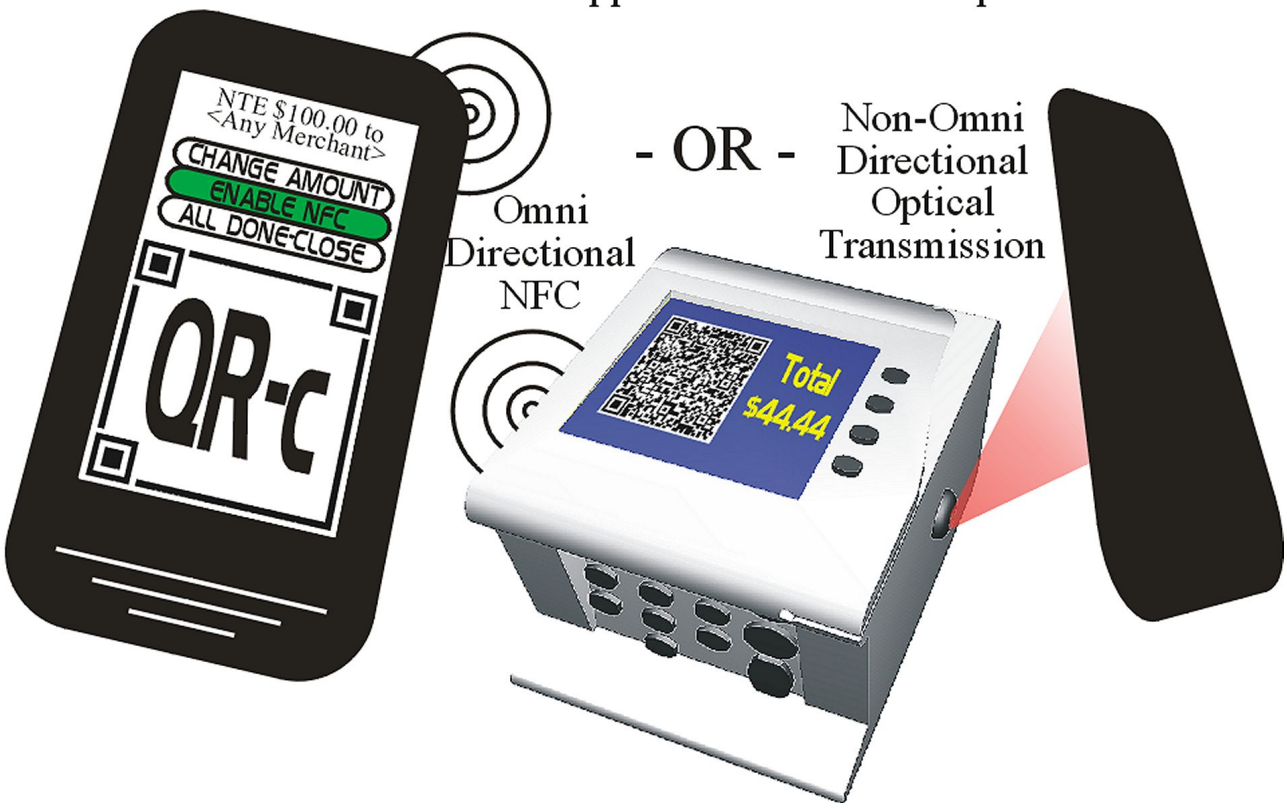
NC3 THE NO COMPROMISE CHARGE CARD

Transmitting Secure NC3 Approvals with Omni Directional Near Field Communications (NFC)

NFC is a transmission method known for ease of use. At its best it is literally tap-and-go. The security problem with NFC[1] is partly technology related including eavesdropping, jamming, counterfeit injection, and faux-middleman. Merchants are not generally prepared to receive or transmit NFC. The other part is the content of the transmission which generally includes the underlying charge card number (UCCN).

NC3's optical transmission and merchants generally have scanners to read the quick recognition codes[2] (QR), which avoids the technology problems. Using a NC3 QR-c code transmitted by NFC solves the transmission content concern as, even if the NFC transmission encryption is cracked, the UCCN can't be revealed because *it isn't there*.

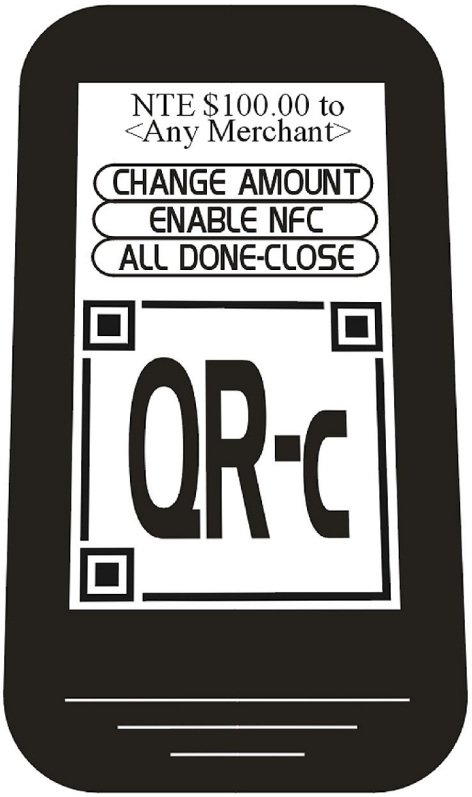
Two transaction approval transmission options



1 See more at www.nc3.mobi/references/#NFC

2 Quick Recognition Codes (QR Code) used with permission. See www.nc3.mobi/references/#QR

The easy way to use NC3 for a rapid transaction is to prepare a charge in advance[3] using the code for <Any Merchant> and a Not-To-Exceed (NTE) value. NTE can be set by the consumer is limited only by their account provider, and changeable on the fly.



If NTE were the same as the maximum charge allowed to that consumer then NC3 would be the same as an NFC enabled charge card with one exception. The charge card still transmits the underlying charge card number which can fall victim to one of the NFC technology problems.

NC3 never transmits the UCCN to the merchant for unparalleled security.

The following is more easily understood if you already have a basic understanding of how NC3 functions using optically based transmission without NFC.

NFC transmission *can* be used without these problems by using NFC to transmit the NC3 QR-c code. The advanced encryption with transaction adaptive elements within QR-c codes is not generic. It is transaction specific. Cracking one won't reveal the others.

The UCCN is secure because even if the one QR-c code is compromised *it can't reveal what isn't there*. Because NC3 uses *asymmetric* encryption the decryption key that reveals the information is *not* the same key to encrypt it and an encrypted QR-c is required for approval.

Q: Could a duplicate of an intercepted QR-c be used to make another purchase?
A: A duplicate of the intercepted QR-c is not usable.

Recall: A perfect duplicate NC3 QR-c is not of criminal use as it is restricted to a single merchant and exact amount. Could re-using the QR-c with <Any Merchant> and <NTE:$100.00> work? Date, time, sequence number and other elements are also used in detecting duplicates. All of these are *within* the encrypted approval so a crook would have to crack each intercepted QR-c individually, determine how the QR-c is constructed (that is encoded), make an appropriate alteration, encrypt each one *properly*, and inject it into the system to seek authorization.

3 See www.NC3.mobi/how-it-works/examples-main see several examples with "Order in Advance"