



BK

Release Notes

BroadKey v2.8

- Added features:
 - PKI elements: generation of certificate signing request (CSR), self-signed certificates (SSC)
 - ECC data in standard DER format: public key (r/w), private key (r/w) and signatures (r/w)
- Performance & size improvements:
 - Speed improvements
 - Stack reduction
- Added tests to improve code coverage

BroadKey v2.7 (Customer-specific release)

BroadKey v2.6

- Modular internal architecture
- New target/build configurations of BroadKey
- Performance numbers in separate document (Profiling) and removed from data sheet?
- Performance & size improvement:
 - Optimized memory usage for code and stack

BroadKey v2.5.1

- Minor improvements in data sheet
- Minor improvements in SW build



BroadKey v2.5

- **NOTICE** – this release contains breaking changes
 - Increase of AC length
 - Increase of PUF SRAM size
- Security:
 - Added fault attack countermeasure
 - Side-channel attack countermeasures added in uECC
- Bug fixes:
 - Fixed PUF health check return error code
 - Fixed inline macro for GNUC-based toolchains
 - Updated cryptogram section in data sheet
- Performance & size improvements:
 - Optimization of uECC
- Added tests to increase test coverage
- Minor documentation improvements

This product is subject to EU export restrictions according to Council Regulation (EC) No. 428/2009, dual-use control category 5D002.

This document contains information which is proprietary and confidential to Intrinsic ID B.V. and is intended for internal use only. The document is provided with the express understanding that the recipient will not divulge its content to other parties or otherwise misappropriate the information contained herein. Please destroy this document if you are not the intended recipient. Thank you.

Copyright in this document rests with Intrinsic ID B.V. Reproduction or publication in any medium of this document, in whole or in part, is expressly prohibited without the prior written permission of Intrinsic ID. Intrinsic ID reserves the right to make any changes to this document without prior notice. The contents of this document is provided AS-IS and without any warranties or guarantees as to accuracy or completeness. Receipt or possession of this document conveys no license under any patent or other intellectual property right of Intrinsic ID.

Intrinsic ID®, QuiddiKey®, QuiddiCard™, iRNG™, Apollo™, BK™, DemoKey™, Citadel™, Spartan™, Confidentialio™, Zign™, Fuzzy ID™ and other designated brands included herein are trademarks of Intrinsic ID B.V. All other trademarks are the property of their respective owners.

www.intrinsic-id.com