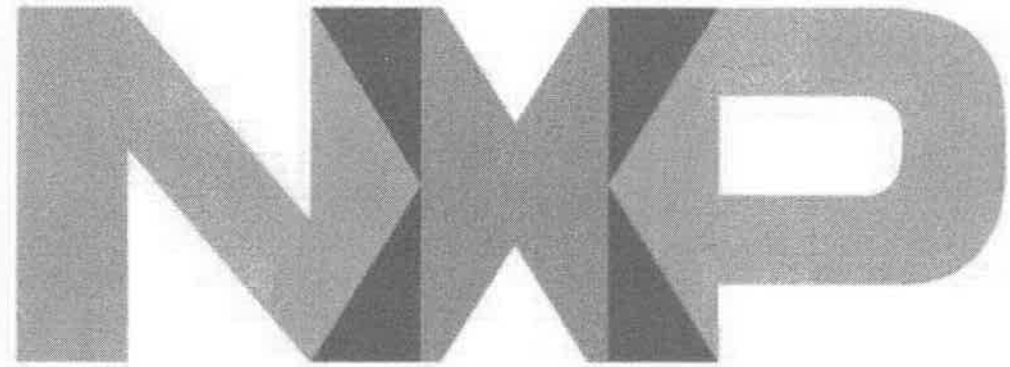


SECURE CONNECTIONS
FOR A SMARTER WORLD

MIFARE Digital Services

Objective of this document

This document on a high level describes the digital solutions to manage MIFARE Products. In this document we will mainly focus on how 2 products i.e. AppXplorer and MIFARE 2GO, are related to each other and serves the customer in tandem.

Digital Products

AppXplorer

It is an intuitive self on-boarding post-issuance platform for MIFARE DESFire EV2 issuers and Service Providers:

- to grow and develop their own scheme,
- acquire more end-customers, and/or
- to act as aggregators for Smart City like schemes

by offering multi-application environment with new additional services to their end-customers/users via any type of Android NFC device or customer facing terminal.

Key targeted markets for AppXplorer are

- Transport for MaaS (integrate other transport schemes) and/or city tourist services/L&E and hospitality
- Corporate/University access with transport and other city schemes, bike/loyalty/micro-payment
- Loyalty with hospitality, L&E and transport (growth market, limited MIFARE exposure with high TAM)

MIFARE 2GO

MIFARE 2GO is the Hub or the TSM to bridge the gap between OEMs & Service Providers. It is focused on digitization and management of virtual and/or physical MIFARE cards on various form factors like Mobile, Wearable or Cards.

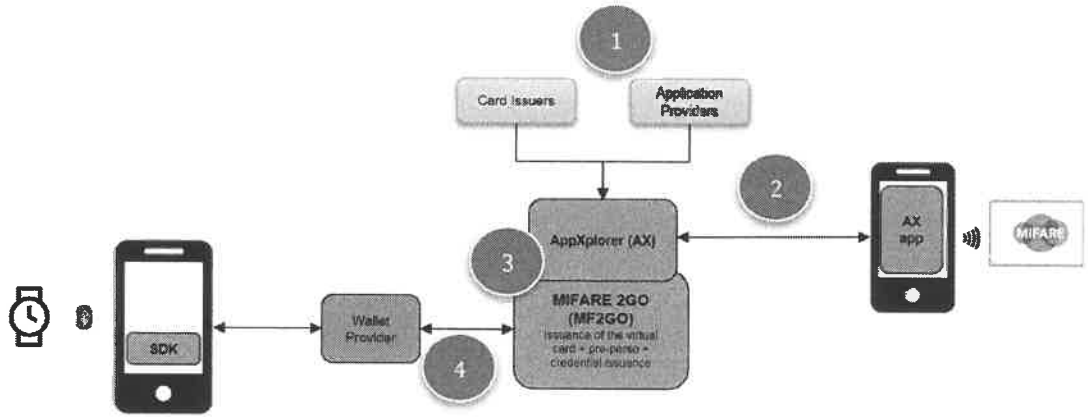
Key targeted markets for MIFARE 2GO is:

- Transit
- Access (Corporate, University, Hospitality, etc)
- Micropayment
- Loyalty
- and many more

MIFARE 2GO & AppXplorer combined product

High level diagram

All Green boxes are NXP deliverables

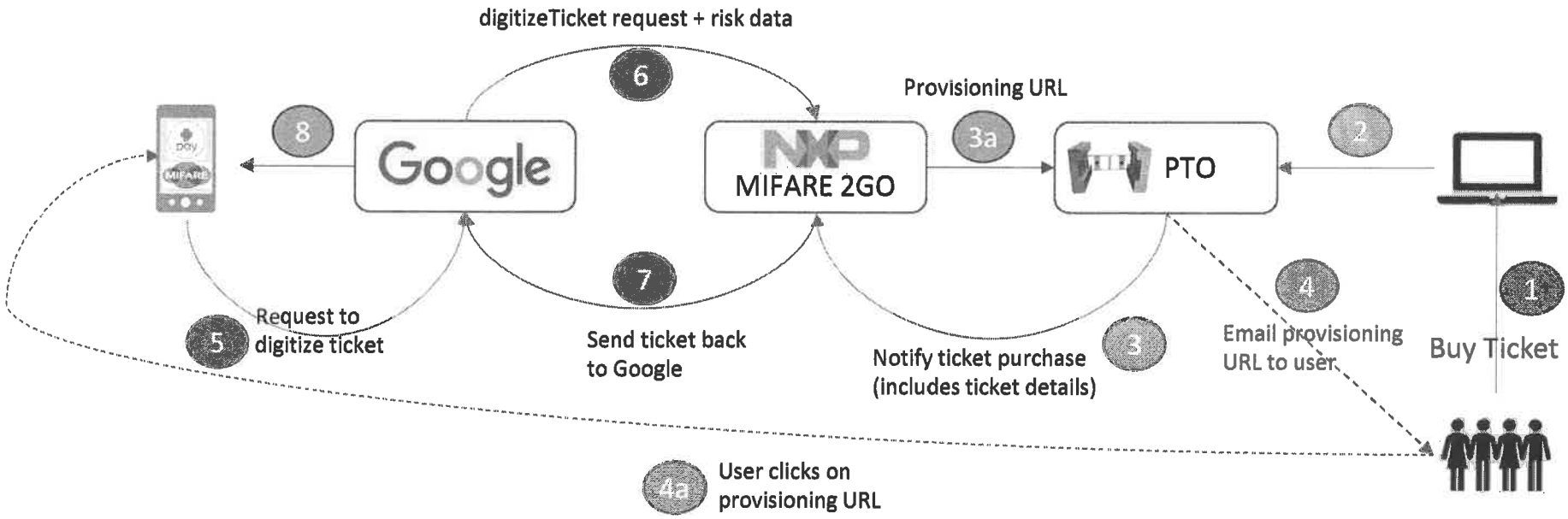


Description

AppXplorer and MIFARE 2GO is closely bonded together to enable Service Providers on MIFARE Digital Services.

Item	Description
1	- "Card Issuers or OEMs" & Application Providers will be onboarded on AppXplorer - AppXplorer will serve as marketing and collaboration platform for both the entities
2	- AppXplorer will also have a mobile application to manage multiple DESFire application on MIFARE DESFire EV2 - AX Mobile application will also manage the content of the physical DESFire EV2 i.e. over the air top-up or card updates
3	- AppXplorer and MIFARE 2GO will be closely tied - Every OEM & Service Provider onboarded on AppXplorer will automatically be enabled on MIFARE 2GO - AppXplorer will be the marketing platform for Service Providers - MIFARe 2GO will be the technical platform for Service Providers to digitize, personalize and manage the content of physical card and virtual card
4	- MIFARE 2GO will connect to OEM wallet to manage multiple applications from several Service Provider in form of virtual MIFARE Card on SE(wearable / mobile) or HCE(mobile) - MIFARE 2GO will manage the life cycle of those virtual card

Purchase and Provisioning Flow Overview



AN4825

MIFARE 2GO Quick Start Guide for SP Integration

Rev. 1.0 — 21 May 2019
482510

Application note
COMPANY CONFIDENTIAL

Document information

Information	Content
Keywords	NXP Secure Services 2GO Platform, MIFARE 2GO, NFC, NFC Wearable Device, PTO, Public Transport Operator, SP, Service Provider, Access Management, Loyalty, HCE, SE
Abstract	This document summarizes on a very high-level all the first information required by a service provider who wants to get to know MIFARE 2GO, one secure cloud service offered from NXP. The content is intended to give a quick overview of what can be achieved with the MIFARE 2GO secure cloud service, what can be offered with MIFARE 2GO, and which use cases can be realised. Furthermore, additionally available MIFARE 2GO documentation and material is listed in this document, which can be requested subsequentially.

Revision history

Revision history

Rev	Date	Description
1.0	20190521	Initial version of the document

1 Introduction

1.1 NXP Secure Services 2GO

The NXP Secure Services 2GO Platform is a full platform for end-to-end delivery of consumer services of many different areas. The end user is provided with direct access to digitization services from service providers (SPs such as access providers, loyalty providers, ...), public transport operators (PTOs), payment network operators (PNOs such as Visa, Mastercard, American Express), and many more..

Thanks to NXP Secure Services 2GO, NFC equipped devices can use the platform for digitizing payment (e.g. credit cards) and MIFARE product-based cards (e.g. transit cards).

Devices which can be linked to the Secure Services 2GO platform, and can make use of MIFARE 2GO, include NFC enabled mobile phones and NFC enabled wearable devices (like smart watches). Mobile phones can utilize the MIFARE 2GO solution based on the phone`s embedded secure element or based on the secure software implementation based on HCE. Wearable devices will make use of the secure element solution only.

1.2 Document purpose – Service Provider Integration Quick Start Guide

This document introduces and focuses especially on the MIFARE 2GO solution, which is one part of the NXP Secure Services 2GO Platform and explains, how it can be used by a service provider who wants to connect to the MIFARE 2GO cloud service.

In this document all the information that is necessary for an SP to get access to MIFARE 2GO is gathered. This bundle of information and support material which is provided to the SP is called "Product Support Package" for the MIFARE 2GO integration.

The Product Support Package is a full set of documentation and software deliverables, enabling SPs to implement their connection to the MIFARE 2GO cloud platform and the usage of the MIFARE 2GO client-side solution.

1.3 Document audience

This document is dedicated to SPs who want to connect their infrastructures (public transport, access management, closed loop solutions, and many more) to the MIFARE 2GO cloud service.

It addresses developers, project leaders and system integrators who have a general technical understanding and overview of a specific SP infrastructure and it gives a first summary of the solution. More in-depth details can be found in the complimentary application notes which are mentioned within this introductory document.

1.4 Structure of this document

Section 2 of this document explains the NXP Service Platform in general and especially gives insights into the MIFARE 2GO cloud service which is part of the overall NXP Service Platform solution. It also highlights the content of the PSP and lists all relevant documentation.

The next chapter, Section 3, goes into detail of the onboarding steps which an SP must execute who plans to make use of the MIFARE 2GO service offering. Details regarding the reader infrastructure preparation as well as about the required server backend modifications are given.

Afterwards, Section 4 gives a very brief summary of all steps which are required to integrate MIFARE 2GO to a service provider`s infrastructure and make it usable for end customers.

2 Secure Services 2GO Platform and MIFARE 2GO

2.1 NXP Secure Services 2GO Platform Overview

The NXP Secure Services 2GO Platform abstracts the link between the NFC device's end-user and the targeted operator / service provider.

When the end-user wants to access a new service, he can access it via the OEM wallet application installed on his mobile phone or from his wearable device. Through the NXP Secure Services 2GO Platform, end customers get direct access to this service.

The use cases which can be realized with the Secure Services 2GO platform are very versatile, giving a lot of flexibility for integrating partners.

Use cases that can be targeted with the Secure Services 2GO are originating in the areas payment, transit, access, government, hospitality, loyalty and many more.

Giving some example use cases:

- In case of public transport-related usage, the available services will include actions related to transit scenarios and the usage of transportation tickets (e.g. buying tickets, downloading tickets, revoking tickets, extending tickets, showing trip information, displaying ticket balance, and many more).
- In case of access management related usage, the available services will include actions related to access scenarios and usage of the access credential (e.g. digitizing the access card, showing access information, displaying access validity, and many more).

The high-level architecture of the complete Secure Services 2GO Platform is displayed in Figure 1.

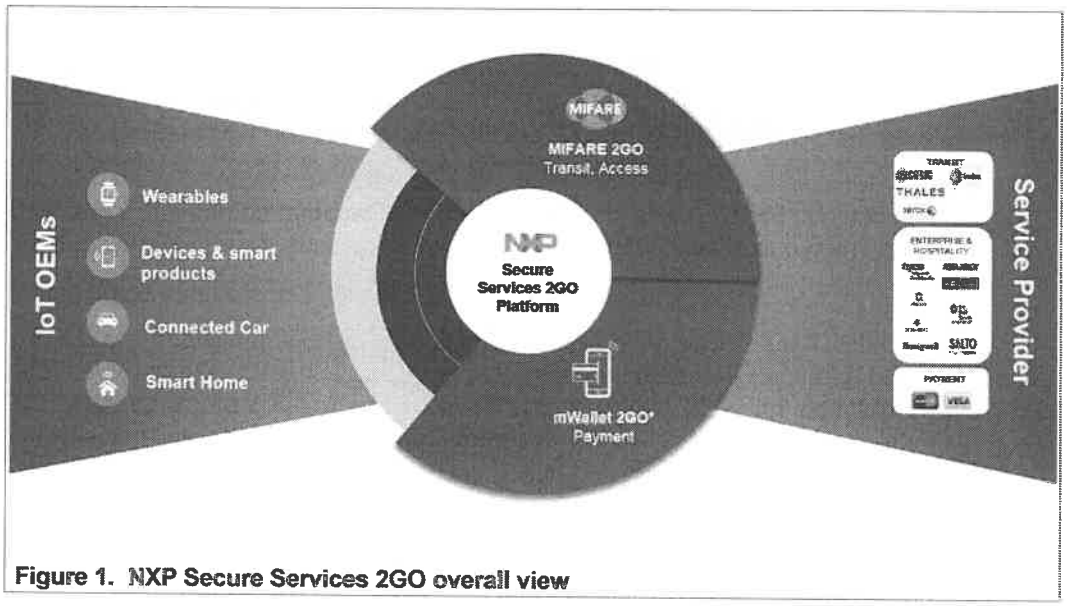


Figure 1. NXP Secure Services 2GO overall view

2.2 MIFARE 2GO Architecture

MIFARE 2GO is one secure service offered by NXP, which is running in the overall umbrella of the NXP Secure Services 2GO Platform.

A simplifyed view of the MIFARE 2GO end-to-end system architecture is displayed in Figure 2.

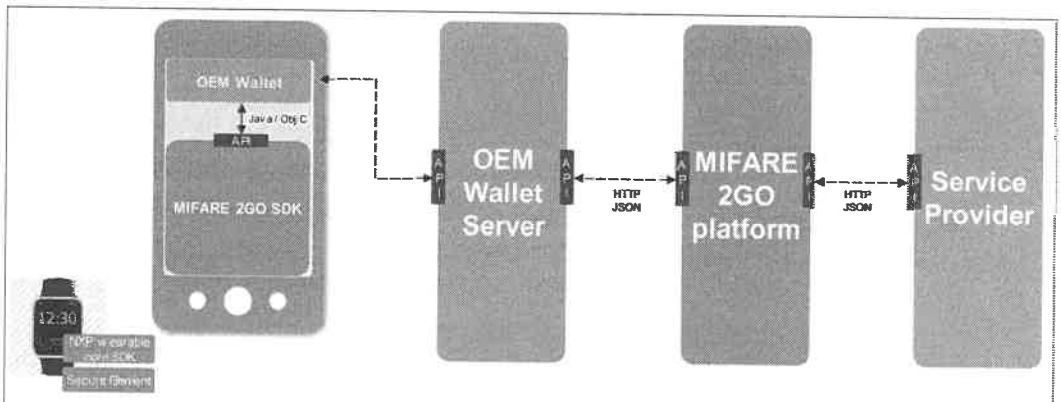


Figure 2. MIFARE 2GO Architecture

The main involved parts of the MIFARE 2GO overall architecture are the following:

- **Mobile phone or wearable device in the hands of the end-user**

In case of the mobile phone, the digitized card will be made available by the OEM Wallet application.

The OEM Wallet application can be utilizing the secure element inside the device for storing digized card details, if the mobile phone is equipped with a secure element. If there is no secure element available on the mobile device, the OEM Wallet application can be utilizing a pure software solution, based on the Host Card Emulation concept, which is additionally equipped with proper risk management.

In case of wearable devices (like smartwatches), the digitized card will always reside within the secure element. No risk managed software solution (HCE) is available here.

- **Wallet Server**

The Wallet Server is provided by the OEM and establishes the connection between the OEM Wallet application running on the end-user`s device and the NXP Service Platform.

- **MIFARE 2GO Platform**

The full server-side solution provided by NXP which bundles all information and establishes the connection between the end-user (via the OEM Wallet application) and the selected service coming from the targeted operator /service provider.

It handles the full integration and can connect multiple registered OEMs with multiple registered service providers (PNOs and SPs), according to the customer´s needs.

The main core areas of the MIFARE 2GO platform are Transit, Access, Loyalty and in general all services which can be realised and based on the MIFARE cards. This includes the digitization of MIFARE product-based cards as well as the connection to MIFARE product-related operators.

- **Service Provider (SP)**

The service provider can connect his own backend server via a defined set of APIs to the MIFARE 2GO cloud service. For each connected service provider, a separate instance is running (a service) which manages the SP-specific data like the structure of the digitized card, the card details, the possible user actions, and many more.

Only a one-time integration between the service provider and the MIFARE 2GO cloud service is needed, giving he service provider access to numerous different OEM wallets. There is no separate integration with each OEM wallet provider required for the SP. Access to MIFARE virtualized cards based on HCE or also on SE can be realized transparently, after one integration with MIFARE 2GO happened.

2.3 MIFARE 2GO In a Nutshell

MIFARE 2GO is one part of the NXP Secure Services 2GO Platform and the core piece of our digitization platform, focusing mainly on MIFARE product-related services like transit, access, closed loop solutions and applications. It is a cloud service for digitizing and managing credentials on any form factor or device. In the MIFARE 2GO ecosystem Figure 3, NXP is connecting the internet of things, allowing service providers to provide access to their service offerings instantly to end customer devices.

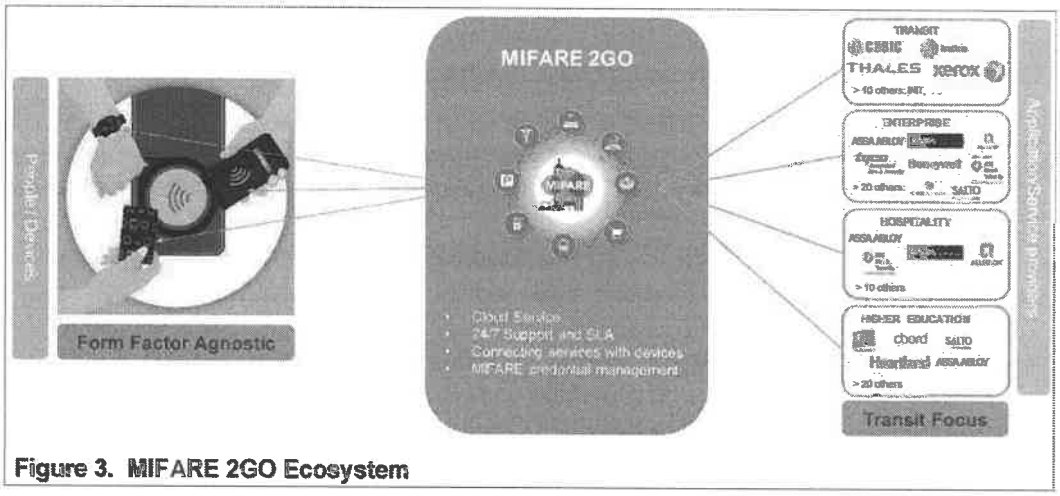


Figure 3. MIFARE 2GO Ecosystem

The MIFARE 2GO ecosystem offers a wide variety of features and use cases which can be consumed by SPs and end-users very flexible and completely individually. This means that a service provider can onboard to the MIFARE 2GO system and select only the features which are relevant for him, for realizing the use cases which are tailor-made for his existing infrastructure and customer base.

2.3.1 Service Offering and supported Features for the Service Provider

SPs which decide to onboard on the MIFARE 2GO system have a vast set of features to choose from:

- Managing the services for end-users in form of offered products
- Managing multiple cards (card images, card data structure, personalization, verification)
- Managing multiple card applications / tickets
- Managing special offers and push special deals and notifications to end-users via push notifications
- Credential lifecycle management (executing card or credential personalization, transfer, top-up actions; activating and deactivating credentials)
- Secure key management and key handling inside MIFARE 2GO (including card personalization using SP keys)
- Full risk and fraud management and notifications, as well as risk checks and security rules management for the HCE solution on mobile devices
- Access to reporting and analytics features and end-user evaluations
- Access to a 24/7 support which helps to solve issues and problems within agreed SLA timeline

2.3.2 Service Offering for the End Customer

- Adding a card to the OEM Wallet application
- Digitizing a card in the OEM Wallet which was bought through any other 3rd party channel (e.g. SPs website, SPs application)
- Viewing all available cards
- Management of available cards (suspension, deletion)
- Access to the card and transaction history
- Possibility to use card update (e.g. top-up) functionalities
- Receiving push notification and special offerings and discounts from the service provider
- Consuming other customized services from the SP which are based on the current end-user location (e.g. recommendations, etc.)

2.4 MIFARE 2GO Integration – Product Support Package

The Product Support Package (PSP) for the MIFARE 2GO integration is composed of the following deliverables:

1. **AN4825xx – MIFARE 2GO Quick Start Guide for SP Integration**
   Application Note, this document.

2. **AN4513xx – Reader infrastructure requirements for MIFARE 2GO**
   Application Note, available in NXP DocStore.

3. **UM4736xx – MIFARE 2GO SP Integration Guide**
   Application Note, will be available in NXP DocStore soon.

4. **AN4826xx – MIFARE 2GO SP Onboarding Guide**
   Application Note, will be available in NXP DocStore soon.

5. **ANxxxxxx – MIFARE Reader Infrastructure Assessment**
   Application Note, will be available in NXP DocStore soon.

6. **AN5333xx – MIFARE 2GO Reader Infrastructure Checklist**
   Application Note, available in NXP DocStore.

7. **ANxxxxxx – MIFARE 2GO Server Infrastructure Checklist**
   Application Note, will be available in NXP DocStore soon.

8. **AN4735xx – MIFARE 2GO API Specification for SP Integration**
   Datasheet, available in NXP DocStore.

9. **UMxxxxxx – MIFARE 2GO Support Structure and Support Guidance**
   User Manual, will be available in NXP DocStore soon.

10. **MIFARE 2GO – SP API Test Environment (API package based on Postman)**
    A Postman API package which can be used for API testing and evaluating. Available upon request.

11. **MIFARE 2GO – SP Sandbox Environment**
    A sandbox environment which can be used for end-to-end testing of APIs and functionality. Available upon request.

12. **MIFARE 2GO – Sample Client-Side APK for SPs**
    A sample Android APK. Implementation is containing the client-side MIFARE 2GO HCE SDK and the HCE implementation. The realization is based on the Google Pay Wallet and can be used for end-to-end testing, as well as for offline testing and demonstration together with the sample reader-side APK. Available upon request.

3 MIFARE 2GO Service Provider Onboarding Steps and Integration Flow

After a service provider made the decision to use the MIFARE 2GO cloud service and integrate with the NXP provided backend, there are multiple steps involved in order to achieve a successful onboarding and integration.

In the following chapter, the key steps are briefly introduced. Some points are elaborated in more detail in separate specific documents which are linked in the respective section.

Before the actual integration can start, all aspects from commercial side need to be sorted out and some pre-conditions need to be fulfilled. These pre-conditions are explained in more detail in Section 3.1.

If all pre-conditions were sorted out and the relevant contracts and plans are in place, the **Onboarding** process for the service provider can start.

Onboarding to the MIFARE 2GO cloud service includes multiple aspects:

- The successful registration of the service provider in the MIFARE 2GO cloud platform
- The availability of all service provider related information (like contact details, service related city, website, etc)
- The enablement of the service provider on the requested OEM Wallet application (linking the service provider with the responsible OEM for a specific device or technology type (HCE / SE)
- The used MIFARE card technology needs to be settled in the MIFARE 2GO backend (MIFARE DESFire, MIFARE Plus, ...)
- The relevant products need to be defined by the service provider and enabled in the MIFARE 2GO cloud platform
  - Definition on number of used card types / card profiles
  - Definition of card layout (content-wise)
  - Definition of product life-cycle (revocation, extension, top-up, ...)
  - Definition of product purchase and update channels
  - And many more
- The envisioned use cases need to be defined on high-level to estimate which APIs and sequence flows will need to be worked on during the integration phase

After the Onboarding process was finished and all organizational and technical first steps have been arranged and sorted out, the actual **Integration** process with the service provider can start.

The actual integration focusses on implementation of required changes on both the reader infrastructure environment and also the software / backend infrastructure environment. It includes all development effort that`s needed to establish a successful connection between the MIFARE 2GO cloud service and the SPs infrastructure.

The two core aspects of the integration are

- The readiness of the reader terminals for mobile phone usage and the implementation of the required command set. See details to this aspect in Section 3.2.

- The SP backend integration and accessibility to the MIFARE 2GO backend servers. Explanation to this aspect can be found in Section 3.3.

3.1 Integration Pre-Conditions

A pre-condition for a successful MIFARE 2GO integration are valid MIFARE 2GO specific contracts. The legal- and business-related contracts which are required for an integration kick-off are:

- MIFARE 2GO specific contract between the SP and NXP for the specific SP`s installation and infrastructure. For this, please reach out to your local NXP sales representative and your request will be taken care of.

- MIFARE 2GO specific contract between the SP and the chosen OEM, who implements MIFARE 2GO on the client-device side. MIFARE 2GO solutions based on SE or HCE can be available for the SP. For the SP the integration with the MIFARE 2GO cloud service is a one-time effort, independing to which solution will be used by the end customer in the end (HCE or SE). MIFARE 2GO acts as an abstraction layer, connecting the SP´s services with all possible end users, independent of underlying used technology.

- The MIFARE 2GO specific customer engagement plan.
  This plan covers all details of the agreed integration between NXP, the service provider and the OEM Wallet provider.
  It includes important information and timelines and elaborates for example:
  - Scope, timelines, milestones and deliverables of the integration
  - Start of the integration and expected closure
  - Pre-requisites for starting the integration
  - Agreements and contracts which need to be sorted out during the integration phase, as well as milestones highlighting when the mentioned contracts need to be signed
  - Technical requirements
    - Especially for reader infrastructure modifications
    - And for backend modifications

3.2 SP Infrastructure Integration and Modifications

For a successful MIFARE 2GO rollout, the infrastructure of the MIFARE product-specific system must be modified in a way, that the communication between all existing contactless NFC terminals and the MIFARE 2GO equipped client-side devices can happen.

This means that the hardware, firmware, and command implementation of all existing NFC terminals possibly must be reviewed and changed or updated. These changes must be carried out on all available terminals, including:

- Enter / Exit gates of the public transport system
- Ticket-vending machines
- Top-up terminals
- Self-service kiosks
- Terminals and reading devices which are used by the staff (e.g. for ticket vending, ticket top-up or customer information)

3.2.1 Analysis of existing Reader Infrastructure

As a first step before modifying anything on the existing terminals and overall terminal infrastructure, we recommend making an analysis of the current status.

This includes the analysis of the overall number of readers which are used and deployed in the full service provider`s infrastructure.

To make the assessment of the current situation as easy as possible, we provide an infrastructure assessment list which is tailor-made for existing MIFARE systems. This assessment covers many different aspects, including hardware, software and secure memory storage of the individual terminal devices as well as the complexity of the overall system. The checklist can be found in document [5], and is called *"MIFARE Reader Infrastructure Assessment"*.

Additionally to this first assessment, a more details checklist goes into specific aspects of the MIFARE 2GO readiness of the reader terminals.

Specifics to command implementation and firmware readiness on the readers is highlighted in the document [6], *"MIFARE 2GO Reader Infrastructure Checklist"*.

Based on this checklist and the system analysis you will be in a good position to estimate whether the infrastructure is already ready-to-go, and a MIFARE 2GO integration can start, or if there will be some upgrade work required. NXP is assisting you with evaluation of your infrastructure and the recommendation of potential changes that must be done in your system.

3.2.2 Requirements to the Reader Infrastructure

- The terminals of the reader infrastructure must be from hardware and software point of view compliant to ISO/IEC 14443 Layer 1 to Layer 4. The specifics of the ISO/IEC 14443 standard can be looked up in the respective documents, referred in [10], [11], [12], and [13].

- In order to interact with the MIFARE 2GO client device, all readers must implement the required MIFARE command set, which is purely based on ISO/IEC 14443-4. This

means, that all command exchange after device activation, happens solely on ISO/IEC 14443-4.

- Furthermore, all commands between the reader and the MIFARE 2GO client device must be exchanged in the ISO/IEC 7816-4 APDU format. This means, that either standardized ISO/IEC 7816-4 commands are selected for the full transactions, or native MIFARE commands are wrapped into the ISO/IEC 7816-4 APDU format. Find details to the ISO/IEC 7816-4 APDU format in [14].

- Certain command implementations must happen in a defined sequence, as per our recommendation.
  - For example the first exchanged command must be the ISO/IEC 7816-4 specified ISOSelect command, selecting the MIFARE application on the client device.

All requirements and recommendations regarding the reader infrastructure are described in a separate document, [2], and also briefly summarized in a quick checklist in [6]. These two documents focus explicitly on the readiness of the terminals and reader firmware implementation, to start interacting with the MIFARE 2GO virtual card on the client side.

3.3 SP Backend Integration and Modifications

As also required for the terminal infrastructure, also the server-side environment of the SP infrastructure must be prepared and ready for a MIFARE 2GO integration.

3.3.1 Analysis of the existing Backend System

The analysis of the currently available solution of the SP´s backend and server infrastructure is needed, to estimate the status of the server system and to evaluate potential changes which must be implemented.

This includes the analysis of the used technologies, tools, hardware modules and general capabilities of the system.

3.3.2 Requirements to the Server Backend System

- For interacting completely with the MIFARE 2GO backend, the implementation of the required set of APIs and correct parameter exchange with the provided MIFARE 2GO APIs is a must.
- The communication between the MIFARE 2GO server and the SP`s server happens via pre-defined API calls. The API request and response parameters are exchanged via the JSON format.
- Security analysis of the SP`s backend must be performed and possible realization of security hardenings could be advised, for guaranteeing an overall secure system.
- For secure storage of keys and other sensitive data, the availability of an HSM or another secure key storage device in the SP´s backend is recommended.

3.3.3 Implementation of the required MIFARE 2GO APIs

The MIFARE 2GO system exposes several APIs, so that the external SP server backend can reach the MIFARE 2GO server, trigger specific actions and exchange or request data.

Additionally to exposing APIs to the outside, MIFARE 2GO also relies on the availability of certain APIs on the SP`s side. In order that the MIFARE 2GO server can send data to and request data from the SP`s backend system, it`s required that some specified APIs are implemented in the SP`s server backend.

The full set of APIs which are made available by MIFARE 2GO and which are requested to be implemented, is listed and explained in detail in [8].

3.3.4 Server-to-Server communication between the SP Server Backend and the MIFARE 2GO Server Backend

To realize specific use cases, a stable connection between the SP servers and the MIFARE 2GO servers must be established.

For initial testing purposes, NXP issues test authorization credentials which can be used to authenticate against the MIFARE 2GO backend. User authentication is always needed to execute an API call toward the MIFARE 2GO backend, see details in [8].

Once the credentials were exchanged with the service provider and an authentication can be established, the PING API which is exposed from the MIFARE 2GO server backend can be used for testing the connection and the stability of the connection between the SP and NXP.

After all APIs which are needed for realizing defined use cases were implemented, load testing and system stability are recommended to be performed, to guarantee a stable functionality of the overall system.

4 NXP´s complete MIFARE 2GO Offering Step-by-Step

Summarizing and further illustrating the above-mentioned integration steps, the complete engagement and integration plan between NXP and a service provider roughly contains four phases.

1. **Engagement with the NXP Business Development Team**
   This establishes the basis and first technical information can be shared with the SP. Legal agreements must be set up and the overall scope of the project will be estimated and agreed.
   Different MIFARE 2GO offering models will be discussed and the most suitable scope will be customized for the SP individually.

2. **Integration Planning and Onboarding**
   The full scope of the project is worked out in details and the integration is planned in phases. Deep dives and analysis of the SP's backend and reader infrastructure must take place in order to estimate the development work that must be carried out.

3. **MIFARE 2GO Integration and Development**
   Development work which must be executed on SP side includes the realization of required APIs and backend server as well as reader infrastructure adaption.
   NXP´s technical Service Platform team, Field Application Engineers and CAS will support during the ongoing Integration.
   As an end-step of the development phase, interoperability testing, load testing will be done, and potentially a certification process can take place.

4. **Rollout and GO-Live of the System**
   After rolling out the system to the full set of end-users, the operational processes must be established on the SP`s side.
   NXP is offering a 24/7 support according to the individually agreed service level agreements. Furthermore, NXP also offers maintenance support. Here the details depend on the agreed maintenance period in the legal MIFARE 2GO contracts.

5 References

[1] **AN4825xx – MIFARE 2GO Quick Start Guide for SP Integration**
Application Note, this document.

[2] **AN4513xx – Reader infrastructure requirements for MIFARE 2GO**
Application Note, available in NXP Docstore.

[3] **UM4736xx – MIFARE 2GO SP Integration Guide**
Application Note, will be available in NXP Docstore soon.

[4] **AN4826xx – MIFARE 2GO SP Onboarding Guide**
Application Note, will be available in NXP Docstore soon.

[5] **ANxxxxxx – MIFARE Reader Infrastructure Assessment**
Application Note, will be available in NXP Docstore soon.

[6] **AN5333xx – MIFARE 2GO Reader Infrastructure Checklist**
Application Note, available in NXP Docstore.

[7] **ANxxxxxx – MIFARE 2GO PTO Server Infrastructure Checklist**
Application Note, will be available in NXP Docstore soon.

[8] **AN4735xx – MIFARE 2GO API Specification for Service Provider Integration**
Application Note, available in NXP Docstore.

[9] **UMxxxxxx – MIFARE 2GO Support Structure and Support Guidance**
Application Note, will be available in NXP Docstore soon.

[10] **ISO/IEC 14443-1 – Identification cards – Contactless integrated circuit cards – Proximity cards – Part 1**: Physical characteristics. ISO/IEC 14443-1:2016, March 2016, ISO/IEC JTC 1/SC 17.

[11] **ISO/IEC 14443-1 – Identification cards – Contactless integrated circuit cards – Proximity cards – Part 2**: Radio frequency power and signal interface. ISO/IEC 14443-2:2016, July 2016, ISO/IEC JTC 1/SC 17.

[12] **ISO/IEC 14443-1 – Identification cards – Contactless integrated circuit cards – Proximity cards – Part 3**: Initialization and anticollision. ISO/IEC 14443-3:2016, June 2016, ISO/IEC JTC 1/SC 17.

[13] **ISO/IEC 14443-1 – Identification cards – Contactless integrated circuit cards – Proximity cards – Part 4**: Transmission protocol. ISO/IEC 14443-4:2016, June 2016, ISO/IEC JTC 1/SC 17.

[14] **ISO/IEC 7816-4 – Identification cards – Integrated circuit cards – Part 4**: Organization, security and commands for interchange. ISO/IEC 7816-4:2013, April 2013, ISO/IEC JTC 1/SC 17.

6 Legal information

6.1 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.

6.2 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.

6.3 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.

6.4 Trademarks

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

MIFARE — is a trademark of NXP B.V.

DESFire — is a trademark of NXP B.V.

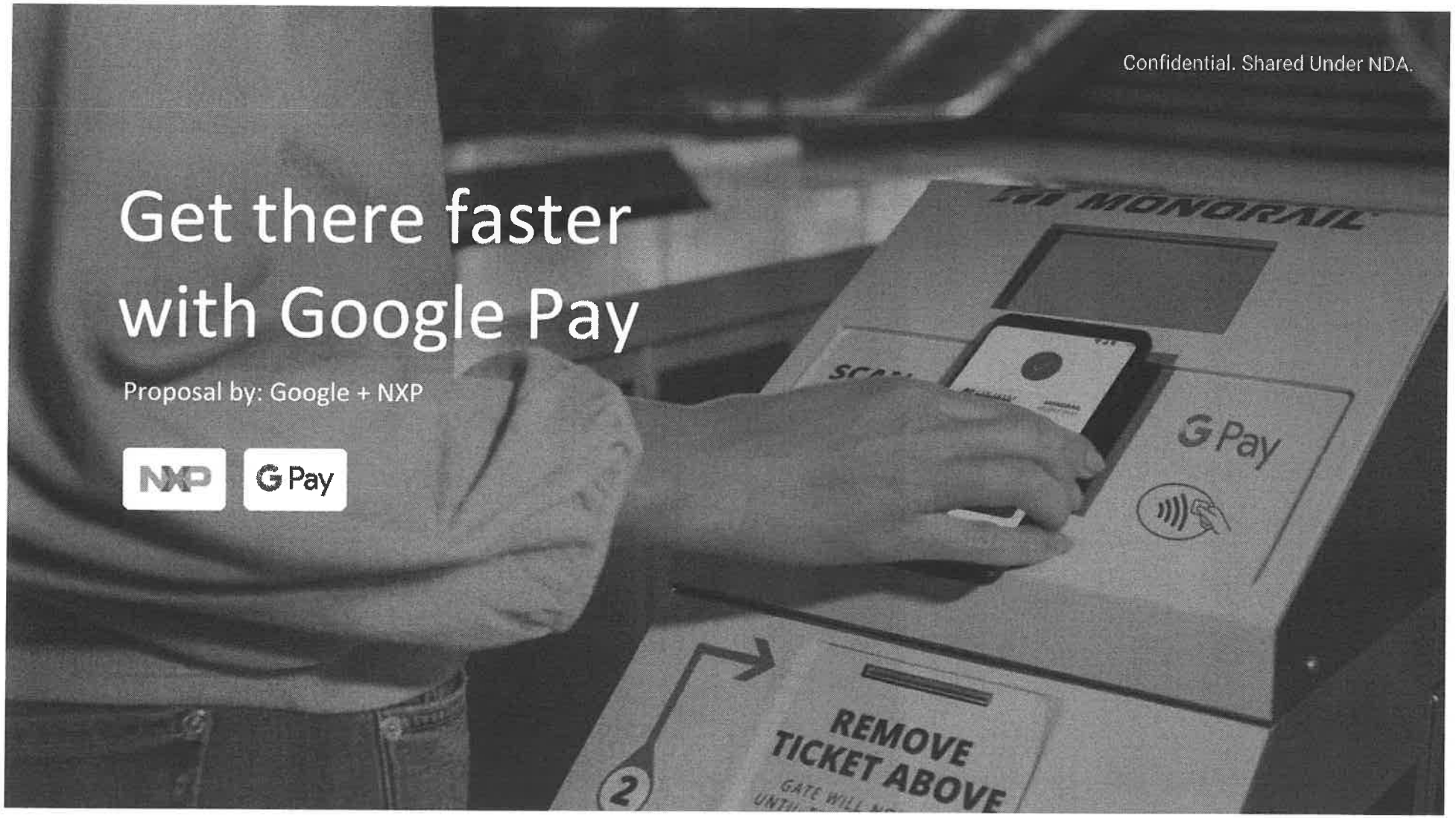
MIFARE Plus — is a trademark of NXP B.V.

Figures

Contents

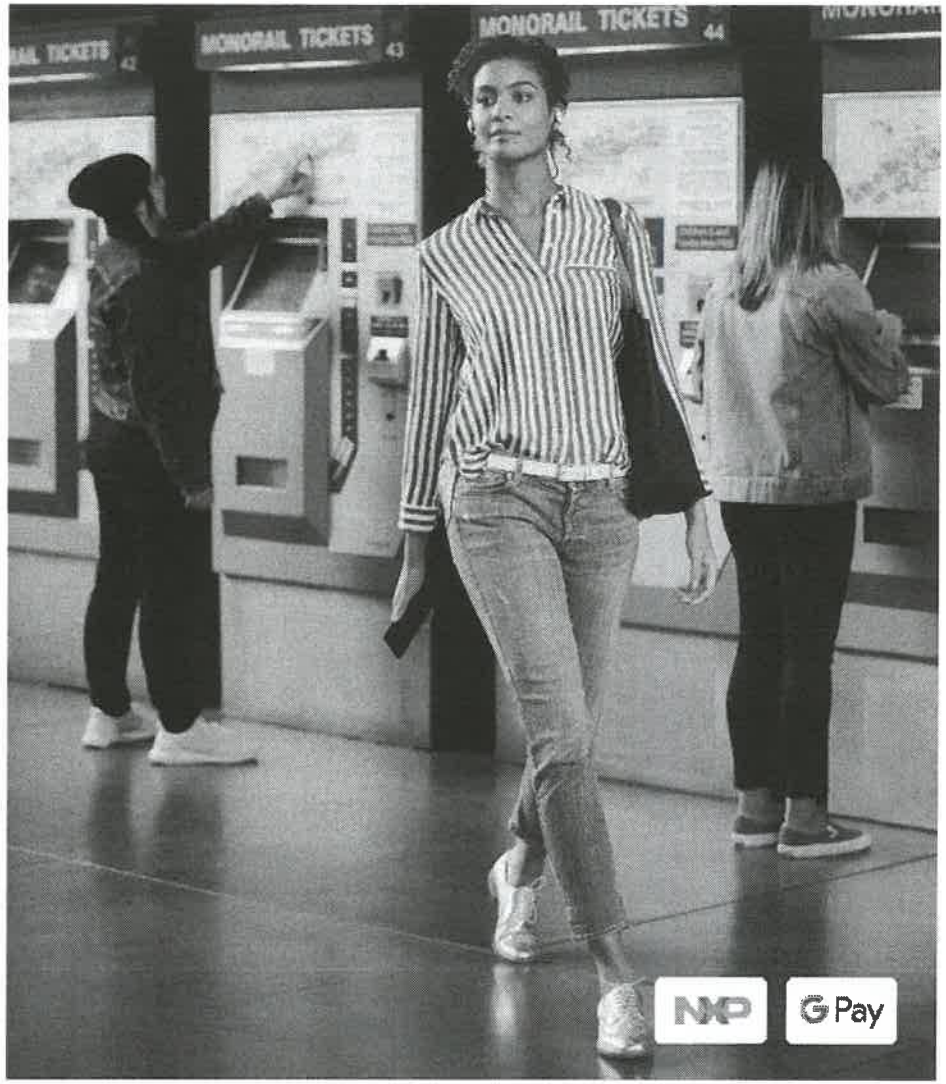
For more information, please visit: http://www.nxp.com
For sales office addresses, please send an email to: salesaddresses@nxp.com

Date of release: 21 May 2019
Document identifier: AN4825
Document number: 482510


Confidential. Shared Under NDA.
Get there faster with Google Pay
Proposal by: Google + NXP
NXP
G Pay
MONORAIL
G Pay
REMOVE TICKET ABOVE
2

Agenda

1. Customer Opportunity
2. Customer Experience
3. Google + MIFARE 2GO Solution
4. Transit Operator Benefits
5. Technical Overview

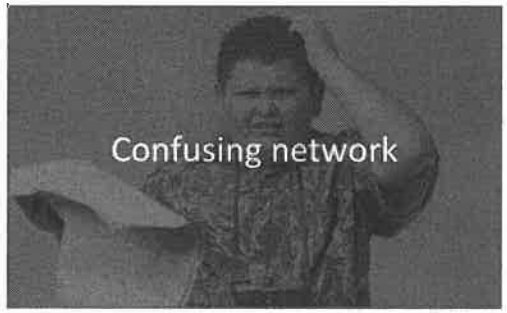


Customer Opportunity

Why partnering with Google - NXP
will improve your customer's experience?

User research highlights primary concerns affecting commuter satisfaction with transit networks:

- Multiple fare options
- TVMs are not consistent and difficult to navigate



- Inherently confusing tunnel network without a map
- No consistent naming conventions for routes
- Navigating from one mode to another is confusing

- Key information (time, space, cost) is not available to users

NXP G Pay

Our Vision - Make it fast and easy for your customers to traverse your area

Amazing immersive transit experience on Android devices

NXP G Pay

We can achieve that vision by leveraging Google - NXP core assets to deliver the following:

Current schedule information
Provide real-time schedules before hand

Simplified fare selection
Help users buy the right ticket for their commute, whether in your app or directly from Google Pay

Advanced warning of ad hoc events
Alert your customers with real-time information as changes occur

Increased awareness
Ability to know & avoid peak travel times, find an empty seat

Simplified planning
Help navigate, predict arrival time

Reminders
Notifications of next stop and direction of travel information on hand

NXP G Pay

Customer Experience

Integrating with Google/NXP, will enable seamless integration
of a virtual transit card into Google Pay,
enabling exciting use cases now and in the future

NXP G Pay

Google Pay is everywhere. Preloaded on devices by major carriers with millions of credit and debit cards on file

Hundreds of millions
Of cards on file

Saved to
Google Accounts

G Pay

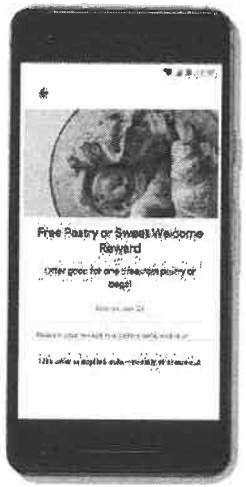
Ready to
pay everywhere

NXP G Pay

Google Pay is more than just about paying at stores and conveying loyalty and offers. It's also about paying for transit.

Payments

Loyalty



Offers

And now.... Transit

NXP G Pay

Google Pay provides options for users to purchase their transit tickets/cards from familiar or new channels

Choose ticket
From any device

Go
The faster, simple way

Receive ticket
In an instant

Buy ticket
In one click

Meet the user
where they are today

- Desktop
- Mobile Web
- Ticket App
- Native in Google Pay

NXP G Pay

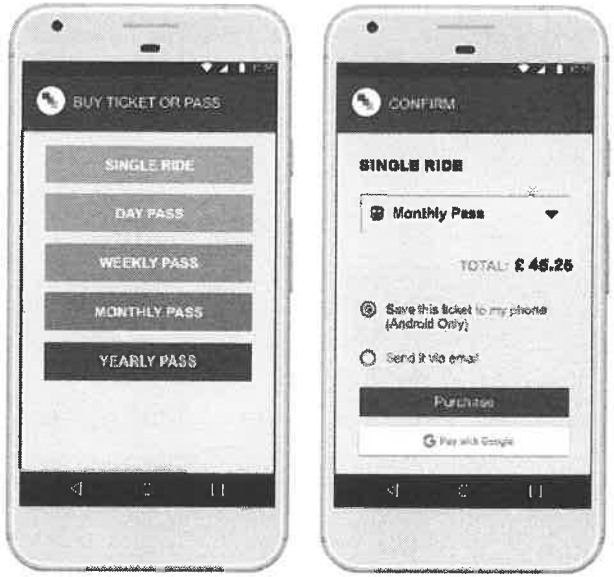
Users can seamlessly buy tickets/cards in just a few clicks with a form of payment previously saved and verified in their Google account

Choose ticket
From any device

Go
The faster, simple way

Receive ticket
In an instant

Buy ticket
In one click



Your application or website

NXP G Pay

No need to wait in line. Users receive their tickets/cards instantly on their phone and they are ready to ride!

Choose ticket
From any device

Go
The faster, simple way

Receive ticket
In an instant

Buy ticket
In one click

Save virtual card to phone

Virtual card instantly provisioned to Google Pay

NXP G Pay

No need to unlock the phone or open up an app. Users save time by holding the phone on the terminal for a simple, fast, reliable transaction

Go
The faster, simple way

Receive ticket
In an instant

Buy ticket
In one click

Choose ticket
From any device

Hold at the terminal

NXP G Pay

Information such as where you can ride and links to refund and lost and found support is helpful to riders and can reduce incoming agency calls

Keep on track
With helpful ride info

Stay in the loop
Get local transit info when you need it

Check your trips
On rich receipts

Rich data when you need it

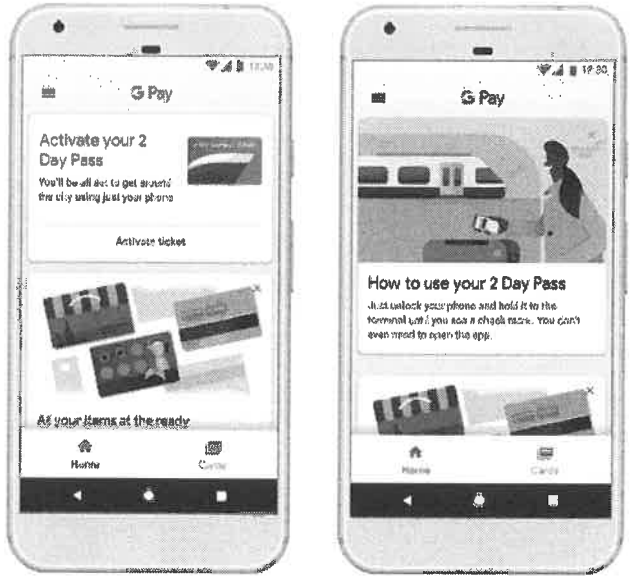
NXP G Pay

Our live feed drives awareness to tourists and commuters - sending a "Get your pass" notification and educating users on how to ride with their phone

Keep on track
With helpful ride info

Stay in the loop
Get local transit info when you need it

Check your trips
On rich receipts



NXP G Pay

Digital rich receipts are provided to the user and help keep track of trips taken and monthly commuter expenses

Keep on track
With helpful ride info

Stay in the loop
Get local transit info when you need it

Check your trips
On rich receipts

NXP G Pay

Solution

Google Pay + MIFARE 2GO

Agencies face challenges that encourage deployment of mobile ticketing

- Cost of paper / smart card issuance and distribution
- Capital of ticket vending machines
- Machine maintenance
- Cost of cash collection

- Limited public service funding
- Limited connectivity to backend offices: no real-time connections
- Large, complex network which is difficult to upgrade

- Unsatisfied users expect mobile ticketing to be available
- Users expecting ease of commute and on time arrivals
- Users choosing alternatives out of convenience e.g., rideshare

NXP G Pay

How can we help? We start with the scale of Android while helping you mitigate the burdensome complexity of mobile innovation

Android is the largest operating system in the world

Over 2 Billion active users

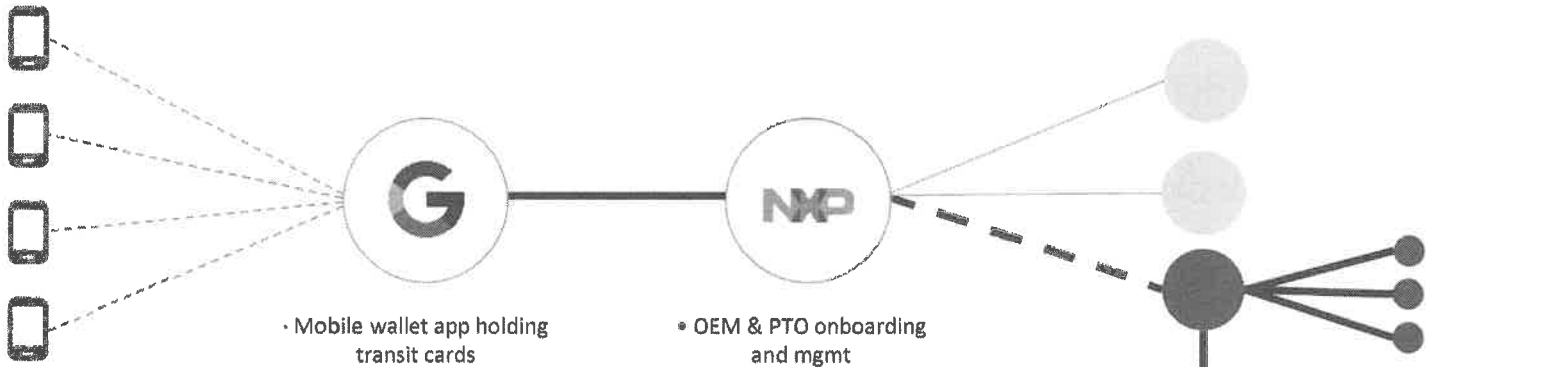
MIFARE the leading non-EMV global contactless scheme

Over 1.2B people on a daily basis

NXP G Pay

Tech Overview & Roles

All Android Devices | Google | Transit Hub Server | Transit Agency | Terminal | Ticket Retail



- Mobile wallet app holding transit cards
- Enhanced user experience & features
- Increase user adoption Go-Marketing & campaigns

- OEM & PTO onboarding and mgmt
- Credential lifecycle Mgmt Perso, Top Up, Transfer, Activate / Deactivate etc.
- Key Management and HSM Services
- Risk Mgmt
- Reporting and Analytics

NXP G Pay

MIFARE 2GO is live and scalable

Maturity

- MIFARE 2GO platform is launched and live
- 24x7 L2 &L3 support
- Yearly uptime of >99.9%
- AOI response time is <700ms
- Hotfix within 5 hours
- 100% uptime since launch, no issue reported

Easy Onboarding
(Sandbox in 48 hours)

- Support all ticket form i.e Passes, Tickets, Stored Value
- Any form of DESFire Structure
- Support of all MIFARE DESFire command OTA
- Can digitize existing physical card with same business validations

Security

- Support multiple type of HSMs
- Support multiple key diversification
- Support multiple key types an crypto

Platform was designed specifically for the MIFARE ecosystem
End-to-End solution testing completed with multiple Transit Operations, System Integrators and Google
Commercial launch and proof points already available

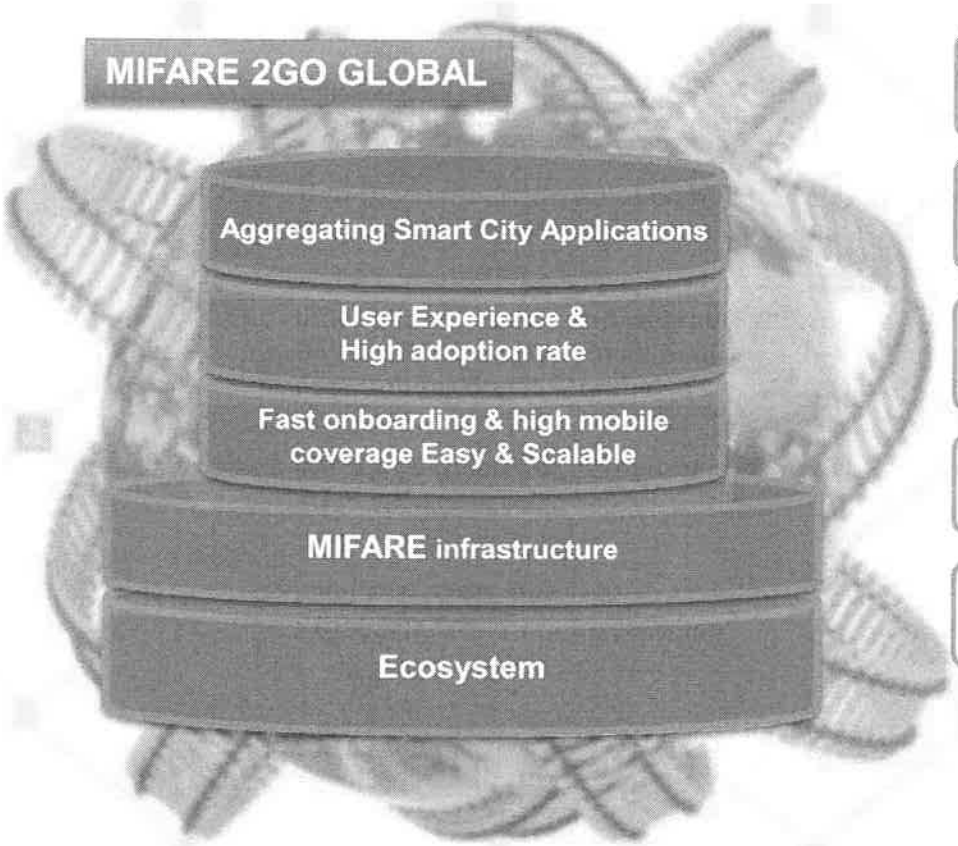
NXP G Pay

Transit Operator Benefits

Distribution, support, performance,
security, reliability, and more!

MIFARE 2GO - A Unique One-Stop-Shop

Mobile Solutions engineered for Service Providers since 25 years



- One Wallet for multiple applications ensuring fast deployment for higher user adoption by lowering fragmentation

- Non-payment driven solution built for Service consumers
- Value added services build around Service

- Independent mobile and wearable OEM coverage
- Full MIFARE support on all platforms (mobile and wearables)
- Fast onboarding (6 Months)

- >77% of Service Infrastructure is compatible with MIFARE 2GO

- >200 FTE (R&D, Integration, Marketing, Sale,....)
- >1000 MIFARE Industry partners

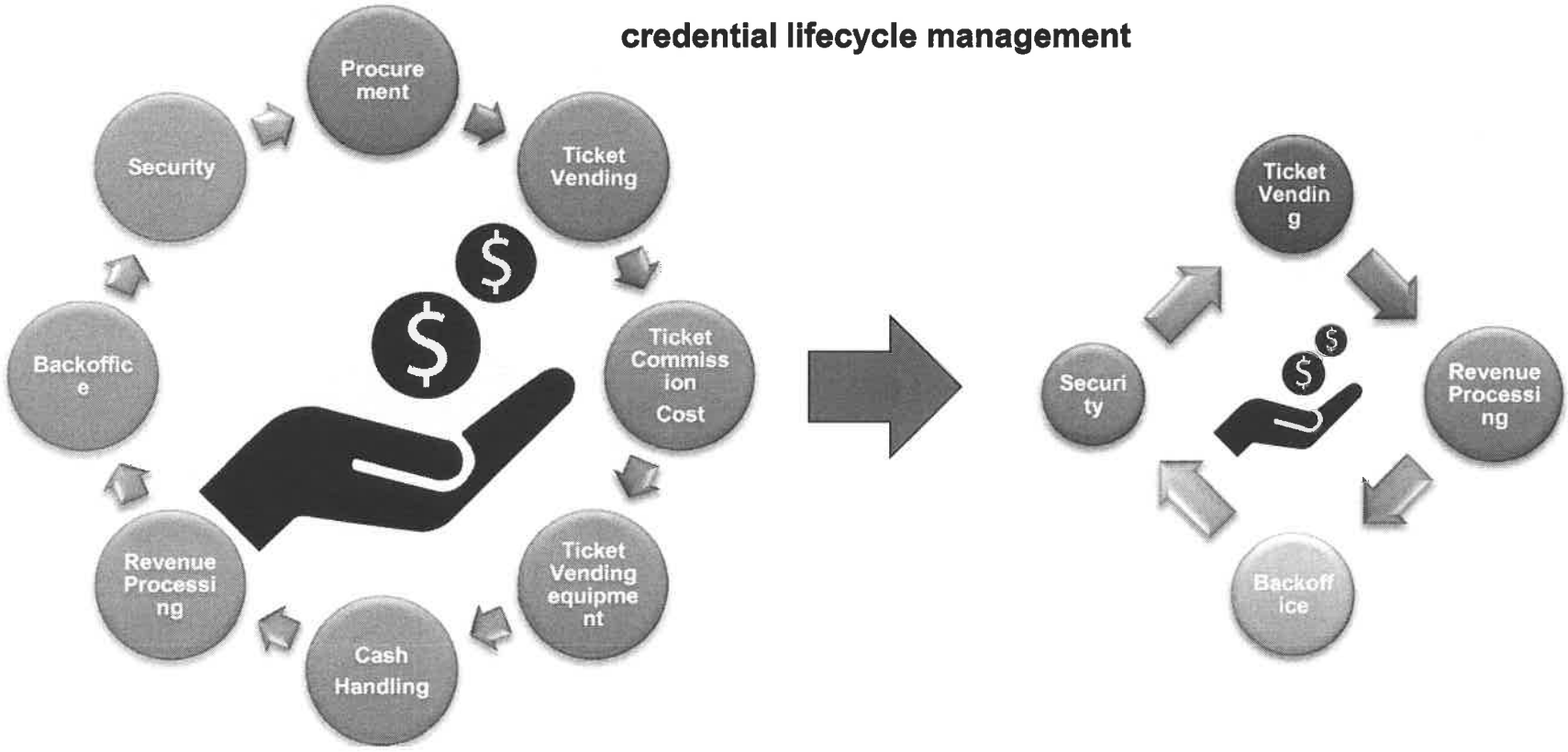
NXP | G Pay

MIFARE 2GO brings cost efficiency

Traditional

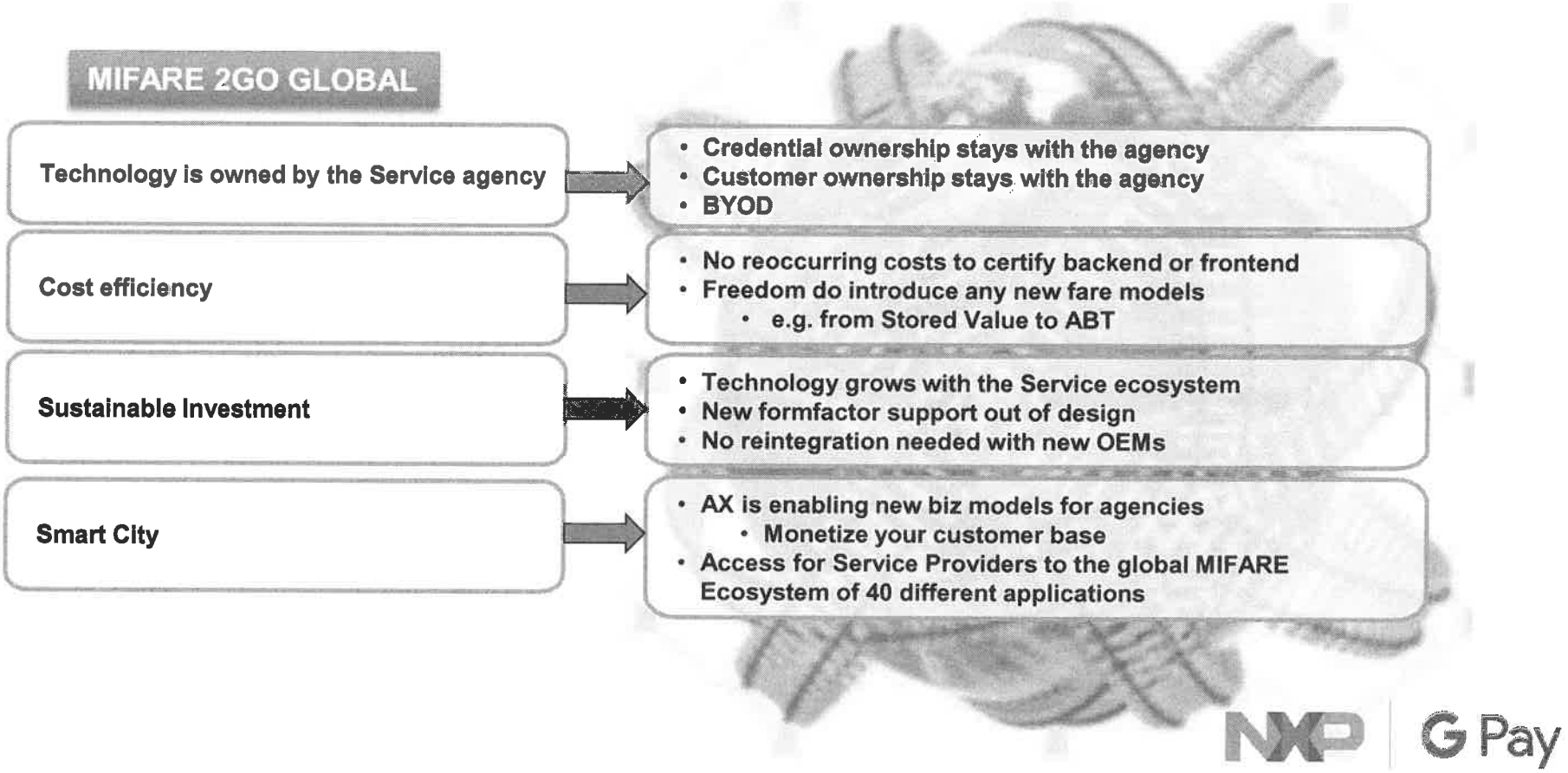
Mobile

credential lifecycle management



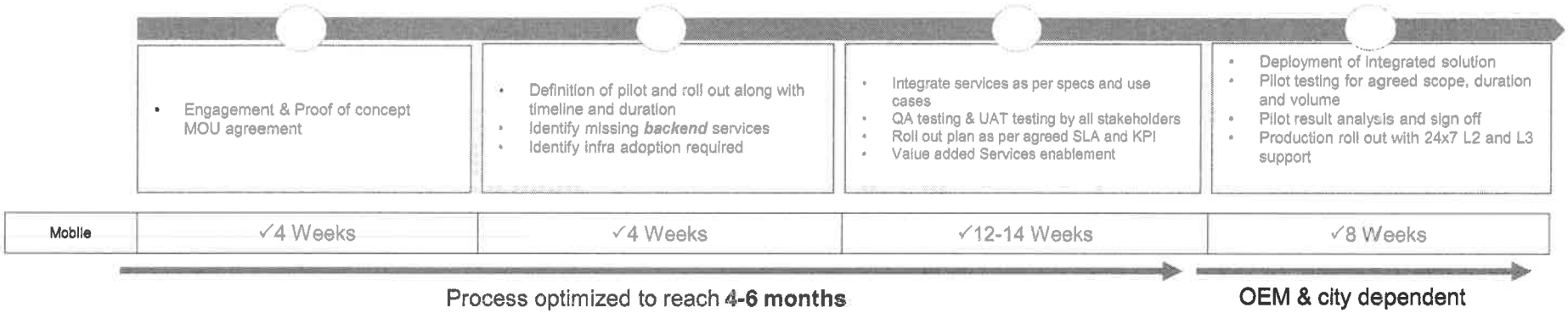
MIFARE Technology – engineered for Service Providers

Solutions for Service Providers since 25 years



NXP | G Pay

Fast deployment & high adoption rates



NXP | G Pay

Strong value of the Google+NXP Integration (1 of 2)

NXP GPay

Strong additional value of Google+NXP Integration (2 of 2)

Distribution

- Access to Google's:
  - Owned and operated properties e.g.,
  - Google Maps, Home, Assistant

  Partnerships with OEMs and Carriers (e.g.,
- Google Pay preloaded on 100 million + devices)
- Future-proof support for evolving form factors and devices (e.g., Fitbit, Garmin)

Performance

- Industry leading security model supported by Google and NXP MIFARE DESFire on the device and cloud
- Fully invested by executive management of Google and NXP

Proven Security

- One transaction protocol (DESFire) across all platforms
- Retrofit into your existing infrastructure
- System-level OS integration enables accelerated and reliable card conveyance

Value

- Future features will come as transparent SW update as part of the continuously driven innovation on user experience
- Extensive (free) digital marketing campaigns across Google channels to drive mobile adoption
- Google Pay call center serves as first line support for mobile ticket operations; 24/7 on-call engineers monitoring Google's systems

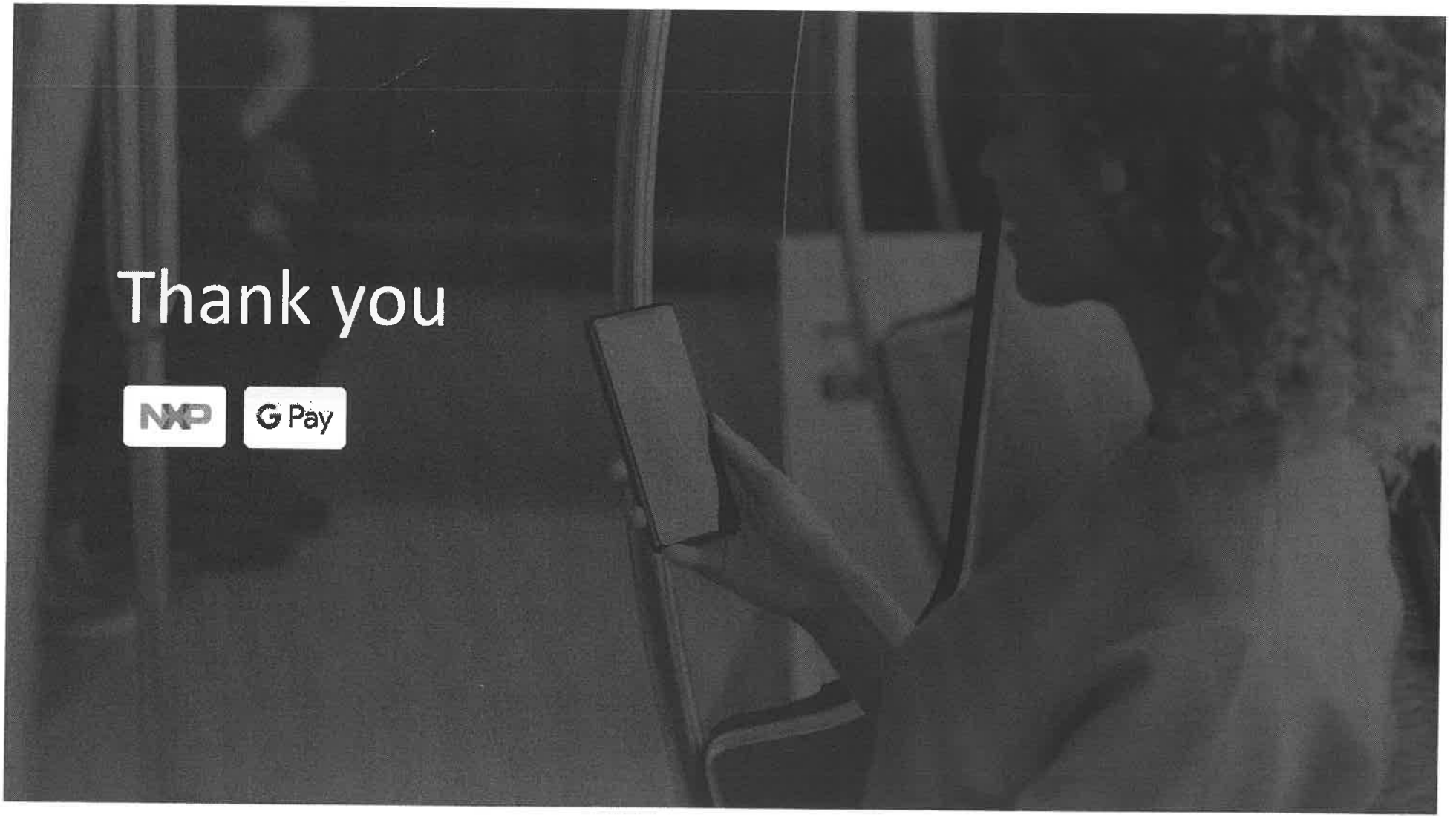
Strong User Focus

- Tight integration with Google enhanced features e.g., live feed, geo-notifications, etc.
- Strong user relationships with existing accounts, credit cards on file, and Google Play Services installed

Device Coverage

Seamless and reliable tap experience tested by Google across entire Android ecosystem

NXP G Pay


Thank you
NXP
G Pay