dPId Pty Ltd
ABN: 25 126 210 320
Helping others to have a future assures our own.
www.dPId.biz

23 Avenel Road,
GYMEA BAY, NSW 2227
Ph: +61 2 9016 4695
Mob: +61 416 276 624
ceo@dPId.biz

AN INEXPENSIVE MEANS OF GENERIC AND INDIVIDUAL IDENTIFICATION BY dPId

dPId provides a means of identification, both generic and individual, that is markedly cheaper, easier to use, surer and superior in performance than GS1. (Australian Innovation Patent 2012100279 issued 8 May 2012. Chinese, US, Indian and European patents are expected to follow.) To learn more: read below.

INTRODUCTION

1. The ability to generically identify items, and to use that identity in commerce, has been available since the advent of the barcode in the 1950's. Individual identification of every object of interest in an organisation has been much more difficult and expensive to achieve. Individual identification is highly desirable because it provides the means by which processes may be managed to the finest possible detail. In many instances this level of control is not required but in those cases where the object is of critical importance to the successful achievement of organisational goals, this individual tracking, and the attribution of the contribution of all involved parties, is absolutely essential.

2. There is an adage that says, "It's better to have it and not need it than to need it and not have it!" In the past, it has been cost prohibitive to individually identify every single object. With NU-ERA, that is no longer the case. Now its affordable to, "Have it and not need it!". NU-ERA stands for **N**umerically **U**nique – **E**ncrypted **R**edundant **A**rray. NU-ERA is actually a suite of technology aimed at making the cost of individual identification both practical and affordable for every organisation in the world.

3. The high cost of individual identification in the past came about because of the technology available and the individual ID systems that were used. Typically objects are identified by a string of characters. A car's number plate is an excellent example of this. The registration plate numbers are issued by separate registries, one in each state and territory with some minimum level of cooperation between these registries so that the numbers issued will always be unique. Once the numbers have to comprehend hundreds of millions or even billions of different objects, the challenge of ensuring the numbers issued are unique becomes significant and that is where dPId's NU-ERA comes in.

DETAIL

The Registry

4. **Inexhaustible supply of Unique Identifiers.** At the heart of NU-ERA is a registry with unique encrypted identifiers ranging from 0 to 7.9228×10^{28}. In other words, it is possible to issue a billion, billion identifiers per year for more than 79 billion years before the pool of unique encrypted identifiers would be exhausted. Without going into too much complexity, in actuality, the NU-ERA identifier and its registry can be of any size. At the moment, there is an operational registry consisting of identifiers that are based on 2^{128} or "128 bits". It is possible, for example, for there to be another registry based on 256 bits identifiers.

5. **Identifiers can be validated.** In all instances the identifiers are encrypted. By being able to decrypt the identifiers, users can verify that the identifier was actually drawn from the dPId registry. This means NU-ERA identifiers can be very useful for detecting counterfeiting. It is very, very difficult for someone to guess an identifier that would correctly decrypt. The 2^{128} identifiers are encrypted using AES256 which is a symmetric encryption algorithm, that is, the key used to encrypt the identifier is the same as the key used to decrypt it. To decrypt and validate AES256 identifiers, users require a special piece of hardware which ensures this key remains hidden or they need to forward the identifier to a dPId server. The 2^{256} identifiers are encrypted using Elliptic Curve Cryptography which is an asymmetric system. The identifiers are encrypted using what is called a "Private Key" known only to dPId. To decrypt and validate these users only need what is called the "Public Key" and some software. Although the identifier is much larger, the asymmetric system has the advantage of not requiring special hardware.

6. **Fixed length identifiers.** Identifiers are of a fixed length and unique. They are therefore ideally suited for use as primary keys in a database. This results in lightning fast performance, even from the largest of databases, when accessing information using a NU-ERA identifier.

7. **Very easy to use.** Numbers are sequential for any client-system but can be associated with any item of interest within an organisation or grouping. This makes it very simple to deploy NU-ERA when barcoding all articles throughout a workplace. Within Defence, it was found that NU-ERA identifiers required around 60% lesss effort to tag articles than that which was required when using the system provided by GS1, its main competitor.

The use of 2D Bar Codes

8. Examples of NU-ERA 128 bit identifiers in "human-readable form[1]" are as follows:
   a. NVyjPzs5VuMM68SptOvOtA==, or
   b. ZI6ROVmkR5xqSQW5wOeUZQ==.

9. **The limitations of a linear barcode.** Trying to write down these identifiers would be tedious for a human and the process would be prone to error. To overcome that, bar codes were invented. Unfortunately, linear barcodes, (see Figure 1) are limited in the amount of information they can represent. To represent the identifier shown above would require a very long barcode (and hence be impractical) so 2D barcodes were invented.

1 This identifier is displayed in what is called Base64 Encoding.

Figure 1: Example of a 3 of 9 bar code for Alpha Numeric Strings

Figure 2: DataMatrix code representing NVyjPzs5VuMM68SptOvOtA==

Figure 3: DataMatrix code representing ZI6ROVmkR5xqSQW5wOeUZQ==

10. **2D Barcode Symbology**. Figures 2 and 3 show the representation of unique encrypted identifiers using a 2D bar code symbology called DataMatrix. These codes can be printed and used with most common bar code readers and even certain smart phones (such as Nokia, Motorola and HTC).

11. **RFID.** NU-ERA identifiers are ideally suited for, and can be accommodated in, even the cheapest of RFID appliances. (See Figure 4, courtesy of Wikipedia.)

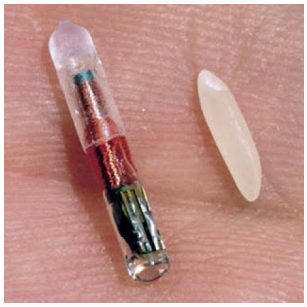

Figure 4: RFID Device next to ricegrain

Printing the Bar Code

12. To attach an identifier to an item requires either a label, a tag or some form of embossing of the item itself. Labels and tags can be made of a variety of materials the most common of which is paper. In the case of labels there is the requirement for an adhesive and tags must be attached by a tie of some description (including sewing). In both instances, there are issues with wear and the ability to stick or tie a label or tag to the object in a manner that will endure. In the case of clothing, it is typical to sew a label onto the garment. Embossing takes the form of painting, engraving, etching or peening an identifier

onto or into the surface of the item; the latter forms of embossing being the more permanent. In recent years, with the development of low-cost lasers, it is possible to quickly, inexpensively and permanently mark any item with a hard or semi-hard surface; even material or paper.

13. When seeking to use a laser, or when wishing to print to a very fine resolution, printing squares or circles as is commonly required by many common 2D barcodes requires that the laser have a sophisticated means of deflecting its beam to trace out the pattern. If a 2D barcode is comprised only of dots and represents an identifier only of a fixed length, this exercise becomes much simpler. The laser can then consist simply of an array of inexpensive laser diodes that can be activated to produce a particular code. The value of using a laser or some form of ink-jet where appropriate is that it is much cheaper than a label or tag and, in the case of a laser, far more durable.

14. The NU-ERA technology suite consists not only of a central registry but also of a novel barcode symbology that is comprised only of dots and is particularly resistant to dirt and damage. Unfortunately this symbology requires a new barcode reader and although dPId has built a prototype reader that demonstrates the ability to read NU-ERA barcodes, it is a long way off from being commonly available to the commercial barcode reader market. Fortunately, DataMatrix barcodes can be represented only in dots as per Figure 5 and read by conventional readers and smartphones.

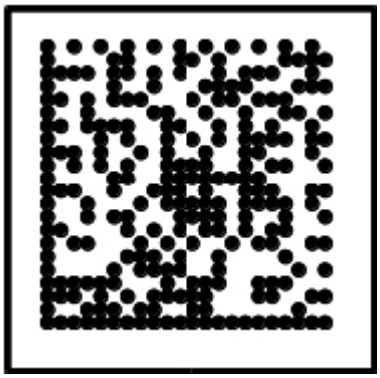

Figure 5: DataMatrix Barcode representing W7pdRRfCEq1bODBzKQcOOg

15. dPId can provide for free all of the software, including the source code, licence free, for the printing of the NU-ERA encrypted identifiers using DataMatrix 2D barcodes. This software will run on any popular operating system such as Linux or Windows.

Comparing NU-ERA to GS1

16. **GS1 is expensive.** Global System One (GS1) is an organisation established by a consortium of industrial giants in the USA. It earns more than a billion dollars per annum. GS1 issues its members unique identifiers either for the purposes of generically or uniquely identifying the items they manufacture or sell. It is expensive to become a member of GS1 and it is expensive to purchase identifiers from them.

17. **GS1 is clumsy, labour intensive and slow.** GS1 is, to some extent, trapped by history and conventional thinking. The method used by GS1 to identify items individually is to take a manufacturer's part number and then append to that a serial number allocated from a registry maintained by each manufacturer. This means that the resultant identifier is hierarchical in its structure and of variable length between manufacturers. In a similar vein, where NATO stock numbers are used, the system is for each country of origin to maintain a registry for each stock number and to allocate a unique serial identifier (often alphanumeric) for that stock number where individual identification is required. The disadvantages of this are:

a. The hierarchical structure means that there is largescale wastage of identifiers.
b. The reliance on numerous organisations maintaining numerous registries is fraught with error and is expensive.

c. The variable length of the identifier, often an alphanumeric string of characters, means that the identifier cannot be used as the primary key in a database table. This significantly degrades the performance of any database using the GS1 identification system.

d. There is no way of validating the identifier in order to determine it is genuine.

e. In adopting GS1, consumers (such as the Department of Defence and Government generally) limit the vendors they can deal with to those that are members of GS1. This means higher prices for consumers and the exclusion of firms that cannot afford membership; mainly small businesses. This, in turn, limits competition and access to innovation.

18. **NU-ERA identifier is inexpensive and simple and fast to use.** By way of comparison, dPId's NU-ERA system of generic or individual identification is:

a. **Inexpensive.** When purchased in bulk, NU-ERA identifiers can cost as little as one thousandth of a cent. There is no requirement for purchasers to be members of NU-ERA. Purchasers do have to provide their contact details and the purpose for which the identifiers will be used. This information is verified prior to the sale of the identifiers. Additionally, dPId provides as much support as possible in the form of free software and advice in order to help its clients make best use of these identifiers.

b. **Fast.** Because NU-ERA unique identifiers are of a fixed length and equal to or less than 128 bits, they may be used as the primary keys in a database table. As a consequence, using this identifier allows extremely rapid extraction of any amount of data from a large modern database such as PostgreSQL.

c. **Capable of validation.** Each NU-ERA identifier is encrypted. With the right equipment or by referring the number to dPId, it is possible to verify the identifier did come from the NU-ERA registry. This makes it very difficult for persons to recycle goods, such as alcohol, and to falsely mark counterfeit, high-value items such as watches and fashion apparel.

d. **Saves on labour.** Tests conducted at the Australian Defence National Supply and Distribution Centre indicated that using NU-ERA identifiers instead of the GS1 system of individual identification, saved around 60% in the labour associated with the tagging of articles.

SUMMARY

19. In summary, dPId's NU-ERA identification technology offers a safe, inexpensive means of uniquely or generically identifying any entity of interest in any organisation or grouping, using a variety of existing ID technologies. It is ideally suited for the Internet and for use with modern databases, offering the means by which all enterprises throughout the world can inexpensively operate in the same space without the fear the identifiers they are using might inadvertently be duplicated by someone else dealing with an entirely different product or service.

Kevin Loughrey
CEO

- End of Paper -