Xenon 1950/1952, Vuquest 3320g, Granit 1910i/1911i/1920i/1990iSR/1990iXR/1991iSR, scan engines N56xx, N66xx, Voyager 1470g/1472g/1602g

User's Guide

Table of Contents

1. Introduction.

Data Matrix DMPS Decoder/Plugin for **Honeywell's Total Freedom Platform** area images is based on 2DTG Data Matrix (DM) decoding library and provides functionality upgrade for 2DTG's DPM Plugin, allowing not only to decode DM symbol, but to perform its Authentication/Decryption to ensure that it is not counterfeited or tampered with.

1.1 Scope and SDK composition

Data Matrix DMPS Plugin package is notated as **DMPS_Plugin_v.17.10.7.zip** and includes the following file:

- DMPS_Plugin_v.17.10.7.moc

Its decoding features are the same as for the Multi-Platform Data Matrix DPM plugin. They are described in detail in the corresponding **User's Guide**. Authentication/Decryption features are built as an extension of the Data Matrix decoding algorithm for embedded platforms, so the decoder can be used both for the DM protection purposes, as it's described in this User's Guide, and regular decoding:

- decoding data encoded into Data Matrices ECC200 in accordance with ISO/IEC 16022 Symbology specification; and
- authenticating Data Matrix symbol if it was enabled for authentication utilizing **DMPS_E** encoding software (User ID/**Authentication key**); and/or
- decrypting Data Matrix symbol if it was encrypted utilizing **DMPS_E** software (Product ID/ **Encryption key**).

Data Matrix Security Encoding software (**DMPS_E**) may be required along with DMPS Plugin to start protecting your products/documents.

Unlike system (Honeywell) decoder, DMPS plugin can decode Dot Peen symbols, as well.

DMPS Plugin provided as a fully functional trial version, but some characters in the output string are replaced with "*". Purchased license unlocks Plugin – no new installation is required.

1.2 References

- 2DTG User's Guide "DPM Plugin Installation Instruction and User's Guide".
- ISO/IEC 16022 - Symbology specification - Data Matrix
- U.S. Patent No.: 8,297,510 B1 "Mathematical method of 2D barcode authentication and protection for embedded processing"

2. Configuring DMPS Plugin

Procedure for the deployment of the **Data Matrix DMPS Plugin** is pretty much the same as for the regular DPM Plugin, but Settings are slightly different.

2.1 Loading Authentication/Encryption parameters into a scanner.

In substance, the plugin is an extension of DMPS_D (decoding Data Matrix Security software for Windows PC) to the embedded platform. It has a proprietary built-in mechanism allowing to

"read" enabled for Authentication Data Matrix and to decrypt it, if it was encrypted/enabled for authentication by DMPS_E (in addition to the regular Data Matrix decoding).

EZConfig (Command Center) is required to load **Authentication (User ID)** and **Encryption (Product ID)** Keys into the Imager:

990009C72U_ID<User ID>.
990009C72P_ID<Product ID>.

Note: for cordless Imager both commands shall be preceded by '**:*:**'

2.2 Enabling required protection settings

(Default position for **Authentication** (**USIG) / Decryption (PSIG) is OFF)**

It can be done both from EZConfig Command Center and by scanning appropriate command codes:

990009C72USIG1 - to enable authenticity check (**User signature ON)** 
990009C72PSIG1 – to enable decryption (**Product signature ON**) 
990009C72USIG0 – to disable authenticity check (**User signature OFF)** 
990009C72PSIG0 – to disable decryption (**Product signature OFF**) 

3. DMPS Reference Test

To ensure that DMPS Plugin is configured correctly and to familiarize yourself better with its features it is recommended to perform the reference test:

NO Protection	Authentication enabled only	Encryption only	Authentication + Encryption
Level 0	Level 1	Level 2	Level 3
			

All symbols have the same encoded text: "2DTG – Your optimum choice in robust performance". Load Authentication/Encryption parameters (from EZConfig command center) that were used when creating these symbols into the Imager:

- **990009C72U_ID*User_Company_Name*133511489C993057B47F82*D6522625657B0E1E656870**
- **990009C72P_IDs#123456789**

There are four steps in this Test (results are summarized in the Table below):

Test "0" If neither Authentication (USIG) or Encryption (PSIG) Key is enabled (USIG=PSIG=0), the DMPS Plugin works as a regular decoder returning decode information even for Authentication enabled Data Matrix – "read" Data Matrix symbols of Level 0 & 1 in the Table above. The return shall be as follows: "2DTG – Your optimum choice in robust performance". Each decoding is accompanied by 1 "beep".
Test 1 **Authentication** Key enabled: • send **990009C72USIG1** command in EZConfig or scan command code from 2.2. "Read" Data Matrix symbols of Level 0 & 1 in the Table above. The "Authentication return" shall be as the table below: Each decoding is accompanied by 2 "beeps". Note: If **Authentication** vetting returns "**Failed**" (Level 0), the matrix can still be decoded.

Test 2

Encryption Key enabled:

- send **990009C72PSIG1** command in EZConfig or scan command code from 2.2 and;
- disable **Authenticity** check **(990009C72USIG0)**

"Read" Data Matrix symbols of Level 2 & 3 in the Table above. The "Encryption mode return" shall be as in the table below:
Each decoding is accompanied by 2 "beeps".

Test 3

Both Authentication + Encryption keys are enabled:

- send **990009C72USIG1** command in EZConfig or scan command code from 2.2 again.

"Read" Data Matrix symbols of Level 2 & 3 again from the table above and compare with the table below.
Each decoding is accompanied by 2 "beeps".

Protection Level	Data Matrix Type	Data Matrix Sample	Plugin's return	"Failed" - Test #
Test 1 Level "1" Protection - Authentication only Plugin setting: **USIG1**	Regular Data Matrix (Level 0)		**Authentication Failed!**	1
	Authentication enabled Data Matrix (Level 1)		**Authenticated!**	
Test 2 Level "2" Protection - Encryption only Plugin setting: **USIG0, PSIG1**	Encrypted Data Matrix (Level 2)		**Decryption OK!**	
	Authentication enabled + encrypted Data Matrix (Level 3)		**Decryption OK!**	

Test 3 Level "3" Protection Authentication + Encryption Plugin setting: **USIG1, PSIG1**	Encrypted Data Matrix (Level 2)		**Authentication Failed! Decryption OK!**	3
	Authentication enabled + encrypted Data Matrix (Level 3)		**Authenticated! Decryption OK!**	

Authentication Failure (Test 1) indicates that vetted symbol was counterfeited. Most probably, original authentication enabled Data Matrix was captured, decoded using regular DM decoder and the obtained data were used for generating counterfeited symbols for placing them on counterfeited goods, documents, etc. It is strongly recommended to replace Authentication key immediately.

Authentication Failure (Test 3) indicates that since the symbol is successfully decrypted, but Authentication failed - Encryption Key was possibly compromised. Authentication Key might be intact - authentication possibly was not enabled – but might be compromised too. In any case, it is strongly recommended to replace both key immediately in this case.

Additional comments on vetting results:

User ID is required not only for authentication process, but for encryption as well. **Encryption Key** is built both from Product ID that is entered into the system by the user and unique User ID / Authentication Key provided by 2DTG. That is why it is important that Authentication Key must be scanned in the system even if DMPS software seems to be used only for encryption/decryption purposes.

If **User Signature (Authentication** vetting) returns "**Authentication Failed!**", the matrix can still be decoded, meaning that counterfeiter has not even recognized that symbol is protected.

4. Appendix 1. Quick Reference Chart.

This Appendix provides a list of the commands related to Plugin installation process or operation. Some of them shall be executed in a Debug mode for the results to be displayed.

4.1 Licensing Plugin

Use Command Center:

990009C72LIC#<License key>.
:*:990009C72LIC#<License key>. (Xenon 1952)

RESET_.

4.2 Plugin Testing and Diagnostics

Enable Debug Mode

PLGDBG1.

Disable Debug Mode

PLGDBG0.

Display Plugin Directory

PLGDIR.

Display Plugin Information

PLGINF.

Enable Plugin

PLGDCE1.

Disable Plugin

PLGDCE0.

4.3 Configure Plugin

Enable authenticity check

990009C72USIG1

Enable decryption

990009C72PSIG1

Disable authenticity check

990009C72USIG0

Disable decryption

990009C72PSIG0

4.4 Removing Plugin

Remove Plugin (including License)

PLGDLA.

Reset (Save)

RESET_.

5. Appendix 2. Plugin Parameters

There are a few useful commands allowing to check out plugin parameters and their settings.

5.1 Plugin Directory (PLGDIR.)

Scan **PLGDIR.** Command code to display Plugin directory

DMPS Plugin	
PLGDIR.	.
OptModes	168
icEveryCode	794
Lic.key	10
icEveryCode.plugin	223964
user.id	64
2097152 total,1872152 free,225000 used	

Note: "**Lic key**"- line above may return one of two values, as follows:

- "**Lic key 0**" – submitted License Key has incorrect syntax.
- "**Lic key 10**" – means that syntax is correct. However, it does not necessarily mean that License Key itself is correct. If Plugin is still in DEMO mode after licensing - check PLGINF (Section 5.2).

"**User.id**" size is different for every customer. Other parameters must be the same.

5.2 Plugin Information (PLGINF.)

Scan **PLGINF.** Command code **twice** to display information about Plugin

```
PLGINF[Decode Plugin Configuration]
        <Decode.plugin>
                [name]:              2DTG_Decode PlugIn
                [company]:  2D Technology Group, Inc.
                [licensed]:             YES
                [active]:             YES
                [majorrevision]:        17
                [minorrevision]:        10
                [build]:              7
                [certificate]:        102148
                [certificatetime]:    2009/08/10 15:00:05
                [guid]:               abcd1234
                [filename]:
icEveryCode.plugin
                [mainroutineorder]:     AFTER
                [barcodeinterceptmode]:   YES
                [entrydatastate]:       MODIFIED
                [chainonexit]:
CHAINIFFAILURE
                [loadstatus]:           SUCCESS
```

Majorrevivion
Minorrevivision indicate the Date of the installed Plugin file → year (yy) / month (mm) / date (dd)
Build

Mainroutineorder indicates the order of the Plugin in the decode routine (AFTER or BEFORE the system decoder)

[licensed]: YES/NO - indicates if the Plugin is licensed or not.

Note:

- Plugin is not licensed (by default) after its download to the scanner. The decode output is modified to make plugin to return "*" instead of some characters (DEMO Mode). Accordingly, the **[licensed]**-line in the print-out above will display "**NO**".
- If licensing (Section 3) failed for any reason (License Key or its syntax is incorrect) plugin will stay in DEMO mode and "**[licensed]"**- line in the print-out above will display "**NO**" (as it's supposed to do for DEMO mode).

- "**[licensed]"**-line displays "**YES**" only when correct License Key is entered to the scanner.

5.3 Authentication/Decryption modes

Switch Plugin to the Debug Mode (**PLGDBG1.**) before proceeding to checking out Authentication/Decryption parameters.

1. To upload or change Authentication Key use EZConfig Command Center for example, EZConfig return for trial Authentication Key:

```
[PLGUIN_DEBUG] USER ID =
<*User_Company_Name*133511489C993057B47F82*D6522625657B0E1E656870>
990009C72U_ID*User_Company_Name*133511489C993057B47F82*D6522625657B0E1E656870
[ACK].
```

2. If Authentication Key (User ID) is incorrect, the return would be as follows:

```
Request:
990009C72U_ID*User_Company_Name*133511489C993057B47F82*D6522625657B0E1E65687
Response:
[PLGUIN_DEBUG] MatrixPluginProcessingBarcode
[PLGUIN_DEBUG] Datalen = 67,   Menu Data is:
U_ID*User_Company_Name*133511489C993057B47F82*D6522625657B0E1E65687
[PLGUIN_DEBUG] USER ID =
<*User_Company_Name*133511489C993057B47F82*D6522625657B0E1E65687>
[PLGUIN_DEBUG] Set UserId FAILED!
990009C72U_ID*User_Company_Name*133511489C993057B47F82*D6522625657B0E1E65687
```

UserId status. If it's corrupted this output will show "**Set UserId FAILED!**" and plugin will become non-operational in case any "signature" is enabled, but it will continue to operate normally if "Signature = 0".

Check Authentication Key (User ID) and try again.

3. To upload or change Encryption Key use EZConfig Command Center for example, EZConfig return for trial Encryption Key:

```
Request: 990009C72P_IDs#123456789
Response:
PLGUIN_DEBUG]
[PLGUIN_DEBUG] MatrixPluginProcessingBarcode
[PLGUIN_DEBUG] Datalen = 15,   Menu Data is: P_IDs#123456789
[PLGUIN_DEBUG] PRODUCT ID = <s#123456789>
990009C72P_IDs#123456789[ACK].
```

5. To check out what Authentication/Encryption mode your imager is in - scan appropriate Command Code (or send Command from the Command center) USIG or PSIG. It should return the result as follows (990009C72USIG1, 990009C72PSIG1) code are scanned

```
[PLGUIN_DEBUG]
[PLGUIN_DEBUG] MatrixPluginProcessingBarcode
[PLGUIN_DEBUG] Datalen = 6,   Menu Data is: USIG1.
[PLGUIN_DEBUG] Signature mode = 1
[PLGUIN_DEBUG] OptMode changed !

[PLGUIN_DEBUG]
[PLGUIN_DEBUG] MatrixPluginProcessingBarcode
[PLGUIN_DEBUG] Datalen = 6,   Menu Data is: PSIG1.
[PLGUIN_DEBUG] Signature mode = 3
[PLGUIN_DEBUG] OptMode changed !
```

Signature mode = 1 => Authentication mode
Signature mode = 2 => Encryption mode
Signature mode = 3 => Both Authentication & Encryption mode

6. Some Scanner Command Codes

6.1 Configure Common Interfaces

USB – Keyboard (HID) Mode

TRMUSB124.

USB Serial Emulation

TRMUSB130.

6.2 Scanner Data Matrix Decoder

Disable System Data Matrix Decoder

IDMENA0.

Enable System Data Matrix Decoder

IDMENA1.

6.3 Enabling Plugin for Granit 1920i

Enabling Plugin for Granit 1920i

EXPMOD2

6.4 Add a Carriage Return Suffix

Add CR Suffix

VSUFCR