/PTT IRAD/FIPS-140

Cryptographic Module Security Policy for QinetiQ BRACER Handset

CMSP for QinetiQ BRACER Handset (Document Reference: QINETIQ/18/02811)

Version: 1.8
Printed by: taevans
Printed on: 09 July 2020

Contents

1 Document Information 1

2 Introduction 2

2.1 Purpose 2

2.2 References 2

2.3 Acronyms 2

2.4 Document Structure 2

3 QinetiQ BRACER™ Handset 4

3.1 Overview 4

3.2 Cryptographic Module Ports and Interfaces 5

3.3 Roles and Services and Authentication 6

3.3.1 Roles 6

3.3.2 Services 7

3.3.3 Authentication 8

3.4 Physical Security 8

3.5 Operational Environment 9

3.6 Cryptographic Key Management 9

3.6.1 Cryptographic Algorithms 10

3.6.2 Cryptographic Keys 10

3.7 Electromagnetic Interference / Electromagnetic Compatibility 13

3.8 Self-Test 13

3.9 Design Assurance 14

3.10 Migration of Other Attacks 14

4 Secure Operation 15

4.1 Maintainer 15

4.2 Crypto-Officer Guidance 15

4.2.1 Initialisation 15

4.2.2 Management 16

4.3 User Guidance 16

4.4 Security guidance and rules 17

CMSP for QinetiQ BRACER Handset (Document Reference: QINETIQ/18/02811)

1 Document Information

Document Title: QinetiQ BRACER Handset Cryptographic Module Security Policy

Document Publication Number: QINETIQ/18/02811

(Internal) Document Identifier: QINETIQ/EMEA/CIT/TN1801386

2 Introduction

2.1 Purpose

This is the Cryptographic Module Security Policy (CMSP) for the QinetiQ BRACER™ Handset. This document describes how:

- The QinetiQ BRACER™ Handset meets the National Institute of Standards and Technology (NIST) requirements for Cryptographic Modules as specified in Federal Information Processing Standards Publication (FIPS) 140-2.
- To run the module in its Approved FIPS 140-2 mode of operation.

This CMSP is for the QinetiQ BRACER™ handset with the following hardware and firmware:

- Hardware: Bracer™ Push-To-Talk Handset (BM1800449), version 1.0.
- Firmware: Bootloader & Main Bracer Application, firmware versions 1.3.0/DB17011

This policy was prepared as part of the Level 3 FIPS 140-2 validation of the module.

2.2 References

The following reference documents apply to this document:

[RD.1] QinetiQ BRACER™ User Guide

2.3 Acronyms

Table 02-01 Acronyms.

FIPS	Federal Information Processing Standard
NIST	National Institute of Standards and Technology
CSP	Critical Security Parameter
CMSP	Cryptographic Module Security Policy
SA	Situation Awareness

2.4 Document Structure

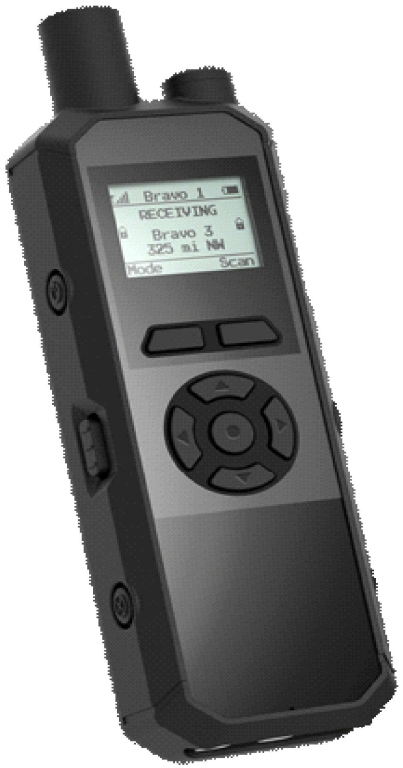
CMSP for QinetiQ BRACER Handset (Document Reference: QINETIQ/18/02811)
This Cryptographic Module Security Policy (CMSP) is one part of the FIPS140-2 validation evidence and documentation. The evidence and documentation is proprietary to QinetiQ and requests for access should be submitted to QinetiQ.
The QinetiQ BRACER™ Handset User guide [RD.1] contains further information about the cryptographic module and its use.
The rest of this document is structured as follows:
• Section 1 (this section), provides an introduction to the document and its purpose;
• Section 2, provides a summary of the product and the FIPS140-2 security policy elements that apply;
• Section 3, provides instructions on security operation of the product.

CMSP for QinetiQ BRACER Handset (Document Reference: QINETIQ/18/02811)

3 QinetiQ BRACER™ Handset

3.1 Overview

The QinetiQ BRACER™ Handset provides a means of using the Iridium services (e.g. Push To Talk (PTT)) with enhanced privacy for both the call content and the establishment of communities (e.g. PTT 'Talkgroups'), while providing an enhanced interface for military/government headsets, as well as providing an integrated asset tracking function compatible with 'Blue Force' asset tracking or Situational Awareness (SA) function.
The figure below shows the physical QinetiQ BRACER™ handset, which is the subject of this document.



CMSP for QinetiQ BRACER Handset (Document Reference: QINETIQ/18/02811)

The QinetiQ BRACER™ handset only operates in an FIPS140-2 Approved Mode of operation as such there is no direct indication of Approved or non-Approved modes (beyond the handset passing the self-test and users can log on). The handset supports a bypass mode which is accessed by the User; the mechanism to activate the bypass is described in the User Guide.

The cryptographic module boundary of the QinetiQ BRACER™ Handset is defined by the handset case, which surrounds all the hardware and software components.

The QinetiQ BRACER™ handset (with an appropriate user logged on) can collect (encrypted) situation awareness (location) data from other QinetiQ BRACER™ Handsets. The (appropriate) user can view the (decrypted) situation awareness data. The (appropriate) user can have the QinetiQ BRACER™ handset encrypt and export the situation awareness data over USB.

The intended product validation level against the different FIPS140-2 areas is shown below.

Table 03-01: Validation levels against FIPS140-2 areas.

Area	Section Title	Level
1	Cryptographic Module Specification	3
2	Cryptographic Module Ports and Interfaces	3
3	Roles, Services and Authentication	3
4	Finite State Model	3
5	Physical Security	3
6	Operational Environment	N/A
7	Cryptographic Key Management	3
8	Electromagnetic Interference/Electromagnetic Compatibility	3
9	Self-Tests	3
10	Design Assurance	3
11	Mitigation of Other Attacks	N/A

3.2 Cryptographic Module Ports and Interfaces

Interfaces on the module can be categorized into the following FIPS 140-2 logical interfaces:

- Data Input interface
- Data Output interface

- Control Input Interface
- Power Interface
- Status Output

The logical interfaces can be mapped into the following physical interfaces:

- External Iridium Antenna Port;
- Internal Antenna Port;
- SIM Card;
- USB Port. This provides data connectivity and power for charging the internal power cells (which are not user changeable);
- Headset;
- User interface. This comprises the display and key pad.
- LED Indicator

The FIPS140-2 logical interfaces that are supported by the various physical interfaces are shown in the following table.

Table 03-02: Logical interfaces on physical interfaces.

FIPS140-2 logical interface	Cryptographic Module Physical Interface
Data Input	Headset, USB, SIM, Internal and External Antenna
Data Output	Headset, USB, Internal and External Antenna
Control Input	User Interface
Status Output	User Interface, LED
Power	USB

3.3 Roles and Services and Authentication

3.3.1 Roles

CMSP for QinetiQ BRACER Handset (Document Reference: QINETIQ/18/02811)

The QinetiQ BRACER™ Handset supports the following identity based roles:

- User (standard and super user). In addition to the services offered to a Standard User a Super User can collect, view, acknowledge and export situation awareness data;
- Crypto Officer.

3.3.2 Services

The QinetiQ BRACER™ Handset provides the following services:

- Show Status via device information menu entry
- Perform Self-Tests
- Generate cryptographic key (SKEK only)
- Zeroise
- Configure Module (including user set-up, PIN)
- Load (BLACK) Transfer keys
- Load (BLACK) Mission keys
- Calls (talk group) (bypass mode)
- Privacy enhanced calls (talk group)
- Generate (encrypted) situation awareness data
- Manage situation awareness data

The following table shows the services available to each role.

Table 03-03: Service available to roles

Service	User Role	Crypto Officer Role
Show Status	Yes	Yes

Perform Self-Tests	Yes	Yes
Generate cryptographic key (SKEK only)	No	Yes
Configure Module	No	Yes
Load (BLACK) Transfer keys	No	Yes
Load (BLACK) Mission keys	Yes	No
Calls (talk group) (bypass mode)	Yes	No
Privacy enhanced calls (talk group)	Yes	No
Generate (encrypted) situation awareness data	Yes	Yes
Manage situation awareness data	Yes (Super User)	No

The module has the following unauthorised services:

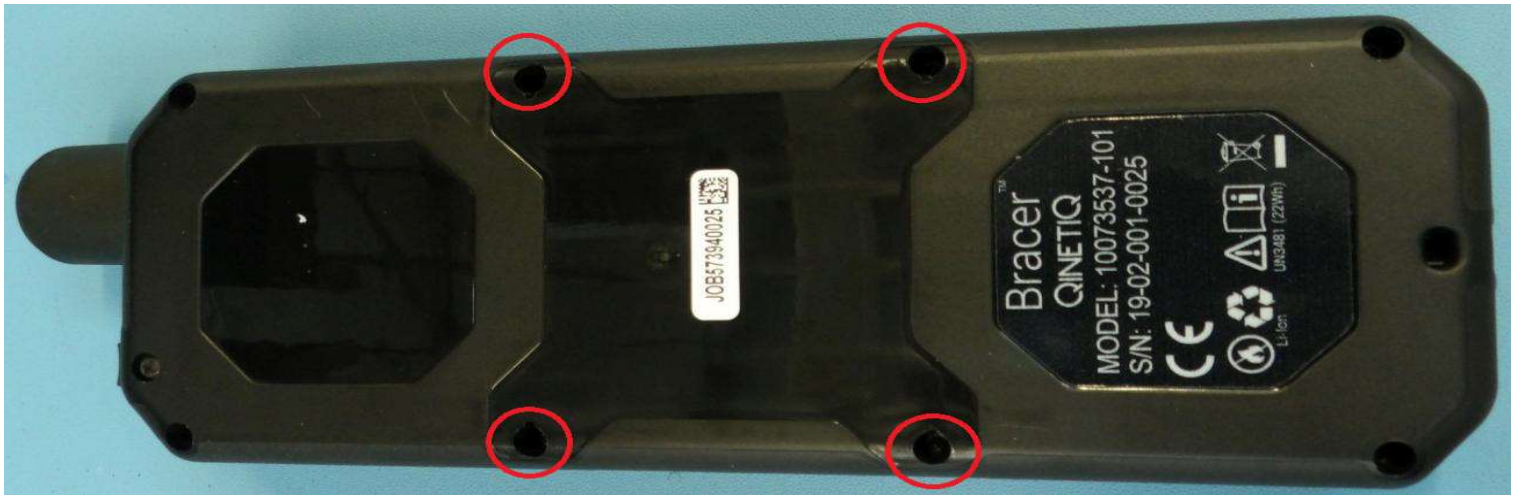
- Zeroise
- Self-tests (Power cycle)
- Show status
- Apply hardware token

3.3.3 Authentication

The cryptographic module provides user identity based authentication, and requires a user to authenticate before access to FIPS approved services.
The PIN comprises a 6 character sequence (the first character may be "X" or 0..9, the other characters may be 0..9). If 3 incorrect entries are inputted the user must wait for 30 seconds before they are allowed to try again. Note that the PIN entry method is via a rocker switch not a numeric key pad, which reduces the PIN entry speed.
A PIN is a 6-character permutation 11 possibilities (first digit) and 10 possibilities (digits 2 to 6). As it is possible to repeat a digit within a PIN there are 11*10^5 possible PINs and therefore the probability of randomly guessing the correct PIN is less than 1 in 10^6.
The probability of successfully authenticating (using random guesses) to the module within one minute (where no more than 6 attempts can be made) is 1 in 6/(11 * 10^5) which is less than 1 in 10^5.

If an authenticated user enters in the correct user ID and PIN the device will enter PTT mode.

3.4 Physical Security

CMSP for QinetiQ BRACER Handset (Document Reference: QINETIQ/18/02811)
The QinetiQ BRACER™ Handset is a multi-chip standalone cryptographic module. The cryptographic module is enclosed in an opaque case, which is designed to be tamper evident and incorporates tamper response mechanism that will zero the Critical Security Parameters (CSP).
The User and Crypto-Officer are to ensure there is no evidence of tampering by: • visual inspection of the QinetiQ BRACER™ Handset for signs of deformity (e.g. discolouring of front lens), damage (e.g. cut to buttons) or scratches (e.g. on case joints). • checking the tamper plugs on the rear of the QinetiQ BRACER™ Handset are intact. The figure below shows the position of the tamper plugs.

If tampering of a QinetiQ BRACER™ Handset is suspected the module should not be used for secure operation nor should any further cryptographic keys be loaded into the module. QinetiQ should be contacted to arrange return of the module to QinetiQ for inspection and any necessary repair.
3.5 **Operational Environment**
The module does not provide a general purpose operating system nor does it allow operators to load any software applications. The module provides a method to update the firmware using an external device (e.g. PC) to a new version. This is a complete replacement of the firmware not a patch or addition. This method involves loading a digitally signed firmware update to the module. If the signature test fails the new firmware will not boot, and will need to be replaced to allow successful boot. If the signature test passes the firmware will be updated and can be booted. Following update of the firmware all existing keys are purged and the Crypto Officer must reinitialise the module. NOTE: To maintain validation for the module, only FIPS-validated firmware may be loaded, and the module must be configured to execute in its defined FIPS mode of operation.
3.6 **Cryptographic Key Management**

3.6.1 Cryptographic Algorithms

The Cryptographic Module implements the FIPS140-2 approved algorithms shown below.

Table 03-04: FIPS140-2 Validated Cryptographic Algorithms.

Approved Function	**Certificate Number**
Symmetric Key Algorithm	
Advanced Encryption Standard (AES) 256 in CTR mode (encryption and decryption)	C377
Advanced Encryption Standard (AES) 256 in ECB mode (encryption and decryption)	C377
KTS-NIST SP800-38F (Key Wrap) AES-256 over 256 bits keys (no padding) (wrapping and unwrapping)	C379
Secure Hashing Algorithm (SHA)	
SHA-256	C378
Random Bit Generator	
Cryptographic Key generation (CKG) SP800-133 (section 1.7 direct symmetric key generation using unmodified DRBG output)	Vendor affirmed
Deterministic Random Bit Generator (DRBG), NIST SP800-90A CTR-DRBG using AES-256 and derivation function.	C408
Asymmetric Key Algorithm	
(Elliptic Curve) Digital Signature (verify) over P-256 using SHA-256	C407

The Cryptographic Module does not implement any cryptographic algorithms that are not FIPS 140-2 listed.

Non-approved but allowed algorithms:
- Raw entropy source for DRBG (NDRNG)

3.6.2 Cryptographic Keys

The cryptographic module has the following Critical Security Parameters (CSP). The only Critical Security Parameter that is exported from the Cryptographic Module is the Storage Key Encryption Key in a cryptographic "split" form.

CMSP for QinetiQ BRACER Handset (Document Reference: QINETIQ/18/02811)

Table 03-05: List of Critical Security Parameters (including cryptographic keys).

Key Name	**Used in Algorithm**	**Source**	**Storage**	**Deletion**	**Purpose**
Storage Key Encryption Key (SKEK)	AES-256 Key Wrap	Generated in cryptographic module	Held in plain text in RAM. Held in non-volatile RAM and on token as cryptographic splits	Secure deletion on power off, tamper event.	To protect other keys held in the cryptographic module.
SKEK Split 1 of 2 (SKEK_1)	Key split	Generated in cryptographic module	Held in non-volatile RAM	On tamper event or zeroise.	To protect other keys held in the cryptographic module.
SKEK Split 2 of 2 (SKEK_2)	Key split	Generated in cryptographic module	Held on token.	Not deleted.	To protect other keys held in the cryptographic module.
Key Encryption Key (Cable) (KEK_Cable)	AES-256 Key Wrap	Loaded into cryptographic module in encrypted form	Encrypted with SKEK and held in non-volatile RAM.	On tamper event or zeroise.	To protect transfer of keys over cables.
Key Encryption Key (Token) (KEK_Token)	AES-256 Key Wrap	Loaded into cryptographic module in encrypted form	Encrypted with SKEK and held in non-volatile RAM.	On tamper event or zeroise.	To protect transfer of keys over tokens.
Mission Keys (MK)	AES-256 in CTR mode	Loaded into cryptographic module in encrypted form	Encrypted with SKEK and held in non-volatile RAM.	On tamper event or zeroise.	Used to protect voice and situation awareness traffic within a talk group or secure call.
Mission Export Key (MEK)	AES-256 in CTR mode	Loaded into cryptographic module in encrypted form	Encrypted with SKEK and held in non-volatile RAM.	On tamper event or zeroise.	Used to protect situation awareness data that is exported.
Public firmware signature (QQ_Pub)	ECDSA verify	Loaded into cryptographic module	Embedded within bootloader.	Not deleted.	To ensure authenticity and integrity of firmware, during updates.
PIN	Authentication	Generated in cryptographic module	Held as salted Hash in non-volatile RAM	On tamper event or zeroise.	To authenticate users.
DRBG-EI	DRBG	Generated in cryptographic module	Held in RAM as generated.	Overwritten as generated. On tamper event, zeroise, power off.	To seed DRBG.
DRBG-State	DRBG	Generated in cryptographic module.	Held in RAM.	On tamper event, zeroise or power off.	To propagate entropy in DRBG.

CMSP for QinetiQ BRACER Handset (Document Reference: QINETIQ/18/02811)

The following table shows the CSP accessed by each service. In this table:

- G = Generate: The service generates the CSP.
- O = Output: The service outputs the CSP.
- E = Execute: The service uses the CSP in an algorithm.
- I = Input: The service inputs the CSP.
- Z = Zeroize: The service zeroizes the CSP by overwriting with alternating 1's and 0's multiple time; following user activation of zeroize, during a full power cycle or on a tamper alarm.

Table 03-06: CSP accessed by service.

Service	SKEK	SKEK_1	SKEK_2	KEK_Cable	KEK_Token	MK	MEK	QQ_Pub	PIN	DRGB-EI	DRBG-State
Show Status	-	-	-	-	-	-	-	-	-	-	-
Perform Self-Tests	-	-	-	-	-	-	-	-	-	-	E
Generate cryptographic key	G	G	G, O	-	-	-	-	-	I,O	G	E
Zeroise	Z	Z	-	Z	Z	Z	Z	-	Z	Z	Z
Configure Module	E	-	-	-	-	-	-	-	G	-	-
Load (BLACK) Transfer keys	E	-	-	I	I	-	-	-	-	-	-
Load (BLACK) Mission keys	E	-	-	E	E	I	I	-	-	-	-
Calls (talk group) (bypass mode)	E	-	-	-	-	-	-	-	-	-	-
Privacy enhanced calls (talk group)	E	-	-	-	-	E	-	-	-	-	-

Generate (encrypted) situation awareness data	E	-	-	-	-	-	E	-	-	-	-
Manage situation awareness data	E	-	-	-	-	-	E	-	-	-	-
Unauthorised Service Apply Hardware Token	-	-	I	-	-	-	-	-	-	-	-

3.7 Electromagnetic Interference / Electromagnetic Compatibility

The QinetiQ BRACER™ Handset is tested for conformance to the Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC) requirements specified by Federal Communications Commission CFR47, Parts 15.107 and Parts 15.109 to Class B.
Compliance with these regulations meets FIPS Level 3 requirements for EMI/EMC.

3.8 Self-Test

The cryptographic module performs the following self-test at power up:

- Firmware integrity check using error detection code (Fletcher 16-bit as in RFC 1145)
- AES-256 ECB, CTR mode - KAT
- AES-256 Key Wrap - KAT
- SHA (SHA-256) - KAT
- DRBG CTR (AES-256) - KAT
- On-board SP 800-90B entropy health tests
- EC-DSA (verify) - KAT

CMSP for QinetiQ BRACER Handset (Document Reference: QINETIQ/18/02811)
If one of the above tests fails then no functions can be performed.
The cryptographic module performs the following conditional self-tests:
• On-board SP 800-90B entropy health tests
• by-pass test
• firmware load validated using ECDSA
The module performs cryptographic algorithm checks when leaving by-pass mode.
Failure of self-test at powerup and conditional self-test is indicate by the LED lighting RED and a message on the screen. Success is the module continuing to boot, showing login screen and continuing to operate.
The cryptographic module will verify the integrity and authenticity of firmware updates (sec 4.1).
3.9 **Design Assurance**
The design assurance for the Cryptographic Module covers the development, manufacturing, delivery and ongoing QinetiQ maintenance of the Cryptographic Module. They are described in:
• QinetiQ BRACER™ Technical Delivery Plan
• QinetiQ BRACER™ Security Management Plan
3.10 **Migration of Other Attacks**
In a FIPS Mode of operation, the module does not claim to mitigate any additional attacks.

CMSP for QinetiQ BRACER Handset (Document Reference: QINETIQ/18/02811)

4 Secure Operation

4.1 Maintainer

An operator may place the module into a state where it can:

- receive authenticated firmware updates over the USB. If the update fails the operator will need to repeat until successful.

An operator may update the firmware in the Iridium Modem. The Iridium Modem firmware is loaded into the cryptographic module and passed to the Iridium Modem, with no security processing in the handset cryptographic module.

4.2 Crypto-Officer Guidance

The Crypto-Officer is responsible for the initialization and management of the cryptographic module. The Crypto-Officer will receive the module from QinetiQ via trusted delivery courier.
Upon receipt of the module the Crypto-Officer should check the package for any irregular tears or openings. Upon opening the package the Crypto-Officer should inspect the Cryptographic Module for tamper evidence (see section 3.4).
If the Crypto-Officer suspects tampering, they should immediately contact QinetiQ.

4.2.1 Initialisation

The Crypto Officer will initialise the Cryptographic Module before use, they will have to:

- Power on the crypto module. The crypto module will automatically:
- delete working key stores
- verify the integrity and authenticity of the firmware
- Insert a USB token, generate a key split of the SKEK and store the split key on the token
- the cryptographic module will generate a Storage Key Encryption Key
- be forced to change the default Crypto-Officer PIN
- Create necessary user accounts and PINs
- Load transfer key encryption keys (KEKs)

CMSP for QinetiQ BRACER Handset (Document Reference: QINETIQ/18/02811)
• Log-off as Crypto-officer
• Pass the device to the User or power off for storage/transport
A User will need to:
• log-on using their PIN
• load mission keys
• power off, ready for transport
4.2.2 **Management**
The Crypto Officer can perform the following management actions:
• log on with PIN
• generate a new PIN for themselves
• generate a new PIN for a user
• add user
• remove user
4.3 **User Guidance**
The User (Standard or Super) can perform the following management actions:
• logon using their identify and PIN
• log off
• load encrypted mission keys
• moving from encrypted to clear modes
• join privacy enhanced talk groups encrypted by the Cryptographic Module to other QinetiQ BRACER™ Handsets

CMSP for QinetiQ BRACER Handset (Document Reference: QINETIQ/18/02811)
• joining talk groups to other Iridium or QinetiQ BRACER™ Handsets
• wake from active standby
• place in active standby
• full power off
The Super Use can perform the following additional actions:
• Collect situation awareness (location) data from other modules (over the air);
• Encrypt and export the collected situation awareness data over the USB.
4.4 **Security guidance and rules**
There are no restrictions on the critical security parameters that are zeriosed.
The module clears previous authentication credentials on power cycle.
A User does not have access to any cryptographic services prior to assuming an authorised role.
The module allows the user to initiate power up self-test by power cycling the module.
Data output are inhibited during key generation, self-test, zeroisation and error states.
Status information does not contain CSPs or sensitive data, that if misused could lead to a compromise of the module.
The module does not support concurrent operators.
The module does not support a maintenance role.
The module does not output intermediate key values.
The module does not support manual key entry.