



# **Report on Initial Evaluation of MIFARE Plus**

***Version 1.0***

***Version date: 2008-11-02***

Bart Preneel  
ABTCrypto & Katholieke Universiteit Leuven

[bart@abtcrypto.dk](mailto:bart@abtcrypto.dk)

## Context

NXP has requested ABTCrypto to evaluate the security of the MIFARE Plus architecture. This report summarizes the findings of the initial evaluation of the security architecture during a limited time period. The security of the implementation of the reader and chips are outside the scope of this evaluation.

## Conclusions

ABTCrypto has analyzed the extensive documentation on MIFARE Plus. The focus of our first evaluation has been *Security Level 3* and the mechanisms to upgrade to this level.

Based on our initial study, we believe that the MIFARE Plus architecture is a solid design, which is based on a detailed analysis of the requirements including security, privacy and feasibility. The solutions proposed take into account the severe constraints offered by the contactless environment. In spite of these constraints, the MIFARE plus architecture allows to deploy applications in areas such as access control and transportation that offer an adequate level of security and privacy. A number of residual risks exists that are carefully documented and analyzed and that are deemed to be acceptable.

It is of course up to the application designer to ensure that the MIFARE Plus architecture is used to develop a secure and privacy friendly application; moreover, the implementers need to ensure that the implementation is correct and secure (which includes an adequate protection against side channels). Finally, the service provider needs to take adequate security measures during deployment and operation. All these aspects are outside the scope of this study.