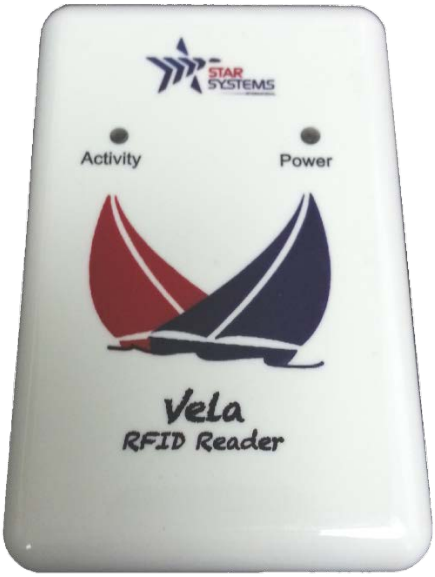
Unit 4, 12/F
Vanta Industrial Centre.
21-33 Tai Lin Pai Road
Kwai Chung, N.T. Hong Kong SAR

Vela Desktop Reader
User Guide



Disclaimer

Star Systems International and the **Star Systems International logo** are trademarks of **Star Systems International Ltd**. in Hong Kong and other countries.

Microsoft, **Windows**, the Windows logo are trademarks of Microsoft Corporation in the U.S. and other countries. All other products names mentioned herein may be trademarks of their respective companies.

Star Systems International Ltd. shall not be liable for technical or editorial errors or omissions contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material. The information in this document is provided “as is” without warranty of any kind - including but not limited to, the implied warranties of merchantability and fitness for a particular purpose, and is subject to change without notice. The warranties for Star Systems International products are set forth in the express limited warranty statements accompanying such products. Nothing herein should be construed as constituting an additional warranty.

This product is not designed, intended, authorized or warranted to be suitable for life support applications or any other life critical applications which could involve potential risk of death, personal injury, property damage, or environmental damage.

Vela Desktop Reader User Manual

Version 4

Contents

Installing Vela Test Tool

Hardware Requirements

- PC with Pentium 4 class CPU or above
- Microsoft ® Windows Vista or above
- 100 MB available hard drive space
- USB 2.0

Software Installation

To ensure reader will work properly, please install the program **before** you connect VELA to your computer.

1. Insert the product CD to the computer OR go to www.star-int.net to download the latest test tool.

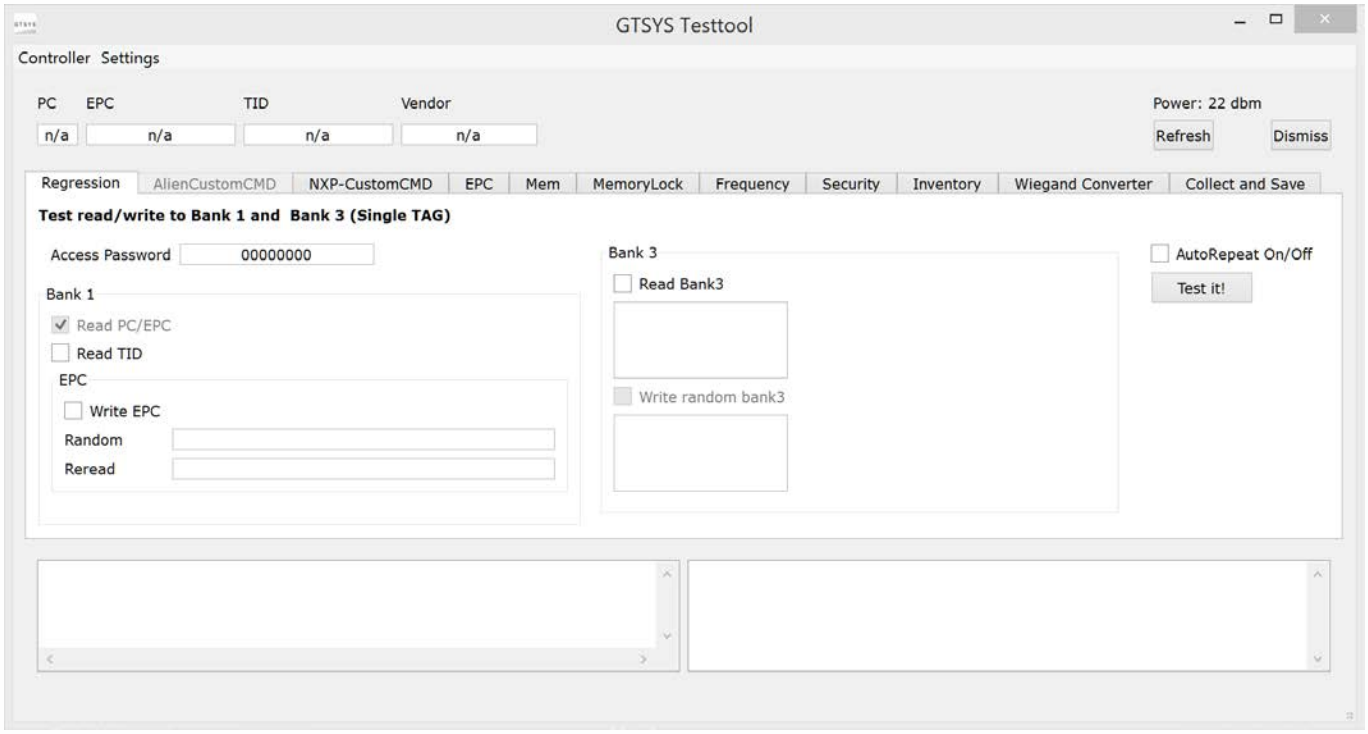
2. Start the **VelaTestTool.msi** program from the CD and follow the instructions in the installation wizard.

3. Connect the reader with the supplied USB cable to the computer. If an error message regarding USB driver shows up, please refer to **Section 4 USB driver installation** to update the USB driver.

Using Vela Test Tool

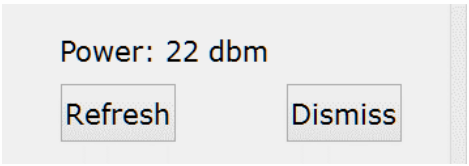
The Vela test tool will be available from the Start menu after the installation process has successfully completed. The path to the program is: **Start → Program → GTSYS → RegTest**

The Vela test tool discovers the reader automatically. Now the reader is ready to read and write RFID tag.

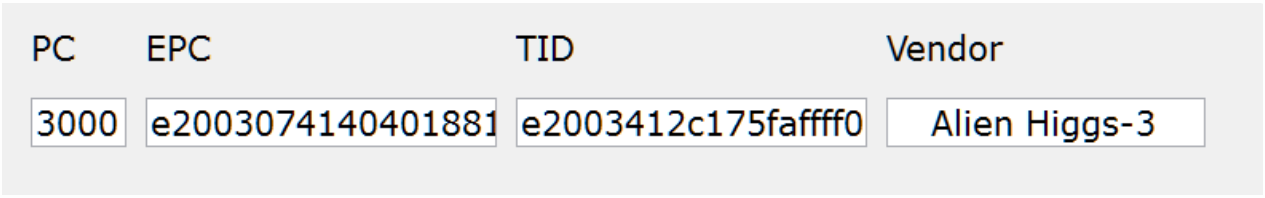


Reading Tags

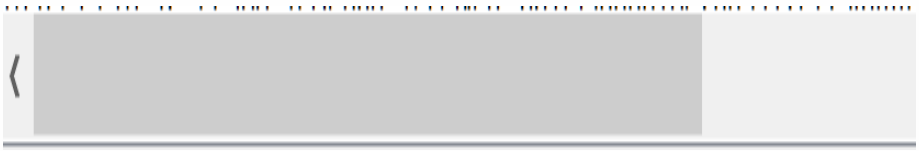
Press the “Refresh” button at the top right corner of the test tool to read a single tag



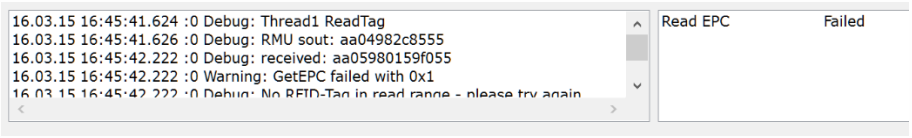
If a tag is successfully read, the tag information will be shown at the top left corner of the test tool



The two windows at the bottom of the test tool will provide debug information for the any reader operations.



If a tag is not present during the read, a “Failed” message will be displayed



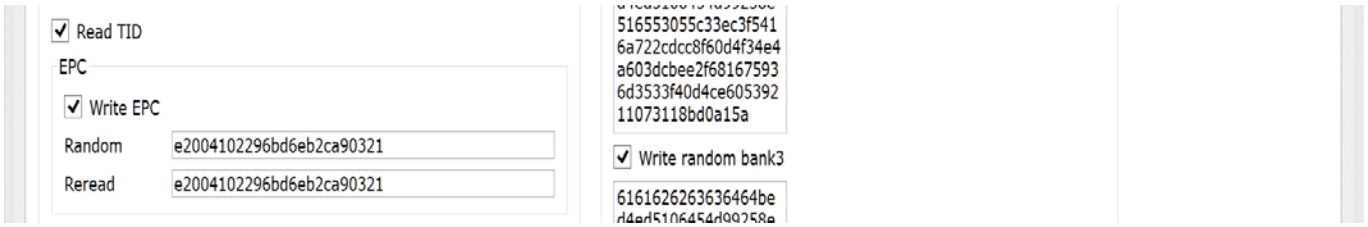
Regression Test

The regression test tab allow user to perform vigorous read/write cycle on a tag to test the function of Vela.

User can choose any number of actions from the following list to be performed during each test cycle. The read PC/EPC option is enabled by default.

- Read TID
- Write EPC
- Read Bank 3 (User Data)
- Write Bank 3 (User Data)

Click the “Test it!” button on the right to perform a round of test

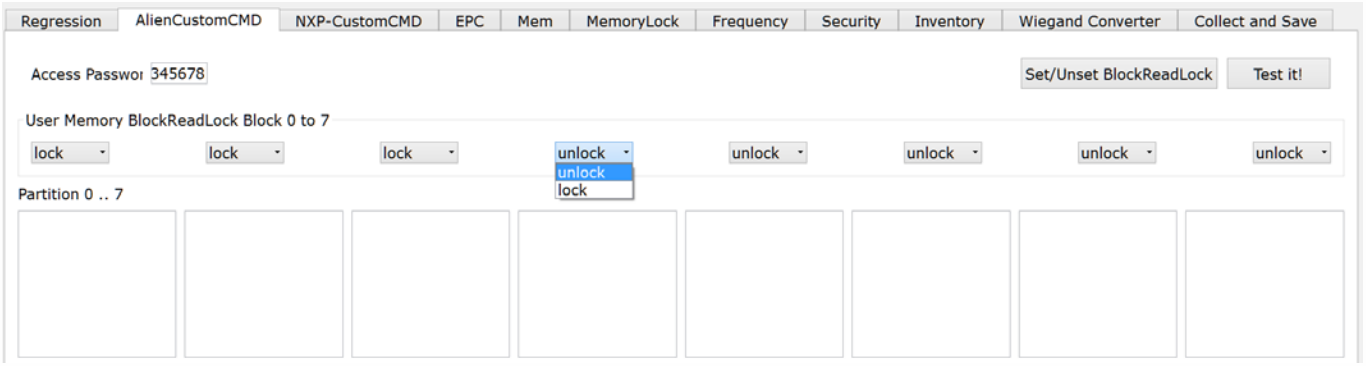


User can check the “Auto Repeat On/Off” box to enable continuous regression test.

NOTE: The regression test may write data to RFID tag that is near the reader, please make sure to only place tag the will go through the test near the reader.

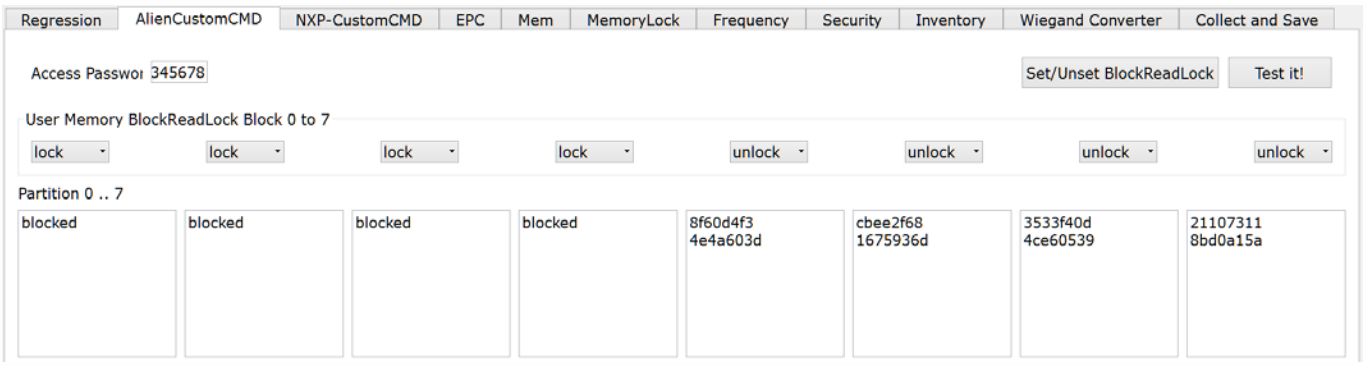
Alien Custom Command

Vela supports Alien's custom User Memory Block Read Lock command on a Higgs3 tag, which allows user to partial set the user memory bank to "read-protect" state. Read protected memory blocks cannot be read by other reader unless the correct access password is provided.



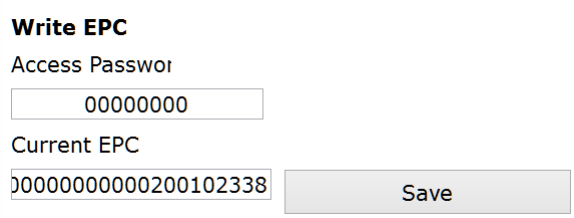
User will need to set a non-zero password (i.e. not 0x00000000) on the tag first to in order for the lock to work. The 512 bit user memory bank is divided into 8 separate 64 bit blocks. User can use the drop down menu to control the lock state of each block

Click the "Set/Unset BlockReadLock" button to execute the change in lock state. Afterwards, user can click "Test it!" to check the lock state of each memory block. The read protected blocks will show "blocked" instead of its original content.



Write EPC

Write EPC tab allows user to re-write the EPC of the tag



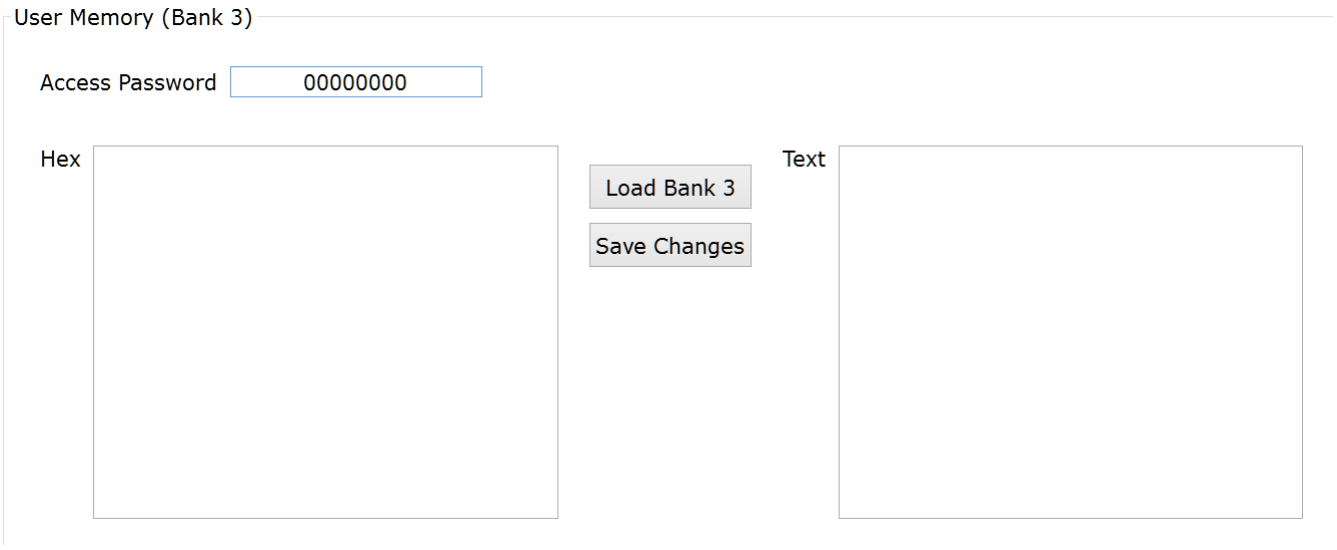
After successfully reading a tag, the EPC will be displayed in the Current EPC text box. User can change the content of the text box and press Save to re-write the EPC.

If the re-write is successful, a success message will be displayed at the lower right status window

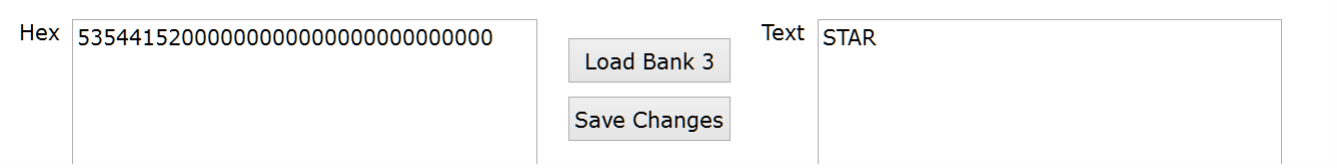
If the EPC memory bank is being locked (not permanently locked), user will need to input the correct Access Password in the text box to re-write the EPC.

Write User Memory

The Mem tab allows user to change the content of user memory bank in the tag.



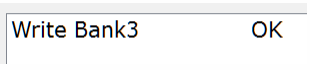
User can click the Load Bank 3 button to view the content of user memory bank first



The hex data of user memory bank is displayed in the left text box. The test tool will automatically translate the Hex data to ASCII character and display it on the right text box.

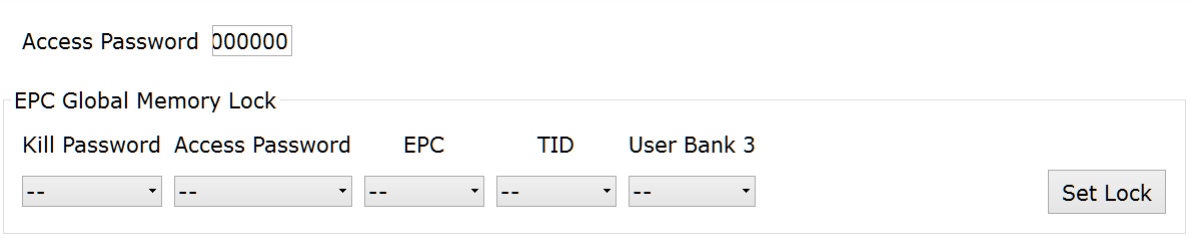
In the above example, 0x53 0x54 0x41 0x52 is translated to STAR in ASCII

User can change the content of user data in the left text box. Please note that the left text box is in OVERTYPE mode so new character will replace the old character in the text box. Afterwards user can click Save Change to write the data to tag. If the write operation is successful, a message will be displayed at the lower right status window

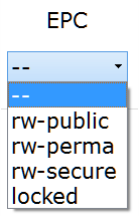


Set Lock State

The MemoryLock tab allow use to set the lock state of different memory bank in the tag.



Each memory bank has a drop down menu with the following options. In order to set the lock state to rw-secure or set the lock state back to rw-public from rw-secure, a non-0 (not 0x00000000) password must first be written to the Access Password. Then user will need to input the correct password in the Access Password text box above to completely the lock state change.



Definition:

rw-public - The memory bank is UNLOCKED and it is open to read and write for public, this is the default state for all memory bank except TID.

rw-perma - The memory bank is PERMANENTLY UNLOCKED and is open to read and write for public, it cannot be locked ever again.

rw-secure - The memory bank is PASSWORD LOCKED and require the correct access password to be able to read or write.

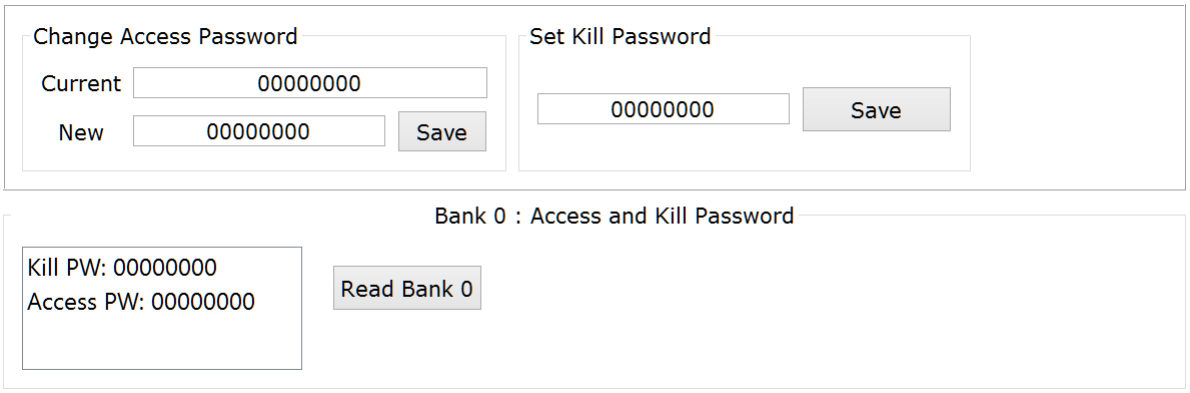
locked - The memory bank is PERMANENTLY LOCKED. It cannot be read, written or unlocked again.

NOTE: TID is permanently locked by default, so user won't be able to change the lock state of it. EPC and User Data will be readable even if locked. If you lock the EPC it only means you cannot re-write it (without password for secure mode or permanently in locked mode). User can use the Alien custom command (Section 3.3) to read-lock the User Data.

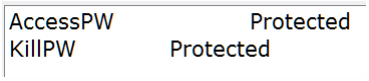
Once the lock state is selected, user can press the Set Lock button to execute the command. If the operation is successful, a message will be displayed at the lower right status window

Read/Write Password

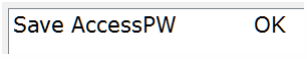
The Security tab allows user to read and write Kill Password and Access Password in the tag memory



User can click the Read Bank 0 button to read both the Kill Password and Access Password in the memory bank. If either of the memory banks is set to rw-secure or locked state (refer to section 3.7 for detail of the lock states) and the correct access password is not used as a key to read, then the reading will fail and the following message will be displayed at the lower right status window

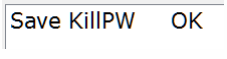


User can use the text boxes in the top left section to re-write the access password. Simply input the new access password into the New text box and click the Save button. If the write operation is successful, a message will be displayed at the lower right status window



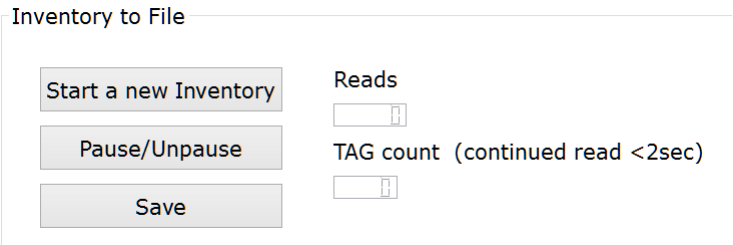
If the tag already have an existing access password, user will need to input the current access password into the Current text box in order to re-write it.

At the top right section, user can input the kill password into the text box and click Save to re-write the kill password in the tag. A message will be displayed at the lower right status windows if the write operation is successful



Collect and Save

The Collect and Save tab allows user to collect all the tag data that has been placed on Vela.



Click the Start New Inventory button and place the tag above Vela to begin reading tags. User will see the Reads count increase and the Activity light on Vela flashing if the unit successfully starts the inventory cycle.

Click the Pause/Unpause button to un/pause the inventory without clearing the previously read data from the start of inventory.

After reading all tags required, click the Save button to save the data to the designated path as CSV file.

Tag Data Format

[EPC],[TID]

Tag with the same EPC will only be recorded once in this mode.

NXP Custom command Ucode DNA features

NXP Ucode DNA features overview

Ucode DNA functions are supported by reader firmware version 6.5.4 QCA onwards.

The NXP Ucode DNA chipset provides advance tag authentication via 128-bit AES unique crypto key and Privacy protection via Untraceable command and 128-bit AES group crypto key.

The table below summarize the passwords and keys used in the Ucode DNA features and their respective roles in the data security scheme.

	Access Password	Key 0	Key 1
Size	32 bits	128 bits	128 bits
Function	Enable DNA functions	Tam-1 authentication	Tam-2 memory access
Re-writable	Yes, not limited	Cannot change once activated	Cannot change once activated
Access hidden memory	Yes	No	Yes
Use for Re-configure memory status	Yes	No	No

To enable the Ucode DNA functions on a tag with Ucode DNA chipset, an access password MUST first be set. Please go the section 3.7 about setting access password.

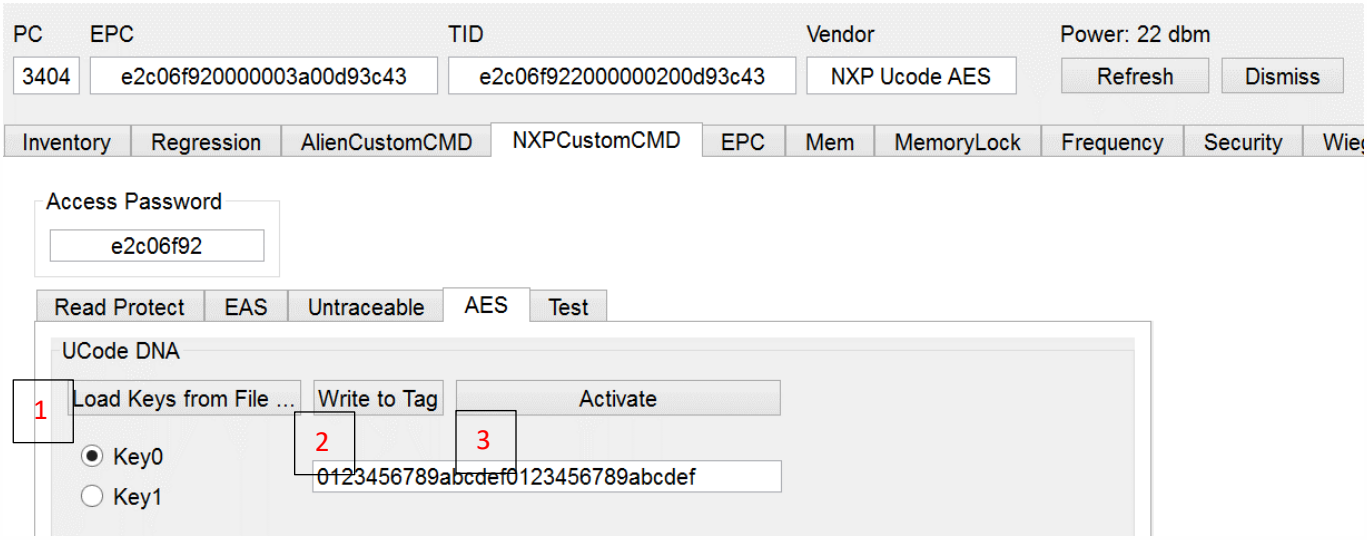
Using Ucode DNA features:

To fully utilize the Ucode DNA features, please follow the steps below:

- Loading AES Keys;
- Authenticate tags using Key0;
- Set to hide specific memory banks;
- Retrieve hidden memory banks' data using Key1;

Loading the AES Keys

Once you have the access password set, next we can load the Key0 and Key1 for the Tam 1 authentication and Tam 2 hidden data retrieval commands sets respectively. Go to the *NXPCustomCMD* Tab, and then *AES* sub-tab:



1. Load a set of keys to the software from a key-file. A key-file is just a plaintext file with two 128bits long hex-string as the key, each separated into two lines. Once the key is loaded to the software, it will be display as shown above. For the purpose of this demo case, the following keys are used.

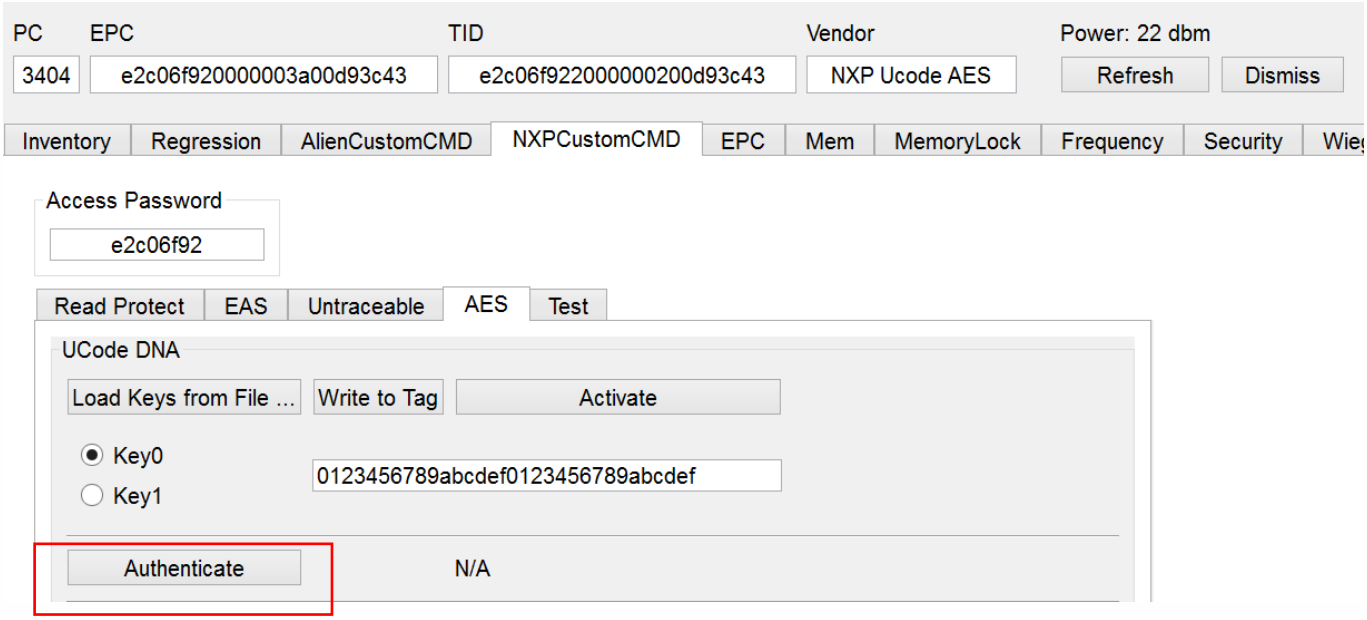
   0123456789abcdef0123456789abcdef ← Key0

   fedcba98765432100123456789abcdef ← Key1

   Please note that the key on the first line will represent key 0, used for TAM-1 authentication. And key on the second line will represent key 1, used for access of hidden memory banks.
2. Write the keys into the tag's memory.
3. Activate the keys in the tag;

WARNING: Please note that once the keys are activated in the tag, they cannot be changed.

Tag authentication



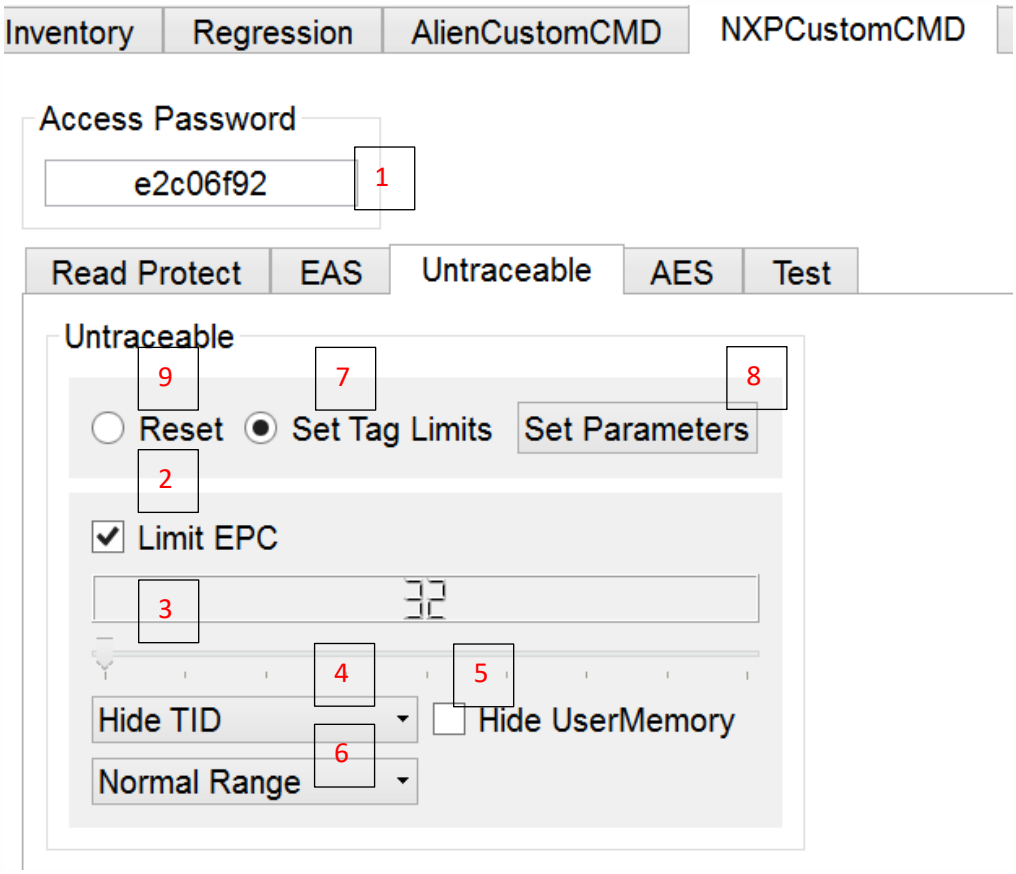
After the keys are activated, you can now perform authentication on the tag.

Since you have already loaded the keys during the step of activating the keys on the tag, you can proceed directly to authenticate the tag, otherwise please load keys to the software by following the step 1 in previous section.

To authenticate the tag, simply click the Authenticate button, the result of the authentication will be displayed next to the button.

Set Untraceable

To use the untraceable feature, go to the *Untraceable* sub-tab:



1. Input the access password to be able to change the settings of the untraceable features; You can choose to hide the EPC, TID, or User Memory bank of the tag. In this demo application, the length of data that can be hidden is fixed.

EPC:

You can limit the length of EPC to the tag will response to query by checking the *Limit EPC* check box (2), move the slide bar to adjust the number of bits of EPC to be shown (3).

TID:

You can change in the drop the box (4) to one of the follow options for hiding the TID:

Show TID – show the full TID

Partly TID – Hide the unique serial number part of the TID

Hide TID – Hide the full TID

User Data:

You can check the Hide *UserMemory* (5)check box to hide the full user data.

Changing the read range of the tag (experimental)

You can change the read range of the tag by selecting one of the option from the drop down box (6):

Normal Range – The tag will response to reader query on normal sensitivity

Toggle Range – The tag will response to the reader's NEXT query on reduced sensitivity (less range)

Reduced Range – The tag will permanently reduce sensitivity (less range) **

**Warning: It is not recommended to choose this option. Even resetting to default untraceable settings, cannot revert to normal range.

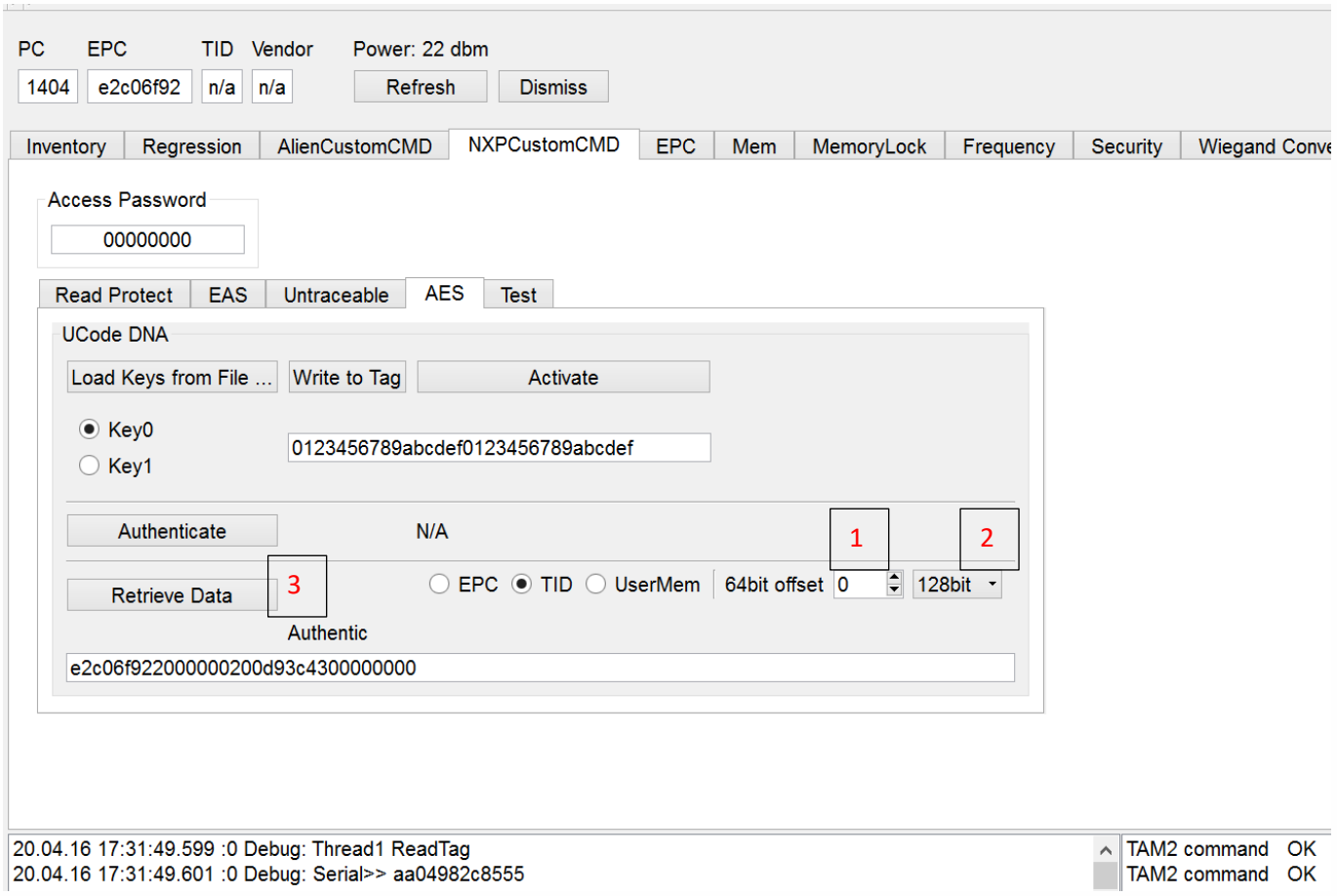
After selecting your desire settings, check the "*Set Tag Limits*" (7) radio button;

Finally click on the *Set Parameters* button (8).

To reset untraceable settings to default values, check the "*reset*" (9) radio button and then click on the Set Parameters button (8).

Retrieving untraceable hidden data using Key1

To retrieve untraceable hidden data using key1, go to the *AES* sub-tab;



Ensure that you have already load the key, if you have not, please refer to section Loading the AES Keys for instruction.

Select the memory bank that you would like to retrieve the hidden data from by checking the radio button respectively.

You can change the offset of the memory per 64 bit units for reading the hidden data (1).

You can also set the length of the data to be read (2). Please note that if you do not select the full length of the memory bank to be read, “00”s will be padded at the back to represent the full length of the memory.

Finally click the “*Retrieve Data*” (3)button to read the hidden data.

USB Driver installation

Some versions of Microsoft Windows Vista/7 lack support for the USB device used in the VELA Desktop reader. Therefore you may need to install the drivers manually.

Download USB Driver

The SSI VELA RFID Desktop reader uses the Prolific PL2303 chip set.

The Driver for Windows Vista/7 can be download from the Prolific web page:

http://www.prolific.com.tw/

Please download the latest version of the driver for your Operating System and install the driver by following the instructions with the download packet.

Hardware Products Warranty Statement

WARRANTY.

All Hardware Products sold by STAR Systems International Limited (SSI) are warranted against defects in material and workmanship under normal use and service for one (1) year from the original date of purchase (the "Warranty"). Any Extended Warranties must be documented on the original invoice as a separate line item. For defects covered by this Warranty, SSI will repair the defect or replace the product, at its sole option and return the product to you.

EXCLUSIONS.

If the defect was caused by any of the following, the Warranty shall not apply and an estimate for repair or replacement will be submitted for your approval prior to work being performed: abuse, mishandling, acts of God, vandalism, accident, electrostatic discharge damage, failure to follow installation or operating instructions, failure to provide a suitable environment, unauthorized modification of the product modification of the printed circuit board by parties other than SSI, and damage that is caused during shipping for warranty service and any product that is returned with the security seal broken.

RMA PROCEDURE.

For Warranty service, the Customer must comply with STAR Systems International Return Materials Authorization ("RMA") policy, which is published on the STAR Systems International website at www.starint.net, and may be updated from time to time. Prior to shipping a product to STAR Systems International for warranty inspection, replacement or repair, an RMA number must be obtained from STAR Systems International's RMA department at +852 3691 9925 or by email at support@star-int.net. RMA forms can be downloaded from the STAR Systems International website or the Customer can receive the form by fax (+852 37474065) or email by contacting the RMA department. One RMA form must be used for each RMA submission and the product should be shipped to the address below. For products covered by this Warranty, the Customers are responsible for payment of shipping costs to the STAR Systems International repair center and STAR Systems International will be responsible for the cost of returning the item. The standard return shipment is "Speed Post". Any other desired "expedited" or overnight shipping costs for warranty repairs will be the customer's responsibility.

DISCLAIMER OF WARRANTIES.

OTHER THAN SET FORTH ABOVE, SSI HEREBY DISCLAIMS ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING WITHOUT LIMITATION, THE WARRANTIES OF Equipment Warranty (Rev 2-2017) MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT.

LIMITATION OF LIABILITY.

IN NO EVENT WILL SSI BE LIABLE FOR ANY CONSEQUENTIAL, INDIRECT, EXEMPLARY, SPECIAL, OR PUNITIVE DAMAGES, WHETHER ARISING OUT OF CONTRACT, TORT, NEGLIGENCE, STRICT LIABILITY OR OTHERWISE. IN NO EVENT WILL STAR SYSTEMS INTERNATIONAL'S TOTAL CUMULATIVE, AGGREGATE LIABILITY, WHETHER ARISING OUT OF CONTRACT, TORT, NEGLIGENCE, STRICT LIABILITY, OR OTHERWISE, EXCEED THE PRICE ACTUALLY PAID BY THE CUSTOMER FOR THE PRODUCT FROM WHICH THE CLAIM ARISES.

This warranty gives the Customer specific legal rights, and the Customer may also have other rights that may vary from local jurisdiction. If the Customer has questions concerning the product or warranty, contact the dealer from which it was purchased. The Customer may also contact STAR Systems International at the following address and ask for warranty assistance.

Appendix

This section provides you with safety information, technical support information, and sources for additional product information.

Safety Information

Your safety is extremely important. Read and follow all warnings and cautions in this document before handling and operating RFID equipment. You can be seriously injured, and equipment and data can be damaged if you do not follow the safety warnings and cautions.

A caution alerts you to an operating procedure, practice, condition, or statement that must be strictly observed to prevent equipment damage or destruction, or corruption or loss of data.

Note: Notes either provide extra information about a topic or contain special instructions for handling a particular condition or set of circumstances.

Global Services and Support

Web Support

Visit the SSI website at www.star-int.net to download our current manuals (in PDF).

Visit the Star Systems University at www.star-int.net and click **Tech Support > Star Systems University** to review technical information or to request technical support for your RFID product.

Send Feedback

Your feedback is crucial to the continual improvement of our documentation. To provide feedback about this manual, please visit the **Contact Us** at www.star-int.net.

Telephone Support

In Hong Kong, Call **+852-3691-9925**. In the U.S.A., call +**1-888-457-7755**.

Outside Hong Kong and the U.S.A., contact your local SSI representative. To search for your local representative, from SSI website, click **Contact Us** at www.star-int.net.

Related Documents

The SSI website at www.star-int.net contains our documents (as .pdf files) that you can download for free.

To download documents

1 Visit the SSI website at www.star-int.net.

2 Click the **Tech Support > Download**.

3 According to your product category, choose **Readers / Antennas / Tag Labels**.