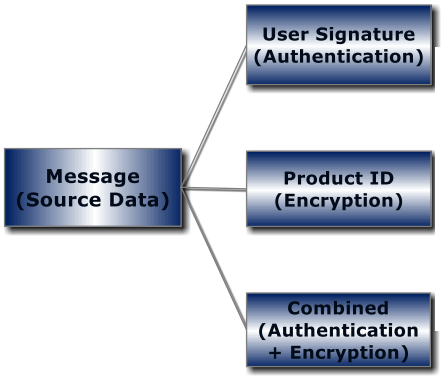
Data Matrix Protection Suite

Protect your brand by protecting your data label



- 3-Levels of Data Matrix Protection against counterfeiting
- Symbol Authentication and Encryption
- Instantaneous Brand Verification Directly at POS
- Effective User Management System

What is DM Protection Suite?

DM Protection Suite (DMPS) is an easy-to-use software package that allows not only to encode and decode text information into Data Matrix symbol, but to digitally protect this symbol from counterfeiting, as well. With DM Protection Suite, protecting your products and documents has never been quicker or easier!

DMPS consists of the two software programs – encoding (**DMPS_E)** and decoding (**DMPS_D)**. Encoding software has a proprietary built-in mechanism allowing either to authenticate the

encoded Data Matrix symbol afterwards or to encrypt it. The Decoding software checks symbol for authenticity or decrypts it while extracting the information from the symbol.

Depending on application, the programs can be used either together or separately. In a "Supply Chain Application", for example, the encoding software can be used on the "manufacturing end" and the decoding software – on the "receiving end".

Anti-Counterfeiting - The New Adoption Driver for Auto ID

"Track and trace" through an "information" label is a main application for the barcode industry. Upgrading this "information" barcode with the protective, anti-counterfeiting features creates new opportunities for suppliers to build a more secure supply chain. It's a natural extension – from tracking an individual item throughout the value chain with barcode to using that same system and that same barcode to ensure that all products within the value chain are authentic.

Protecting labels, which are circulating in supply chain anyway, instead of building separate product protection systems, makes this approach very cost effective. Though creating security system for an open supply chain, requiring protective barcode deployment across a number of levels of a commercial value chain – from the point of manufacture through the point of sale – would still take some time and discipline, such systems for more closed, mission critical supply environment can be implemented just today utilizing **DPMS** capabilities.

Authentication, actually, has been one of the major news for the RFID developer and supplier communities for the last couple years. According to VDC Research, the use of anti-counterfeiting and authentication applications in the RFID industry is expected to increase more than 100% over the next 3 years and listed as one of the most important adoption drivers.

Barcode industry is not there yet but it will surely follow this course.
.

How does it work?

DMPS employs the concept of Digital Signature for data authentication. A digital signature scheme allows one to sign an electronic message and later the produced signature can be validated by the owner of the message or by any verifier. It normally utilizes asymmetric algorithm - a private key for signature generation, but a public key (which corresponds to, but is not the same as, the private key) - for signature verification. This is nearly always very computationally intensive and can not be used on DSP-based platform (scanner).

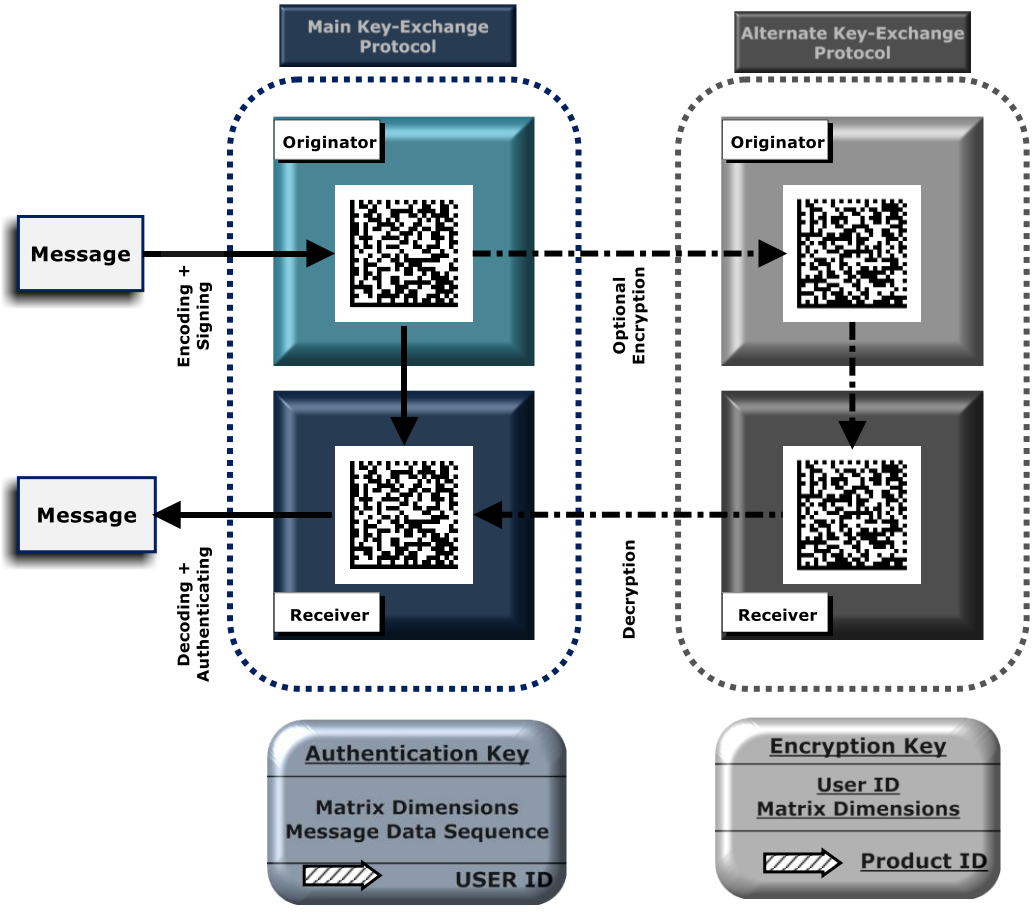
Our patent pending method makes use of symmetric key algorithms integrated into the encoding/decoding mechanism. This makes our software suitable for embedded processing.

As it is always a case with the symmetric-key algorithms, the single secret key is a subject of a certain key-exchange protocol. If this protocol is compromised the whole scheme may become dysfunctional.

To strengthen the Authentication mechanism, **DMPS** also offers one more layer of protection - additional encryption (on top of authentication) and establishing an alternate key-exchange protocol. This algorithm also satisfies the embedded processing requirements.

For the sake of convenience **DMPS** treats two above mentioned algorithms as two types of digital signatures – **User Signature** and **Product Signature**. The term "signature" is used only to underline the fact that each Data Matrix, generated using these algorithms, will have the unique digital characteristics distinct from any other Data Matrix symbol with the same encoded message/data.

User ID and **Product ID** – are those secret keys that are communicated within the above mentioned key-exchange protocols.

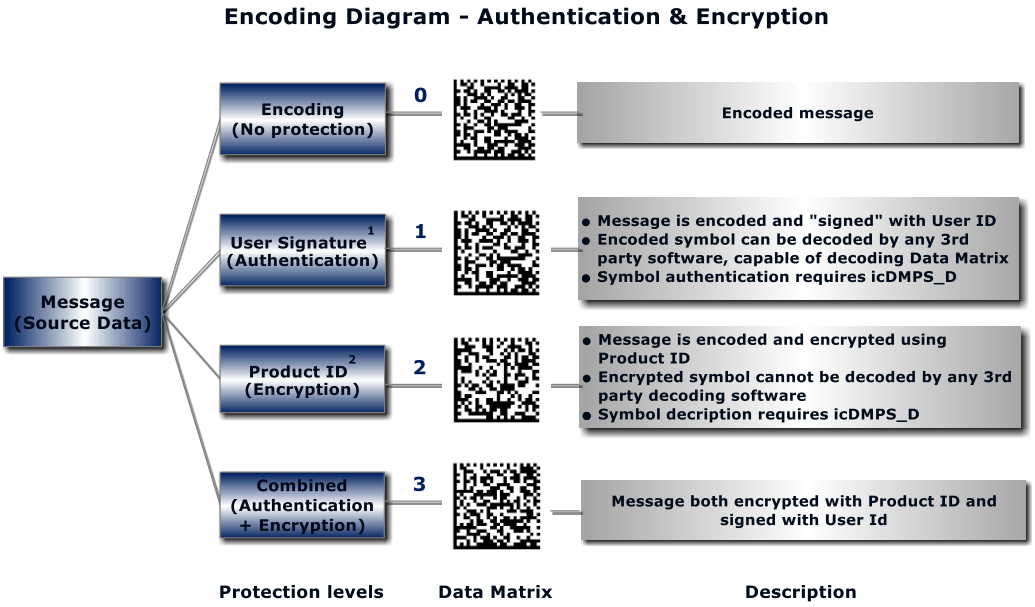


Both Authentication and Encryption keys are calculated using Random Number Generator (RNG) that uses all the data shown above as the input parameters. The length of this data string

(input parameters) might be from 368 up to 2048 bits. Since the Authentication Key depends on encoded data sequence, it is different for every Matrix going through the Algorithm, which, in turn, makes it very difficult to break.

Protection Levels

Protection Levels correspond to the type of signature chosen – **User Signature** or **Product Signature** – when encoding the message/data:



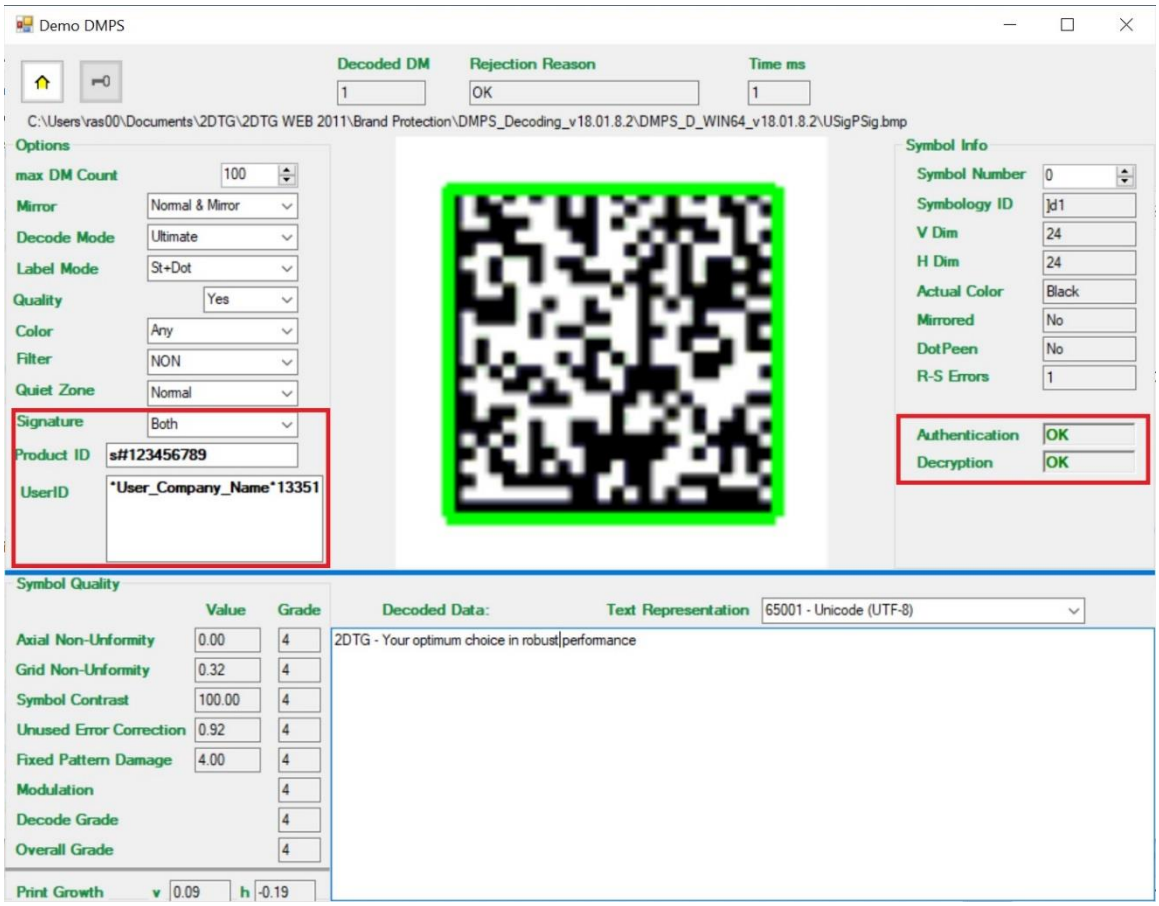
User Signature – provides protection from "*repeated encoding*" (when original Data Matrix is captured, decoded and the obtained data are used for generating counterfeited symbols) by providing Matrix authentication. It also verifies the encoded data integrity. The method allows Data Matrix to be "readable" by any standard, third party decoding software thus precluding a potential attacker from even knowing that the barcode is protected. If counterfeited symbol is discovered in the supply chain, for example, one can go backward through the chain authenticating symbols at each stage and quickly find out where the fake product was injected.

Product Signature - provides protection both from *"repeated encoding"* and "*direct copying"* by encrypting the Data Matrix symbol. Unlike the User ID, which is designed to be a "permanent" characteristic of the "User" within the certain application class, Product ID is an arbitrary alphanumeric number (Serial Number, Batch Number, Tracking Number, etc.) and can be changed at any time, thus making the task of counterfeiting and copying symbols very

Decrypting and Authenticating Data Matrix Symbol

The Decoding software (DMPS_D) decrypts symbol or checks for authenticity while extracting the information from it.

GUI for the decoding application looks pretty much the same way as for DM Enterprise Decoder (2DTG User's Guide "**Data Matrix Decoding SDK (Professional, DPM, Enterprise editions)** with two additional Sections (shown in Red below):



Signature option allows to choose the "level of protection":

- None
- UserSign – **Authentication** only
- ProdSign – **Encryption** only
- Both – **Authentication + Encryption**

The result is shown in "**Symbol info**" section.

DMPS_D is also available for embedded platforms and as a Plugin for the commercial Honeywell scanners Xenon 1950/1952 or Android APP for mobile computer CT60 - making it a very convenient tool for POS inspections.

User Management

Encoding software (**DMPS_E)** comes with 2DTG's **User ID** Generation software (User IDs are required for digitally signing Data Matrix symbols), and unique **Master ID** file. The file contains a string of 87 alphanumeric characters that are actually used for generating the **User ID** files that are, in turn, used for digitally signing the encoded (Data Matrix) information. The syntax of this string is as follows:

Installation Key*Unique Identifier

(29 characters) (58 characters)

The Company can generate any number of **User IDs** with one **Master ID** that it receives from 2DTG depending on the application, which it is going to be used for.

Digital Signature approach is recommended to be used within a defined circle of companies/organizations, associated by the intent to protect the integrity of a supply chain, or document exchange, or any other information exchange. Accordingly, every company/organization, belonging to this circle, should receive from the Master Company a **User ID** that is associated with the symbols to be protected.

The **user.ID** file contains the string of up to 100 alphanumeric characters having syntax as follows:

***User Name*689B18B4DEFF181276F245*033FA9F560B6830036CADC**

Up to 53 characters Unique Identifier

In addition, every member of this circle should have Digital Signature enabled decoding software by 2DTG – **DMPS_D.**