STid
Electronic Identification

STid Mobile ID®
Bluetooth® Smart
Secure and intuitive access control through mobile devices

Bluetooth® mobile solutions

APPLICATION NOTE / FAQ

Table of Contents

I. Introduction

This document describes the approach to be used when developing a personal identification project using the STid Mobile ID® Bluetooth® access solution, to ensure optimal outcomes in the required configuration and installation conditions.

II. Bluetooth® Smart technology – General principles

Bluetooth® is a communication standard that uses radio waves in a frequency band between 2.4 and 2.5 GHz.

STid Mobile ID® uses this technology to authenticate users via an app installed on their smartphone.

Reading distances are a key factor for access control applications. With Bluetooth® technology, advertised ranges are for information purposes only. They define a detection zone. Distances depend on the smartphone and its position relative to the reader. For example, a phone in a pocket will not be detected at the same distance as a handheld phone.

III. Frequently Asked Questions

A. STid Mobile ID® app

1. What is the STid Mobile ID® app?

The STid Mobile ID® app is a virtual wallet for storing access cards. It can receive and store an unlimited number of cards. Each virtual card has a secure identification identifier which is either predefined or programmed by the client/user.

2. What mobile platforms is STid Mobile ID® compatible with?

STid Mobile ID® can be downloaded on Google Play (Android) or the App Store (iOS). 95% of smartphones on the market use one of these 2 operating systems

STid Mobile ID® is compatible with Bluetooth® Smart smartphones running Android 5.0 and iOS 9.0 and later.

3. How much does STid Mobile ID® cost?

The STid Mobile ID® app is free of charge. A free virtual CSN card – STid Mobile ID® – is stored in the app with a unique reference number allocated at installation.

B. Interoperability

1. What readers are compatible with STid Mobile ID®?

All following models in the Architect® Blue and Architect® One Blue ranges are compatible with STid Mobile ID®.

ARC1S/BT

ARCS-A/BT

ARCS-B/BT

ARCS-C/BT

2. Can we use other readers on the market?

In order to ensure the highest levels of security and support all functionalities provided by the STid Mobile ID® solution, only Architect® Blue and Architect® One Blue are compatible with the STid Mobile ID® solution.

3. Can we continue to use conventional access cards?

Yes. Architect® Blue and Architect® One Blue readers support a large range of different technologies: Bluetooth® Smart (4.0), NFC, all 13.56 MHz MIFARE® chips (MIFARE Classic, Classic EV1, Ultralight®, Ultralight® C, MIFARE® Plus, MIFARE® Plus EV1, DESFire® EV1 & EV2, DESFire® 256, etc.), iCLASS® / PicoPass® chips (CSN only) and CPS3 French health professional cards.

4. Will the mobile access solution operate with all access control systems?

Architect® Blue readers are identical to Architect® readers, and maintain the same system compatibility.

Like all STid access solutions, STid Mobile ID® operates with all access control systems. TTL readers (Wiegand / Data Clock – ISO2) and readers with RS485 serial connections are available. The encoder comes with a USB cable.

C. User-friendliness

1. What are the advantages of your mobile solution over a conventional RFID solution?

STid Mobile ID® contributes to the acceptance of corporate Security Policies. Its user-friendly functions make it instinctive to use. STid offers a range of identification modes which allow users to be identified without taking out their phone, whether or not they're using it, and even if it's on standby.

2. What is Badge mode?

Touch your smartphone on the reader like a conventional RFID card.

3. What is Slide mode?

With your phone in your pocket or handbag, simply slide your hand over the reader to open the doors. The patented capacitive technologies activate the reader and initiate communication with the smartphone.

This mode is not available with the ARC1S or ARCS keypad in Badge or Key mode.

4. What is Tap Tap mode?

Tap your smartphone twice in your pocket for proximity or remote access entry.

5. What is Hands-free mode?

Just walk past the reader! Nothing else to it!

6. What is Remote mode?

Use the smartphone like a remote control to remotely check your access points.

7. Can all the identification modes be activated on a reader?

It is possible to use more than one mode in line with your corporate security policy. However, combining some modes is not recommended:


\+ = **Not recommended**

Hands-free mode takes priority over all other modes, because it requires no action for authentication.

\+ = **Not recommended**

You have to take out your phone to unlock it.


\+ = **Recommended**

Use Badge and/or Slide and/or Tap Tap mode for building access control and Remote for car park access.

8. When readers use Slide mode, is it normal for more than one nearby phone to be authenticated?

Yes, users activate the reader by passing their hand over it. This launches communication with all phones within range that have Bluetooth® on, the app activated and a virtual card corresponding to the reader configuration.

9. What happens if Slide mode and RFID card reading modes are activated on the same reader?

Bringing an RFID card near the reader will launch the Slide mode if it is activated on the reader, because it will also detect the hand that is holding it. If the mobile application is activated within the range of the reader, RFID card will be read first then Slide mode authentication will take effect.

10. What happens if ApplePay is configured on iPhone ou NFC active with Android™?

When the ApplePay Wallet is configured, the payment card may appear when you present the phone to the reader in card mode. This is normal, as the reader will wake up the card in NFC mode. However, it will not generate any transaction, with the credit card.

When the NFC is activated on an Android™ device, and if the reader is configured to read NFC ID's, you may encounter some conflicts, as the reader will get both numbers.

11. Can multiple Architect® Blue readers be installed in the same area?

Yes, with the exclusive, patented STid technology, you can distinguish between different entrances by distance and/or by changing the site code. Depending on the reading mode selected, the reader will only operate if you perform a deliberate action with your smartphone within the selected range.

A minimum distance between two readers is required if one of them is in "Hands-free" mode.

12. Is it possible to configure the reading distance?

Yes, reading distances can range from 0 to 20 meters and can be configured individually for each mode.

13. Does the solution function with the phone on standby?

Yes. All identification modes operate with the phone in standby or in operation, locked or unlocked, depending on the limitations of the phone version or of his OS.

14. Does the mobile application have a big impact on battery life?

One of the main features of Bluetooth® Smart is its low energy consumption. Like all apps, battery use depends on how frequently it is used.

15. What happens if the phone runs out of battery?

You won't be able to use your smartphone for identification if its battery is dead. Bluetooth® Smart technology only operates with your phone on. It is advisable to have a spare RFID card with you in case you need it.

16. What should I do if authentication stops working with the phone?

First:

- Check that "Airplane/Flight Mode", "Do Not Disturb" or "Ultra Eco" energy-saving mode are not activated.
- Check that you have Bluetooth® turned on.
- Check that the mobile application is turned on.

If the problem remains, restart the app and/or turn Bluetooth® off and on again and/or turn smartphone off and on again.

D. Security

1. How do you secure the data stored in the app?

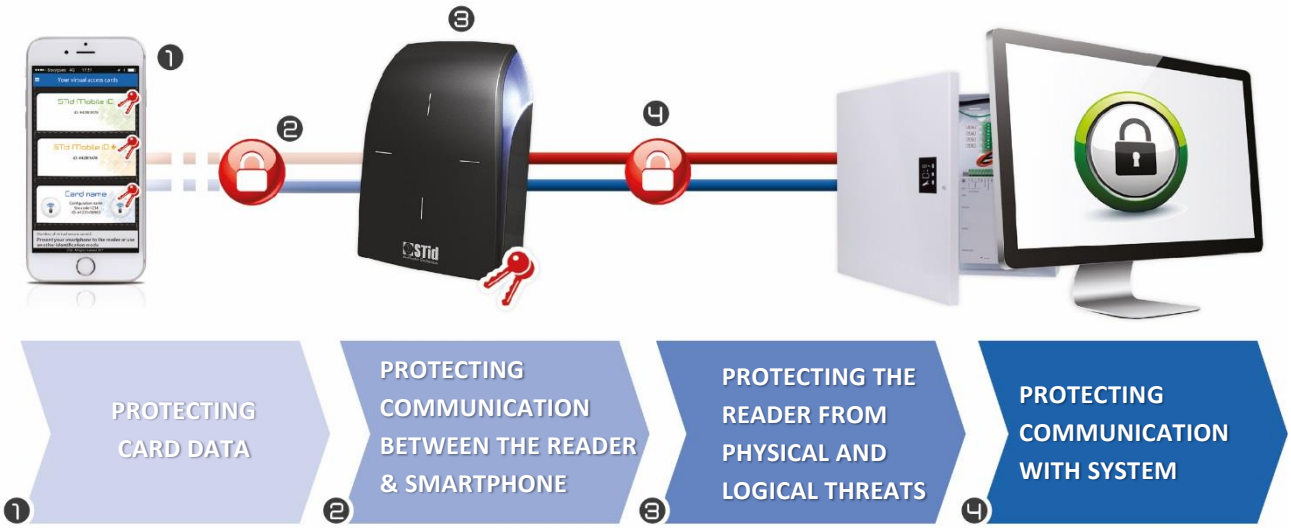
STid protects the data stored in your smartphone OS via encryption (AES 128), authentication (SHA-256) and securing the code. These methods use public algorithms that comply with the French General Security Framework (RGS) published by ANSSI (French Agency for Information System Security) to encrypt and authenticate data in the app using a unique key for each user.

STid gives you the option of adding extra layers of security by requiring the smartphone to be unlocked (authentication via PIN, biometrics, voice recognition, etc.).

2. How do you secure data exchanges?

Between the smartphone and the reader

STid protects data exchanges via encryption (AES 128), authentication (SHA-256) and securing the code. These methods use public algorithms that comply with the French General Security Framework (RGS) published by ANSSI (French Agency for Information System Security) to encrypt and authenticate application data using a unique key for each user.



3. How do you secure the data stored in the reader?

Sensitive data is stored in a EAL5+ certified component (with the same level of security that is used for banking).

Each Architect® Blue & Architect® One Blue reader has an innovative motion detection based tamper protection system. It protects sensitive data by deleting authentication keys (patent pending). Unlike the current market solutions (mechanical switches, optical sensors, reed switches, etc.), the reliability of the accelerometer-based technology means it cannot be bypassed.

You can also add extra layers of security using additional modules: standard or random keypad.

4. How do you ensure data security?

Our STid Mobile ID® app is continuously monitored and checked by specialist external security auditors to ensure a constant level of security.

E. Virtual card management

1. What is a virtual card?

A virtual card is a digital version of your access control card in a mobile application. Your virtual card has an identification code and functions like an RFID card.

2. How many virtual cards type do you offer?

STid offers three types of access card to meet your various needs:

The STid Mobile ID+ card is a version of the STid Mobile ID® card, and therefore keeps the same number.

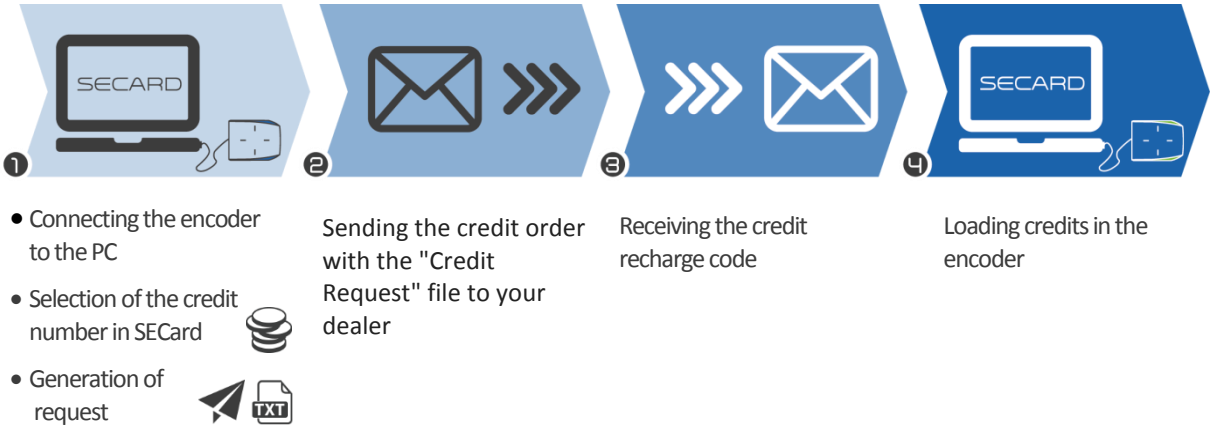
3. What tool is available for managing the virtual cards?

You can configure your virtual cards using **SECard**:

- 100% local sandboxed programming
- Full control over security and configuration settings
- Plug & Play – no development

4. How do I order credits and load them onto the encoder?

To order virtual cards, send a credit request via the SECard Programming Kit. Please note that credit requests must be accompanied with a purchase order directed to your reseller.



5. What is the value of the credits?

- 1 STid Mobile ID+ upgrade = 1 credit
- 1 Virtual Access card = 5 credits

6. Where are the credits stored?

In Offline mode, your credits are securely stored in the crypto processor EAL5+ contained in the encoder associated with your SECard Programming Kit.

7. How I use the credits?

When encoding virtual card with SECard, credits corresponding to the type of virtual card are automatically debited from the encoder.

8. What happens if the encoder stops working?

At our production facility, we can retrieve the number of credits remaining on an encoder that has stopped working. If the encoder is destroyed this will become impossible, and the remaining credits will also be lost.

9. How can I create, modify and delete the virtual cards?

In Offline mode, you can use the SECard Blue Programming Kit to manage your virtual cards. Users can delete the virtual card stored on their smartphones via the app.

For deleting cards, we advise that you revoke the ID from your access control system, as you would for a conventional access control card.

10. What happens if we uninstall the application?

All cards stored in the application will be deleted and lost when it is uninstalled.

11. What happens if we lose the phone?

In Offline mode, you have to delete the system ID, in the same way you would if you lost your RFID card. A new virtual card then has to be created.

12. What should we do to move MIFARE® DESFire® RFID cards to smartphones?

A SECard function allows you to copy the parameters of your DESFire® cards onto smartphones. Simply click to apply your current DESFire® configuration and you can then program Virtual IDs on the smartphones, which will be immediately recognized by your readers, without requiring specific reconfiguration.

F. Configuration of access readers

1. What tools are available for reader configuration?

Configure your Bluetooth® Smart readers with the same tool as for other STid 13.56 MHz MIFARE readers: the SECard Programming Kit. Use it to create physical or virtual master cards for configuring readers (including parameters and keys).

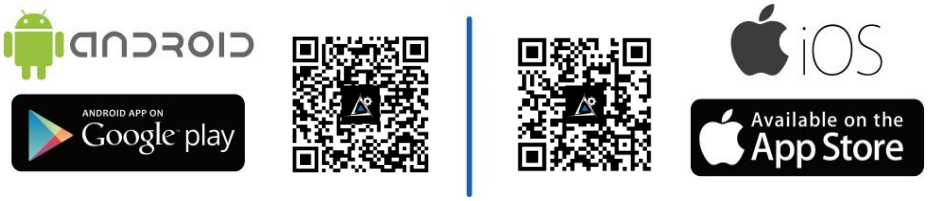
Configure your readers using a physical or virtual RFID card via the STid Settings app.

2. What is the STid Settings app?

STid Settings is a virtual configuration card wallet which stores them in your smartphone for use in configuring readers.

3. What mobile platforms is STid Settings compatible with?

STid Settings can be downloaded to Google Play (Android™) and App Store (iOS) phones. 95% of smartphones on the market use one of these 2 operating systems.



4. How much does the STid Settings app cost?

The STid Settings app is free of charge.

5. Does creating virtual configuration cards in STid Settings use credits?

No. Creating virtual configuration cards is free of charge. You can create as many as you want.

G. Smartphone compatibility

Performance differences may occur depending on the model and version of the smartphone and its operating system.

However, to guarantee the best user experience, we perform tests on a wide range of phones to apprehend their comportment. Below are the models qualified by STid.

Nexus	6P	Android 7.0	
	6	Android 7.0	
	6	*Android 5.x*	*Non-functional*
Huawei	P9	Android 7	Slowness
Samsung	S6	Android 6	
	S7	Android 6	
	S7	Android 7	
	S4	Android 5	
	A5	Android 6	Slowness

iPhone	5C	iOS 10.2.1	
	5S		
	6		
	6+		
	6S+		
	7		
	7+	iOS 10.3	

Note 1: This list is subject to change.

Note 2: This list is not exhaustive: Apps can operate on smartphones not included in this list.

IV. Project Development

There are certain important steps that must be followed when setting up a Bluetooth® configuration on a new or existing site.

A. Site analysis

Not all readers on the same site will be configured with the same modes and authentication ranges.

The following basic information needs to be gathered in order to define the configuration:

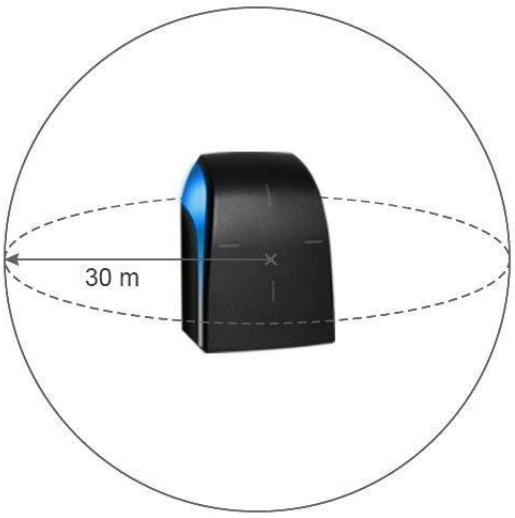
- Site map
- Direction of traffic
- Modes and authentication ranges for each reader
- Number of entrances to be secured
- Number of people to identify
- Smartphones models used by staff

B. Testing

From the outset, we recommend defining the tests required to validate the configuration with the client.

C. Important

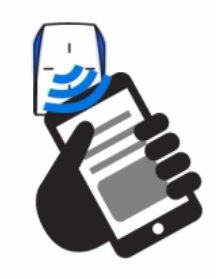
- In operation, Bluetooth® readers emit in a spherical zone around the reader.



- Detection distances depend on the smartphone model and its position relative to the reader.
- Personal identification is a voluntary action. It requires activation of Bluetooth® and the STid Mobile ID® app on the smartphone.

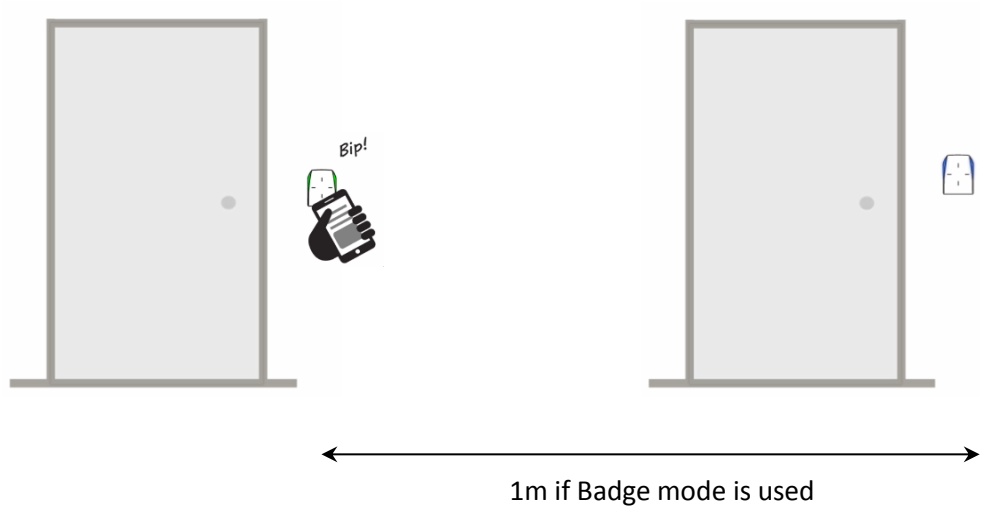
V. Badge mode

The smartphone is used like a physical access control card.



This identification mode is appropriate in the following cases:

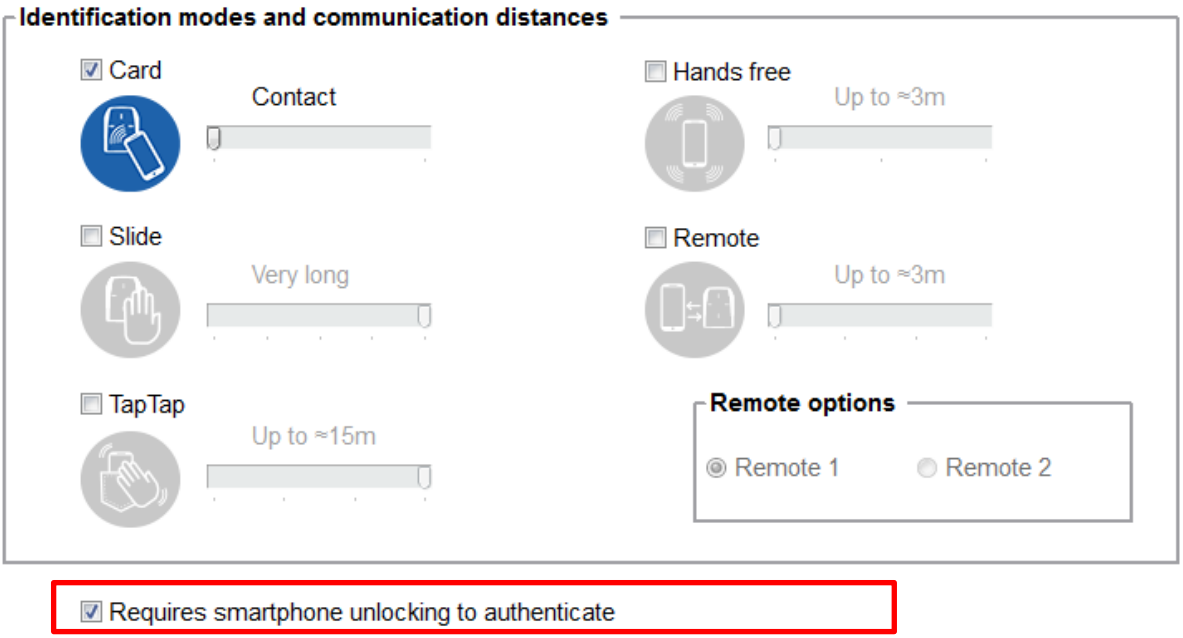
A. More than one reader installed in the same area



Only one of the readers is activated for authentication.

B. Installations requiring strong authentication

In this case, the option requiring the phone to be unlocked for the reader to authenticate with the card should be used.



Depending on the smartphone, it can be unlocked using fingerprint detection, code PIN, voice recognition or pattern.

Important: this is not a default feature on smartphones. It needs to be activated.

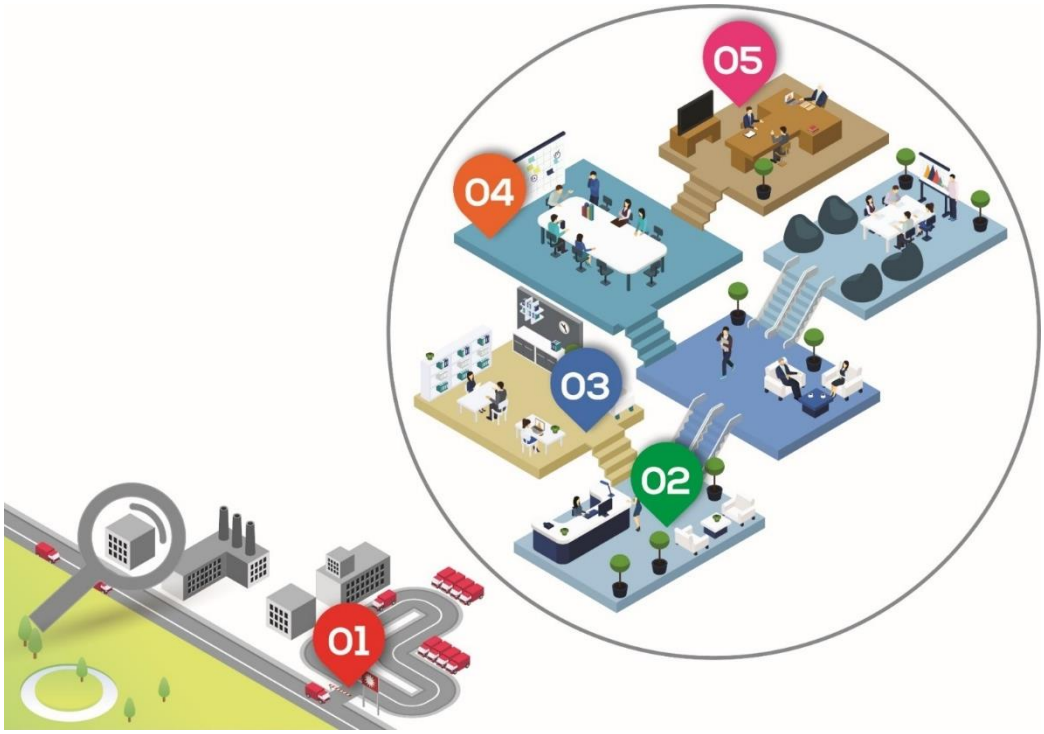
VI. Example of a typical installation

A. Site analysis

Access point		Direction of movement	Identification mode	Configuration name
01	Car Park Barrier	In and Out	Remote mode Hands-free mode	Car Park Entrance Car Park Exit
02	Entrance / Reception	In	Badge mode Tap Tap mode	Reception
03	Server Room	In	Badge mode: phone must be unlocked	Server
04	Meeting Room	In	Badge mode Slide mode	Office 1
05	Management Office	In	Badge mode Slide mode	Office 2

1. Site map

- Direction of movement
- Define modes and identification ranges for each reader



2. Testing

Access point		Requirement	Range	Test
01	Car Park Barrier	Car/Bike/Motorbike access Entrance and exit – 2 different configurations	Remote mode: up to 20m Hands-free mode: up to 3m	Check that distances are appropriate for intended use. If they are too large or too small, adjust the ranges in the configuration.
02	Entrance / Reception	None / No reader within 4 meters	Badge mode: up to 50 cm Tap Tap mode: up to 3m	Check that distances are correct. If they are too large or too small, adjust the ranges in the configuration.
03	Server Room	Strong authentication Reader 4 within 3 meters	Badge mode: contact Phone must be unlocked to initiate authentication	
04	Meeting Room	Reader 3 within 3 meters	Badge mode: contact Slide mode: close proximity	Adjust the Slide distance to ensure the reader does not authenticate with the phone of the person in the neighboring office.
05	Management Office	None / No reader within 2 meters	Badge mode: up to 50 cm Slide mode: close proximity	

B. Virtual access card settings

- Define the name of the virtual card: e.g. “STid Access”.
- Configure the Blue Mobile ID security settings: one key / two keys and enter the key(s).
- Display Remote buttons for car park access.

C. Configuration of access readers using SECard

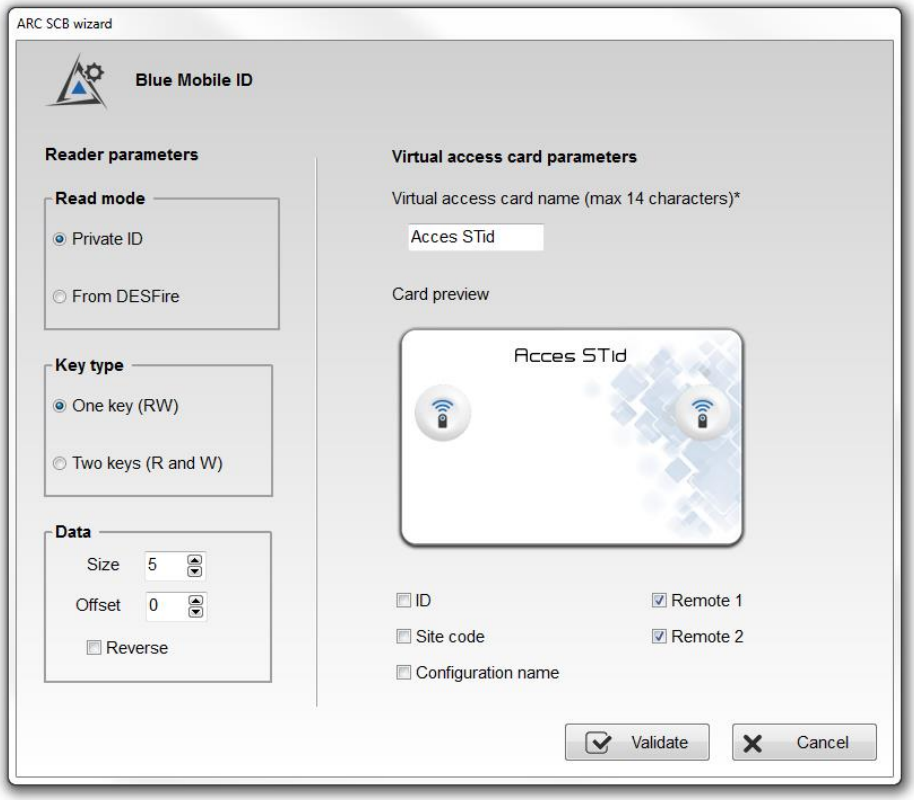
A site code needs to be defined for the installation. For example, “5A5B”.

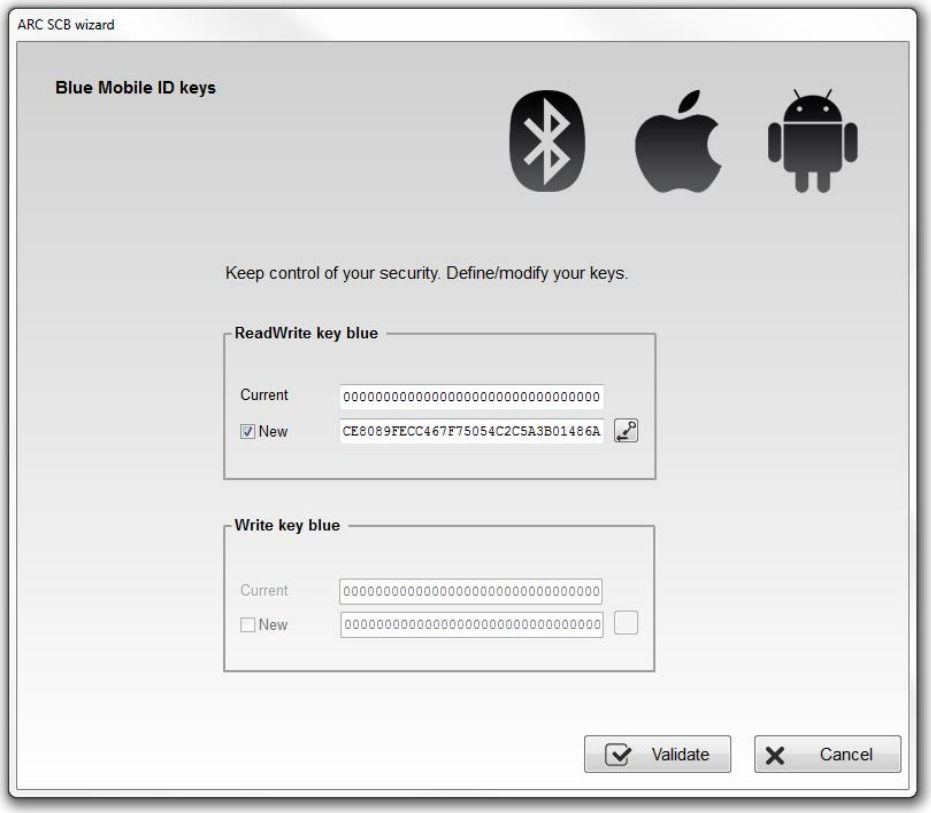
We will then have 6 configuration cards to set up. STid offers 2 options for this:

- Virtual card with the free STid Settings app – virtual SCB cards are free and you can store as many as you want.
- MIFARE® DESFire® EV1 card – ensure you have enough DESFire® EV1 4K CCTW380 cards.

For each of the configurations, it is necessary to create the corresponding configuration badge before proceeding to the new one.

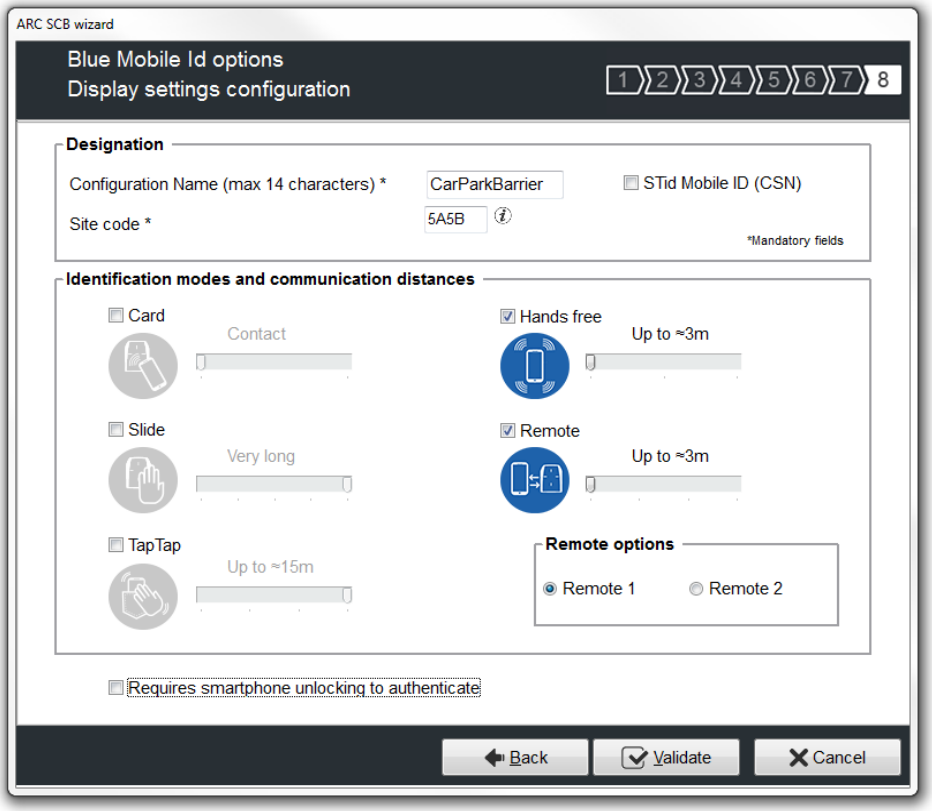
1. SECard settings for creating virtual user cards





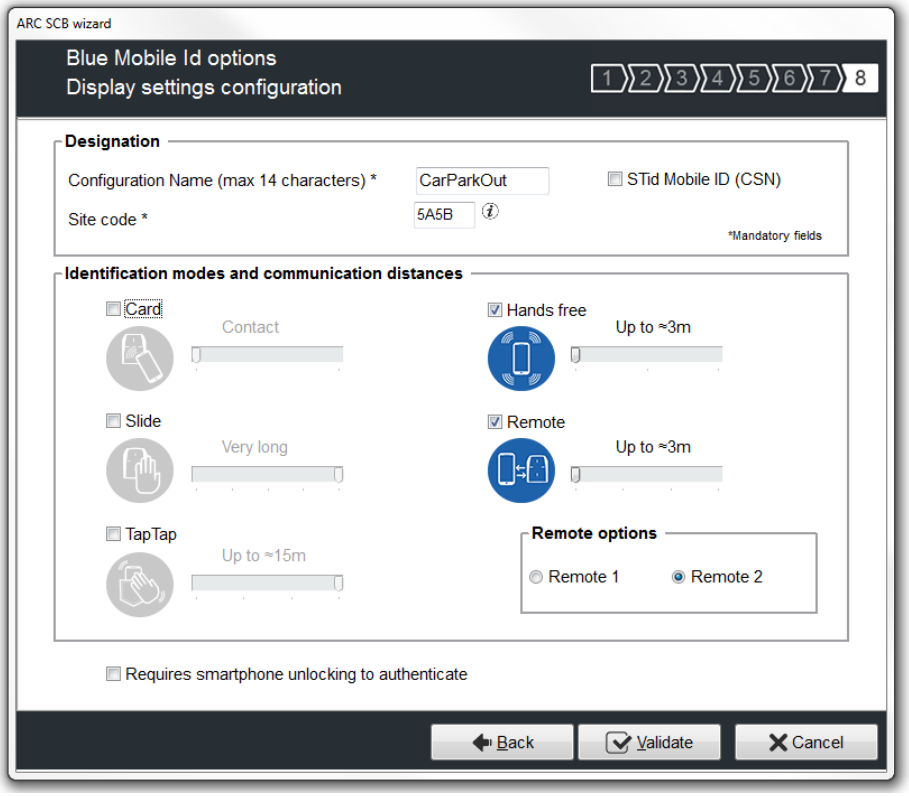
2. SECard settings for creating the Car Park Entrance configuration card

Button 1 will be allocated to the entrance reader

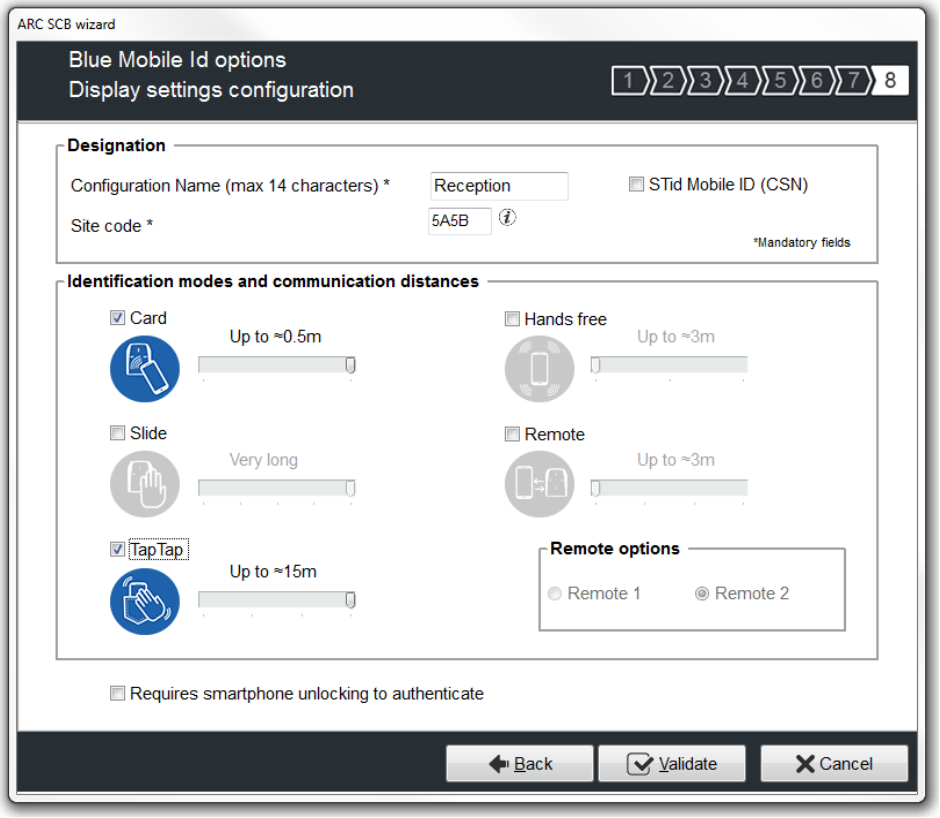


3. SECard settings for creating the Car Park Exit configuration card

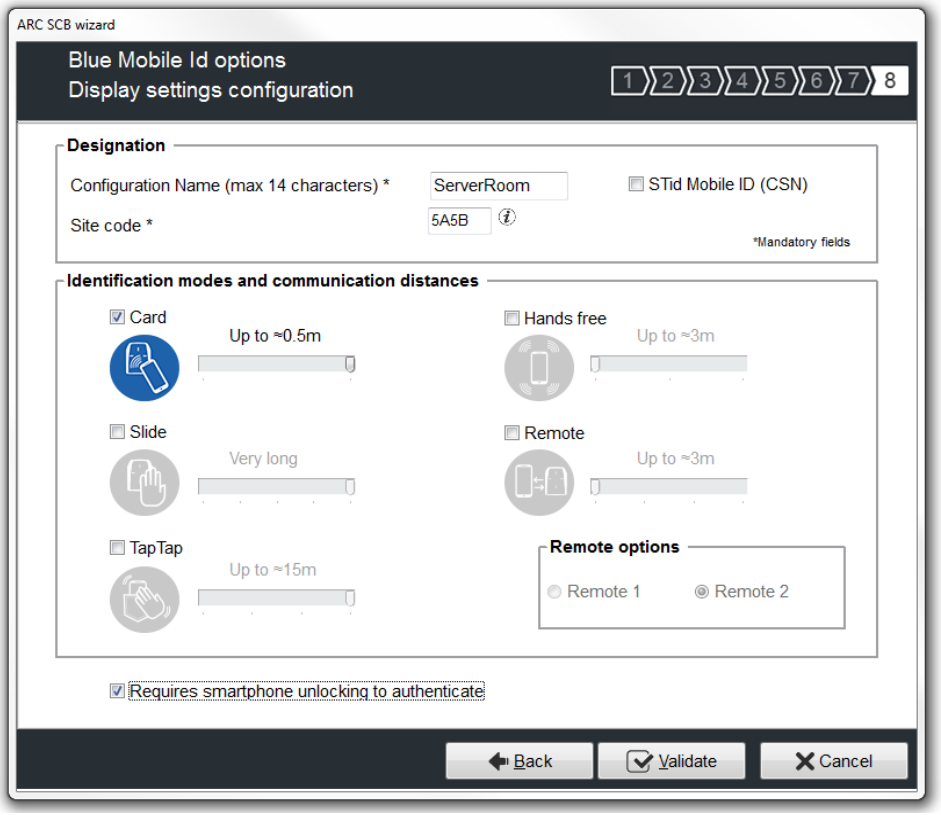
Button 2 will be allocated to the exit reader



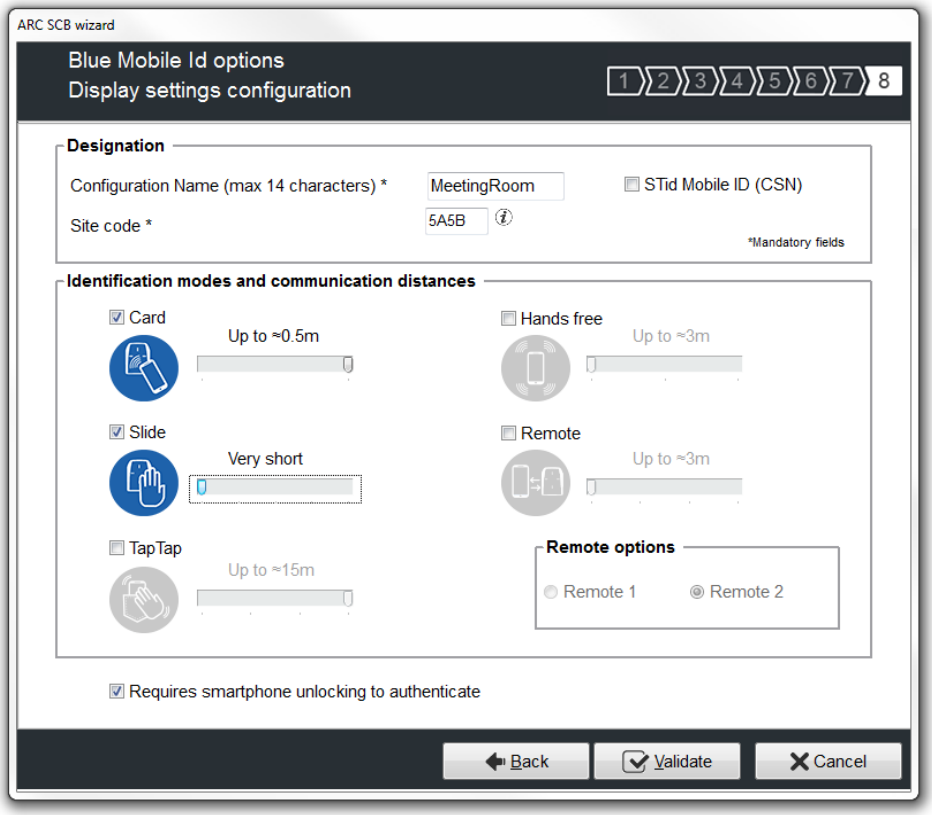
4. SECard settings for creating the Reception configuration card



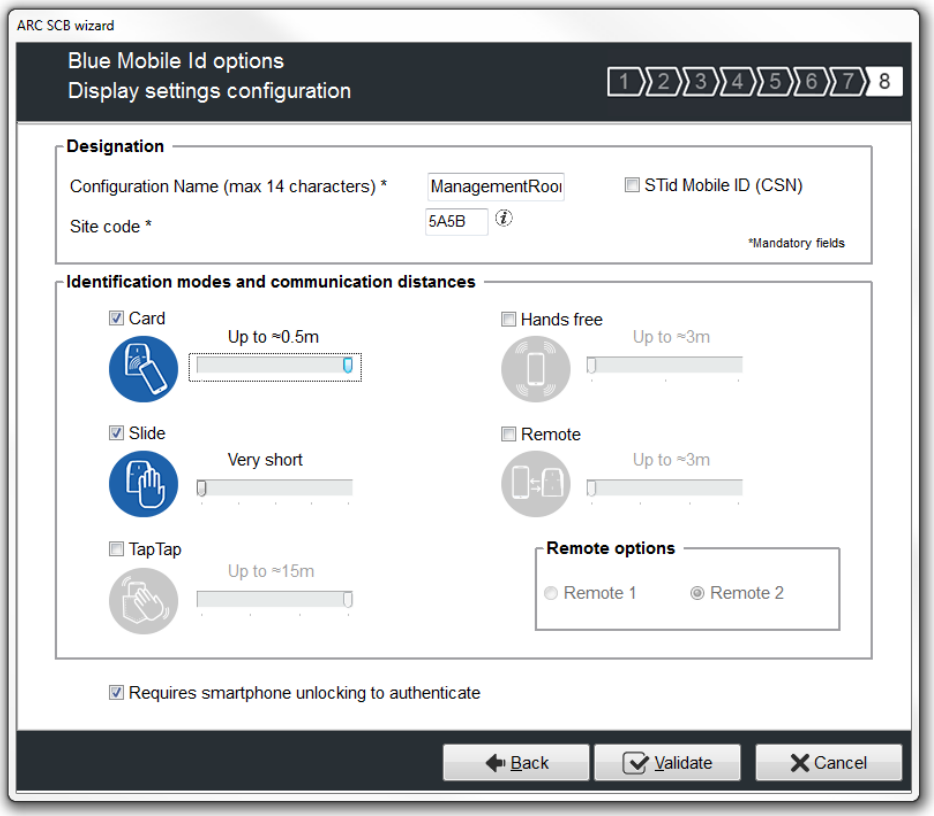
5. SECard settings for creating the Server Room configuration card



6. SECard settings for creating the Meeting Room configuration card



7. SECard settings for creating the Management Office configuration card



8. Preview of configuration cards in STid Settings app