AN12321

NTAG 424 DNA (TagTamper) features and hints - LRP mode

Rev. 1.0 — 15 January 2019 Application note

524410 COMPANY PUBLIC

Document information

Information	Content
Keywords	NTAG 424 DNA, NTAG 424 DNA TagTamper, Configuration, Personalization, LRP mode
Abstract	Guidelines for personalization, configuring and backend calculations of NTAG 424 DNA with focus on LRP mode

Revision history

Rev	Date	Description
v. 1.0	20190115	Initial version

1 Abbreviations

Table 1. Abbreviations

Acronym	Description
AES	Advanced Encryption Standard
AID	Application IDentifier
APDU	Application Protocol Data Unit
DF-Name	ISO7816 Dedicated File Name
C-APDU	Command APDU
CMAC	MAC according to NIST Special Publication 800-38B
CRC	Cyclic Redundancy Check
IC	Integrated Circuit
KDF	Key derivation function
LRP	Leakage resilient primitive
LSB	Lowest Significant Byte
LSb	Lowest Significant bit
MAC	Message Authentication Code
NDEF	NFC Data Exchange Format
NFC	Near Field Communication
NVM	Non-volatile memory
PCD	Proximity Coupling Device
PICC	Proximity Integrated Circuit Card
PRF	Pseudo Random Function
R-APDU	Response APDU (received from PICC)
SDM	Secure Dynamic Messaging
SSM	Standard Secure Messaging
SUN	Secure Unique NFC Messaging
UID	Unique IDentifier
URI	Uniform Resource Identifier
URL	Uniform Resource Locator

2 Introduction

LRP can be found:

2.1 About this document

This document addresses developers who are developing LRP algorithm for secure messaging on NTAG 424 DNA.

This application note is a supplementary document for implementations using the NTAG 424 DNA. This document shall be used in addition to:

- "NTAG 424 DNA - Data sheet" [1]
- "AN12304 Leakage Resilient Primitive (LRP) Specification" [2]
- "AN12196 NTAG 424 DNA and NTAG 424 DNA TagTamper features and hints" [3].

Note: This application note does not replace any of the relevant functional specifications, data sheets or design guides.

2.2 LRP facts

- LRP is a software protocol built on top of well-known cryptographic constructions (AES).
- LRP is a Pseudo-Random-Function (PRF). A PRF is an efficient, deterministic function that maps an input to an output.
- LRP operates on an input block size of 16 bytes, the same as for AES. LRP partially re-uses the structure of AES and also calls the AES encryption and decryption functions several times

2.3 Key benefits of using LRP

- LRP provides leakage resilience
- provides fault attack security
- provides side-channel attack security
- can be used as a drop-in replacement for AES

3 Definition of variables used in examples

The following symbols are used to abbreviate operations in the examples:

Symbol	Description
"="	Preparation of data by SAM, PICC or host
"<" or ">"	Direction of communication
||	The concatenation operation
$\oplus$	exclusive-OR operation
X << 1	The bit string that results from discarding the leftmost bit of the bit string X and appending a ‘0’ bit on the right
0^s	The bit string that consists of s ‘0’ bytes
E_{AES}(Kx, M)	AES-128 encipher in CBC mode, IV all 0x00, using key - K of number x, M is cipher input
D_{AES}(Kx, M)	AES-128 decipher in CBC mode, IV all 0x00, using key - K of number x, M is cipher input
E_{LRP}(Kx, M)	LRP encipher using key - K of number x, M is cipher input
D_{LRP}(Kx, M)	LRP decipher using key - K of number x, M is cipher input
MAC(K,M)	Message authentication code of message M using secret key K
MAC_t(K,M)	Truncated message authentication code of message M using secret key K. Truncated to 8 bytes, using S14 || S12 || S10 || S8 || S6 || S4 || S2 || S0. Even-numbered bytes shall be retained in MSB first order.
KDF: PRF(key, message) = CMAC(Kx, message)	A NIST recommended key derivation using pseudorandom functions. Pseudo random function: CMAC algorithm

3.1 Byte order

3.1.1 LSB representation

Represented least significant byte (LSB) first are:

- plain command parameters consisting of multiple bytes
- ISO/IEC 14443 parameters during the activation

3.1.2 MSB representation

Represented as most significant byte (MSB) first are:

- cryptographic parameters
- keys
- random numbers exchanged during authentication
- TI (Transaction Identifier)
- computed MACs

4 Example: Authentication using AuthenticateLRPFirst

In this example, an authentication using the Cmd.AuthenticateLRPFirst is executed, establishing successfully the LRP secure messaging. As mandatory action before being able to use Cmd.AuthenticateLRPFirst and so establishing the LRP secure messaging is setting the IC into LRP mode with the SetConfiguration command, as shown in Section 5.

The key number which is used for the authentication is key 0x03, an application key, with the key default value.

Key Number = 0x03

Key Value = 0x00000000000000000000000000000000

Table 2. Authentication using Cmd.AuthenticateLRPFirst

Step	Command		Data Message
1	KeyNo	=	03
2	KeyValue	=	00000000000000000000000000000000
	AuthenticateLRPFirst Part 1		
3	CLA	=	90
4	Ins	=	71
5	P1	=	00
6	P2	=	00
7	Lc (Length of the data)	=	08
8	Data	=	0006020000000000
9	Le (Length expected)	=	00
10	Cmd.AuthenticateLRPFirst C-APDU (Part 1)	>	9071000008000602000000000000
11	R-APDU (Part 1) = AuthMode || RndB || SW1 || SW2	<	0156109A31977C855319CD4618C9D2AED291AF
12	AuthMode	=	01
13	RndB	=	56109A31977C855319CD4618C9D2AED2
14	RndA generated by PCD	=	74D7DF6A2CEC0B72B412DE0D2B1117E6
15	RndA || RndB	=	74D7DF6A2CEC0B72B412DE0D2B1117E656109A31977C855319CD4618C9D2AED2
16	Session Vector (used for session key calculation) = fixed counter || fixed length || dynamic context || fixed label	=	0001008074D7897AB6DD9C0E855319CD4618C9D2AED2B412DE0D2B1117E69669
	AuthenticateLRPFirst Part 2		
17	Ins	=	AF
18	Data = RndA || PCDResponse	=	74D7DF6A2CEC0B72B412DE0D2B1117E689B59DCEDC31A3D3F38EF8D4810B3B4

Step	Command		Data Message
19	PCDResponse = MAC_LRP (KSesAuthMACKey; RNDA || RNDB)	=	89B59DCEDC31A3D3F38EF8D4810B3B4
19	Cmd.AuthenticateLRPFirst C-APDU (Part 2)	>	90AF00002074D7DF6A2CEC0B72B412DE0D2B1117E6189B59DCEDC31A3D3F38EF8D4810B3B400
20	R-APDU (Part 2) = PICCData || PICCResponse || SW1 || SW2	<	F4FC209D9D60623588B299FA5D6B2D710125F8547D9FB8D572C90D2C2A14E2359100
21	PICCData = Enc_LRP (KSesAuthEncKey; TI || PDCap2 || PCDCap2)	=	F4FC209D9D60623588B299FA5D6B2D71
22	PICCData decrypted = Dec_LRP (KSesAuthEncKey; PICCData) with IV = EncCounter	=	58EE9424020000000000020000000000
23	PICCResponse = MAC_LRP (KSesAuthMacKey; RndB || RndA || PICCData)	=	0125F8547D9FB8D572C90D2C2A14E235
24	Calculated PICCResponse == Received PICCResponse	=	Yes, correct.
25	TI	=	58EE9424
	PDcap2	=	020000000000
	PCDcap2	=	020000000000

After the authentication, the two session keys SesAuthENCKey and SesAuthMACKey can be generated. The detailed steps for generating the session keys are explained in [Datasheet]. The session keys always consist of one key and of the related 16 secret plaintexts. In this example, the session keys have the following values:

SesAuthENCKey = {SesAuthENCUpdateKey, 16 plaintexts} with
SesAuthENCUpdateKey = E9043D65AB21C0C422781099AB25EFDD

SesAuthMACKey = {SesAuthMACUpdateKey, 16 plaintexts} with
SesAuthMACUpdateKey = F56CADE598CC2A3FE47E438CFEB885DB

5 Example: Bringing the IC into LRP Secure Messaging Mode using SetConfiguration

In this example, the IC is brought into LRP mode by using the Cmd.SetConfiguration with Option 0x05.

This is an irreversible action and permanently disables AES secure messaging, meaning LRP secure messaging is required to be used for all future sessions. Detailed process is described in [].

Table 3. Bringing the IC to LRP Mode by using Cmd.SetConfiguration

Step	Command		Data Message
1	SetConfiguration Option	=	05
2	Session Encryption Key (SesAuthEncKey)	=	66A8CB93269DC9BC2885B7A91B9C697B
3	Session MAC Key (SesAuthMACKey)	=	7DE5F7E244A46D22E536804D07E8D70E
4	**Encrypting the Command Data**		
5	IV_Input (IV_Label || TI || Cmd Counter || Padding)	=	A55AED56F6E600000000000000000000
6	IV_Label	=	A55A
7	TI	=	ED56F6E6
8	Cmd Counter	=	0000
9	E($K_{SesAuthEnc}$, Basis for the IV))	=	DA0F644A4986275957CF1EC3AF4CCE53
10	IV	=	DA0F644A4986275957CF1EC3AF4CCE53
11	PDCap2.1	=	02
12	Data for Cmd.SetConfiguration	=	00000000020000000000
13	Padded Data	=	00000000020000000000800000000000
14	Encrypted Data = E($K_{SesAuthEnc}$, Padded Data)	=	41B2BA963075730426D0858D2AA6C498
15	**Generating the MAC for the Command APDU**		
16	IV for MACing	=	00000000000000000000000000000000
17	MAC_Input (Ins || Cmd Counter || TI || Cmd Header || Encrypted Data)	=	5C0000ED56F6E60541B2BA963075730426D0858D2AA6C498
18	MAC = CMAC(KSesAuthMAC, MAC_Input)	=	2F579E77FAB49F83
19	**Constructing the full Command APDU**		
20	CLA	=	90
21	Ins	=	5C
22	P1	=	00
23	P2	=	00

Step	Command		Data Message
24	Lc (Length of the data)	=	19
25	Data (Cmd Header || Encrypted Data || MAC)	=	0541B2BA963075730426D0858D2AA6C4982F579E77FAB49F83
26	Le (Length expected)	=	00
27	Cmd.SetConfiguration C-APDU (Cmd || Ins || P1 || P2 || Lc || Data || Le)	>	905C000019050041B2BA963075730426D0858D2AA6C4982F579E77FAB49F8300
28	Cmd Counter	=	0100
29	Cmd.SetConfiguration R-APDU	<	9100 (00 = SUCCESS)

6 Supporting tools

6.1 Software

Name	Description	Source
RFIDDiscover 4.5.1.8	PC software tool to evaluate NTAG 424 DNA PICC	NXP DocStore
NXPRdLib	C# API for developing Windows-based applications	NXP DocStore
TapLinX	Java-based SDK for developing Android applications, supporting all NXP RFID products, also NTAG 424 DNA	https://www.mifare.net/
TagInfo	Android and iOS based application to get detailed info of tapped NXP RFID products	Google PlayStore, Apple AppStore
TagWriter	Android application to configure, write NDEF data to NXP RFID products	Google PlayStore
TagXplorer	Desktop cross-platform Java application, PC/SC readers supported	https://www.nxp.com/
Java Lib - LRP	Java-based LRP calculation tool	Part of AN12304
Python Lib	Library written in Python	Upon request at sales representative

7 References

[1] **Data sheet** — NTAG 424 Product data sheet, doc.no. 4654**[1]

[2] **Application note** — AN12304 Leakage Resilient Primitive (LRP) Specification

[3] **Application note** — AN12196 NTAG 424 DNA and NTAG 424 DNA TagTamper features and hints, doc.no. 5072**

[4] **Application note** — AN11350 NTAG Originality Signature Validation, doc.no. 2604**

[1] ** … document version number

8 Legal information

8.1 Definitions

Draft — The document is a draft version only. The content is still under internal review and subject to formal approval, which may result in modifications or additions. NXP Semiconductors does not give any representations or warranties as to the accuracy or completeness of information included herein and shall have no liability for the consequences of use of such information.

8.2 Disclaimers

Limited warranty and liability — Information in this document is believed to be accurate and reliable. However, NXP Semiconductors does not give any representations or warranties, expressed or implied, as to the accuracy or completeness of such information and shall have no liability for the consequences of use of such information. NXP Semiconductors takes no responsibility for the content in this document if provided by an information source outside of NXP Semiconductors. In no event shall NXP Semiconductors be liable for any indirect, incidental, punitive, special or consequential damages (including - without limitation - lost profits, lost savings, business interruption, costs related to the removal or replacement of any products or rework charges) whether or not such damages are based on tort (including negligence), warranty, breach of contract or any other legal theory. Notwithstanding any damages that customer might incur for any reason whatsoever, NXP Semiconductors' aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the Terms and conditions of commercial sale of NXP Semiconductors.

Right to make changes — NXP Semiconductors reserves the right to make changes to information published in this document, including without limitation specifications and product descriptions, at any time and without notice. This document supersedes and replaces all information supplied prior to the publication hereof.

Suitability for use — NXP Semiconductors products are not designed, authorized or warranted to be suitable for use in life support, life-critical or safety-critical systems or equipment, nor in applications where failure or malfunction of an NXP Semiconductors product can reasonably be expected to result in personal injury, death or severe property or environmental damage. NXP Semiconductors and its suppliers accept no liability for inclusion and/or use of NXP Semiconductors products in such equipment or applications and therefore such inclusion and/or use is at the customer's own risk.

Applications — Applications that are described herein for any of these products are for illustrative purposes only. NXP Semiconductors makes no representation or warranty that such applications will be suitable for the specified use without further testing or modification. Customers are responsible for the design and operation of their applications and products using NXP Semiconductors products, and NXP Semiconductors accepts no liability for any assistance with applications or customer product design. It is customer's sole responsibility to determine whether the NXP Semiconductors product is suitable and fit for the customer's applications and products planned, as well as for the planned application and use of customer's third party customer(s). Customers should provide appropriate design and operating safeguards to minimize the risks associated with their applications and products. NXP Semiconductors does not accept any liability related to any default, damage, costs or problem which is based on any weakness or default in the customer's applications or products, or the application or use by customer's third party customer(s). Customer is responsible for doing all necessary testing for the customer's applications and products using NXP Semiconductors products in order to avoid a default of the applications and the products or of the application or use by customer's third party customer(s). NXP does not accept any liability in this respect.

Export control — This document as well as the item(s) described herein may be subject to export control regulations. Export might require a prior authorization from competent authorities.

Evaluation products — This product is provided on an "as is" and "with all faults" basis for evaluation purposes only. NXP Semiconductors, its affiliates and their suppliers expressly disclaim all warranties, whether express, implied or statutory, including but not limited to the implied warranties of non-infringement, merchantability and fitness for a particular purpose. The entire risk as to the quality, or arising out of the use or performance, of this product remains with customer. In no event shall NXP Semiconductors, its affiliates or their suppliers be liable to customer for any special, indirect, consequential, punitive or incidental damages (including without limitation damages for loss of business, business interruption, loss of use, loss of data or information, and the like) arising out the use of or inability to use the product, whether or not based on tort (including negligence), strict liability, breach of contract, breach of warranty or any other theory, even if advised of the possibility of such damages. Notwithstanding any damages that customer might incur for any reason whatsoever (including without limitation, all damages referenced above and all direct or general damages), the entire liability of NXP Semiconductors, its affiliates and their suppliers and customer's exclusive remedy for all of the foregoing shall be limited to actual damages incurred by customer based on reasonable reliance up to the greater of the amount actually paid by customer for the product or five dollars (US$5.00). The foregoing limitations, exclusions and disclaimers shall apply to the maximum extent permitted by applicable law, even if any remedy fails of its essential purpose.

Translations — A non-English (translated) version of a document is for reference only. The English version shall prevail in case of any discrepancy between the translated and English versions.

8.3 Licenses

Purchase of NXP ICs with NFC technology

Purchase of an NXP Semiconductors IC that complies with one of the Near Field Communication (NFC) standards ISO/IEC 18092 and ISO/IEC 21481 does not convey an implied license under any patent right infringed by implementation of any of those standards. Purchase of NXP Semiconductors IC does not include a license to any NXP patent (or other IP right) covering combinations of those products with other products, whether hardware or software.

8.4 Trademarks

Notice: All referenced brands, product names, service names and trademarks are the property of their respective owners.

NTAG — is a trademark of NXP B.V.

Tables

Contents

Please be aware that important notices concerning this document and the product(s) described herein, have been included in section 'Legal information'.

For more information, please visit: http://www.nxp.com
For sales office addresses, please send an email to: salesaddresses@nxp.com

Date of release: 15 January 2019
Document identifier: AN12321
Document number: 524410