

Loading an applet on SMAOT100NFC card using SIMAlliance Loader v2

This is a step-by-step guide on how to use SIMAlliance Loader v2, a free tool from SIMAlliance, to load and install an applet on one of our USIM cards.

We will use the OTASession to this and for that we'll need to configure the 03.48 settings (KiC,KiD, SPI, algorithm etc).

So, the things we need for this guide / lesson are:

- 1. APC and a standard smart card reader (link)
- 2. SIM card: SMAOT100NFC
- 3. the app (*.cap) we want to put on the card
- 4. SIMAlliance Loader v2 (link)

Start	



Start the program (with Administrator rights or you may have communication error with the smart card reader)

Insert the SIM card in the smart card reader



Explore with Explorer

SIMAlliance Loader v2	-	
File Help		
	1	
🔊 Explorer		
Tools Help		
Gemalto Prox-DU Contact_10800		
Smart C	Property	Value
	Tool Version	1.2.0
3		

- 1. Click on Explorer button
- 2. Select your smart card reader (*contact mode* if you have a dual interface reader)
- 3. Click on "Scan" button

You should get an error: "POR error: Insufficient security level"

This is because we have not yet made the necessary configurations...

4. Click on "OTA configuration" button



OTA configuration

S OTA Configurations Settings							
OTA Configuration	Property Notes	Value					
⊞ 🧐 SMS	Active security Active transport	03.48 SMS					
		1301800203.4000000					

Select SMS as the transport mechanism

OTA configuration - 03.48		
S OTA Configurations Settings		
CTA Configuration	Property	Value
i i i i i i i i i i i i i i i i i i i	SPI1-SPI2-KID-KIC	00210000
Integrity	Counter management	No counter available
	Counter value	000000000
Confidentiality	Counter step (decimal)	1
Command Packet	TAR	000000
	Mode	Compact
	-	

We will now set some parameters starting with some general 03.48 settings.

From your supplier you should have received some documentation on your card regarding codes, keys and other settings. Here you'll need the TAR value.



OTA Integrity setting (KiD)

S OTA Configurations Settings		
OTA Configuration	Property	Value
	Integrity	Cryptographic checksum
	KID algorithm group	DES
Confidentiality	KID algorithm	Triple DES in outer-CBC mode - 2 keys
	KID key index	01
Command Packet	Active KID key	F

Enter or select the values according to the screenshot above.

For the SMAOT100NFC card the KiD = 15. In binary value, transformed from Hex, it's 00010101. And this shows us the properties to be set for Integrity.

0001 : key index 01 : Triple DES in outer -CBC mode using 2 keys 01 : DES

See next figure

The coding for KiC and KiD is shown below:

B8	b7	b6	b5	b4	b3	b2	b1	
								<pre>00: Algorithm known implicitly by both entiti 01: DES 10: Reserved 11: Proprietary implementations 00: DES in CBC mode 01: Triple DES in outer-CBC mode using two different keys 10: Triple DES in outer-CBC mode using three different keys 11: DES in ECB mode for KIC 11 : Reserved for KID</pre>
								(keys implicitly agreed between both entities



OTA confidentiality setting (KiC)

Source of the setting of the set of	the second s	
CTA Configuration	Property	Value
	Ciphering	Ciphering
Integrity	KIC algorithm group	DES
() Integrity	KIC algorithm	Triple DES in outer-CBC mode - 2 keys
📑 Confidentiality	KIC key index	01
	Active KIC key	7A
OTA Command Packet		
A Configuration	Property	Value
03.48	Command Packet integrity	Cryptographic checksum
Integrity	Command Packet ciphering	Cyphering
Confidentiality		
😻 Command Packet		
OTA Broof of reasint		
OTA Proof of receipt		
Configuration	Property	Value
03.48	Proof of receipt setting	Required to be sent
Integrity	Proof of receipt integrity	Cryptographic checksum
Confidentiality	Proof of receipt ciphering	Cyphering
Contractionality		
Command Packet		
裬 Proof of receipt		

After this step, click "OK" and work with Explorer tool again, and we will try to scan the card again.

Scan with Explorer



Click the "Scan" button, and ...



Card content



So, you should have no errors, and you should have one package under the Card Manager.



Loader



Now it's time to start playing with the "loader" tool. Click on the "loader" button and a new window appears.

Add OTA session



We are going to use OTA to install an app on the card. So right-click on the chip icon and select "Add node / Add OTAsession".



OTA Session & Add applet

🛃 Loader - Untitled0.scl		
File Edit Tools Help		
Gemalto Pro	x-DU Contact_10800 👻	
🧇 0 Root 🖉 🦉	Property	Value
	Notes	
	Secured data length (decimal)	90
Add node 🕨 🗰 Add Package	Send Terminal Profile	
Collapse node 🛛 🛛 Add Applet	Group APDUs	
Expand node 🛛 🕄 Add Applet STK	Jse Default OTA Config	
☆ Move first ▲ Add Applet UTK ☆ Move up ▲ Add APDU ↓ Move down ▲ Add Script ↓ Move last ▲ Add SCP Session	.ocal Config	1
🗙 Delete	Set As Default Get Default Local Config	
لــــــــــــــــــــــــــــــــــــ]	
Design Vi 📄 Copy		
Paste		

- 1. Check the "Send Terminal Profile" checkbox
- 2. Right-click "OTASession" icon and select "Add node / Add Package"



Select the application and add applet

🛎 Loader - Untitl	ed0.scl		
File Edit Tools	Help		
	l 🗸 🕑 🌜	Gemalto Prox-DU Contact_10800 👻	
♦ 0 Root I RST ■ ● 2 OTASes	sion	7. Property Valu Notes File Name AID	le
🗄 · 🖤 3 F	Add node 🔹 🕨	Add Applet	
	Collapse node	Applet STK ity Domain AID	
	Expand node	Acd Applet UTK optional component	
1	Move first	Toolchain	
	Move up		
	Move down	2	
•	Move last	File Name Toolchain	
 >	Celete		

- 1. Click on "File Name" and select your app
- 2. Right-click on the package icon and select "Add node / Add Applet"

e Edit Tools Help					
	Gema	Ito Prox-DU Contact_10800	•		
> 0 Root		Property		Value	Τ
	ATT.	Notes			٦.
		Name			1
2 UTASESSION		Status		Selectable	1
🖃 😈 3 nfc.cap		Package AID		A000000DD0000DD00000DD0000	1
4 A000000		DD AID		A0000000DD0000DD00000DDD00	1
		Instance AID		A0000000DD0000DD00000DDD00	1
AN 57.		Application privilege		00	
		Non volatile memory f	or installation	0000	1
		Volatile memory for in	stallation	0000	1
		Applet specific parame	eter		1
		Token			1
		Contactless Services			ľ
		Contactless Protocol F	Parameters		1
	N 157	User Interaction Para	meters		١.
		/ · · ·			-
		Contection Services			
		Contactiess Dervices			

You should now have a screen looking like this.

As we in this guide have chosen an NFC app, we also have to make some Contactless



Services configurations... so that's the next step.

Click on "Contactless Services" button and a new window will pop-up.

Add contactless pro	dd contactless protocol profiles					
Contactless Configurations Setting Contactless Configurations Setting Configurations Set	ings fo	or applet: 4 A000	00000	DD0000DD000000DDD00DD00		
Contactless Services			Pro	perty		Value
Contactless Protocol Paramet			Conta	actless Protocol Parameters		
User Interaction Parameters Reader Mode Parameters	User Interaction Parameters Reader Mode Parameters Reader Mode Parameters Add node Expand n Move firs Move up Move dor Move last X Delete X Cut Copy Paste	er Interaction Parameters ader Mode Parameters Add node Collapse node Expand node Move first Move oup Move down Collapse node Add Contactless protocol profiles Add Protocol parameters for type A Add Protocol parameters for type B tial Contactless Activation State cognition Algorithm porithm Identifier 		None None		
al		 Move last Delete Cut 	nti	nuous Processing Selected nuous Processing		None
			mm	nunication Interface Access Parameters nunication Interface Access		
		Copy ntactless Protocol Parameters Profile Structure Paste tocol parameters for type A				
	2	Import				

Right-click on "Contactless Protocol Parameters" and select "Add node / Add Contactless protocol profiles"

fill in properties	

Contactless Services	Property	Value
Contactless Protocol Parameters	Contactless Protocol Parameters Profile Type	Type A
Contactless protocol profil User Interaction Parameters	Contactless Protocol Profile Identifier	Reserved for proprietary usage - 90
	Contactless Protocol Profile Identifier Name	1234

Fill in / Select the values as above



Select Type A

Contactless Services	Property	Value
Contactless Protocol Parameters	Contactless Protocol Parameters	800181A206A00490021234
Contactless protocol profiles	Protocols for Implicit Selection	800181
contactiess protocor promes	Type A	
User Interaction Parameters	Type B	
Reader Mode Parameters	Type F	
	Initial Contactless Activation State	None
	Recognition Algorithm	
	Algorithm Identifier	None
	Algorithm Parameter	
	Continuous Processing Selected	
	Continuous Processing	None
	Communication Interface Access Parameters	
	Communication Interface Access	
	Contactless Protocol Parameters Profile Structure	A206A00490021234
	Protocol parameters for type A	
	Protocol parameters for type B	

Check the box "Type A"

Done!

Installing applet on card

🛎 Loader - SMAOT100NF	FC.scl		
File Edit Tools Help			
	Gemalto Pr	ox-DU Contact_10800 👻	
🧇 0 Root	T	Property	Value
	A77.	Notes	A
E CTASession		Name	
1 2 afa ana		Status	Selectable
3 ntc.cap		Package AID	A000000DD0000DD00000DD0000
🖪 4 A000000	0DD0000DD00000DDDD00DD	AID	A000000DD0000DD00000DDD00
		Instance AID	A000000DD0000DD00000DDD00
×77.	Application privilege	00	
	Non volatile memory for installation	0000	
		Volatile memory for installation	0000
		Contactless Services	
Design View			
85F448CA623844' Status: '9000' # # # TERMINAL RESPONSE APDU 80140000 lc:: Besponse:	2 - DC cmdData: 810301130082	2028281830100 expStatus: ????	
Status: '9000'			

Now everything is prepared in order to install the nfc application on the card.

Just click on the "RUN" icon and APDU commands will be sent to the card, and you can see



them in the terminal window.

You should only have blue and black text. Red text indicates some kind of error.

Exploring the card again		
🛃 Explorer		
Tools Help		
Gemalto Prox-DU Contact_10800.		
😵 Smart Card	Property	Value
🖶 🖶 🦓 Card Manager 🛛 👘	Name	
Package A000001515350	AID	A000000DD0000DD00000DDD00DD00
	Life Cycle State	Selectable
	Application Privilege	00
Applet A000000DD0000DD00000DDD00	DD	
<	4	
Design View		

Using "Explorer" tool again and scanning the card, shows us the package and the applet now on the card!