New Enabling Technologies in Digital Commerce

SEPTEMBER 2014
# CONTENTS

1. Introduction 03

2. Executive Summary 04

3. The Customer Journey 06

4. A Mobile Wallet 10

5. One-way Beacon 14

6. Two-way Beacon 16

7. Secure Element NFC 19

8. Host-based card emulation NFC 22

9. QR Codes 24

10. Wi-Fi 26

11. Conclusions 29
Introduction

This paper outlines the role several emerging mobile technologies can play within digital commerce – the use of digital services to bring buyers and sellers together. It is aimed at senior executives within mobile operators and adjacent sectors, such as banking and retail. The paper explains the potential capabilities of various medium and short-range wireless technologies, while exploring how they can be combined with cellular networks into a broader consumer engagement proposition within the digital commerce market. The paper maps out the potential role of the various technologies as part of a consumer journey from the planning stage through to in-store interactions and transactions.

Although the mobile technologies covered in this paper can be used to enhance the consumer experience in many different sectors of the economy, including transport, entertainment, hospitality and city administration, this paper focuses primarily on their role in the retail sector. The diverse and intensely competitive retail industry is exploring a wide range of digital commerce technologies and solutions as it strives to find the optimum balance between serving consumers online and in-store. The service providers working with the GSMA have identified a large number of retail use cases. Some of these potential use cases are discussed in this paper.
Executive Summary

As online shopping booms, bricks and mortar retailers are looking to harness emerging mobile technologies to enrich the in-store experience and find new ways of engaging, attracting and interacting with customers. The seven emerging technologies described in this paper can all enhance various stages of the customer retail journey. Mobile operators, banks, merchants and other participants in the digital commerce value chain need to consider the various strengths and limitations of each technology and how they can complement each other and well-established technologies, such as cellular connectivity and GPS (the global positioning system).

Here is a high level summary of the value that can be added by each of these technologies:

**Mobile wallet** is a software application designed to be analogous to a traditional physical wallet. A well-designed mobile wallet will put the consumer in control, enabling them to use their handset to access the digital commerce services and content they want in a way that is both straightforward and secure.

**One-way beacons** are an inexpensive way to enable mobile apps to determine the precise location of the user’s device and then display relevant information. But service providers need to be careful not to overwhelm consumers with notifications.

**Two-way beacons** could make some kinds of in-store interactions easier (particularly in places without reliable mobile or Wi-Fi coverage), however, merchants may find them relatively expensive to deploy and consumers may be wary of using them.

**Secure element** near field communication (NFC) enables consumers to access services and content by tapping their device against a reader or tag. The secure element can be used to store and transfer sensitive data. Although secure element-based NFC services can be relatively expensive and complex to deploy, the technology can provide a very secure and intuitive consumer experience while complying with the banking industry’s established processes and security standards.

**Host card emulation NFC** which doesn’t require a secure element, can be relatively straightforward to deploy for services that don’t require robust security, such as redeeming low-value coupons. The measures required to secure transactions via host card emulation NFC, such as interaction with a cloud-based server, are still being designed and the actual impact on deployment cost and service usability is not yet clear.
QR codes can be used to enable consumers to access content or services either in-store or on the street. Although they are relatively inexpensive to deploy, QR codes don’t typically provide an intuitive or elegant experience for the consumer, limiting their uptake and usage.

Wi-Fi is a highly versatile and relatively inexpensive technology which enriches the customer journey by providing connectivity and information on a consumer’s location. However, Wi-Fi typically isn’t secure enough or reliable enough to be used for ‘mission-critical’ applications, such as transactions.

How each of these technologies are used in practice will depend heavily on local market factors (e.g. how many consumers have NFC-enabled handsets) and the strategies of individual merchants. However, it is likely many consumers will want a mobile wallet or equivalent app to help them organise their interactions with multiple merchants. Without an aggregation app (or wallet), a consumer needs to juggle dozens of apps and websites to make use of different merchants’ vouchers, offers and loyalty programmes.

Moreover, in many markets, secure element NFC is likely to be widely adopted to enable secure, quick and straightforward transactions. Although host card emulation NFC could have a role to play, it will need to be bolstered by additional security mechanisms to protect sensitive data. As the ecosystem underpinning secure element NFC becomes increasingly mature and streamlined, more and more merchants and banks are likely to adopt this technology to secure their interactions with customers in-store.

Of the seven emerging technologies discussed in this paper, mobile wallets and secure element NFC are likely to play the broadest role in digital commerce. Both technologies can enhance and enrich each stage of the customer journey, while giving consumers a sense of control and peace of mind. These factors are likely to be critical to driving consumer adoption. To be successful, a business has to maintain the trust and confidence of its customers.

Retailers are looking to harness emerging mobile technologies to enrich the in-store experience and find new ways of engaging, attracting and interacting with customers.
3. The Customer Journey

As online shopping booms, bricks and mortar retailers are looking to harness emerging mobile technologies to enrich the in-store experience and find new ways of engaging, attracting and delivering service to their customers. Mobile operators can help merchants attract new customers and increase their footfall, while facilitating consistent customer journeys, making it easier for consumers and store staff to interact using digital technologies. Wireless technologies can also enhance the consumer’s journey to and from the store, helping them with travel arrangements and other activities, such as a visit to a café, a restaurant, the cinema or a tourist attraction.

The mobile operator can also play a role in reaching out to those customers not engaged with the merchant or retailer to increase their footfall.
EXAMPLES OF HOW VARIOUS TECHNOLOGIES CAN ENHANCE A CUSTOMER SHOPPING JOURNEY

**KEY**

- SMS/MMS
- WALLET APPLICATION
- LOCATION BASED SERVICES
- NFC/HCE/TOKENS/BARCODE/QR CODES
- IBEACON BLUETOOTH
- LOW ENERGY
- WIFI

**Figure 1**

OUTWARD TRAVEL

- Service updates
- Parking location
- Getting there
- Timetable
- Travel info

PLANNING

- Offers
- Information
- Social
- CRM/KYC
- Maps / location
- Day Planning
- Parking

IN STORE

- Queue, fast track
- Guides
- Stock alternatives
- VIP Services
- Information
- Check in

TRANSACTING

- Coupon
- Offering
- Receipting
- Loyalty redemption
- Loyalty accumulation
- Payment
- CRM/KYC
- To do / shopping list
- Guides

POST TRANSACTION

- Up selling
- Cross selling
- Social
- CRM/KYC
- Further information
- To do / shopping

RETURN TRAVEL

- Services updates
- Getting home
- Parking location
- travel info
- Timetable
The GSMA believes mobile operators and the broader ecosystem need greater clarity as to where certain technologies would add value in the customer journey, and would best suit a type of interaction. To that end, we have divided the customer journey for bricks and mortar shopping into six overlapping stages, during which the consumer makes decisions based on the information available to them:

- **Planning** – the consumer decides where to shop.
- **Outward travel** – the consumer decides which shops and other merchant outlets to visit.
- **In-store** – the consumer decides what to buy.
- **Transacting** – the consumer decides how to pay and whether to make related purchases.
- **Post transaction** – the consumer decides what to do next.
- **Return travel** – the consumer reflects on the merchants they have interacted with.

Figure 1 references the following technologies:

**SMS/MMS** – These messaging technologies can be used to send information to a consumer regardless of their make and model of handset and whether they have a specific app. As the capabilities of SMS and MMS are well understood, these technologies aren’t discussed in depth in this paper.

**Mobile wallet application** – A consumer can use an application on their mobile device as a gateway to many other applications, such as loyalty schemes, vouchers and payment cards, from different merchants and banks. A section of this paper explains the potential role of the mobile wallet in a holistic digital commerce proposition.

**Location-based services** – The use of mobile networks and/or GPS to enable apps running on a mobile device to determine a consumer’s location. Mobile operators can enable application developers to tap the location-finding capabilities of their networks via application programming interfaces (APIs). As such location-based services are widely used and widely understood, these technologies aren’t discussed in depth in this paper.

**Bluetooth Low Energy beacons** – Typically fixed in one place, a beacon uses the Bluetooth Low Energy (BLE) standard to transmit (and sometimes receive) information. A section of this paper covers the potential roles of one-way beacons and two-way beacons in a holistic digital commerce proposition.

**NFC/Barcodes/QR codes** – These short-range technologies enable a consumer to interact with their immediate surroundings. A section of this paper covers the potential role of the several different variants of these technologies in a holistic digital commerce proposition.

**Wi-Fi** – Although Wi-Fi is widely used to provide connectivity, this widely-deployed technology can also enhance digital commerce in other ways. A section of this paper explains the potential role of Wi-Fi in a holistic digital commerce proposition.

The use of mobile networks and/or GPS to enable apps running on a mobile device to determine a consumer’s location.
A Mobile Wallet

What is a mobile wallet?

A mobile wallet is essentially a digital version of a physical wallet in that it is designed to store commerce-related collateral, such as payment cards, stored value, loyalty cards, vouchers, tickets and receipts. To that end, a mobile wallet is typically an application that aggregates data from other applications on the consumer’s mobile device.

As individuals use their mobile device to interact with many different service providers, and download many apps, there is a danger that their customer journey becomes fragmented - different applications have different ways of completing transactions and performing other tasks, potentially confusing the customer. Consumers, merchants and store staff need a consistent approach to surfacing relevant offers, digital vouchers, loyalty programmes, payment cards, tickets, receipts and other related items in a multi merchant environment, such as walking down the street and looking at many shops. A mobile wallet can meet that need.

The potential role in the customer journey

A mobile wallet can play a role in every aspect of the customer journey, supporting merchants by providing notifications, information, offers and coupons in the planning, outward-travel and in-store stages of the journey. During the outward travel phase of the journey, the wallet can help a consumer arrive at their destination by flagging the availability of parking spaces or the times of rains and buses. It can also provide the consumer with a ‘street-level’ view of offers, coupons and information relevant to their location and the time of day. It can also act as a gateway to the apps of nearby merchants.

As merchants want consumers to have an in-store experience on their mobile device, brand presence and positioning is extremely important, so a wallet should respect merchants’ brand positioning and ensure it isn’t overpowered by the wallet branding. In some cases, a merchant may prefer its own app to perform some of the functions associated with a wallet.

In-store, a wallet can be used to facilitate a transaction, enabling the consumer to choose which coupons to apply and which payment card to use. After receiving a digital receipt recording the transaction, the mobile wallet can then be a conduit for any related notifications, information and offers in the post transaction and return travel phases of the customer journey.

Moreover, a mobile wallet can help merchants and loyalty providers draw a direct correlation between their digital marketing, offers, advertising campaigns, loyalty programmes and coupon distribution and actual sales – i.e. close the loop. For example, a wallet working in tandem with mobile technologies, such as NFC, can help merchants and brands determine the effectiveness of a specific promotional campaign by registering the redemption of coupons and loyalty points at point of sale. This information could be available in real-time and at an individual device level, enabling a brand to refine its proposition to individual consumers mid-way through a campaign.
Example use cases

Outward travel: As he walks down his local high street at 5pm in the afternoon, John's handset vibrates – his mobile wallet is notifying him that the television he looked at online is available at a nearby electronics store. John opens the wallet app, which shows him where the electronics store is. It also flags that he has two vouchers that can be used on the high street – one for a café-bar and the other for a supermarket. Moreover, the wallet displays the time of the next bus home, the films showing in the local cinema that evening and a notification from the town's cycle store that he now has enough loyalty points for a free bike service.

In-store: In the café-bar, John opens his wallet to pay for a coffee and sandwich. The wallet asks him if he would like to use the voucher. He clicks yes and touches his NFC-enabled handset against the point of sale terminal. The terminal shows John the new loyalty card balance, the wallet displays his preferred payment card and John touches the point of sale again to confirm the transaction. A digital receipt appears in John's wallet showing him how many loyalty points he now has and notifying him that the café-bar will have live music on Saturday evening.

Strengths

• Provides simplicity and consistency for the consumer to store and use digital equivalents to items that would typically live in a physical wallet.
• Provides a personalised ‘street level’ view of relevant merchants and their apps that can leverage a rich contextual and historical awareness of the consumer to show relevant and timely content.

Architecture

• A mobile wallet will need to be underpinned by a robust authentication system that ensures the user is entitled to access the services that can be accessed via the wallet.
• A mobile wallet should be supported by application programming interfaces (APIs) and a software development kit (SDK) that make it straightforward for merchants, banks and other service providers to develop compatible services and applications (see Figure 2).
• Mobile operators’ mobile wallets should function in a consistent way so that a service provider doesn’t have to adapt its service offering to be compatible with each wallet application1.

A WALLET AND A MERCHANT APP CAN WORK TOGETHER TO BRIDGE THE PHYSICAL AND DIGITAL WORLDS

Figure 2

1. To this end, the GSMA has developed a technical proposal for a consistent approach to NFC Coupons and Loyalty Acceptance. Please see: http://www.gsma.com/digitalcommerce/nfc-15-mobile-commerce-nfc-coupons-and-loyalty-acceptance-technical-proposal
In summary: A well-designed mobile wallet will put the consumer in control, enabling them to access the digital commerce services they want in a way that is both straightforward and secure.
5. One-way Beacon

What is a one-way beacon?

Bluetooth beacons can help apps running on mobile devices to determine their precise location. A beacon broadcasts a Bluetooth Low Energy (BLE) signal over a distance of up to 50 metres that can be detected by compatible devices. The signal is short and simple, and typically does not change. As a result, most beacons do not require any connectivity and are often very small and battery powered. They are typically inexpensive to mass-produce, with the BLE chip costing less than a dollar. However, to receive a signal from a BLE beacon, a consumer must have a device with a BLE chip, compatible software and Bluetooth switched on.

The potential role in the customer journey

BLE beacons are particularly well suited to helping mobile devices determine their precise location in a store, so that a mobile wallet or merchant’s app can check-in and then relay information and offers relevant to the consumer’s immediate surroundings. Note, the wallet or app should ask the consumer for permission to use information about their location in this way. In outdoor locations, such as in the vicinity of advertising billboards, a BLE beacon could be used to help entice consumers into stores or to use specific services. Moreover, a beacon could be used to detect when a consumer is leaving a store, so that the retailer’s app can thank them for visiting and/or making a purchase.

Example use cases

Outward travel: Sarah’s wallet receives a signal from a Bluetooth beacon indicating that she is very near her favourite beautician. The wallet buzzes to notify Sarah that her loyalty account with the beautician now has enough points to qualify her for a free manicure. Sarah walks into the shop and books an appointment.

In-store: By monitoring signals from the nearby Bluetooth beacon, the fashion app on Sarah’s phone is aware that she has spent five minutes looking at hats without moving on to the checkout. It sends her a notification: Click here for a 10% off coupon – valid today only. Sarah clicks on the link and downloads the voucher.

Strengths

• Beacons can be easy to install, as most don’t need connectivity.
• Beacons provide accurate proximity information, even indoors.
• Beacon hardware is inexpensive.
• Beacons can be very small and discreet.
• Beacons can run on batteries for several months.
• Some smartphones and tablets can broadcast BLE signals and can be configured to act as beacons.
Considerations

- Consumers’ smartphones must have Bluetooth 4.0 or BLE to receive information from beacons.
- Apps must be beacon-enabled by the developer. In this case, the app will need to have access to an up-to-date map of relevant beacons.
- In many cases, apps will need to have Internet access (either via a cellular network or a Wi-Fi network) to act on a signal from a beacon.
- The consumer’s smartphone operating system must support BLE.
- The consumer must have enabled Bluetooth on their smartphone.
- Apps need to avoid excessive notifications that could prompt the consumer to disable Bluetooth.
- If apps are badly coded, beacons could drain a handset’s battery life.
- As beacons can be insecure, the owner may have to encrypt their identifying information to avoid beacons being spoofed/hi-jacked or hacked. The Apple iBeacon specification, for example, in its standard form does not prevent unauthorised use of beacons.
- It can be costly to maintain an estate of disconnected devices.

Examples of deployments

Some retailers, such as Anthropologie, American Eagle Outfitters, Banana Republic, Best Buy, Burberry, Carrefour, Hamleys, Hugo Boss, Longchamp and Macy’s are already beginning to deploy beacons.

In summary: A one-way beacon is an inexpensive way to enable mobile apps to determine the precise location of the user’s device and then display relevant information. But there is a danger they could be used to bombard users with notifications.

THE POTENTIAL ROLE OF BLE BEACONS IN THE CUSTOMER JOURNEY

Figure 3
Two-way Beacon

What is a two-way beacon?

A two-way beacon uses Bluetooth Low Energy (BLE) to interact with an app running on a compatible mobile device over a distance of up to 50 metres. A two-way beacon can receive, as well as transmit, information and is typically connected to a retailer’s point of sale or IT systems via Wi-Fi. A two-way beacon will typically be mains powered, rather than battery powered, and is more expensive than its one-way counterpart. To interact with a BLE beacon, a consumer must have a device with a BLE chip, compatible software and Bluetooth switched on.

The potential role in the customer journey

A two-way beacon could enrich the in-store experience by enabling consumers to check-in and then receive personalised offers and notifications, and complete transactions. As it can receive information, a two-way beacon can directly notify a retailer (via Wi-Fi or via a fixed-line) that a consumer is in store, rather than relying on an app on the consumer’s smartphone to relay that information over a cellular or Wi-Fi network. A two-way beacon could also be used to trigger a transaction in a number of different ways. For example, it could send the transaction details to the consumer’s handset and then ask them to pay online using a mobile or digital wallet, such as PayPal, or via an EMV-enabled transaction.

Example use cases

**In-store:** When Harry arrives in a shoe shop, a beacon sends the retailer’s app on his handset a message asking whether he would like help from a shop assistant. He clicks yes and the beacon alerts an available member of store staff via Wi-Fi that a male customer in the boot aisle needs help. One of the assistants comes to help Harry.

**Transacting:** Having received a prompt from the in-store beacon, the wallet app on Harry’s handset asks if he would like to identify himself to the shoe shop. Harry clicks yes and his mobile wallet sends his ID to the beacon, which then relays that information to the retailer’s point of sale system, which then displays a photo of Harry. When he has chosen some shoes, Harry can pay by simply verbally confirming the transaction to the cashier, who then selects the appropriate photo and ID in the point of sale system. The retailer validates the transaction via Harry’s wallet provider, which debits the transaction from his preferred debit card. Harry receives a digital receipt by email.
Strengths

- Can enable interactivity between a merchant and a consumer in locations where there is no mobile or Wi-Fi connectivity.
- Doesn’t significantly drain the consumer’s handset battery.

Considerations

- Two-way beacons are more expensive than one-way beacons and will require connectivity (typically Wi-Fi) and a reliable power supply (typically a mains connection).
- Using two-way beacons to enable payments would require merchants to adapt their existing point-of-sale systems.
- Transacting via a beacon requires consumers to significantly change their in-store behaviour. It might not be clear to consumers which beacon they are interacting with, making them wary of initiating a transaction.
- A transaction enabled by a two-way beacon would effectively be a card-not-present transaction, similar to an online transaction, involving a higher level of risk and, therefore, higher interchange fees.
- As beacons are inherently insecure, this puts constraints on payment applications that would use them as a bearer. And no standards are available to implement payments on BLE.

Examples of deployments

PayPal is piloting PayPal Beacon – a BLE device that will connect to a customer’s PayPal app when they enter a store (assuming the customer has opted-in). The beacon relays the customer’s details to the point of sale system. When the consumer is ready make a purchase, they tell the cashier they are paying with PayPal and the transaction is automatically completed.

In summary: Although two-way beacons could make some kinds of in-store interactions easier (particularly in places without reliable mobile or Wi-Fi coverage), merchants may find them expensive to deploy and consumers may be wary of using them.
Secure Element NFC

What is secure element NFC?
Near Field Communications (NFC) is a contactless radio technology that can transmit small amounts of data between two devices within a few centimetres of each other. Many debit cards, credit cards and mobile phones now contain NFC chips.

A secure element is a distinct tamper-resistant piece of hardware, such as a universal integrated circuit card (UICC) or an SD card, which can be used to protect sensitive data or applications from malware or other unauthorised apps. A secure element is generally divided into secure domains, which can ring-fence a specific application, such as a bank’s payment app containing the payment credentials (i.e. secret cryptographic keys), and ensure it isn’t compromised by another application. In combination with an NFC handset, a secure element can emulate an NFC-enabled plastic card, enabling the consumer to complete payments, redeem vouchers or collect loyalty points by tapping their device against an NFC reader. The secure domains are typically managed and provisioned by trusted service managers (TSMs) – one working on behalf of the owner of the secure element, such as a mobile operator, and one on behalf of the service provider, such as a bank.

The potential role in the customer journey
A secure element can play a role throughout the customer journey. A voucher delivered over a mobile network in the planning or travel stages could be stored on the secure element to ensure it isn’t hacked or replicated by a malicious app running on the consumer’s handset. In-store, a mobile wallet or the retailer’s app could activate a voucher stored in the secure element, readying it to be redeemed at the point of sale. To complete a transaction, NFC could enable a consumer to make a payment using a debit or credit card stored on the secure element by tapping their handset against a contactless point of sale terminal.

Example use cases
Planning: Jill receives a SMS from her favourite French restaurant with an offer of two main courses for the price of one. She clicks on the link, which opens the restaurant’s website from where she can download a voucher into her wallet. She selects her mobile wallet provider and the download begins. As Jill doesn’t have the restaurant’s app on her handset, the voucher is stored in the wallet’s secure domain on the secure element and a visual representation of the voucher appears in her wallet.

Transacting: At the end of the meal in the French restaurant, the waiter bring overs a portable NFC-enabled point of sale terminal and keys in the amount due. Jill opens her wallet, which asks her if she would like to use the two-for-one voucher. She clicks yes and taps her phone against the point of sale terminal, which validates the voucher via the NFC interface and then shows the new balance. Jill again taps her phone against the point of sale terminal, transmitting details of her payment card, which are stored in the bank’s secure domain in the secure element. The point-of-sale terminal asks her to key in her PIN number to complete the transaction.
Strengths

- Handsets equipped with NFC enable people to interact with their immediate surroundings and online services in an intuitive and straightforward way: An NFC interaction requires a deliberate, yet simple, action on the part of the consumer.
- Although many point-of-sale terminals in merchant locations don’t yet support NFC, the technology is gaining traction with retailers as NFC-enabled payment cards proliferate.
- An application stored on a secure element can be disabled remotely if a service needs to be withdrawn.

Considerations

- Many older smartphones don’t have built-in NFC chips and will need an NFC case to interact with NFC tags and readers.
- Secure element NFC requires the owner of the secure element (typically a mobile operator) to be involved in the provisioning of the payment, ticketing or merchant app. This requires appropriate business processes and infrastructure to be in place.
- Mobile operators are working through the GSMA to simplify the relatively complex ecosystem involved in the provisioning and management of UICCs as secure elements.

Actual deployments

More than 20 mobile operators, including China Mobile, Orange, SingTel, Turkcell and Vodafone, have launched NFC services secured by the UICC. Apple has unveiled new handsets equipped with a secure element and an NFC chip that will support a new service called Apple Pay. Apple says actual payment card numbers are not stored on the device nor on Apple servers. Instead, a unique Device Account Number is assigned, encrypted and securely stored in the secure element of the device. Each transaction is authorised with a one-time unique number (a token) using the Device Account Number and instead of using the security code from the back of your card, Apple Pay creates a dynamic security code to securely validate each transaction.

This aligns with the GSMA’s position that a Secure Element is preferable to some of the proposed alternatives in the market. Having said this, Apple does not use the actual SIM card as its Secure Element. The Apple Watch will apparently also support NFC payments using the Apple Pay service. Significantly, Apple will reportedly bear part of the transaction risk and secure reduced interchange fees from banks and card schemes as a result – reductions of up to 0.25% are rumoured. Apple is also assuming some of the risk of fraudulent transactions using its TouchID biometric sensors, NFC, and geolocation data to assure partners of non-fraudulent transactions.

In summary: Although secure element-based NFC services can be relatively expensive and complex to deploy, the technology can provide a very secure and intuitive consumer experience while complying with the banking industry’s processes and security standards.
Host-based Card Emulation NFC

What is host-based emulation NFC?
Near Field Communication (NFC) is a contactless radio technology that can transmit small amounts of data between two devices within a few centimetres of each other. Many debit cards, credit cards and mobile phones now contain NFC chips.

Host-card emulation NFC enables an application running on the phone to use a NFC handset’s host processor to imitate a plastic NFC card and interact with a NFC terminal in card emulation mode. Instead of storing sensitive data on a secure element, host-based card emulation stores this data in the cloud or in a trusted execution environment (TEE), a combination of hardware and software on the device’s processor, which is more secure than standard handset memory. To mitigate the risk that data stored in the cloud is intercepted or a TEE is hacked, a bank may issue limited-use tokens that act as an alias for the real Primary Account Number (PAN). These tokens, which can be used to authenticate a payment, will only be valid for a limited period of time, a specific number of transactions or purchases in particular stores.

Example use cases
Outward travel: While waiting at a bus stop, Terry scans a billboard advertising a new film. He taps a NFC tag on the billboard and receives a link to a trailer for the new film. He uses a cellular connection to watch the trailer on the bus.

Transacting: Arriving at the cinema with his girlfriend, Terry asks for two tickets for the new film. To pay for the tickets, he taps his NFC handset against the point of sale, transferring a one-time token issued by his bank. After Terry has entered his PIN number, the point of sale uses the token to authorize the transaction and transfers the tickets to Terry’s handset via NFC. The tickets, which are only valid for a specific screening of the film, are stored on his TEE. When they enter the cinema, Terry taps his handset against the assistant’s NFC terminal to validate the tickets.

The potential role in the customer journey
NFC can play a role in the outward travel and in-store phases of the customer journey by enabling the consumer to access information, offers and vouchers by tapping NFC tags or readers. If there is no secure element on which to store incoming vouchers, they could be stored in the handset’s TEE. Host card emulation NFC can also be used to transfer a token to a point of sale to complete a transaction. If the token isn’t stored on the TEE, the device will need to have a connection to the cloud.
Strengths

- Handsets equipped with NFC enable people to interact with their immediate surroundings and online services in an intuitive and straightforward way: An NFC interaction requires a deliberate, yet simple, action on the part of the consumer.
- The use of host-card emulation (HCE) eliminates the need for a trusted service manager (a TSM) to provision and manage a secure domain on a secure element.
- Standards for tokenisation are under development. In March 2014, EMVco, which is collectively owned by American Express, Discover, JCB, MasterCard, UnionPay and Visa, published a technical framework for tokenisation. The primary focus of this initiative is ‘card-not-present’ payments, which could include HCE NFC-enabled transactions.

Requirements

- Many older /iOS smartphones don’t have built-in NFC chips and will need a NFC case to interact with NFC tags and readers.
- Although many point-of-sale terminals in merchant locations don’t yet support NFC, the technology is gradually gaining traction with retailers as NFC-enabled payment cards proliferate.
- HCE is only currently supported in the Android 4.4 KitKat and BlackBerry OS 10 operating systems.
- HCE NFC requires the phone to be turned on and the relevant payment app running in the mobile phone OS. In high throughput environments, such as mass transit payment at gate, this may be an issue.
- Whereas a UICC has the advantage of being fully standardised with well-recognised processes, HCE and tokenisation are still immature technologies that are implemented differently in different handsets, increasing complexity for banks and other service providers. Moreover, both HCE and tokenisation have yet to be fully tested in a mass market commercial environment.

Security

- Long-term storage of sensitive data, such as PANs, PINs and keys, isn’t appropriate within the mobile handset operating system, which is inherently insecure.
- Although a TEE is more secure than the standard memory space in a handset, it is not as secure as a physical secure element and is unlikely to be used to store an actual payment application: In many cases, HCE, will likely depend on a connection to the cloud to authorise transactions (in line with a specific risk management logic and methodology). However, the TEE could be used to store a token that is valid for transactions below a value certain threshold in certain stores for limited time period, such as a day.
- If a consumer’s payment credentials are stored in the cloud, the issuing bank needs to ensure they are accessed by a legitimate device, application and user, implying the need for additional authentication measures, such as device fingerprinting and risk based authentication, to maximise the chances of detecting unauthorised access.
- Although it it gains independence from mobile operators, the issuing bank will have to invest in server side platforms to manage cloud-based authentication services and token management.

Actual deployments

The latest versions of the Android and BlackBerry operating systems support host card emulation, while Visa announced in February 2014 that clients will have the option to host Visa payWave-enabled accounts in a secure, virtual cloud that could enable host card emulation. Still, the technology is immature and has yet to be proven in a large scale commercial deployment.

In summary: The measures required to secure transactions via host card emulation NFC, such as interaction with a cloud-based server, are still being designed and they actual impact on deployment cost and service usability remains to be observed in the field. For services that don’t require a high-level of security, such as redeeming low-value coupons, host-card emulation NFC could be relatively straightforward to deploy.

---

QR Codes

Overview of QR codes
Typically printed on a billboard, a poster, a shelf-edge or a magazine, a QR code is designed to be scanned by a consumer using the camera on their mobile phone. If the device has a suitable app then it can translate the QR code into a link and open the related web page or app, which will provide the consumer with some specific piece of information, an offer or even a downloadable voucher. An image of a QR code can also be stored on a handset so it can be scanned by another device – airlines increasingly enable consumers to store a boarding pass on their mobile device and then validate it with a QR code.

Their role in the customer journey
QR codes can be used across the customer journey. They can be printed in an advert in a magazine or a leaflet to trigger a consumer to download an app, information or a voucher in the planning stage of the journey. They can also be printed on outdoor billboards or in-store posters and shelf-edges to enable a consumer to download some relevant collateral, supporting the outward travel and in-store stages of the journey (in a similar fashion to an NFC tag). In the transaction phase, a QR code can be scanned by an appropriate terminal to validate a voucher or a ticket.

Example use case
Planning: As he flicks through a magazine, an advert for a festival catches Peter’s eye. He uses his phone camera to scan the QR code on the advert, which opens a link to the web page where he can buy tickets. After he has completed the transaction online, a ticket with a QR code arrives in his mobile wallet.

Transacting: When Peter and his friend arrive at the festival, he opens his mobile wallet and shows the ticket with the QR code to the attendant at the ticket gate. The attendant scans the QR code and then asks Peter and his friend to provide some identification. They both show their driver’s license to verify their identity.
Strengths

• As all smartphones have cameras, they are capable of scanning QR codes if they are equipped with the right software.
• QR codes are very flexible in that they can be displayed just about anywhere.

Considerations

• To validate a QR code displayed on a device, a terminal will need an optical scanner and compatible software.
• To actually obtain information from a QR code, a mobile device will need Internet connectivity it can use to access the related link.
• Scanning a QR code is a relatively cumbersome process involving several steps.
• QR codes are easy to copy and are therefore inherently insecure.

Actual deployments

Many merchants and brands have printed QR codes in their literature and on adverts to help consumers navigate to their web sites.

In summary: QR codes are relatively inexpensive to deploy, but they don’t typically provide an intuitive or elegant experience for the consumer, limiting their uptake and usage.
Wi-Fi overview

A short-range wireless technology offering high data throughput speeds, Wi-Fi is widely used to provide Internet access inside buildings, including retail stores, hotels, venues, cafes, bars and restaurants. Premises owners typically offer Wi-Fi connectivity. Each router has a range of up to 50 metres indoors and 100 metres outdoors, via one of three different models. Free access to Wi-Fi can simply be an inducement to visit the merchant’s premises. Alternatively, Wi-Fi may be offered as a free service that requires the user to register and receive marketing messages and advertising, or it may be provided as a paid-for service designed to increase revenue in shops. As each Wi-Fi router transmits an identifier, Wi-Fi signals can be used by a mobile app (which has access to an appropriate database) to determine its location, in a similar way to a BLE beacon (see previous section).

Its role in the customer journey

Wi-Fi can be used to provide basic connectivity throughout the customer journey. In the travel and in-store stages, it can also be used to help a mobile app determine its location and then access relevant content, such as venue information, offers or vouchers, over the Internet. Moreover, Wi-Fi can also be used to facilitate transactions, whereby the consumer makes an online payment, rather than using a point of sale terminal in the premises.

Example use cases

In-store: When Jean enters her local supermarket, her smartphone automatically logs onto the free Wi-Fi network. As she registered for the service on her previous visit, the Wi-Fi network recognises her handset and informs the store’s customer relationship management (CRM) system that Jean is in the store. As the store has Jean’s mobile phone number, it sends her a text message welcoming her to the store and containing a link to a personalised list of offers. Jean opens the link and touches one of the offers, the store then uses the Wi-Fi network to show her a store map indicating which aisle the product is in.

Post transaction: The store’s Wi-Fi network detects Jean is leaving the supermarket, prompting the retailer’s CRM system to send her a thank you text message with a link to a digital receipt showing her loyalty points balance and voucher for a free coffee in the supermarket’s café.
Free access to Wi-Fi can simply be an inducement to visit the merchant’s premises.

**Strengths**
- Nearly every smartphone supports Wi-Fi.
- Wi-Fi routers are already widely deployed in retail stores, hotels, venues, restaurants and cafes.

**Considerations**
- The user typically has to connect manually the first time.
- Some people disable the Wi-Fi on their mobile device so as to preserve the battery life.
- Many Wi-Fi networks aren’t designed to authenticate users.
- Wi-Fi networks typically aren’t secure.
- As they operate in unlicensed spectrum, Wi-Fi networks often suffer from interference, impacting the quality of the connectivity.

**Actual deployments**
Several mobile operators, such as Everything Everywhere and O2 UK, are working with merchants to deploy Wi-Fi in their stores. In some cases, these systems are used to relay targeted marketing messages to consumers.

In summary: A highly versatile and relatively inexpensive technology, Wi-Fi can play a significant role in enriching the customer journey. However, Wi-Fi isn’t typically secure enough or reliable enough to be used for ‘mission-critical’ applications, such as transactions.
Conclusions

Each of the technologies discussed in this paper can enhance various stages of the customer journey in a retail environment. Whereas some of them will play a pivotal role, others will be more tangential. The table that follows summarises the key attributes of each technology.

As the table outlines, each of the technologies discussed in this paper can add value at various stages in the customer journey. For example, BLE beacons and Wi-Fi can help to pinpoint a consumer’s precise location and provide them with immediately relevant information, while NFC is well-suited to enabling consumer-initiated interactions, such as a payment, as NFC’s limited range gives the consumer a sense of control and security.

Looking across the customer journey, many consumers will want a mobile wallet or equivalent app to help them organise their interactions with multiple merchants. Without an aggregation app (or wallet), a consumer would need to interact with dozens of apps and websites to make use of different merchants’ vouchers, offers and loyalty programmes.

Moreover, in many markets, secure element NFC is likely to be widely used to enable secure, quick and straightforward transactions in bricks and mortar stores. As the process of provisioning secure elements matures and becomes more streamlined, this technology will become more appealing to both banks and merchants. Apple’s move to include NFC payment on the secure element will help to drive supporting infrastructure on the merchant side including NFC point of sales (PoS) terminals that will accelerate the overall adoption of NFC. If it is to play a major role, host card emulation NFC will need to be bolstered by additional security mechanisms that can protect sensitive data.

However, technology choices should take into account local factors, such as the availability of Wi-Fi, in-door cellular coverage and how many consumers have NFC handsets.

Mobile operators and banks should also carefully evaluate the value that each of these technologies can bring to different kinds of merchants – whereas some merchants may prefer to use their stores primarily as showrooms for their online offerings, others will want to complete the majority of their transactions in store.

Ideally, an operator-supported digital commerce proposition will enable merchants, banks and other service providers to scale up where a level of consistency or interoperability is required, while mixing and matching mobile technologies in line with the merchants’ requirements.

Where possible, each of these emerging technologies should be implemented in a consistent way that enables the industry to gain economies of scale and consumers and merchants to become familiar with their role in the customer journey. To that end, mobile operators need to work with each other, as well as adjacent industries, to ensure the consumer gets the best possible experience, whilst delivering merchants the widest possible footfall.

In summary, both mobile wallets and secure elements look set to become fundamental enablers of a compelling customer retail journey. Both technologies can simplify consumers’ lives by helping them manage and store payment cards, vouchers, loyalty programmes, tickets, receipts and other commerce-related collateral. Moreover, mobile wallets and secure elements can also help consumers, merchants and banks keep this collateral safe and private. Security is crucial: To be successful, any digital commerce proposition must maintain the trust and confidence of both upstream and downstream customers.
<table>
<thead>
<tr>
<th>TECHNOLOGY</th>
<th>RANGE</th>
<th>WHICH STAGES OF THE CUSTOMER JOURNEY CAN IT SUPPORT?</th>
<th>PRIMARY ROLE</th>
<th>STRENGTHS</th>
<th>CONSIDERATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile Wallet</td>
<td>Not applicable</td>
<td>Every stage of the customer journey</td>
<td>Enable consumers to manage commerce-related content, such as offers, vouchers, loyalty programmes and payment cards</td>
<td>Provides simplicity and consistency for the consumer&lt;br&gt;Provides a personalised 'street level' view of relevant merchants and apps</td>
<td>Should be underpinned by a robust authentication mechanism&lt;br&gt;Should act as a gateway to merchants’ apps and/or content</td>
</tr>
<tr>
<td>One way beacon</td>
<td>Up to 50 metres</td>
<td>Outward travel&lt;br&gt;In-store</td>
<td>Enable consumers to receive location-relevant information and offers</td>
<td>Low cost to install&lt;br&gt;Simple to install&lt;br&gt;Precise location-finding</td>
<td>Danger of bombarding the consumer with notifications&lt;br&gt;Beacons can be insecure</td>
</tr>
<tr>
<td>Two-way beacon</td>
<td>Up to 50 metres</td>
<td>In-store&lt;br&gt;Transacting</td>
<td>Enable consumers to interact with a merchant</td>
<td>Enables interactivity where there is no Wi-Fi or cellular connectivity</td>
<td>Requires changes in consumer behaviour&lt;br&gt;No standards to implement payments on BLE</td>
</tr>
<tr>
<td>Secure element NFC</td>
<td>A few centimetres</td>
<td>Every stage of the customer journey</td>
<td>Enable consumers to securely store commerce-related content, such as vouchers, tickets and payment cards</td>
<td>High level of security&lt;br&gt;Simple and intuitive</td>
<td>Requires provisioning of the commerce application by the owner of the secure element</td>
</tr>
<tr>
<td>Host card emulation NFC</td>
<td>A few centimetres</td>
<td>Outward travel&lt;br&gt;In-store&lt;br&gt;Transacting</td>
<td>Enable consumers to receive and validate low value vouchers and tickets</td>
<td>Streamlines the deployment of NFC-based services</td>
<td>May require a connection to the cloud to securely authorise transactions&lt;br&gt;Requires the phone to be turned on and the relevant payment app running</td>
</tr>
<tr>
<td>QR codes</td>
<td>Depends on the size of the code</td>
<td>Outward travel&lt;br&gt;In-store&lt;br&gt;Transacting</td>
<td>Enables consumers to download a relevant app, information or a voucher</td>
<td>All smartphones are capable of scanning QR codes if they are equipped with the right software&lt;br&gt;QR codes can be displayed just about anywhere</td>
<td>Scanning a QR code is a relatively cumbersome process&lt;br&gt;QR codes can be easy to copy and can be insecure&lt;br&gt;May require new point of sale equipment</td>
</tr>
<tr>
<td>Wi-Fi</td>
<td>Each router has a range of 50 metres</td>
<td>Outward travel&lt;br&gt;In-store</td>
<td>Enables consumers to receive location-relevant information and offers</td>
<td>Nearly every smartphone supports Wi-Fi&lt;br&gt;Wi-Fi routers are already widely deployed in retail stores, hotels, venues, restaurants and cafes</td>
<td>Some people disable the Wi-Fi on their mobile device&lt;br&gt;The user typically has to connect manually the first time&lt;br&gt;Wi-Fi networks typically aren’t secure</td>
</tr>
</tbody>
</table>
About the GSMA

The GSMA represents the interests of mobile operators worldwide. Spanning more than 220 countries, the GSMA unites nearly 800 of the world’s mobile operators with 250 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and Internet companies, as well as organisations in industry sectors such as financial services, healthcare, media, transport and utilities. The GSMA also produces industry-leading events such as Mobile World Congress and Mobile Asia Expo.