A Series of White Papers on Mobile Wallets
Part 2

Control Points in Mobile Wallets

Mobile Wallet Task Force

Mobey Forum, February 2012

Mobile Wallet Task Force

Chair:

Amir Tabakovic	PostFinance, Switzerland

Contributors:

Shaun Abraham	Bank of America
Jonathan Bye	Royal Bank of Scotland
Terje Larsen	DNB Bank
Kristian Thure Sorensen	Nykredit
Wim Westerhof	Rabobank
Olivier Denis	SWIFT
Georg Fasching	Luup
Lara Hiess	PEACHES
Christian Mari	Oberthur Technologies
Sirpa Nordlund	Mobey Forum
Gerhard Romen	Nokia
Ville Sointu	Tieto
Fred Stortelers	FSM Consultants
Per Harald Strom	Nets
mChannel working group	European Payments Council

Editor:

Tim Haines	Armitage Communications

Contents

1 Executive Summary

News stories and articles about mobile wallets, their deployment and use are appearing more frequently in the media. There is clearly much interest in the commercial potential of mobile wallets by a variety of organisations in the communications and financial industries and beyond. There is also considerable jockeying for market position among key players striving to win the interest of consumers.

As with any new commercial proposition, the early stages of development are extremely important to its ultimate success or failure. Mobey Forum believes that the most effective way for the industry to create successful mobile wallet business is by adopting an open systems approach in which any mobile wallet can access and be served by multiple content providers.

To this end, it is important to set out and understand how the mobile wallet ecosystem can be influenced by various stakeholders. An essential component of mobile wallet operation that enables a mobile wallet stakeholder to influence how a part of the ecosystem operates is defined as control point. Mobey Forum suggests that a clear description of specific control points would be helpful, because that shows how the many different stakeholders can become involved and influence the building and operation of the mobile wallet ecosystem.

Mobey Forum has identified the following control points:

- **Connection from and to the mobile wallet:** Controls which types of mobile device, operating system and mobile wallet implementation can be connected to relevant services and controls the delivery of content according to the designated user level.

- **Distribution channels for the mobile wallet:** Controls the distribution of the mobile wallet and application to the user.

- **Customer acquisition and enrolment:** Controls how users are signed up to mobile wallet services. Acquisition and enrolment is key because it controls the main access route to existing customer segments and marketing channels.

- **Bearer / connection technology:** Controls the various bearers and connection technologies needed for interaction between the mobile wallet on the device and relevant services.

- **Channels to get value into and out of the mobile wallet:** Controls how users put funds into their mobile wallets and how they can transfer value to a merchant or other individual.

- **Data flow:** The data flow to and from the mobile wallet can be controlled by a variety of stakeholders and intermediaries.

- **Data ownership:** The variety of data around mobile wallets is wide, encompassing payments, commerce, products, location, preferences, loyalty and more. The use of such data should always be under the consent of the end user.

These control points help to manage how a mobile wallet is set up and used. The first three control points in the list above govern mobile wallet initiation. They help to ensure the user has the right device and determine how the mobile wallet application is installed on the mobile wallet and how the user activates the installed mobile wallet.

The other control points enable the mobile wallet to be used. They manage how the mobile wallet connects to the network, how the data flow is organized, which stakeholder has access to this data and how the value gets into and out of the mobile wallet.

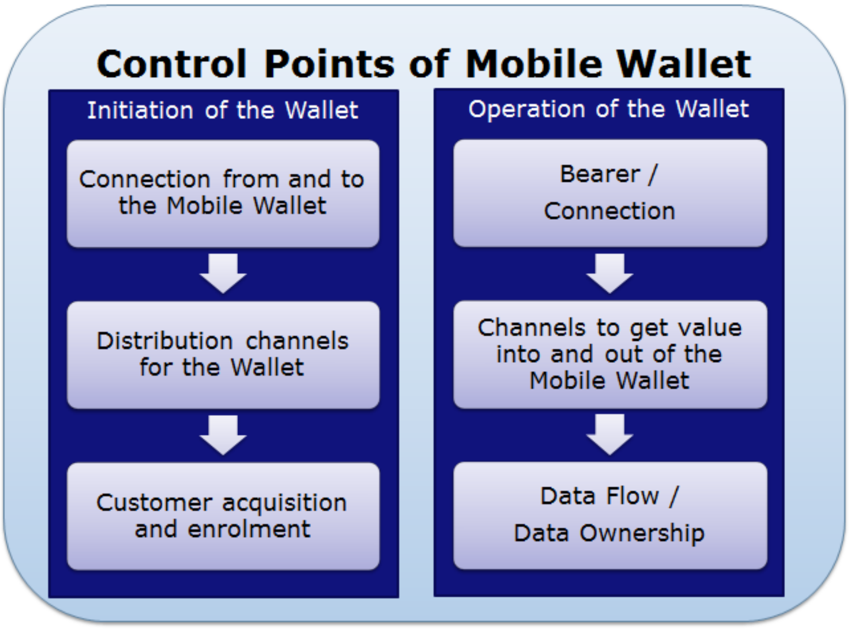

Control Points of Mobile Wallet
Initiation of the Wallet
Connection from and to the Mobile Wallet
Distribution channels for the Wallet
Customer acquisition and enrolment
Operation of the Wallet
Bearer / Connection
Channels to get value into and out of the Mobile Wallet
Data Flow / Data Ownership

Figure 1: There are two groups of control points that govern how a mobile wallet is set up and used

These control points provide a framework for stakeholders to cooperate in the operation of the mobile wallet. They also enable a clear understanding of who controls specific aspects of the mobile wallet and to help avoid conflict between overlapping stakeholder interests.

2 Introduction: The aim of this white paper

Mobey Forum is publishing a series of white papers about mobile wallets. The first white paper, “Mobile Wallet – Definition and Vision”, gave an overview of mobile wallets and described the importance of an open platform for mobile wallets.

This second white paper in the series covers the control points that can be applied to all types of mobile wallet implementation, regardless of the underlying connection technology. Mobile wallets may connect via proximity technologies, such as Near Field Communication (NFC) to a point of sale, or communicate over distance, at an entirely different location to the point of sale, for example for online payments or for person-to-person money transfer.

A mobile wallet control point is an essential component of mobile wallet operation that enables a mobile wallet stakeholder to control how a part of the ecosystem operates.

The paper aims to address fundamental issues such as:

- What are the Control Points?
- Who are the potential Control Point stakeholders?

The white paper will also map some existing mobile wallet systems to the defined control points, and de-mystify the essential components of mobile wallets independent of the technologies and business models being used.

There is currently much hype around the mobile wallet, but little analysis. With these white papers, Mobey Forum addresses this shortfall and provides some clarity on the topic for financial organizations and other stakeholders

In particular, this white paper describes an approach based around specific control points that provide a neutral way to ascertain how stakeholders are placed to manage these points.

3 Mobile wallets: The industry challenges

Implementing a mobile wallet is not easy. It is one thing to agree on the theory (which can prove to be difficult in itself), but another to agree on the practice.

From a user perspective the physical wallet has the distinct advantage that it is ubiquitous in terms of what can be put into it. It is possible to mix and match the contents according to individual needs, and even competing brands coexist peacefully within the physical wallet. The only standardization implemented is the size of payment cards.

The look and feel of the mobile wallet, compared to a physical wallet, is another important consideration for stakeholders.

While most users have only one physical wallet, they may have multiple virtual wallets, but they must be able to see significant benefits to be motivated to shift to a mobile wallet. These benefits could include a better user experience, greater convenience, higher security or other value-adding services not available within the physical wallet.

With many industry players vying for position in this nascent market, standardization and interoperability are likely to be difficult to achieve. Many players see the mobile wallet as a new opportunity to interact more strongly with their customers. This can lead to many competing solutions and a fragmented market, which will make potential users hesitant about adopting a mobile wallet.

Through cooperation, representatives from the various parts of the industry will be able to address these issues and develop common business models and technical standards. If this does not happen, the market itself is likely to decide which solution will become the de facto standard, potentially enabling a majority of control points being dominated by single players.

Mobey Forum believes the need goes beyond just reaching agreements on standards. By putting into place business models that cover the whole ecosystem, the industry will be able to address issues like compliance, governance, liability, security, support and more.

It's important to keep in mind, however, that the consumer will take the lead while choosing which mobile wallet to use, meaning considerations should include consumer benefits and convenience.

4 Setting some common terminology

Mobile wallet ecosystems are in their early stages with a variety of players from different backgrounds contributing to their development. This inevitably leads to different terminology being used to describe similar concepts. To avoid confusion it is important to set some common terms that can be used universally by all players.

In this series of white papers, Mobey Forum proposes the following definitions for some of the new terminology used in this paper:

Mobile Wallet Ecosystem
All the services and infrastructure that enable and support mobile wallets and their use.

Mobile Wallet
The functionality on a mobile device that can interact securely with digitized valuables.

- **Mobile Wallet Content**
  Digital content residing within the mobile device and on secure servers that provides value or is of value to the mobile wallet user and one or more stakeholders. The mobile wallet could contain different tradable value including currency and other value such as coupons, loyalty points, credits or virtual currencies.

Mobile Wallet Control Point
An essential component of mobile wallet operation that enables a mobile wallet stakeholder to control how a part of the ecosystem operates.

Mobile Wallet Stakeholder
Any organization or individual that provides, provisions, or uses mobile wallets and their associated content and ecosystem. The key groups of mobile wallet stakeholders include:

- **Mobile Wallet Provider**
  The organization/brand that issues the necessary mobile wallet functionality to the Mobile Wallet User.

- **Mobile Wallet Content Provider**
  The organization/brand that issues content for use in the mobile wallet.

- **Mobile Wallet User**
  An individual who uses a mobile wallet and manages its content to control their personal data and access financial services remotely.

- **Payment Service Provider**
  A bank, financial institution or mobile network operator that holds a licence to provide mobile payment services.

5 Mobile Wallet Stakeholders

A wide range of mobile wallet stakeholders from different backgrounds and with a variety of motivations is essential to ensure robust, competitive and effective mobile wallet services for users. The mobile wallet ecosystem is dynamic and fast-developing, with potential for stakeholders to take on additional roles and for new players to enter the market. For example it is conceivable that banks, mobile network operators and device manufacturers will see increased representation from technology firms looking to control market share of the mobile wallet by trading access to their customer base for access to the mobile wallet, or using the mobile wallet to leverage their own services.

This section outlines the key mobile wallet stakeholders.

5.1 Banks and other payment institutions

As the institutions that handle their customers' financial services through various channels, it is natural for banks and other payment institutions to aspire to leading roles in mobile wallet services and position their brands in this new financial environment. Banks and payment institutions are also well placed to bring additional value to mobile wallet transactions in the form of trust and security, as well as personal financial management tools.

With their existing payment infrastructure and services, banks bring several important contributions to the ecosystem. Banks are highly trusted by people to handle personal financial management and have the security processes and systems in place to do so safely. The banks already hold customers' financial accounts and are established issuers of payment cards and other instruments.

On the other hand, banks' legacy payment systems may present some challenges in adapting quickly enough to the fast pace of developments in mobile phones and wallets. To take advantage of the opportunities as they arise will require innovation and flexibility. Banks and other payment institutions will need to address issues such as time to market, speed of execution, new security and authentication schemes, as well as gaining a solid understanding of the opportunities of using mobile devices.

5.2 Payment Scheme Owners

Several Payment Scheme Owners such as American Express, MasterCard and Visa have high interest in mobile wallet development. These scheme owners are clearly motivated to address mobile wallet opportunities in order to support their customers (the financial institutions) and thus widen their financial services business and strengthen their brand position in mobile services, mainly in the mass (High Street) market.

Card schemes are present across existing point of sale networks and support established payment instrument issuers and acquirers. Therefore, payment scheme owners are likely to be essential contributors to the mobile wallet ecosystem. They also have existing, proven security infrastructure to bring to the table.

Currently much of the development is centred on international payment card scheme owners. However, it is not yet clear what the intent of and implementations by the international card scheme owners with regards to mobile wallets will be.

There are also mobile wallet-related scheme-driven initiatives from non-card payment schemes such as PayPal. Other initiatives in effect create a “virtual and physical payment scheme” such as M-PESA.

5.3 Device Manufacturers

Mobile device makers will be able to use their strong branding and their sales and distribution to promote their handsets to consumers. This will also lend further credibility in consumers’ minds about the capabilities of mobile wallets.

The contribution of device manufacturers to the ecosystem comes principally from their control of the device hardware, ensuring that the necessary functionality can be integrated into the device to deliver an excellent customer experience.

However, while some manufacturers enjoy direct contact with large numbers of users, this is not true of all device makers. Furthermore, they will need to develop partnerships in order to benefit from opportunities arising from local service usage.

5.4 Merchants

Merchants and retailers already play a significant role in the success of mobile payments. Similarly, their involvement and commitment is vital for the success of the mobile wallet.

Mobile wallets can offer merchants a new way to interact with their customers. Merchants already enjoy good payment systems in the form of debit and credit cards. They are more likely to invest time and resources in accepting mobile wallet payments if they are popular with customers and are more cost effective, faster, easier and safer than other payment methods.

An added incentive may also come in the shape of the mobile wallet being an effective way to establish brand exposure and closer customer relationships by offering loyalty incentives, discounts and other marketing offers.

5.5 Mobile Network Operators

The business of being a Mobile Network Operator (MNO) has changed substantially in recent years. Transforming from simply managing network infrastructure that delivers basic communications services, MNOs increasingly seek out new ways to generate revenue from services and build greater customer loyalty. Mobile wallet services can provide just such an opportunity.

MNOs can be significant contributors to the success of mobile wallets because they hold the mobile communications services customer base, control the network and SIM card and have the capability to put the required applications and functionality onto their customers' mobile devices via the SIM card. MNOs can also contribute extensive distribution networks with widespread retail outlets.

However, most MNOs have limited experience of the payments industry compared to other players. This can be a reason for new partnership relations with financial institutions. Some of today's mobile wallet implementations may be driven by the need for customer retention rather than as business cases in their own right.

5.6 Operating System Providers

Mobile device Operating System (OS) providers are motivated to address the mobile wallet market because it gives them an opportunity to widen the range of services available via their OS and create new marketing messages.

OS providers, such as Google, can embed and control vital security provisions and native applications for mobile wallet into their OSs and dynamically update them to ensure that devices remain secure as the market develops. They are also critical in ensuring a high-quality and convenient end-user experience of mobile wallet.

5.7 Public and legal authorities

Public organizations (for example in health care) and legal authorities (for example tax bodies) can use mobile wallets to help administer consumer services and identification credentials such as passports, driving licenses, social security numbers, tax identification numbers, digital signatures and health cards.

It is a regulatory requirement in some countries to identify customers through a government process when providing online payment solutions. It could be favourable for government authorities to be able to integrate existing national identity providers into the mobile wallet authentication scheme.

These contributions to the mobile wallet ecosystem come from public and legal authorities' wide scope of influence and the connection to the public. Roaming mobile wallet use will encounter challenges created by different national regulations in each country, caused by a lack of harmonization leading to a need for standardization and interoperability.

5.8 Users

It is the users that generate value for the other stakeholders in the ecosystem by selecting handsets, making transactions, accepting coupons, and generally creating data. Users will experience the feeling of having value in their mobile wallets, regardless of where that actual value is stored and will be driven by convenience, cost and the offerings from the other stakeholders in the ecosystem.

Users may control which mobile wallet they want to use and which content they want in their mobile wallet by making the necessary arrangements with the mobile wallet content provider and mobile wallet provider.

Market conditions and available distribution channels will determine the choice open to the user – see section 6.2.

5.9 Value Added Service Providers

Internet technology companies, such as Amazon, Google, Groupon and Paypal have built extensive ecosystems to support online value-added services that serve huge numbers of customers. For these players, a mobile wallet is another application that fits into their ecosystem by providing mobile commerce services to their customers, as well as new mobile-specific, commercially-relevant customer data (such as one user per device and geo-location).

Value added service providers fulfil their corporate customers' (merchants) needs by offering technology-based consumer profiling (customer relationship management, persuasion profiling), acquisition (advertisements, online stores, couponing) and retention (loyalty programs). A mobile wallet opens up several new opportunities through frequent use of the device hosting the mobile wallet application; clear consumer identification; payment capabilities; the potential to integrate existing content; and to bridge the gap between online commerce and proximity payment at the merchant point-of-sale.

6 Mobile Wallet Control Points

A mobile wallet control point is an essential component of mobile wallet operation that enables a mobile wallet stakeholder to control how a part of the system operates. Control points can drive the business model, the gains for some of the stakeholders and implementation options for mobile wallets.

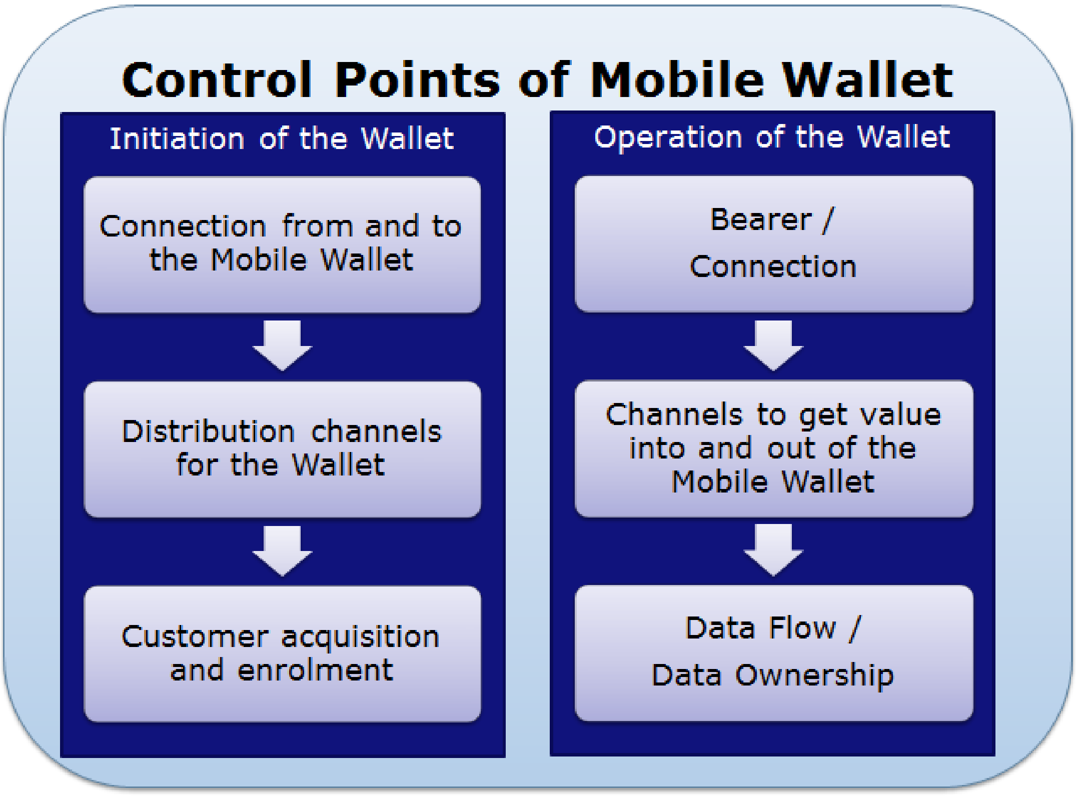
Mobey Forum has identified the following control points:

- Connection from and to the mobile wallet
- Distribution channels for the mobile wallet

- Customer acquisition and enrolment
- Bearer / connection technology
- Channels to get value into and out of the mobile wallet
- Data flow
- Data ownership

Figure 2 shows that these control points fall into two main groups. The first group concerns the initiation of the mobile wallet. The control points determine if and how users can enable a mobile wallet application on their devices. They help to ensure the user has the right device and determine how the mobile wallet application is installed on the mobile wallet and how the user activates the installed mobile wallet.

The second group of control points concerns the operation of the mobile wallet. These control points enable the mobile wallet to be used. They manage how the mobile wallet connects to the network, how the data flow is organized, which stakeholder has access to this data and how the value gets into and out of the mobile wallet.



Control Points of Mobile Wallet

Initiation of the Wallet

Connection from and to the Mobile Wallet

Distribution channels for the Wallet

Customer acquisition and enrolment

Operation of the Wallet

Bearer / Connection

Channels to get value into and out of the Mobile Wallet

Data Flow / Data Ownership

Figure 2: Control points and how they enable and manage the use of mobile wallets

6.1 Control points for the initiation of the mobile wallet

6.1.1 Connection from and to the mobile wallet

Access management controls which types of mobile device, operating system and mobile wallet implementation can be connected to relevant services. Access management controls the delivery of content according to the designated user level, for example authentication or authorization of the mobile wallet content.

The mobile wallet provider is the prime candidate to controls the connection from and to the mobile wallet.

6.1.2 Distribution channels for the mobile wallet (not the content)

This channel is used to distribute the mobile wallet/wallet application to the user. It is the mobile wallet stakeholders listed below that are likely to determine which channels are available to take the product to market.

This control point encompasses not only the initial distribution of the mobile wallet but also redistribution, software updates and more, as well as blocking of the mobile wallet should a user lose their phone.

The technology for distributing mobile wallets to end users can include Bluetooth, direct download from a server, side-loading through a data cable and installation from a memory card. These all have different uses in the market but are too fragmented to describe in this white paper.

Device manufacturers
Mobile wallet capability may be embedded in a hardware manufacturer's devices, for example like an e-mail client or a dedicated preloaded application. Updates and new releases could be made through firmware upgrades directly on the device. In situations where the device is otherwise locked down, the integration of a preloaded mobile wallet is a reliable way of including a graphical user interface for a mobile wallet service.

OS platform vendors
Operating system platform vendors can implement mobile wallet functionality as part of the operating system similar to today's messaging, calendar and contacts. *(For further details, see "Mobile Wallet – Definition and Vision", Mobey Forum, section 3 "Motivation and market for mobile wallet").*

MNOs
A mobile wallet can be distributed through an MNO's retail or online channels. In most cases, MNOs would distribute a mobile wallet by using their real estate, the SIM card with the mobile wallet application on it. Typically, MNOs offer a limited number of device manufacturers and models, enabling the mobile wallet application to be pre-installed on selected devices.

Application stores
Application stores are a distribution channel to be implemented as a downloadable application to the mobile device. The mobile wallet can be distributed through OS providers' market stores such as Apple Appstore, Android Market Windows Phone Marketplace as well as through other independent App Stores. This also enables the application download to be used for marketing purposes while focusing it to countries in which the mobile wallet operates.

Some banks operate their own application distribution channel because of commercial, legal or security considerations.

Other distribution methods
Other methods exist to distribute the mobile wallet to end users, including Bluetooth, direct download from a server, side-loading through a data cable and installation from a memory card. These all have different uses in the market but are too fragmented to describe in this white paper.

6.1.3 Customer acquisition and enrolment

The acquisition and enrolment of users involves business processes for signing up users to mobile wallet services, including but not limited to registration, marketing, education, promotion and training. Acquisition and enrolment is key because it controls the main access route to existing customer segments and marketing channels.

The enrolment control point also includes the provisioning of the authentication credentials into the mobile devices to enable payments, especially for card-based payments using NFC. The one who owns the credentials, that is the keys for the Secure Element and the one who controls the provisioning of the Secure Element have the ability of gatekeeping who is in and who is not in. This is true for the various types of secure elements, which are described in Mobey Forum's White Paper 'Alternatives for Banks to Offer Secure Mobile Payments', whether they are embedded, on the SD card or on the SIM.

Note: Alternatives for Banks to Offer Secure Mobile Payments is available at: http://www.mobeyforum.org/Press-Documents/Press-Releases/Alternatives-for-Banks-to-offer-Secure-Mobile-Payments

The control point is typically owned by:

- **Banks and other payment institutions.** These organisations have the experience and obligation to carry out the Know Your Customer (KYC) process that is usually needed when a payment instrument is issued. They also have the cash management products that merchants need for receiving payments in an orderly way. Finally, they have access to a large customer base.

- **Mobile Network Operators (MNOs).** Some large MNOs are well positioned for this process because they have access to large numbers of customers and because they typically have a large physical network of agents and outlets. In many markets, MNOs subsidise devices, giving them close control over which mobile wallet implementations are accepted in their networks. An important issue is that an MNO can pre-install mobile wallet software on the phone – the first point of contact with the mobile wallet for the consumer.

- **Merchants or public institutions** (for example a public transport company). Although the role of a merchant or public institution is typically to issue applications to the mobile wallet, in some markets they may also control the acquisition and enrolment process. These stakeholders possess an existing relationship with a large customer base and are familiar with customer identification and marketing.

- **Other Mobile Wallet Providers.** The mobile wallet provider can be several of the key stakeholders described in chapter 5, or any other player able to target a large customer base. This is a new role in the market, and it is too early to define with confidence which stakeholder or stakeholders will typically adopt this role.

Acquisition best practices help to ensure that users can easily obtain mobile wallets. Furthermore, individual mobile wallet content can have identity requirements specific to the market or the mobile wallet content provider and these may broaden the generic mobile wallet acquisition and enrolment process.

6.2 Control points for the operation of the mobile wallet

6.2.1 Bearer / connection technology

Access management supports the various bearers and connection technologies between the mobile wallet accessed on the mobile device and the end points related to the mobile wallet content. The control point is used to set connection exclusivity, cross-network compatibility, or to limit specific connection types.

These bearers commonly include SMS, USSD, WAP, Bluetooth, NFC, Wi-Fi, cellular technologies (GPRS, EDGE, WCDMA/HSPA, LTE) or other means. Another bearer is the contactless interaction between a mobile and a point of sale terminal as part of a card model payment, though this is not directly connected to the mobile wallet as such.

As an example, USSD or SMS bearers may require the use of a short code. The allocation of this short code is usually done by the MNO. By requiring all MNOs to allocate the same short codes for mobile wallet services, a country can ensure users can benefit from mobile wallet services on multiple networks. In several mobile wallet schemes in emerging markets, a common short code has not been negotiated, thus limiting the user to a single network.

Stakeholders for this control point include MNOs and device manufacturers.

6.2.2 Channels to get value into the mobile wallet (the content)

To make payments from the mobile wallet, the user will need at least one channel to add or access funds. Depending on the implementation, this could be a direct link to their bank account or credit/debit card, or via dedicated mobile accounts, for example stored value/prepaid accounts. New virtual currencies are on the horizon, examples include Facebook credits or Linden dollars (Second Life), but they will need broader acceptance across regions and countries and may be subject to central bank or regulatory approval.

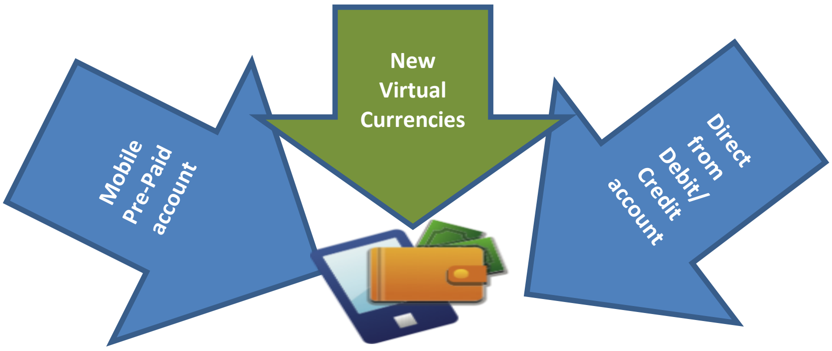


Figure 3: Channels to get financial value into the mobile wallet

Value can also be added into the mobile wallet in the form of coupons or special offers.

These channels will typically be controlled by banks, other payment institutions or the issuers/managers of virtual currencies. They will vary depending on the type of market. In many rural areas of cash-heavy societies with little access to bank branches or cash machines, agent networks licensed by mobile wallet stakeholders will facilitate cash deposits and withdrawals, help with account registration and administration, and offer other services relevant to mobile wallets and their content.

6.2.3 Channels to get value out of the mobile wallet (the content)

Using the value in the mobile wallet requires a channel or channels for interaction between the mobile wallet and a given merchant or between two individuals in order to transfer value or pay for goods and/or redeem coupons or loyalty points. These interaction channels will use both remote-based (online initiated from the mobile device) and proximity-based (NFC) technologies.

This payment channel can be one of the existing payment instruments, but can also be combined with other channels for coupons and loyalty, as is the case with the Google Wallet, or simply to transfer value between two users.

6.2.4 Data flow

Controlling the data flow can be achieved through various means – managing the transaction/session, providing the interconnection between payment networks, and any protocol conversion point (man in the middle).

Ownership of the data flow control point belongs to stakeholders who control specific parts of the ecosystem. This can, for example, be an MNO, if traffic is bound to a specific network. It could also be the encryption of the Secure Element (SE), because a payment service provider can only provide data having the encryption / decryption keys.

Even in an open mobile wallet ecosystem, certain intermediaries can control the data flow between stakeholders.

6.2.5 Data ownership

Data ownership can encompass any financial transaction data, not just the payment but extending to commerce, products, location, preferences, loyalty and many more. The control point is the use of that data by the owner for various commercial or other purposes or to allow its use with and by other parties.

Data ownership is a particularly sensitive topic in financial services. The heavily regulated payment industry is rightfully concerned about customer and payment data in unregulated, recent transactional ecosystems.

In most countries, banks and other payment institutions are prohibited from using payment data outside their own domains. While this is still the case in mobile wallets and online payments, the question of who really owns the data remains unanswered. Customers believe they own the data they produce. Retailers believe they own the data that customers produce when buying their products. Meanwhile, payment institutions have a legitimate requirement to keep payment and transaction data secure and private.

While the issue of data ownership clearly extends beyond the mobile wallet ecosystem, the introduction of mobile wallets creates new considerations because it involves combinations of different stakeholders and industries to generate new data.

This new data can be combined with existing data and used in many ways. Examples include making the data anonymous to provide business intelligence, and using the data to personalize content and services for customers.

Data control outside specific transaction and payment information processes is currently largely unregulated for new services such as mobile wallet. However, this freedom should not mean that it becomes the norm to use consumer data without the user’s consent.

Mobey Forum supports transparent and open solutions that allow customers to control who has access to which parts of their data. It is equally important to make it easy for customers to understand what is being shared and the consequences of allowing mobile wallet stakeholders to use this data.

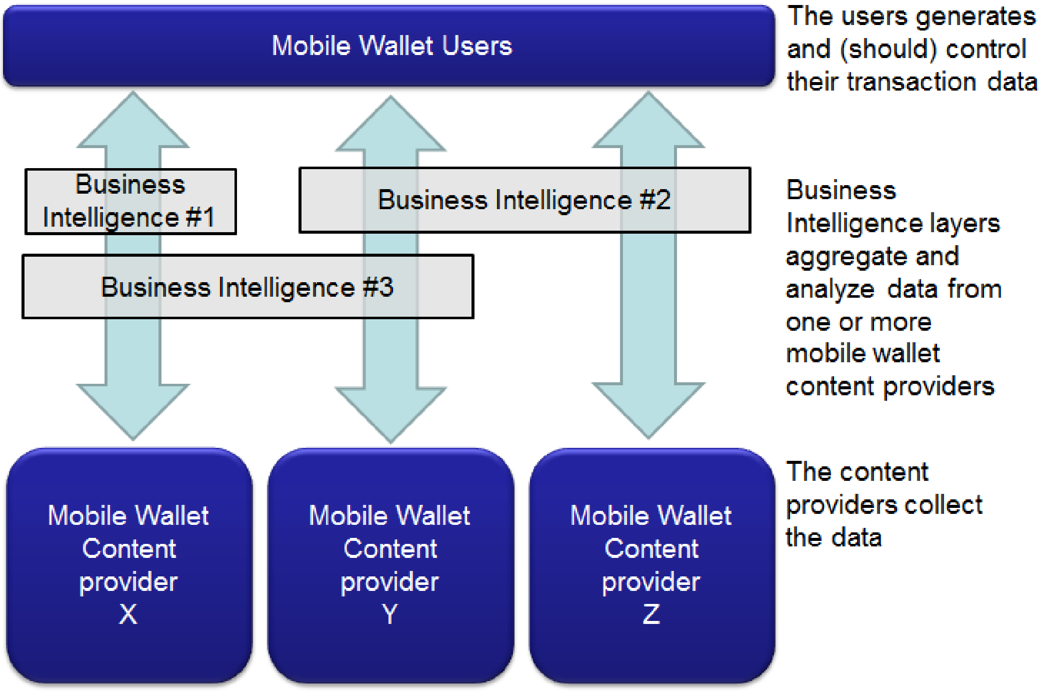

Mobile Wallet Users
The users generates and (should) control their transaction data
Business Intelligence #1
Business Intelligence #2
Business Intelligence #3
Business Intelligence layers aggregate and analyze data from one or more mobile wallet content providers
Mobile Wallet Content provider X
Mobile Wallet Content provider Y
Mobile Wallet Content provider Z
The content providers collect the data

Figure 4: Ownership and control of the data flow

The control point is typically owned by mobile wallet content providers that, depending on the service provided, may include:

- **Banks and other payment institutions**
  For data related to payment
- **Value added service providers**
  For data related to loyalty scheme and/or coupons
- **Public and legal authorities**
  For the data regarding identity and certificates.
- **Merchants**
  May use data for own purposes
- **MNOs**
  Manages data-related branchless banking

The aggregation of data from individual mobile wallet users and making it anonymous helps to maintain users' privacy and their trust in mobile wallets.

Finally, it should be noted that the POS terminal and its software is an essential part of data ownership and its role need to be considered further as mobile wallet ecosystems develop.

7 Conclusion

There are many approaches to establishing the mobile wallet ecosystem. Most include different stakeholders who rely on each other to get the ecosystem up and running.

In this white paper, Mobey Forum establishes a new term called the “control point”, illustrating how particular stakeholders can control one or more parts of the mobile wallet ecosystem. In many cases, a control point may be under the control of more than one stakeholder.

Mobey Forum believes it is in the interest of each stakeholder to be crystal clear about why it should control a specific control point, the resulting consequences of that control and how to resolve conflicting stakeholder interests over control points. The control points also provide a focus for the value that each stakeholder brings to the mobile wallet ecosystem (for example costs savings or specific expertise) and to support full cooperation between stakeholders.

Today’s market, described in terms of (still low level) mutual synchronisation between the roles of the different stakeholders, is proof of the lack of maturity of this new mobile wallet market.

Mobey Forum will follow the market developments and update this white paper as we see significant developments.

Stakeholder	**Relevant Control Points**							
	Connection from and to the mobile wallet (6.1.1)	Distribution channels for the wallet (6.1.2)	Customer acquisition and enrolment (6.1.3)	Bearer / connection technology (6.2.1)	Channels to get value into the mobile wallet (6.2.2)	Channels to get value out of the mobile wallet (6.2.3)	Data flow (6.2.4)	Data ownership (6.2.5)
Banks and other Payment Institutions	•		•		•	•	•	•
Payment Scheme Owners	•					•	•	•
Device Manufacturers	•	•	•	•			•	•
Merchants		•			•			•
Mobile Network Operators	•	•	•	•		•	•	•
OS Providers	•	•					•	•
Public and legal authorities							•	•
Users						•	•	•
Value Added Service Providers	•		•				•	•

Table 1: Control Points most relevant for each stakeholder (numbers in brackets refer to relevant sections in this white paper)

8 Glossary of abbreviations

EDGE	Enhanced Data Rates for GSM Evolution
GPRS	General Packet Radio Service
HSPA	High Speed Packet Access
MNO	Mobile Network Operator
KYC	Know Your Customer
LTE	Long Term Evolution
NFC	Near Field Communication
OS	Operating System
POS	Point of sale
PTA	Public Transport Authority
SD	Secure Digital (as in SD Card)
SE	Secure Element
SIM	Subscriber Identity Module
SMS	Short Messaging Service
USSD	Unstructured Supplementary Service Data
WAP	Wireless Application Protocol
WCDMA	Wideband Code Division Multiplexing Access

Appendix:
Understanding existing mobile wallet implementations

This appendix gives a brief overview of some mobile wallet implementations and also includes some high level descriptions of yet to be launched mobile wallets to show how these implementations use control points. This is by no means an exhaustive list of today's implementations. The existing implementations are constantly evolving, and thus the information in this Appendix may become outdated.

1. Google Wallet

Google Wallet is available as a software update to Nexus S phones on the Sprint Network, through distribution channels such as Amazon.com and Best Buy. Other MNOs selling the Google Nexus S do not have access to the application and it is not available in the US Android Market.

The usage channels for the Google Wallet are currently Citi MasterCard and/or a Google Prepaid card on the MasterCard platform. Google is working on adding other cards to the solution. The payment channel for Google Wallet is thus currently controlled solely by MasterCard, whereas Google controls the channel for both adding and redeeming coupons and other offers.

Controlling the data flow in Google Wallet

The Google Wallet was launched in a closed-loop setup in close cooperation between Citi, Sprint and Google. The application is only available on a specific handset, the Google Nexus S, sold through Sprint's distribution channels like Amazon.com and Best Buy. Other MNOs selling the Google Nexus S do not have the option to distribute the Google Wallet application. Nor is the application available in the US Android Market, but is pushed to Nexus S phones on the Sprint Network through a software update. This means that Google effectively controls the distribution of the wallet (though technically assisted by Sprint).

The channel to get monetary value into the Google Wallet is currently Citi MasterCard and/or a Google Prepaid card (on the MasterCard platform). Google is working on adding other cards to the solution.

The channel to get monetary value out of the Google Wallet is currently controlled solely by MasterCard.

Another type of value in the Google Wallet is coupons. With coupons, Google controls both channels for adding and redeeming coupons and other offers.

Controlling the data flow in Google Wallet

The different partners in the Google Wallet setup control different parts of the data flow:

- Sprint controls the network
- MasterCard controls the payments network

- Citi controls the KYC and the issuing of the payment cards
- Google controls the access to the 'Google Universe' because a Gmail account is needed for activating the Google phone and thereafter the wallet.
- First Data acts as a single point of entry for the other stakeholders, such as merchants.

First Data has a critical role as the macro infrastructure provider. Its role is to shield stakeholders from ecosystem complexity, aggregate Service Providers, aggregate the broader ecosystem, minimize relationship complexity, maintain neutrality in the ecosystem, minimize capital investment for stakeholders and ensure operational security and reliability.

With Google Wallet, Google controls and uses data generated from customer behaviour and the redemption of offers to produce meaningful campaigns and loyalty offers for users. While not having direct access to receipts or transaction data, Google knows the context and background of every payment and every redeemed offer made through the Google Wallet, creating a valuable mobile commerce asset.

2. Isis Mobile Wallet

Isis, a joint venture between AT&T Mobility, T-Mobile USA and Verizon Wireless, is expected to launch in Salt Lake City, Utah and Austin, Texas in mid-2012, with a national rollout to follow so a detailed description of its implementation is not yet possible.

Isis has announced support from six leading device manufacturers – Samsung Mobile, LG, RIM, Sony Ericsson, HTC and Motorola Mobility, with support for the Android, Blackberry, and iOS platforms. Isis-ready handsets will be distributed through MNO retail locations.

Isis has also announced support from the top four payment networks – VISA, MasterCard, American Express and Discover and is expected to announce bank partners in 2012.

Controlling the data flow in the Isis Mobile Wallet

Isis operates a B2B2C platform, bringing together all the players needed to promote the development and growth of the mobile commerce ecosystem:

- The MNOs will control the secure element
- Gemalto has been selected to secure the over-the-air provisioning of sensitive information
- Banks will issue cards and service their customers through custom widgets within the wallet
- Merchants will deploy their own offer, loyalty and reward programs.

3. Cityzi Wallet

With Cityzi Wallet, customers are enrolled through combinations of MNOs, financial institutions and a public transport authority, with a MNO required in each case.
The distribution channel is via banks and MNOs. Access management is achieved by logging on to the banks' content, rather than at the wallet level and is driven by the MNO. The banks act as payment service providers. There is a lack of ownership of access management.

Controlling the data flow in the Cityzi Mobile Wallet

In terms of data flow, there is no perceivable difference for the card issuer and public transport authority. To access their balances, users need the BNP Paribas application. The MNO has a gatekeeper role here, while data ownership rests with the payment service provider.

4. M-Pesa, Kenya

M-Pesa has become the most popular mobile money service in Kenya since its commercial launch in 2007 and is now used by around 16 million of the approximately 40 million strong Kenyan population. The service is provided by Safaricom, the MNO holding a 78% market share. Services provided include recharge, bill payment and sending money from one mobile user to another, as well as the ability to transfer money to a savings account held with Equity bank. Safaricom uses a retail network of 19,000 exclusive money agents for registration, as well as cash deposits and withdrawals.

Controlling the data flow in the M-Pesa Mobile Wallet

From a control point of view, all control points are held by the MNO - even the bank partner is white labelled and not publicly known. Initially focused on consumer retention and reducing costs for paper-based recharge coupons, its scale in that country has enabled a solid business model with a new ecosystem of new solution providers on top. Other M-Pesa named services have been rolled out in Tanzania, Afghanistan and India but have not yet gained similar traction.

5. Nokia Money

Nokia Money is a broad ecosystem initiative that is working with a wide range of banks and MNO interaction, enabling a broad uptake of mobile money services. It has a special business model in India and another one for outside India.

Nokia Money - India

As the launch country and due to the huge population of 1.2 billion people, Nokia has decided to drive the go-to-market (i.e. distribution, retail channel management and consumer acquisition) itself, while cooperating with numerous banks. The banks provide the accounts and hold mobile money licences granted by the central bank, the

Reserve Bank of India, for the full service product including money transfer. As such, the service is branded by bank, for example Union Bank Money or Yes bank Money.

From a control point of view, Nokia provides the acquisition / enrolment and wallet distribution, with all other control points are held by the payment service provider partners.

Nokia Money - other countries

In other countries, Nokia will not provide the go-to-market as such. It will provide the mobile phones with an open and brand agnostic mobile client as well as enabling interaction with the payment back-end. Opening of its additional retail and distribution channel to the partner is an option, depending on the type of partnering involved.

All control points will be held by the Payment Service Provider, while Nokia will provide only the distribution channels for the wallet

6. Osaifu-Keitai

Literally meaning "Wallet Mobile", Osaifu-Keitai was launched in 2004 by NTT DoCoMo. The system refers to mobile phones that integrate Sony´s Mobile Felica chips, as well as to services provided by applications on these phones. Although it was developed by NTT DoCoMo, the system is supported by the other mobile phone operators, making it the *de facto* standard mobile payment system in Japan.

Osaifu-Keitai services include electronic money, identity card, loyalty card, pulic transport fare collection (including railways, buses and airplanes), or credit card. The service now features DoCoMo’s own payment scheme, iD, along with a number of third party payment services, transit ticketing, loyalty programs, airline check-in and others, like Edy, Mobile Suica and others. Payment capability is now in more than half of Japanese subscribers’ phones.

The chips and their operating system are licensed via Felica Networks, which is owned by NTT DoCoMo, Sony and Japan Rail East.

Mobile wallet	**Relevant Control Points**						
	Connection from and to the mobile wallet **(6.1.1)**	*Distribution channels for the wallet* **(6.1.2)**	*Customer acquisition and enrolment* **(6.1.3)**	*Bearer/ connection technology* **(6.2.1)**	*Channels to get value into and out of the wallet* **(6.2.2 / 6.2.3)**	*Data flow* **(6.2.4)**	*Data ownership* **(6.2.5)**
Google	Issuer MNO Google Android	Google Android	Google Issuer (Citi)	NFC only	Banks	Card Payment business as usual Google	Google Banks and other payment institutions
ISIS	MNOs Banks and other payment institutions	MNOs (AT&T, Verizon, T-Mobile)	MNOs (AT&T, Verizon, T-Mobile), through carrier retail stores or remotely for users with capable devices	MNOs Device Manufacturers (control embedded hardware, WiFi etc.)	**Channels to get value in wallet:** MNOs (AT&T, Verizon, T-Mobile) Card Scheme Providers Banks and other payment institutions Value Added Service Providers (offers/deals) **Channels to get value out of wallet:** Merchants	MNOs Banks and other payment institutions (if SE control exists) Card scheme providers (if SE control exists) `	Mobile User Banks and other payment institutions (payment initiator) Card Scheme Provider (payment initiator) Value added Service Provider (TBA) Government Entities Merchants
Cityzi	MNO	MNO	MNO Banks and other payment institutions PTA (Public Transport Authority)	NFC only	Banks and other payment institutions PTA	Payment Card PTA MNO	Banks and other payment institutions PTA MNO
M-Pesa Kenya	MNO – USSD only	MNO – SIM card	MNO	USSD	MNO	MNO	MNO

Nokia Money - India	Banks and other payment institutions	Nokia	Nokia	SMS WAP 3G Wi-Fi	Banks and other payment institutions shared with Nokia	Banks and other payment institutions	Banks and other payment institutions
Nokia Money – other countries	Banks and other payment institutions	Nokia	Banks and other payment institutions		Banks and other payment institutions	Banks and other payment institutions	Banks and other payment institutions
Osaifu-Keitai, Edy, Suica	MNO	MNO	Banks and other payment institutions, Felica Networks	Felica/NFC	Banks and other payment institutions	Banks and other payment institutions	Banks and other payment institutions

Table in Appendix: Stakeholders roles in various control points in real world implementations