NC3 THE NO-COMPROMISE CHARGE CARD

What Merchants don't have, Crooks can't steal.

Can NC3 be cracked? / Partial Dual Encryption (PDE)

(this document is not intended for all readers)

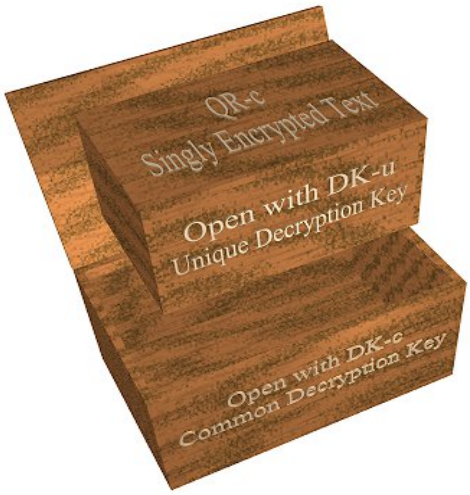
Think about Matryoshka nested dolls. One large doll holds a medium sized doll. The medium sized doll holds a smaller doll. Until you open the large doll you don't even know there are other dolls. Encryption need not be a single process. You can encrypt material once, then encrypt it all a second, or more, time. The downside is that *none* of the information can be accessed until *all* of the information is available. PDE is applied to a consumer's payment authorization, a quick response code from the consumer to a merchant, a QR-c. It allows for some information to be viewed without encryption (plain text), other information to be visible to a post-merchant processor, and the last bit visible only to the provider. This is multiple protection levels with controlled partial visibility.

Two keys are for encryption, two for decryption. Two are common to a group of consumers. Each consumer has two unique keys.

EK-c Common Encryption Key
DK-c Common Decryption Key
EK-u Unique Encryption Key
DK-u Unique Decryption Key

← The whole chest represents a QR-c showing the plain text portion to anyone who looks. To open the chest you need the DK-c.

Once the chest is opened with DK-c now we see a second chest and the information that had been encrypted once is now visible. →



← Lift the second chest up. To open it we need to apply the DK-u.

The DK-u is applied, the lid opened, and the doubly encrypted material is visible. →

All the information is in a single chest, a single file, a single QR code. Different information is available at each level of protection.

For those inclined there is more detail on the pages following.

A little more technical detail for those inclined.

In preparing an encrypted QR-c, a block is prepared with the NC3 code (an identifier for the specific consumer that is not derived from the underlying consumer credential or card number) and all other information.

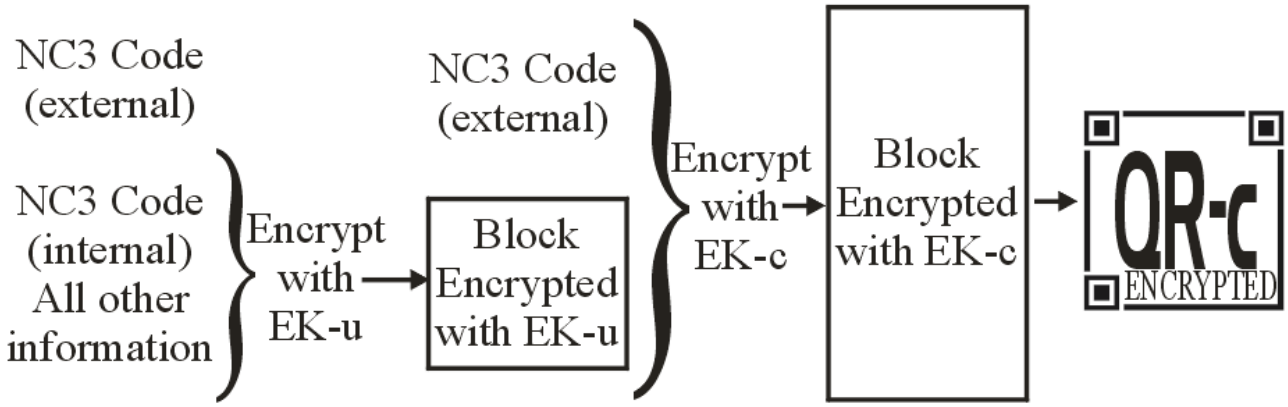
This copy of the NC3 code is called “internal” meaning internal to the block that will be doubly encrypted. There is also an “external” copy of the NC3 code. The external copy will be only singly encrypted.

The block is encrypted with EK-u, the encryption key unique to that single NC3 code.

The resulting block and the external NC3 code are then encrypted with the EK-c, the common encryption code. Reading the encrypted QR-c will reveal only encrypted material easily interpreted as random characters. Casual inspection will not even reveal the existence of double encryption of part of the contents nor is there a clear demarcation between the three segments.

Partial Dual Encryption with Unique and Common Keys

Encryption Sequence

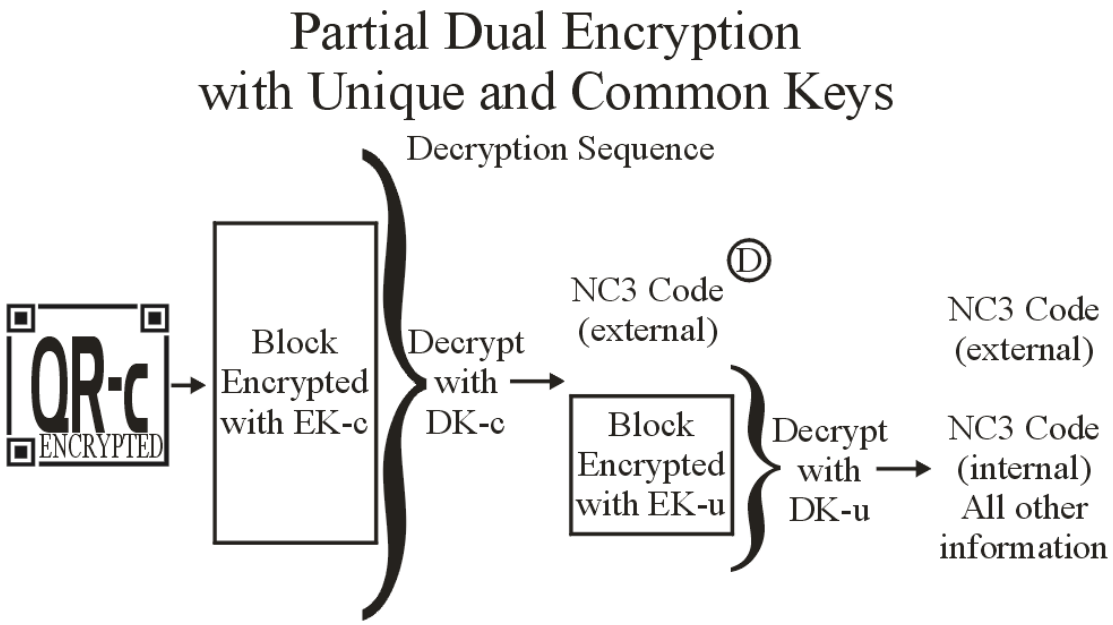


When the encrypted QR-c arrives it is translated from a QR-c to an encrypted block which is then decrypted with DK-c, the common decryption key.

This exposes the external NC3 Code (see Circle-D) which is used to locate the appropriate unique decryption key.

DK-u is used to decrypt the doubly encrypted block which exposes the internal NC3 and the other information. The internal NC3 must match the external NC3 for the QR-c to be valid and processed.

In this manner, even if the common encryption is compromised, the block containing the amount and NC3 (internal) are not. Changing the NC3 code (external) provides no benefit to a thief.



This document is a summary of the PDE concept.

Additional technical details are not included in this public documentation.