Josef Ressel Center for User-friendly Secure Mobile Environments (u‘smile)

University of Applied Sciences Upper Austria
FH OÖ Forschungs & Entwicklungs GmbH

# NFC Tag with Cloning Protection

Contact:
Dr. Michael Roland

Softwarepark 11
4232 Hagenberg/Austria

+43 (0)50804-27149
michael.roland@fh-hagenberg.at
www.usmile.at • www.fh-ooe.at

## Motivation

NFC and RFID tags are often used to uniquely identify individual objects (e.g. by giving each object a unique serial number). These unique IDs (UIDs) that are typically burnt into NFC tags during manufacturing are regularly misused for the purpose of authentication (given the assumption no tag can change its UID). For instance, many access control systems rely on the UID to grant access to buildings. Similarly, the UID is often used to verify that a specific tag was scanned with a mobile device. However, this means that any such system can be tricked by creating a malicious tag that transmits the same serial number as an original tag [1]. Hence, the UID on its own is unusable for the purpose of authentication.

Several products exist that could (at least partially) fulfill authentication purposes. MIFARE Ultralight C and MIFARE DESFire allow mutual authentication based on a symmetric key (shared secret). This is suitable in scenarios where the shared secret can be sufficiently protected. However, if the authenticity of a tag should be verified by an app on a mobile device, the shared secret would need to be stored within the app to permit offline verification. Hence an attacker may be able to retrieve this shared secret by dissecting the app.

NXP’s new NTAG21x tags [5, 6] provide an ECC based signature over the tag serial number (UID). This supposedly provides a means to authenticate the tag. However, a closer look at the signature feature reveals, that a static signature (based on a private key only known to the tag manufacturer) is stored on the tag during manufacturing. Hence, the signature only prevents creation of arbitrary UIDs but not the duplication of UIDs with known signature. Consequently, tags where both the UID and the static signature are known can still be cloned.

HID Trusted Tag Services [7] are a means specifically designed for authenticating NFC tags. However, this system relies on an online backed that does the actual authenticity verification. Tags cannot simply be verified offline within an app.

Consequently, it seems as there is currently no solution available that provides authenticity verification for NFC tags that can be used in an offline fashion (i.e. without communication with a backend server).

## Objective

The goal of this master’s thesis is to implement an NFC Forum Type 4 tag on top of the Java Card platform (a ready-made implementation like [8] could be used as a starting point) that provides support for authenticity verification. Tag authentication should be implemented using challenge-response authentication (using dedicated commands beyond the Type 4 Tag Operation specification) and counter-based one-time authentication codes embedded in NDEF URI records (cf. [7]). Different authentication methods (i.e. symmetric/asymmetric, different algorithms, key strengths, etc.) should be implemented and compared. The thesis should evaluate the different implementations with regard to their strengths and weaknesses (in particular: (offline) validatability on mobile phones, execution times, and potential communication problems due to power-intensive operations).

## Literature

[1] stackoverflow: *Serials on NFC Tags - truly unique? cloneable?*, http://stackoverflow.com/q/21700718/2425802

[2] stackoverflow: *NFC Tag as authentication tool*, http://stackoverflow.com/q/22327274/2425802

[3] stackoverflow: *How to prevent NFC tag cloning?*, http://stackoverflow.com/q/22878634/2425802

[4] NXP: MF0ICU2 MIFARE Ultralight C – Contactless ticket IC, Product Data Sheet 137632, Rev. 3.2, Jun. 2014

[5] NXP: *NTAG210/212 NFC Forum Type 2 Tag compliant IC with 48/128 bytes user memory, Product Data Sheet 242330, Rev. 3.0*, Mar. 2013

[6] NXP: *NTAG21x Originality Signature Validation*, Application Note AN11350, Rev. 1.0, Mar. 2013

[7] HID: *HID Trusted Tag Services*, https://www.hidglobal.com/sites/hidglobal.com/files/resource_files/hid-trusted-tag-services-ds-en.pdf

[8] Y. Müller: *JavaCard applet for speaking NDEF*, https://github.com/slomo/ndef-javacard