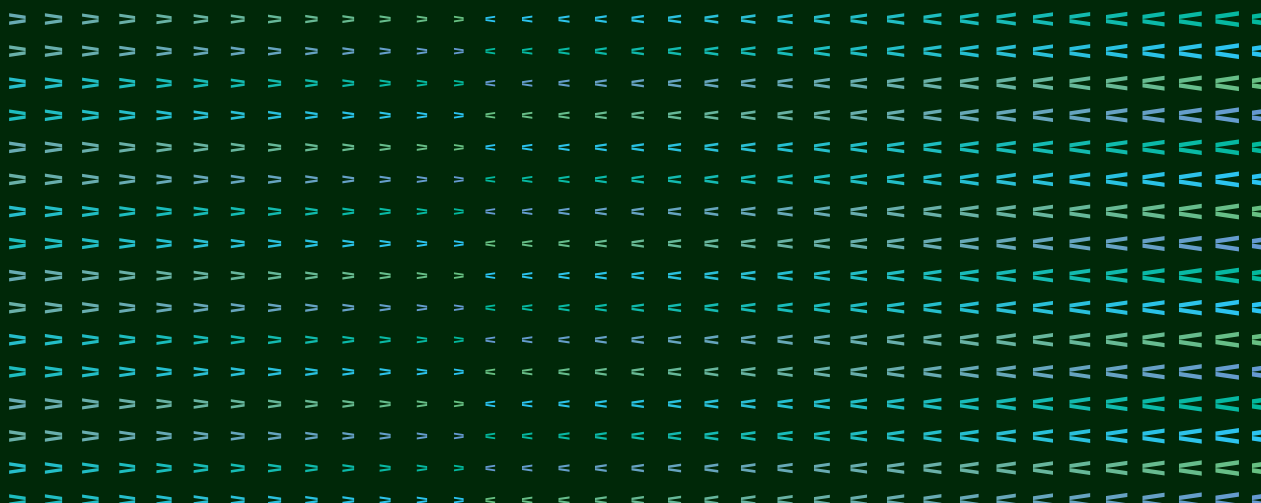
salto
INSPIRED ACCESS

Security Advisory

RFID Credentials Security Advisory

As part of our commitment to providing a secure smart access technologies for our users, we issue security advisories to keep you informed about potential vulnerabilities, security threats, and recommended actions.

saltosystems.com



Salto Systems S.L.

Document ID :	SAL_2024_001
Title	RFID Credentials Security Advisory
Date	2024/03/06
Rev	1.0

RFID Credentials Security Advisory

Salto Systems Advocates Transition to Enhanced Security Credentials

Salto Systems, a renowned pioneer in access control solutions, is proactively encouraging its clients and partners to transition from MIFARE Classic® credentials to more secure alternatives, specifically MIFARE DESFire®. This strategic recommendation is in response to recent security developments that underscore the vulnerabilities of MIFARE Classic® credentials. The transition is essential to uphold the highest security standards for access management systems and safeguard valuable assets.

Back in 2008, Salto Systems informed its clientele, following reports from security experts at Radboud University of Nijmegen and University College London, that they had successfully compromised the security of MIFARE Classic® credentials by retrieving the algorithm and devising attack methods to break their encryption keys.

Although SALTO's hardware is largely compatible with, or can be upgraded to, more secure credential technologies like MIFARE DESFire®, MIFARE Classic® credentials have remained popular among our customers.

Recent developments have introduced cloning devices that significantly lower the barrier to cloning non-secure credentials, including MIFARE Classic®, making the need for system security updates more pressing than ever.

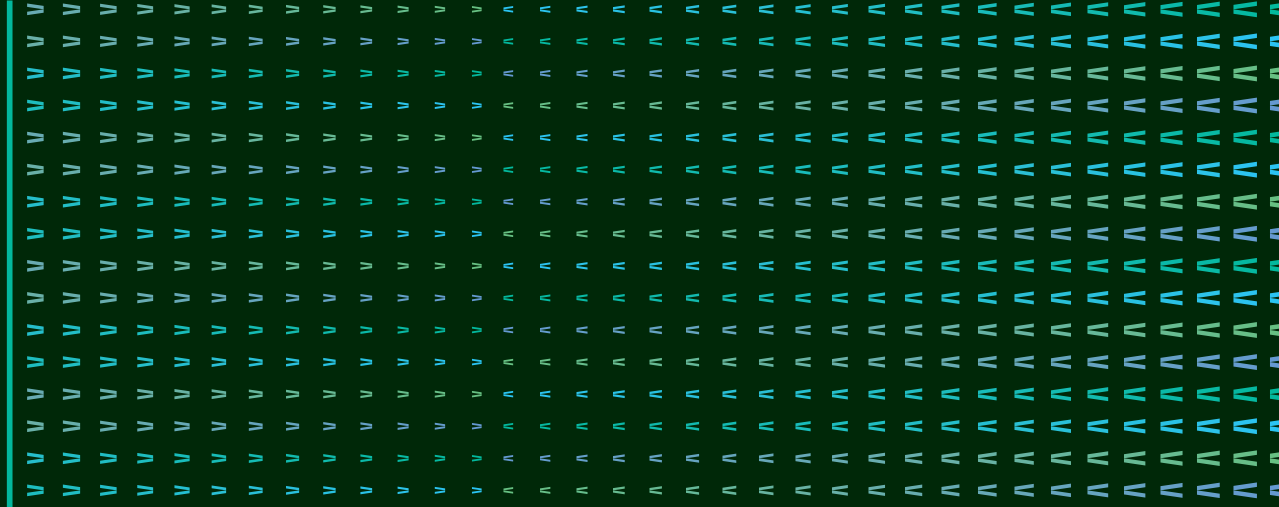
The documented vulnerabilities of MIFARE Classic® underscore the urgent necessity for security system updates. For existing installations, Salto Systems, in alignment with NXP's recommendations, suggests exploring alternatives like MIFARE DESFire® for new access management implementations requiring robust security. Salto Systems is prepared to assist in finding the ideal solutions.

During the transition period, we strongly recommend updating the firmware of your locks. As new cloning tools emerge, new attack vectors surface. While this update may not resolve all security issues for MIFARE Classic®, it will mitigate the emergence of other vulnerabilities. This firmware update will enable secure continued use in the case of MIFARE UltralightC® credentials.

Attacks targeting IC security are a natural part of the security product lifecycle, similar to computer viruses. While our partners, like NXP, continually enhance the security of existing product lines and develop new, highly secure offerings, Salto Systems continuously monitors and incorporates the latest and most secure credential solutions into our products.

Salto Systems remains committed to ensuring the safety and security of our clients' access management systems. Our recommendation to transition away from MIFARE Classic® to more secure credential systems, such as MIFARE DESFire®, underscores our dedication to protecting our client's assets and upholding the highest security standards in the ever-evolving field of access control.

For further information and support throughout this transition, don't hesitate to get in touch with Salto Systems and consult with our team of experts.



SALTO Systems, as one of the world's leading "smart access" brands, is seriously committed to protecting the privacy of all its customers and users, as well as the safety and security of our products and services. That's why security is embedded in everything we do.

—