

# SPRINGPASS BY SPRINGCARD

**Contactless Solutions** 

• 2021• PSL21043-AB S M R



# SpringPass

#### SPRINGPASS BY SPRINGCARD

It's a web service allowing to generate NFC passes. It aims to dematerialize contactless cards or RFID badges by virtualizing them in your mobile wallet.

A mobile wallet is the digital equivalent of a physical wallet. A place to store and organize dematerialized cards on a smartphone.

It keeps credit cards, loyalty cards, coupons, membership cards, transit tickets and more, in one place.

Unlike plastic and cardboard cards contained in a physical wallet, a pass can be updated at any time (for example the balance of loyalty points which changes).

A pass can also remind a customer when is the best time to use it (for example their discount pass). The mobile wallet offers the next customer management system, while providing security, efficiency, optimization and modernization.

Our service <u>https://springpass.springcard.com/</u> provides test passes for Apple Wallet and Google Pay.

These passes are for use with SpringCard readers and applications supporting Apple VAS or Google Smart Tap.



#### **iOS & ANDROID**

Apple Wallet is the iOS application that stores virtualized passes (barcode or NFC). It is pre-installed on all latest generation iPhones and implements the Apple VAS secure transaction compatible with our SpringCard readers.

Android's counterpart is Google Pay, which implements the Google SmartTap secure transaction.

Compared to barcodes and QR codes, both solutions are faster, easier to use and considerably more secure - and therefore more attractive for the end user and more efficient for the cashier or office staff.



### WALLET, AN ENVIRONMENTALLY FRIENDLY SOLUTIONS

Your mobile wallet is a pre-installed application on most smartphones. For iPhone it's called Apple Wallet, for Android it's called Google Pay.

Apple Wallet and Google Pay are becoming an everyday, reliable and preferred use for mobile payments, customer management for loyalty systems, coupons, ticketing and more.

From now, you have access to an environmentally friendly place to store, in a secure way and in a digital version, all of your plastic cards and paper tickets.

# **ZOOM on Apple VAS**



#### USE OF APPLE VAS WITH OUR READERS SPRINGCARD

Apple Pay is based on the open EMV (Europay Mastercard Visa) specifications for contactless payment.

According to the EMV specification, «Value Added Services» refers to the use of the payment card for non-payment purposes, such as loyalty or identification.

Apple VAS is therefore the non-payment part of the Apple Pay solution.

It builds on NFC with Apple's proprietary extension to ISO / IEC 14443, called ECP (Enhanced Contactless Polling).

Only Apple certified readers (like SpringCard's PUCK reader) can use ECP and perform Apple VAS transactions.

#### SAFETY AND USE

Apple VAS uses Elliptic Curve Cryptography (ECC) and AES to secure pass transmission from the smartphone to the reader or to the application running in the terminal.

The pass stores up to 64 bytes of data; it is normally used - just like a barcode would be - to transmit a short identifier that is only relevant to the back-end system.

#### PASS CONTENT

The visual description of the pass is determined by the list of available fields visible on the pass.



DIGITAL WALL

My cards:

BONUS CARD

# Pass Apple VAS

#### WHAT IS THE PASS ?

An Apple Wallet pass is a file with the .pkpass extension (Apple «passbook» format).

This file is in fact a ZIP archive whose extension has simply been changed, and which itself contains in several files:

> the visual description of the pass, (background color or image, logo, text, barcode),

> the identifier of the organization holding the pass, the associated security key and the useful data to be transmitted by NFC to the readers of this organization,

> the digital signature, RSA signature of all pass data, and the developer X509 certificate who holds the signature key.



#### **THE .PKPASS FILE**

The .pkpass file can be transmitted to the iPhone by any means: download link (unique URL), attachment in an email, direct opening by an application installed on the smartphone...

For this .pkpass file to be accepted by Apple Wallet, the RSA digital signature must be correct and the X509 certificate must prove that it has been generated by a developer authorized by Apple.

It is exactly the same principle as for the signature applications.

The signature of the .pkpass file uses the same mechanisms as the signature of the .ipk file of an application you want to distribute through the App Store.



#### WHAT IS THE DIFFERENCE BETWEEN AN NFC PASS AND A "NOT-NFC" PASS

What makes the difference between an NFC pass and a «not-NFC» pass is the content of the X509 certificate.

A pass signed by a standard developer certificate will only have access to the barcode function, but if the pass is signed by a developer certificate on which Apple has added the «NFC approved» extension, then the pass will be able to be transmitted to readers via NFC.

As Apple drastically limits the list of developers to whom it grants this precious sesame, it is usually necessary to go through a developer who already has it.

# **ZOOM on Google Smart Tap**

The Google Smart Tap protocol also based on the open EMV (Europay Mastercard Visa) specifications for contactless payment, and designed as an EMV VAS (Value Added Services) application.

The solution is fully compliant with the ISO / IEC 14443 standard and the dialogue between the reader and the smartphone is based on the concepts and syntax of the NFC Forum.



#### SAFETY AND USE

Google SmartTap uses Elliptic Curve Cryptography (ECC) and AES to secure the transmission of a pass from the smartphone to the reader or to the application running in the terminal.

The pass is able to store a few fields of varying lenght.

In most situations, and to stay compliant with both barcode-based systems and with Apple VAS, the pass transmits nothing more than a short ID which is only relevant to the back-system. end.



## Pass Google Smart Tap



This URL can be transmitted to the Android mobile by any means: redirection in the mobile's web browser, clickable link in an e-mail, direct opening by an application installed on the smartphone, etc.

The Google Pay application then opens automatically by the Android system thanks to its configuration which manages all such URLs.

When the URL opens in a web browser, there are two steps to follow:

1- the user is invited to identify himself with his Google account,

2- The user is then redirected to a page offering to transfer the pass to the Google Pay application on their smartphone.

The smartphone then receives its pass in real time thanks to the push system.

### CONTENU DU PASS ANDROID

 $\odot$ 

La description visuelle du pass (couleur ou image de fond, logo, texte, code-barre).

### \*\*\*\*

L'identifiant de l'organisation titulaire du pass (Collectorld), la clé de sécurité associée (clé publique ECC de l'organisation) et les données à transmettre en NFC aux lecteurs de cette organisation.



La liste des champs disponibles dépend du type de pass. Il n'y a pas de signature numérique accessible au développeur, puisque tout est contrôlé par les services de Google.

# Reading an NFC pass

Reading an NFC pass requires an ISO / IEC 14443 Proximity Pairing Device (PCD), extended to support Apple's VAS ECP, a secure element to store ECC private keys, and software to run the EMV VAS transaction, both as implemented by Apple VAS and as implemented by Google Smart-Tap.

The software that performs the transaction could be implemented:

- either in the reader itself: in this case we use the term Smart Reader;
- or in an application running on a PC or an on-board host computer (terminal).

In the latter case, the reader remains a «silent» PC / SC coupler between the application and the smartphone.





#### **SMART READER**

PUCK, SpringPark, etc. have SmartReader models to read Apple VAS and Google SmartTap NFC passes. All you have to do is configure the reader with your Merchantld (Apple) and Collectorld (Google); and load your ECC private keys into the secure element of the reader. The reader then executes transactions on its own and transmits the ID read to your system via serial, USB or network. PUCK's keyboard emulation mode immediately replaces a barcode reader. The innovative part of SpringPark with its MQTT protocol suitable for direct connection to your cloud-based back-end system.



### **PC/SC APPLICATION**

PUCK and Prox'N'Roll PC / SC implement all contactless layers (NFC); the transaction (APDU) must be implemented in the host computer. For ease of development, SpringCard offers .NET libraries already approved by Apple and Google. At your option, ECC private keys can be stored in the secure element of the device (PUCK only) or in a software safe on the computer.

# **Pass benefits**

#### WHY DEMATERIALIZE YOUR CARDS TO THE MOBILE WALLET PASS?

- **#1** Anti-loss and easily identifiable in the wallet of your customers' smartphones
- **#2** Saves time on updates and reduces development costs
- **#3** Evolution and personalization of your CRM thanks to the update of the pass interface
- #4 Sending information by notifications that are displayed on the locked screens of smartphones
- **#5** The pass is automatically issued and chosen among all other passes available in the wallet
- **#6** Environmentally friendly solution, thanks to the elimination of paper and plastic supports







### A DISTRIBUTION NETWORK FOR MULTI-USE PASSES



### Integrate pass in your business

SpringPass service is the easiest way to digitize your business; your customers and prospects; thanks to billions of iPhone and Android users.

SpringPass lets you interact with your customers anytime, anywhere with location-based notifications; updates and information sent in real time. SpringPass lets you interact with your customers anytime, anywhere with location-based notifications; updates and information sent in real time.

Do you want to subscribe to the SpringPass by SpringCard service to develop and digitize your business?

Contact us and together we will develop your tailor-made project.

#### SPRINGCARD SUPPORT YOU

ARE YOU A DEVELOPER? RECEIVE OUR PROCESS AND API

DO YOU HAVE SOME QUESTIONS ? WE ANSWER IT !

### **ABOUT SPRINGCARD**

#### CONTACTLESS & 13.56MHZ RFID & NFC SOLUTIONS AND READERS

SpringCard is a company that designs and produces contactless readers by combining different technologies. With 20 years in the field experience in 13.56MHz systems, we offer you more than just technical skills.

PARIS (FR) - ANGERS (FR) - SAN DIEGO (USA)



www.springcard.com