



# The NCrypt-it™ Solution

## Cryptographic Extension for BREW®

Qualcomm Government Technologies NCrypt-it Cryptographic Extension for BREW provides an easy to use library of cryptographic algorithms for developers looking to provide applications requiring advanced encryption. NCrypt-it is the only NIST certified cryptographic module available on the BREW platform.

NCrypt-it makes advanced encryption possible on commercial BREW enabled handsets. The extension enables applications to provide end-to-end security without requiring additional network elements for implementation. Whether your application is for a government customer, querying protected databases, handling sensitive financial data, or communicating corporate strategies, NCrypt-it can provide the privacy and sensitivity your information requires.

The NIST FIPS 140-2 validated NCrypt-it extension uses advanced encryption libraries from Certicom Corporation to support end-to-end encryption. NCrypt-it supports AES and Elliptic Curve algorithms commonly used by the U.S. Government. The implementation of the FIPS pre-validated extension can shorten the development process allowing developers quick and efficient access to markets requiring enhanced security.

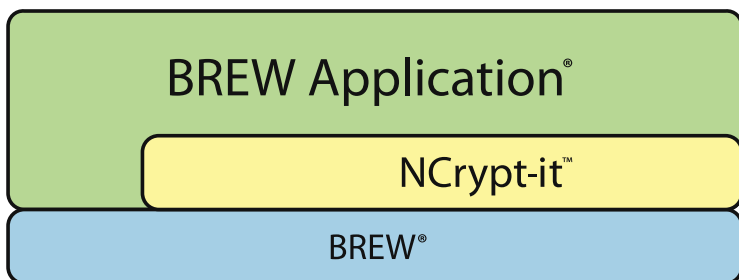


### Features:

- > NIST FIPS 140-2 level 1 validated
- > Advanced Encryption Standard (AES) encryption
- > Elliptic Curve Cryptography (ECC) for key agreement
- > Digital Signatures



When incorporating the NCrypt-it extension into BREW applications, developers will receive a NIST FIPS 140-2 validated solution and access to advanced encryption libraries.

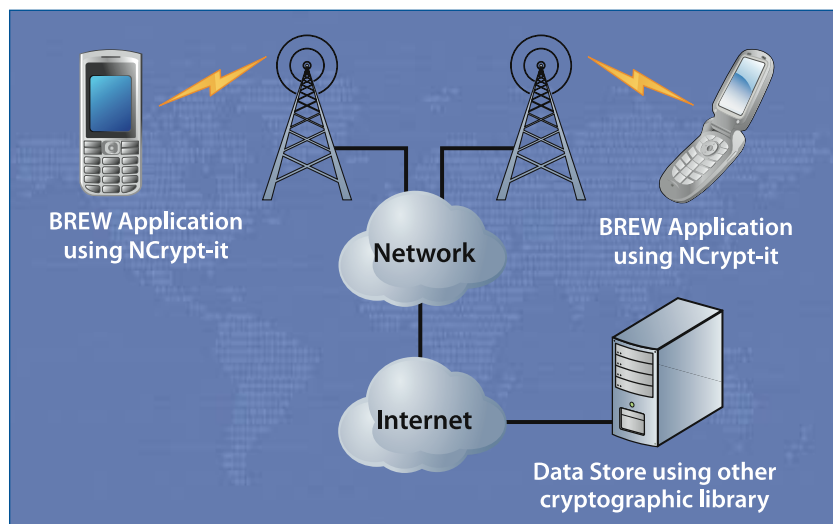


## NCrypt-it supports the following algorithms:

- > Elliptic Curve Diffie-Hellman (ECDH)
- > Elliptic Curve MQV (ECMQV)
- > Advanced Encryption Standard (AES)
- > Triple DES (3DES)
- > Diffie-Hellman
- > FIPS 186 compliant random number generator (RNG)
- > Digital Signature Algorithm (DSA)
- > Elliptic Curve Digital Signature Algorithm (ECDSA)
- > SHA family (SHA1 through SHA512)
- > HMAC
- > RSA

## Relative cryptographic strength of supported algorithms:

Cryptograph Strength	Symmetric Algorithm	HASH Algorithm	Elliptic Curve Asymmetric Algorithm	RSA/DSA/DH Asymmetric Algorithm
80 Bits	3DES (2 Key)	SHA-1	160 Bits	1024 Bits
112 Bits	3DES (3 Key)	SHA-224	224 Bits	2048 Bits
128 Bits	AES-128	SHA-256	256 Bits	3072 Bits
192 Bits	AES-192	SHA-384	384 Bits	7680 Bits
256 Bits	AES-256	SHA-512	512 Bits	15360 Bits



The NCrypt-it extension contains cryptographic libraries enabling applications to provide end-to-end security solutions between devices or back-end data stores. By using the NCrypt-it extension developers can avoid the lengthy NIST validation process and bring applications to market faster.

## FOR PRODUCT AVAILABILITY INFORMATION, PLEASE CONTACT:

Qualcomm Incorporated  
 GOVERNMENT TECHNOLOGIES  
 5775 Morehouse Drive  
 San Diego, CA 92121  
 TOLL Free: 877-461-4411  
 Email: [qgov@qualcomm.com](mailto:qgov@qualcomm.com)  
[www.qualcomm.com/qgov](http://www.qualcomm.com/qgov)