

Document ID AAGS-HOSP-SA-2026-01	Revision 1	Date 26 th Jan 2026	Document category Security Advisory	
Confidentiality level PUBLIC			Status Approved	Page (of) 1 (3)

Academic Research Publication Referencing MIFARE Ultralight AES

Hospitality

TLP:WHITE

Disclosure is not limited.

Overview

Vingcard is aware of an academic research publication titled "BREAKMEIFYOUCAN", published on January 20, 2026.

The publication describes a potential vulnerability against MIFARE Ultralight AES and MIFARE Ultralight C smart card products **when deployed without recommended security configurations**.

This advisory is intended to clarify the applicability of the research to Vingcard products.

Advisory Status

Investigation Done

While our product investigation is done, we will continue to monitor the threat environment and update this advisory if this situation changes. Our security teams are actively monitoring our environments and updated our defence-in-depth tools.

Document ID AAGS-HOSP-SA-2026-01	Revision 1	Date 26th Jan 2026	Document category Security Advisory
Confidentiality level PUBLIC	Status Approved		Page (of) 2 (3)

Vulnerability Description

According to information relevant to Vingcard implementation detailed in the NXP Semiconductors advisory, the described vulnerability scenario is only feasible when MIFARE Ultralight AES cards are:

- Configured with non-diversified keys shared across multiple cards
- Deployed without key protection and secure messaging enabled
- Not enforcing limits on failed authentication attempts

The vulnerability scenario further requires physical possession of multiple cards using the same unprotected key and access to a legitimate reader in a relay scenario.

Vingcard Security Controls

Vingcard deploys MIFARE Ultralight AES cards in line with NXP's security guidelines and best practices. Vingcard implementations include the following security measures:

- **Per-card key diversification**, ensuring each card uses a unique cryptographic key
- **CMAC-based secure messaging** enabled
- **Authentication attempt limiting** through use of the authentication counter

NXP has confirmed that the presence of any one of these mitigations is sufficient to prevent the described attack.

Customer Guidance

Vingcard AES customers are not affected by the vulnerability scenarios disclosed in the NXP advisory.

Customers operating Vingcard systems can continue to rely on the security of their deployed solutions. Vingcard remains committed to secure-by-design principles, responsible disclosure, and continuous security improvement.

If you have any doubts to if you are running your Vingcard platform in the recommended secure way please reach out to your sales representative.

Customers with specific questions are encouraged to contact NXP directly.

Document ID AAGS-HOSP-SA-2026-01	Revision 1	Date 26 th Jan 2026	Document category Security Advisory	
Confidentiality level PUBLIC			Status Approved	Page (of) 3 (3)

REVISION HISTORY

Revision	Date	Description
1	26 th Jan 2026	Initial Release

TERMS OF USE

THIS DOCUMENT IS PROVIDED "AS IS". IT DOES NOT IMPLY ANY KIND OF GUARANTEE, WARRANTY, OR UNDERTAKING, NOR DOES IT EXPAND THE SCOPE OF ANY GUARANTEE, WARRANTY OR UNDERTAKING MADE IN ANY AGREEMENT TO WHICH AN ASSA ABLOY GROUP COMPANY IS A PARTY, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. ANY USE OF THE INFORMATION CONTAINED HEREIN OR MATERIALS LINKED FROM THIS DOCUMENT IS AT YOUR OWN RISK. ASSA ABLOY GLOBAL SOLUTIONS RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME.

A STANDALONE COPY OR PARAPHRASE OF THE TEXT OF THIS DOCUMENT THAT OMITTS THE DISTRIBUTION URL IS AN UNCONTROLLED COPY. UNCONTROLLED COPIES MAY LACK IMPORTANT INFORMATION OR CONTAIN FACTUAL ERRORS. THE INFORMATION IN THIS DOCUMENT IS INTENDED SOLY FOR END USERS' LAWFUL USE OF ASSA ABLOY GLOBAL SOLUTIONS PRODUCTS.