 References

[8] N58 bluetooth operation guide v03.doc
3 Device Identification And Inspection

3.1 Device Functions

The N58 is a mPOS terminal for financial transactions in an attended environment. It provides 15 buttons keypad, LCD, Security Magnetic Reader (MSR), IC Card Reader (ICCR), contactless card reader, USB, Bluetooth and Audio port (optional).

3.2 Appearance

Please check whether the appearance of N58 is the same as follow:
3.3 Version Information

Hardware version

The hardware version is printed on the label which is on the back of device. It is to be notice that the label should not be torn off, covered or altered.

Firmware Version

V1.0.5

The software version can be view as following:

1. Power on N58, and press ‘CLEAR’ key continuously to enter ‘System Manager’ menu;
2. Press ‘↓’ key to select ‘About’ item and press ‘ENTER’ key;
3. In ‘Version’ menu, you can see the Boot version, Kernel version and Firmware version.

3.4 Identification

For security, when receive the device via shipping, it must be inspected and authenticated, if pass, you can use the device, please inspect as
following:
1. Check if the origin that providing the N58 device is authorized, if not authorized, please reject.
2. Check if the device’s name, firmware, hardware and application version are meet the approved identification number of PCI PTS POI in the website (www.pcisecuritystandards.org).
3. Check if the appearance of N58 is altered, if found some trace, please reject the device.
4. Check if something overlay on the LCD display in order to prevent overlay attack.
5. Check if the ICC card slot has wire out or something that suspicious, if so, reject the device.
6. Check if the Magcard reader slot has other reader or some bugger, if found, reject the device.

3.5 H/W specification

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CPU</strong></td>
<td>32-bit secure CPU</td>
</tr>
<tr>
<td><strong>Display</strong></td>
<td>1.8&quot; black-and-white LCD, 128*64</td>
</tr>
<tr>
<td><strong>Keypad</strong></td>
<td>10 alphanumeric keys, 5 function keys</td>
</tr>
<tr>
<td><strong>Magnetic Card Reader</strong></td>
<td>Compliant with ISO7811, ISO7812; Track 1/2/3, bi-directional swipe</td>
</tr>
<tr>
<td><strong>IC Card Reader</strong></td>
<td>1 user card (EMV4.3)</td>
</tr>
<tr>
<td><strong>PSAM Slot (Optional)</strong></td>
<td>1 PSAM slot, compliant with ISO7816</td>
</tr>
<tr>
<td><strong>Contactless Card Reader (Optional)</strong></td>
<td>Supports Mifare classic, Mifare Ultralight, Mifare DESFire, ISO 14443 A &amp; B, SONY FeliCa</td>
</tr>
<tr>
<td><strong>Internal PIN Pad</strong></td>
<td>Supports MK/SK, Fixed, DUKPT;</td>
</tr>
<tr>
<td>Internal Wireless</td>
<td>Optional, Bluetooth</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>Peripheral Port</td>
<td>1 micro USB device, 1 Audio jack(Optional)</td>
</tr>
<tr>
<td>Working Environment</td>
<td>Temperature: 0°C ~ 50°C(32°F ~ 122°F); Humidity: 10% ~ 90% (non-condense)</td>
</tr>
<tr>
<td>Storage Environment</td>
<td>Temperature: -20°C ~ 60°C(-4°F ~ 140°F); Humidity: 5% ~ 95% (non-condense)</td>
</tr>
<tr>
<td>Certification</td>
<td>PCI 4.x, EMV4.3 Level 1 &amp; 2</td>
</tr>
<tr>
<td>Cable</td>
<td>USB, use for charge and download</td>
</tr>
<tr>
<td>Size</td>
<td>116<em>60</em>16mm</td>
</tr>
<tr>
<td>Weight</td>
<td>100g</td>
</tr>
</tbody>
</table>
4 Security Guidance

This section is mainly describe the security about how to use the device and how to development process. Before using the device, you should inspect the device carefully as following.

4.1 Environmental Requirements

N58 as mPOS doesn’t provide a privacy shield, so it can’t be used in a fixed site, when using, please hand up and cover by hand to take care it is not overlooked when entering PIN code.

1. Temperature & Humidity Environments
   Operation Temperature & Humidity : 0 ℃ ~ 50 ℃ / 10% ~ 90% (non-condense)
   Storage Temperature & Humidity : -20 ℃ ~ 60 ℃ / 5% ~ 95% (non-condense)

   If your Environment status is over that range, the terminal is not always working.

2. Power Environments
   Supply voltage is outside of range, approximately 1.65 < V < 3.70

   Terminal should stay away from all sources of heat, to prevent vibration, dust, moisture and electromagnetic radiation (such as a computer screen, motor, security facilities etc.).

4.2 Self-Test

N58 using self-tests to check firmware integrity. The self-test is performed:

1. Every time the unit is powered on
2. Every time the unit is rebooted
3. At least once every 24 hours

   N58 performs a self-test, which includes firmware, application, stored keys, authenticity and any other sensitive properties tests to check
whether the device is in a compromised state. If the result is failed, the device displays the lock icon and more tamper information on LCD and the device and its functionality fail in a secure manner. When the device goes to the “Compromised” mode, all the stored keys are removed as well. The merchant must return the device to NEWPOSTECH for the repair. Self-tests are not initiated by an operator.

4.3 Periodic Security Inspection

For the security using of N58, after a period using time, the device must be inspected, only pass, the device can be used continue.
1. You can look out the tampered information on LCD display to check if the device is tampered, if tampered, please contact the authorized service or NEWPOS.
2. Check if the appearance of N58 is altered, if find some trace, please reject the device.
3. Check if something overlay on the LCD display in order to prevent overlay attack.
4. Check if the Magcard reader slot has other reader or some bugger, if found, reject the device.

4.4 Change Default Values

When manufacturing in factory, the device of N58 is set to default password. So for security, when shipping the device to customer, the administrator must re-set a valid password to replace the default password.

When updating the firmware, the passwords must be changed otherwise cannot run any application and others service.

The default passwords are as following:
1. ADMIN1 Password: 41758241
2. ADMIN2 Password: 14285714

When changing, the new passwords cannot be the same to the old passwords.
4.5 Installation Guidance

User should refer user manual before installation this device.

The device consists of following items:

- 1 Device
- Power cable and connector
- User manual

All softwares are installed before deliver to end user. So, user can use PIN entry normally.

This device is mobile handheld POS and it doesn’t provide a privacy shield and can’t be used in a fixed site. And used to mobile attended environment. It is recommended that the position of the terminal on check stand must be in such a way to make cardholder PIN spying infeasible. The customer should be advised to take care that he is not overlooked when entering his PIN code.

The N58 is designed to be portable, does not need installation and charging by USB port. Before using, please check if the origin that providing the N58 device is authorized, check if the appearance of N58 is altered, check if the ICC card slot has wire out or something that suspicious, check if the magcard reader slot has other reader or some bugger, if you find the above problems, please refuse to use and please contact to NEWPOS or agency provider.

4.6 Configuration Setting

The N58’s firmware does not need any configuration setting.

4.7 Sensitive Roles

There are different user roles as following:

- Administrators
  System maintenance functions, such as firmware/application download, key loading and password changing. Only the authorized administrators
can access to them under dual control and split knowledge.

- End Users
The end users can process the PIN-based transaction.

4.8 Update/Download

Customer obtains appropriate firmware from firmware information list, which could be downloaded on our official website. Customer can also find other relevant information about the firmware, and decide whether firmware update could help platform work well. If required firmware could be downloaded from us using legal ID, customer can download such firmware via local download. When local download is being used for firmware update, POS is supposed to be used in secure environment, and get firmware data using serial port transmission.

After firmware is downloaded, old firmware in the terminal will immediately verify whether the signature is legal. Any non-signed firmware will be considered as unauthorized, and cannot be updated. Terminal type information is already contained in firmware, and firmware will also choose whether it could work in existing terminal. If terminal type is not compatible, firmware will not be updated. When firmware update is completed, restart POS again, and new firmware version will be shown.

4.9 Software develop Guidance

When developing applications, the developer must respect the guidance described in the document [6].

4.9.1 The development process

During the software development, the following steps must be implemented:
1. Software development/programming according to requirement;
2. After the software development, developer must take functional test (self test);
3. Code review, audit, and digital signature;
4. Undergo a full testing (detailed test);
5. If some bugs are found, the tester will feed back to the relevant developer to fix up;
6. Only after the testing and passed, can the software be released to production.

4.9.2 SRED applications development
1. Account data read from IC, magnetic stripe card must be encrypted at once.
2. The plain-text account data can not output of N58 device.
3. After transaction or time out or other abort, the plain-text account data must be deleted immediately.

4.9.3 Bluetooth security guidance
For secure data exchange via Bluetooth communication and the compliance with PCI PTS, The following points need to take attention for N58.

2. Have a good knowledge about Bluetooth technology and security policy.
3. Performing Bluetooth device pairing in security environment that attackers cannot observe passkey entry and eavesdrop on Bluetooth
pairing-related communications.
4. Bluetooth device should not set to standby mode except as needed for pairing or connection.
5. Performing Bluetooth device pairing as infrequently as possible because the pairing information may be leaked. Please power off and close Bluetooth device when N58 Bluetooth is not used.
6. Not set the PIN Code or passkey to simple 0 or static number, and should be sufficiently random and the length should be more long such as 6.
7. Users should provide a list of precautionary measures they should take to better protect handheld Bluetooth devices from theft. For example, Save each N58’s information such as serial number into database, when the N58 is stolen, and inform the server to remove the N58 terminal from service. Additional, a Bluetooth device is lost or stolen, users should immediately delete the missing device from the paired device lists of all other Bluetooth devices.
8. Security Mode 3 provides link-level security prior to link establishment, while Security Modes 2 and 4 allow link-level connections before any authentication or encryption is established, so it’s recommended that using Security Mode 3 that is the most security mode, and Security Mode 4 with Service Level 3 is also more security. And using security mode 2 and 4 when pairing should in security environment.
9. The Security Mode 1 and Just Work of SSP are not secure, so should not be used.
5 Key Management

5.1 Key Management systems

N58 supports the following key systems:

- Fixed key
- MK/SK key
- DUKPT

MK/SK key, a master key and session key hierarchy. The Session Keys are encrypted/decrypted by Master Keys.

DUKPT, the technique is based on a unique key per transaction.

2. N58 supports the following cryptographic algorithms:

- TDES(112 bits and 168 bits)
- SHA-256(digest signature, 256 bits)
- RSA-2048(signature verification, 2048 bits)

3. N58 supports the following symmetric key types:

TMK: Terminal master key. It’s generated by the acquirer and used to decrypt the MAC key, the PIN key.

TPK: Terminal PIN encryption key. It’s generated by the acquirer and used to generate the PIN BLOCK.

TAK: Terminal MAC encryption key. It’s generated by the acquirer and used to calculate the MAC value.

TKD: Terminal Account data encryption key. It’s generated by the acquirer and used to encrypt account data (SRED).

5.2 Key Loading

When the product are manufactured, The initial keys including TMK, Fixed key and initial DUKPT are injected into N58 under dual control and split knowledge in security environment.

And the working keys including TPK, TAK and TDK that are
encrypted by TMK are downloaded into N58 in logon transaction.

The key loading method for application is referenced in ANSI X9 TR-312010.

### 5.3 Key Replacement

Keys should be removed from the device whenever the compromise of the original key is known or suspected, and whenever the time deemed feasible to determine the key by exhaustive attack elapses. Keys can be removed by the sensitive service of “Clear Key” in N58’s menu. After key removal, the device should return to Key Injection facility for the secure key loading.

### 5.4 Key Table

<table>
<thead>
<tr>
<th>Key Name</th>
<th>Purpose</th>
<th>Algorithm</th>
<th>Size</th>
<th>Storage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Master Key</td>
<td>Decryption of session keys (PEK, MAC)</td>
<td>TDES</td>
<td>128/192 bits</td>
<td>The key was encrypted by SIEK and the cipher-text was saved in file system</td>
</tr>
<tr>
<td>PIN Key</td>
<td>Online PIN encryption key</td>
<td>TDES</td>
<td>128/192 bits</td>
<td></td>
</tr>
<tr>
<td>MAC Key</td>
<td>Message authentication</td>
<td>TDES</td>
<td>128/192 bits</td>
<td></td>
</tr>
<tr>
<td>EAK</td>
<td>Encrypt account data.</td>
<td>TDES</td>
<td>128/192 bits</td>
<td></td>
</tr>
<tr>
<td>Fixed MAC key</td>
<td>Message authentication</td>
<td>TDES</td>
<td>128/192 bits</td>
<td></td>
</tr>
<tr>
<td>Fixed PIN key</td>
<td>Online PIN encryption key</td>
<td>TDES</td>
<td>128/192 bits</td>
<td></td>
</tr>
<tr>
<td>Fixed EAK</td>
<td>Encrypt account data.</td>
<td>TDES</td>
<td>128/192 bits</td>
<td></td>
</tr>
<tr>
<td>DUKPT Key</td>
<td>Online PIN encryption key and Message authentication</td>
<td>TDES</td>
<td>128/192 bits</td>
<td></td>
</tr>
<tr>
<td>Auth key</td>
<td>Authentication on keys for financial transaction</td>
<td>RSA</td>
<td>2048 bits</td>
<td></td>
</tr>
</tbody>
</table>
5.5 Signature and Verification

The N58’s kernel/applications must be digitally signed before it was released. The kernel and applications are signed by NEWPOS. The file data will use SHA256 to compute the hash result and use the RSA-2048 private key to encrypt the hash result.

When the kernel was downloaded to the terminal, the boot will save the kernel in RAM temporarily and use the RSA public key to verify it, if it was verified successfully, the kernel will be saved in the flash. If verified failed the kernel which was saved in RAM will be erased right now.

When downloading the application, the kernel will save the application data in RAM temporarily and then verify it. If verify successfully the application will be saved in file system, if failed it will be erased right now.

5.6 Key removal

If tamper event is detected, all the keys in the device will be erased automatically.

After the keys are loaded to device, they will be available until administrator wants to erase all keys for decommissioning or tampering detected.
6 Device Maintenance

1. Decommissioning/Removal
   Permanent removal
   When the device is no longer used, it can be decommissioned and removed from service. And then must remove all the keying material that used to decrypt any sensitive data.
   Temporary removal
   If just temporary removal, it’s not need to remove the keys.

2. Tamper-Response
   When the device is tampered, some tampered information you can see from LCD display, you can contact your authorized service or NEWPOS to maintain it.
7 Vulnerability Detection and Follow-up Action

When new vulnerabilities, threats or bugs are detected via public resource or the customers, NEWPOSTECH performs analysis to see if the new vulnerabilities, threats or bugs may impact on the N58 security. NEWPOSTECH contacts PCI lab and gets consulted if there is a delta evaluation is necessary.

If the vulnerabilities, threats or bugs impact on the N58 security, N58 immediately informs customers of the vulnerabilities, threats or bugs analysis result via e-mail and send the patch to the customers. If Hardware change needs to be involved to fix the issue, customers should return their N58 devices to N58 manufacturing facility for the repair.

When a new vulnerability occurs, NEWPOS’s security team will send a vulnerability notification email to the customers (especially their security managers).

New firmware:
ftp://customer:loadsoftware@121.15.134.230/N58/firmware/xxx

Bug report contact with NEWPOSTECH email:
support@newpostech.com
8. Tamper Detection and Response

8.1 Tamper Trigger Events

- Front case removal
- Back case removal
- Physical penetration on all the sides of the device
- MSR head cover removal
- MSR connector removal
- Temperature is $> 110^\circ$C or $< -30^\circ$C.
- Supply voltage is outside of range, approximately $1.65 < V < 3.70$
- Stored sensitive data authentication failed during the Self-test

8.2 Tamper Response

- Remove the stored key file.
- Make the device unavailable and display the attack source information on the screen.