**Technologies and Architecture**

There are various technologies that are currently being used for the implementation of mobile payment. Each has its own advantages and disadvantages and are used in different contexts based on the technology that best meets the needs of the consumers. For example, USSD is used mainly in developing countries because of its ease of use as well as not needing a smartphone or additional hardware to operate. The seven technologies we investigated are listed and explained below.

**USSD (Unstructured Supplementary Service Data) 1**

This technology relies on sending information using radio waves. Although not popular in North America, it makes up most of the mobile web traffic in developing countries. Worldwide, it has a usage rate of approximately 4% of mobile users (2013). Although a convenient and attractive choice for users in developing countries, the technology is not commonly used in North America because it sends information in plain text format, which means that anyone who intercepts the data can read the data without needing to decrypt it. This makes data interference and theft much easier because the intercepting party can read exactly what the sender and receiver are sending to each other. Because of the simplicity of the technology, it is easy to use as well as easy to implement with other programs that can manipulate the data.

**BLE (Bluetooth Low Energy) 1**

Bluetooth Low Energy is a newer technology that hasn’t yet gained full acceptance, despite having some attractive key points. BLE has a transfer rate of 1Mbit/sec, while only using 10mW of power. This is a very attractive point for mobile devices, as battery power is a very important consideration for any program running on a mobile device. Bluetooth Low Energy is similar to Bluetooth in that they both use radio waves to send and receive information. However, BLE has a rather large transmission and reception range – 50 m to 150m. Despite having a transfer rate of 1Mbit/sec, BLE is not designed for file transfer, is only used for small chunks of data, and does not support streaming. BLE has a 40% usage rate and is already embedded in many smartphones on the market today. Additionally, it is easy to use, consumes very little power, and is well-supported. Unfortunately, range seems to act as a double-edged sword; although having a large range is good for the user not needing to be close to the receiving terminal, it does pose security risks, as anyone within a 50-150m radius can potentially intercept the data. Additionally, BLE does not provide for backwards compatibility, so does not work with other version of Bluetooth.

**SMS (Short Message Service) 1**

SMS has a very high usage rate and is nearly ubiquitous nowadays. Most people are familiar with SMS, as it is the format used to send text messages between devices. Many retailers are already using SMS as a solution to a number of different problems, such as digital promotional codes, confirmation codes, and sign-up procedures. Similar to USSD, SMS sends information using radio waves and in an unencrypted state. Because of this, it has lower security than other transmission methods (an additional security layer is required if information needs to be sent in encrypted format). Some of the advantages of SMS include it being present on nearly all mobile devices worldwide and does not require the device to be a smartphone. This can be used to capture a larger mobile audience in areas where the consumer base does not have a high percentage of newer technologies, such as in developing countries. Unfortunately, SMS is usually regulated by data charges for each message sent. This can make it more expensive for the consumer. As well, SMS is an asynchronous technology, which can make communication between sender and receiver slower because devices must talk “back and forth” instead of simultaneously.

**WAP (Wireless Application Protocol) 1**

Though not a hardware technology, WAP is a standard protocol that enables wireless communication between enabled devices. It operates with many different networks, as well as proprietary Wi-Fi. Many people use this protocol, and as such, there is a worldwide penetration rate of 38%. Users may be familiar with LTE (Long-Term Evolution), which is a newer technology enabling greater data transfer throughput, which runs on the WAP protocol. Because WAP is a robust protocol with security layers, it provides a greater security than that offered by USSD, BLE, or SMS. Additionally, the protocol also enables synchronous data transfer, making it faster and more secure than SMS. The downside of WAP is for the consumer, who must pay for data over the network through which it is being transmitted.

**QR Codes 1, 3**

QR codes have been around since the mid 1990’s, and were developed in Japan by Denso Corporation. The QR code is designed to be read by a camera and then processed by the mobile device’s internal processing software. Nowadays, there is a 16% usage rate worldwide. A QR code is a square with black and white areas that encode information vertically as well as horizontally. Because of a high information density in QR codes, they can be used to provide a visual encoding of much information about the product upon which it is placed. Alternatively, the data on the QR code can be a URL which can then be used by the mobile device to connect with a website. QR codes are used in mobile payment as a way of storing and passing information between devices that are optically enabled. In other words, a consumer can display a QR code on their mobile screen and the retailer can scan this code to apply the information present in the form of coupons, discounts, unique identifiers, or event tickets. Because QR codes only provide a one-way interaction, they are more cumbersome to use as a payment method, since the paying device first needs to generate a QR code which the retailer must then scan. Despite this, QR codes are only available with smartphones and there are definite security risks involved, as when someone deliberately modifies the QR code in order to redirect the user to a malicious website. This kind of attack can be used in the same way as a phishing attack, where users are directed to websites that mimic the expected website, but that exist to steal passwords or personal information.

**NFC (Near Field Communication) 1, 2, 4**

Near Field Communication is a newer technology that has been in development for several years now. It has received a lot of support and backing from large companies such as Google and more recently, Apple. Unlike other forms of mobile communication, NFC uses magnetic fields instead of radio waves in order to communicate. Using NFC, two mobile devices are able to communicate at a distance of 4-10 cm. This is more amenable to transactions that require a consumer to tap or bring their phone into close proximity of a receiver terminal at the POS. This feature makes NFC very attractive from a security standpoint, as someone who wishes to read the data being transferred would need to be within 10 cm of the transmitting device. This would obviously be quite noticeable when making a transaction. Traditionally, hackers would be able to sit in a coffee shop with their RF-enabled laptop which would snoop on the data being transmitted from customers to the retailer. This is no longer possible with NFC. Due to being in development for a long time, NFC has had a rather low adoption rate (8% in 2013), but has since become quite popular with the introduction of Apple’s iPhone6. Since the release of Apple Pay at participating retailers, the usage rate of NFC nearly doubled in the first week of the iPhone 6 alone. NFC is an attractive option as it is faster and easier than traditional debit card payments (~15 seconds per transaction). Additionally, it is secure because there is a security layer implemented in the NFC chips. Yet another benefit of NFC is that it is compatible with RFID chips, which has the benefit that with the proper software, users will be able to grab information from any RFID chip attached to products. In other words, NFC provides for the same kind of information sharing capabilities in QR codes that appear on products. Because an RFID chip can contain more information than a QR code, a consumer could use their phone to get product specifications on their device by waving the device near the product. Unfortunately, this technology, because it uses magnetic fields instead of radio waves, needs additional hardware to operate (though this is present in many newer device models). This creates a barrier to use in countries where there is a low smartphone use. However, it is also possible to use an SD or SIM card with an embedded NFC chip to upgrade to this functionality.

**Sound Wave Payment 1, 5**

The final technology investigated is that use by Alipay Wallet. Sound Wave Payment is a technology first developed by startup Naratte as “Zoosh tech” that uses ultrasonic sound waves to send information to the receiving device. Since ultrasonic is outside of the human hearing range, it can be added to a jingle or sound clip on a device and then played at the POS to send the desired information. Currently, this technology is used widely in China as part of the Alipay Wallet suite. SWP has the disadvantage of being asynchronous. As well, it is largely environment-dependent and is subject to audio interference (data may not be received intact if there are other ultrasonic sound waves in the close vicinity. This can add a security risk, since third party hackers can corrupt or interfere with the data transmitted by transmitting their own ultrasonic sound waves. On the plus side, however, it is relatively inexpensive for the retailer and consumer (phones are already enabled to produce sound waves, and the retailer can buy a simple microphone that will pick up the sound waves for about 4 dollars).

**References**

1. Lerner, T. (2013). *Mobile Payment*. Mainz: Springer Fachmedien Wiesbaden. (pp.39-50)

2. *Apple’s iPhone 6 NFC chip is restricted to Apple Pay.* Retrieved Nov. 11, 2014 from <http://www.theverge.com/2014/9/16/6204999/iphone-6-nfc-chip-locked-to-apple-pay#ooid=JrcHI3cDo6P9WbwZtLPsrmN47s3xpkL->

3. *History of QR Code | QRCode.com* . Retrieved Nov. 17, 2014 from <http://www.qrcode.com/en/history/>

4. *Near Field Communication: What is Near Field Communication?* Retrieved Nov. 11, 2014 from <http://www.nearfieldcommunication.org>

5. *Alipay Launches Sound Wave Payment Technology in Beijing Subway | Tech Crunch*. Retrieved Nov 11, 2014 from <http://techcrunch.com/2013/04/14/alipay-launches-sound-wave-mobile-payments-system-in-beijing-subway/>