Impinj Application Note

Brand Protection with Monza® R6-P and S6-C

Rev 1.0 April 06, 2015

1 Background

This application note describes a brand protection solution for retail and consumables. While this solution can be deployed on other Monza products, it is well-suited to the retail-optimized Monza R6-P (MR6-P) and Monza S6-C (MS6-C).

The journey from manufacturer to retail floor is rarely direct and this provides opportunities for inferior products to enter the supply chain. RAIN RFID has become an integral feature in supply-chain logistics and the management of retail inventory. Time and again, the exceptional accuracy and visibility provided by RAIN RFID has been shown to provide a compelling *return on investment (ROI)*. In this application note, therefore, we describe a solution that uses these very same tags to simultaneously provide enhanced levels of brand protection.

2 Introducing the Brand Protection Code

The brand protection scheme described in this note is built around the concept of a *Brand Protection Code (BPC)*. This is computed by the brand owner, or their representative, which can be verified at future points in the supply chain including at the retailer.

The BPC is derived from the chip *tag identification (TID)* number, a unique number that is encoded and fixed by the chip manufacturer. The TID cannot be falsified or copied into a similar RAIN RFID chip. The BPC is computed using a cryptographic algorithm and, in one scenario, the brand owner generates and stores a secret key. This key is then used to compute what is referred to as a *message authentication code (MAC)*. There are many ways to compute a MAC and Impinj recommends using one of two mechanisms approved by the *National Institute of Standards and Technology (NIST)*; (a) a mechanism called HMAC that is described[1] in FIPS 198-1 or (b) a mechanism called CMAC that is described[2] in SP 800-38B. In both cases the MAC computation output should be truncated to the 32 leftmost bits.

[1] National Institute of Standards and Technology. FIPS 198-1: The Keyed-Hash Message Authentication Code (HMAC). July 2008. Available via csrc.nist.gov/publications/fips/fips198-1/FIPS-198-1_final.pdf.
[2] National Institute of Standards and Technology. SP 800-38B: Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication. May 2005. Available via csrc.nist.gov/publications/nistpubs/800-38B/SP_800-38B.pdf.

2.1 Using the Brand Protection Code

Different deployments can use different inputs to the BPC computation. However all deployments should include the TID at a minimum. In practice, the more information that is used as input to the BPC computation, the less versatile the solution may become. However, such additional information might include the *Electronic Product Code (EPC)* and administrational or business-event driven data. The important issue is that any information used in the generation of the BPC should be equally available to those that might verify the BPC. This process is illustrated in the figure below.

After the BPC is generated it should be written to user-memory. The BPC need not be locked/permalocked after writing, though it can be if preferred. While the contents of unlocked memory can be changed or deleted and this would cause MAC verification to fail, the cryptographic properties of a MAC are such that it is not practical to generate a false BPC for a given TID.

2.2 Supporting the Brand Protection Code

As mentioned previously, any information that is used in the generation of the BPC should be available to those that wish to verify the correctness of the BPC. Much of this information – *e.g.* the TID and the EPC – can be read directly from the tag. Other information can be exchanged within the business information systems that are typically used to manage the shipping and tracking of goods.

The requirement that brand owner and retailer have access to all inputs to the MAC computation also extends to the secret key. There are many different models for handling keys with the most suitable for a given deployment depending on many factors. Globally, however, vast amounts of secret key material are securely exchanged every day and solutions are both well-developed and readily available.

3 Conclusion

Monza R6-P and S6-C couple the outstanding sensitivity of Monza R6 with the advantages of a modest amount of User memory. Among such advantages is the ability to support a simple mechanism for retail brand protection. Interestingly, this mechanism can also be combined with a range of Loss Prevention solutions that are described in a companion application note.

Notices

Impinj gives no representation or warranty, express or implied, for accuracy or reliability of information in this document. Impinj reserves the right to change its products and services and this information at any time without notice.

EXCEPT AS PROVIDED IN IMPINJ'S TERMS AND CONDITIONS OF SALE (OR AS OTHERWISE AGREED IN A VALID WRITTEN INDIVIDUAL AGREEMENT WITH IMPINJ), IMPINJ ASSUMES NO LIABILITY WHATSOEVER AND IMPINJ DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATED TO SALE AND/OR USE OF IMPINJ PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT.

NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY PATENT, COPYRIGHT, MASK WORK RIGHT, OR OTHER INTELLECTUAL PROPERTY RIGHT IS GRANTED BY THIS DOCUMENT.

Impinj assumes no liability for applications assistance or customer product design. Customers should provide adequate design and operating safeguards to minimize risks.

Impinj products are not designed, warranted or authorized for use in any product or application where a malfunction may reasonably be expected to cause personal injury or death or property or environmental damage ("hazardous uses") or for use in automotive environments. Customers must indemnify Impinj against any damages arising out of the use of Impinj products in any hazardous or automotive uses.

Impinj, Monza, AutoTune, TagFocus, FastID, Enduro, Integra, ItemEncode, ItemSense, xArray, xPortal and Monza Self-Serialization are trademarks of Impinj, Inc. All other product or service names are trademarks of their respective companies.

These products may be covered by one or more U.S. patents. See www.impinj.com/patents for details.