On privacy aware carriers for value-possessed e-invoices considering intelligence mining

Shih-Chao Cha*, Hao Wang †, Zhiyuan Tan ‡, Yuh-Jzer Joung§, Yen-Chung Tseng§, and Kuo-Hui Yeh¶
*Dept. of Information Management, National Taiwan University of Science and Technology, Taipei, Taiwan
†Norwegian University of Science and Technology, Norway
‡School of Computing, Edinburgh Napier University, UK
§Dept. of Information Management, National Taiwan University, Taipei, Taiwan
¶Dept. of Information Management, National Dong Hwa University, Hualien, Taiwan
¶Dept. of Computer Science and Engineering, National Sun Yat-sen University, Kaohsiung 804, Taiwan R.O.C.

***Abstract*—Intelligence mining is one of the most promising technologies for effectively extracting intelligence (and knowledge) to enhance the quality of decision-making. In Taiwan, the government curtails underground economic activities and facilitates tax management via ubiquitous e-invoice information processing and intelligence mining for B2C transactions with management realized via privacy-preserved and robust consumer carriers. In this paper, we study the concept of carriers, a medium that facilitates the transfer of an e-invoice from a business to a consumer in a B2C transaction. Implementations of carriers not only depend on the underlying hardware, software, and network infrastructures that support their services, but also on consumers willingness to use them. In this paper, we review Taiwans Second Generation E-invoicing System, which is designed to promote the use of e-invoices in the consumer sector, and identify four problems that require further attention. These problems are: (1) no e-invoice data for immediate review; (2) limited readability of carriers by POS (Point of Sales); (3) lack of seamless integration into purchase behaviors; and (4) carrier traceability. We then discuss possible solutions to overcome these concerns, in hope of offering some insight into future mobile commerce based on e-invoice carriers in the cloud computing era.**

I. Introduction

In recent years, governments around the world have been promoting e-invoices as part of their agendas to reduce paper consumption, integrate e-invoices with digitalized government processes, and curb tax evasion. E-invoicing (or electronic invoicing) is defined as the "sending, receipt, and storage of invoices in electronic format without the use of paper-based invoices as tax originals [1]." The term has been associated with e-commerce in the context of Electronic Data Interchange (EDI), which delivers information such as purchase orders and invoices from business to business. As businesses utilize e-invoices on a much larger scale nowadays than in the past, new standards have been established, for example, to enable integrity of data, authentication of transactions, and interoperability across borders [2], [3].

Although e-invoices have been successfully adopted for some B2B transactions, in terms of quantity, they account for only a very small portion of the total number of business transactions. For example, in Taiwan, over 8 billion paper invoices are produced in a given year, while only 300 to 400 million invoices were B2B.[1] However, electronization of B2C transactions is still in an early stage. One major reason for this is consumers acceptance. Even so, the electronization of B2B transactions was a natural product of the advent of certain information and communication technologies. Maintaining transaction records in electronic form not only helps businesses speed up the transaction process and facilitates its management, but also lends itself to more advanced applications, such as market forecasting, CRM, etc.

For consumers, a transaction record is most often used for checking if the items and amounts are correct.[2] Unless consumers can somehow easily review the details of a transaction via other means, paper-based invoices seem indispensable for offline B2C transactions. Fortunately, recent advances in mobile devices might help solve the problem. For example, Google Wallet allows its users to store debit cards, credit cards, gift cards, etc. in an NFC-enabled Android phone for secure and fast mobile payment [4]. Transaction details can certainly be stored in the wallet as well.

Once transaction records can be easily accessed by consumers, the benefits of e-invoices become more evident to them, for managing personal expenditures and finances, for example. Imagine how the value of e-invoices can be enhanced if consumers can review their expenditures in given time intervals and according to different categories. In fact, some stores already offer such services through their membership programs. Customers who shop with loyalty cards may have their transaction records maintained in the stores information systems where they are available for them to review. This also helps the stores to offer better, customized services. Since loyalty cards are issued by stores independently, it is difficult for a consumer to access his/her transaction records at different stores simultaneously (say, for cross-referencing purposes). The deployment of e-invoices on a national scale in the consumer sector helps to resolve the problem.

[1] Internal information.

[2] Sometimes a transaction record may be kept as a proof of purchase for possible return of items. However, as long as businesses keep transaction records in their information systems, returning items with receipts is not necessary.

In Taiwan, the government has implemented a project entitled “the Second Generation E-invoicing System” to promote e-invoices in the consumer sector [5]. The project involved building a platform to store all transaction records for tax-related auditing, as well as offering many innovative services based on the “big data”. Consumers can also access their transaction records and related services through the platform.

B2C invoices typically contain none of the buyers information. To allow an e-invoice to be linked to a consumer, the concept of “carriers” has been conceived [6]. Conceptually, an *(e-invoice) carrier* is an identifiable container for carrying e-invoices, but in essence it is just an identification that is used to associate e-invoice data to an entity. For instance, loyalty cards, membership cards, identity cards, and cell phone numbers can all be used as carriers. Multiple carriers are allowed in Taiwans e-invoice platform, not only to ease the integration of existing systems into the platform, but also to alleviate security and privacy concerns by allowing a single carrier to retrieve all the transaction records of a citizen. The platform also makes it much easier and more convenient to claim winnings from a lottery mechanism that is unique to Taiwans invoice system. The lottery mechanism was designed to incentivize buyers to request copies of invoices. This is aimed at ensuring merchants will faithfully report their sales, thereby reducing tax evasion and boosting the government’s tax income.

Despite the above advantages, many consumers are still reluctant to use carriers to collect e-inovices. According to internal government information, of all the issued B2C e-invoices in Taiwan, only 5% are associated with carriers. This then motivates us to conduct a case study on e-invoice carriers in Taiwan and discuss the potential problems and solutions. In short, we identify four problems that require further attention: (1) no e-invoice data for immediate review; (2) limited readability of carriers by POS; (3) lack of seamless integration with purchase behaviors; and (4) carrier traceability. We examine each problem in detail and propose possible solutions to overcome relevant concerns. We hope that our study will offer some insight into a more successful deployment of B2C e-invoice systems in the cloud computing era.

Note that conventionally an “invoice” is a request for payment of a sale, while a “receipt” is a proof of payment. Nevertheless, the two include similar contents, such as a list of goods or services offered, the amount of the payment, buyer or seller information, the transaction date, etc. Herein, we will use the terms “e-invoice” and “digital receipt” interchangeably to refer to a bill received by a buyer upon payment, for the following two reasons:

1) This paper focuses on B2C transactions, and from a buyer’s perspective, s/he usually receives a proof of purchase, rather than a request for payment, in a transaction.
2) Taiwan officially uses the term “Uniform Invoice” to represent the bill received by a buyer during a transaction, the digitalization of which naturally becomes “(uniform) e-invoice”. Since we are focusing on Taiwan’s “e-invoice” system, we will adhere to the terminology in use to avoid confusion.

II. Related Work

A growing body of literature recognizes the importance of the management and utilization of electronic receipts. There are three main categories of applications of the electronic receipts, namely provision of value-added services, receipt recognition and individual privacy protection.

To start with the provision of the value-added services, several researchers have proposed different schemes and incentives for people in order to reduce the number of paper receipts issued. Ho et al. [7] conducted an examination with questionnaires to evaluate acceptance of mobile payment with digital receipts. The authors provided three ways for customers to obtain receipts: traditional paper receipts, Two-dimensional (2D) barcodes, and Near Field Communication (NFC). Besides, a mobile application with value-added services, such as the control of personal spending and purchase tracking was provided to users. The results showed that most people were willing to use mobile payment with digital receipts because of the value-added services and time savings. Wadsworth et al. [8] and Tokunaga et al. [9] proposed platforms for customers to manage their receipts through a web interface. Wadsworth et al. [8] integrated the cash register system (CRS) and the receipt management system (RMS) to increase user convenience by enabling them to search for a particular receipt (with consistent a format) in just seconds. Likewise, Tokunaga et al. [9] provided functions to allow users to review their daily digital receipts and share their receipts online. In comparison with [8], [9], Vadde et al. [10] introduced an Android App with NFC technology to allow customers to communicate with a billing kiosk and get digital receipts. In this way, the users can view receipts using app on their phones, which can help them manage their spending. Hasan and Khalid [11] proposed a Multimedia Messaging Services (MMS)-based solution to send digital receipts to users smartphones. MMS include a variety of multimedia content such as images, documents or audio, which can have a higher level of personalization for users.

Next, receipt recognition is also an important application because of the high cost of traditional (i.e., paper-based) document processing. Shen and Tijerino [12] presented an extraction ontology to recognize the contents of Japanese receipts. These extracted data with different fields could be used for a specific accounting system. Altmeyer et al. [13] implemented a smartphone application to allow German customers to take photos of receipts and extract useful information therefrom, such as the stores name, purchased items, and their prices. Thus, the users can track their expenses and manage their budgets. In addition, the authors introduced game elements to enhance the accuracy of recognition and provide incentives for users to use the application. Similarly, Suponenkovs et al. [14] combined the technologies of image recognition and machine learning to recognize receipts and analyze extracted data.

In addition to consumer utilization of the digital receipts, privacy protection is also important since these receipts may reveal sensitive information such as the consumer's purchase history and habits. Lee et al. [15] utilized the transaction ID instead of the IDs of the seller and buyer to prevent the leakage of participants IDs in transactions. Paci et al. [16] utilized cryptographic methods and OCBE protocols to design a privacy-preserving protocol on NFC enabled devices which can protect private information recorded in the receipts.

III. Taiwan's E-invoice System

In Taiwan, invoices are formally called "Uniform Invoices". The name was coined because every official invoice must follow the same printed format specified by the government (and until the 1990s, all blank invoices were supplied by the government). In addition to the usual data such as the date, items, and amount of a transaction, each invoice records the seller's ID, which was assigned by the government when a company registered its name and business. Every company must register in Taiwan. The seller IDs allow the government to trace transactions so as to collect taxes from sellers. Each invoice in an issuance period has a unique alphanumeric serial, called the Uniform Invoice Number or UIN. The UIN is integral to an innovative lottery mechanism uniquely tied to Taiwan's invoice system.

The lottery mechanism, referred to as the Uniform Invoice Lottery (UIL), is implemented to give prizes to some invoice holders periodically as an incentive for citizens to request invoices when completing transactions. Periodically (currently every two months), the UIL draws several winning UINs. Each invoice whose UIN matches specified portions of the drawn UINs entitles the holder to claim cash prizes ranging from 200 NTD to 10 million NTD. The average odds of winning are moderately high at 0.3$\sim$0.4%, thus incentivizing citizens to acquire invoices for transactions. As a result, customers essentially monitor the businesses, ensuring that they honestly produce invoices. In the early years of the Taiwanese government, the UIL had great success in curbing tax-related exploitation (i.e. tax evasion), leading to a substantial increase in tax income [17]. Please refer to [18] for an overview of Taiwan's uniform invoice system.

The advent of information technology has made it possible to electronically create, process, exchange, and transmit invoices. The first major electronization of uniform invoices was initiated in 2000. The target was B2B transactions, as during that time, Taiwan's IT industries were building enterprise resource planning (ERP) systems to integrate their supply chains. By selecting some major companies to pilot e-invoicing, the intent was that these companies could push their suppliers to adopt e-invoicing as well. The suppliers may then, in turn, push the e-invoicing technology onto their own supply chains, creating a "ripple effect" to speed up the adoption rate. The e-invoicing project was subsequently expanded in 2005 to include its coverage to online B2C transactions. On Dec. 6th, 2006, the first generation e-invoice platform began to operate, allowing businesses to create, transfer, exchange, or store e-invoices over the platform.

As mentioned earlier, the number of B2B transaction invoices accounts for only a very small fraction of all transactions that occur in business. Therefore, the Taiwanese government established a three-year project in May 2010 to promote use of e-invoices in the consumer sector. Several major retail chain stores have joined the project to collect first-hand user feedback for future improvement.[3] The project also aims to build a second generation e-invoice platform that improves upon the previous generation in terms of security, efficiency and scalability due to the vast amount of e-invoice data generated by B2C physical channels.

Below, we introduce the e-invoice specifications, followed by the platform's services in the B2C sector and the concept of a universal carrier in the platform.

A. E-invoice Specifications

Under the Message Implementation Guideline (MIG) [20], the electronic data an e-invoice contains is formatted as an XML file of standardized structure. The current MIG revision classifies the data into three major types:

- Main: identifiable information of the parties involved in each transaction, the date, carrier identification (if used), counterfeit random number, etc.
- Details: the name, unit price, quantity, and amount of goods transacted
- Amounts: total sale, tax-related data, currency, etc.

Most fields are typical for an invoice, and while some are designated to support carriers, such as the carrier identification field, others are for security purposes. For instance, the 4-digit counterfeit random number generated during a transaction aids in uniquely identifying an e-invoice. Without it, an imposter could duplicate an e-invoice of a specific UIN and claim the UIL prize before the legitimate customer does so.

The conversion from traditional paper-based invoices to e-invoices involves a parallel adoption in which both systems run simultaneously. At present, customers can still receive a paper copy of e-invoices if they desire. An e-invoice printed on paper also uses a standardized format, as shown in Fig. 1. In general, a paper e-invoice should be a strip of rectangular paper 5.7cm wide and of variable length. The top 4.5cm contains the date and time of transaction, period of issuance, UIN, counterfeit random number, amount, a Code 39 barcode, and a QR code. The 19-character-long barcode is a concatenation of the period of issuance, UIN, and counterfeit random number. This barcode makes reading an e-invoice into kiosks or other machines easier. The 2cm by 2cm QR code records 77 characters, including those in the barcode and a 24-character validation code. A validation code is the concatenation of the UIN and counterfeit random number encrypted in AES and encoded in Base64; it is used to strengthen the security of the counterfeit random number.

[3]Taiwan boasts the highest density of convenience stores in the world, with each store serving approximately 2,500 people on average [19]. These stores offer a wide range of daily items, such as food and toiletries. Promoting e-invoices through the chain stores helps speed up the adoption rate.

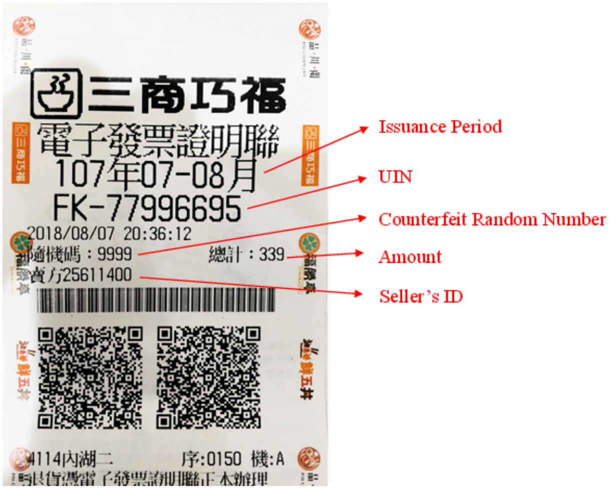

Fig. 1: A sample B2C paper e-invoice.

B. B2C e-Invoice Service Infrastructure

Whether paper-based or paperless, the life cycle of a B2C e-invoice follows the dataflow depicted in Fig. 2. A customer can engage in the process in several ways. For ease of understanding, each box represents a possible action on the corresponding relation, and similar actions are labeled with the same number or letter of the alphabet. First, a customer must register (1) and create an account in the platform. Then, he can import (2) his e-invoice carriers into his account so that the platform knows whom these carriers belong to. Note that more than one carrier can be imported to an account. During a transaction at a POS counter, if a customer presents his carrier[4] and requests an e-invoice (3), the e-invoice will be bound to the carrier holder (A) so that the customer may use the carrier to inquire (4) for the e-invoice later on. The e-invoice is also uploaded to the business's information system and to the e-invoice platform (B) for storage and processing. The customer may either present his carrier at the POS counter to check if he has won the UI lottery, or be informed automatically by the system the next time he presents the carrier (5). A customer can also configure her/his account so that the system automatically sends a notification when an e-invoice wins the UIL. Prizes can also be automatically transferred to a delegated bank account.

Registration, carrier import, and e-invoice inquiry can also be done at a kiosk commonly available in most retail chain stores in Taiwan. Should a customer win the UI lottery, they can use their carrier to claim the prize and perform a fund transfer to a delegated bank account, or alternatively, to convert the prize to a store credit on their loyalty/membership card (6). Performing this task at an e-invoice platform portal, a POS counter, or a kiosk saves the customer a trip to a branch of the national post office to claim a lottery prize, which requires presentation of a printed invoice copy.

[4]Currently, the supported carriers include value-added cards (e.g. iCash [21]), RFID cards (e.g. EasyCard [22]), debit cards, and General Carriers (see the next section).

Moreover, because each invoice has the potential to win a cash prize in the UIL, many customers donate their invoices to philanthropic organizations to help them raise funds. Traditionally, this is done via dropping paper invoices into designated charity boxes located in shops. With e-invoices, each organization can apply for a General Carrier (dubbed "Love and Care" serial code) (see the next section). A customer can present the serial code verbally or through a barcode to transfer an e-invoice to the corresponding organization. A customer may also donate their e-invoices to an organization at a kiosk (7) or through the e-invoice platform. Therefore, the evolution of this technology can also help philanthropic organizations raise funds through invoice donations.

C. General Carriers

A customer must register on the e-invoice platform in order to use its services. Originally, a Citizen Digital Certificate (CDC) that includes relevant citizenship information such as name, national ID number, bank account, etc. was required for registration. This requirement was met with much resistance, however.

Originally, the CDC was in the form of an IC card that could only be acquired at a Household Registration Office (for a small fee). To use the certificate on web services hosted by government, one needed a card-reader plugged into a computer to read the IC chip. Unfortunately, the card-readers do not come with standard PCs, so they have to be purchased separately (occasionally free card readers will be given to new applicants [23]). Although the CDC was released 10 years ago in 2003, the total number of citizens who have applied for this service remains at a level comprising a low percentage[5]. While the demand for e-invoices could spur the application of the CDC, the incentive may not be strong enough to yield a significant boost of the adoption rate. Besides, the technological learning curve involved also discourages those who lack computer skills from participating.

Second, tying up e-invoices with a CDC makes citizens purchases easily traceable and irrefutable. The government could, under legal circumstances, investigate a certain individual's purchasing records. This privacy concern, combined with the inconvenience of using the CDC, fueled demand for a simpler, anonymous carrier. The concept of a "General Carrier" was thus proposed in March 2012 [26] to solve the problem. It was also meant to be a "universal" carrier that allows a person to use it at different stores. Without this characteristic, one would need to carry a variety of carriers issued by different stores in order to collect e-invoices at the stores.

A General Carrier is an ID consisting of an 8-character serial code with a leading backslash followed by 7 letters, numbers, or symbols, as shown in Fig. 3. It can be presented as a Code 39 barcode to be read by machines. To apply for one, a user simply supplies a working cellular phone number and an e-mail address to the e-invoice platform. Since this serial code

[5]According to [24], the accumulated number of CDCs issued in 2011 was 2.5 million, which was less than 1/3 of the 7.9 million of households paying income taxes (paying tax online is one of the major purposes of CDC) [25].

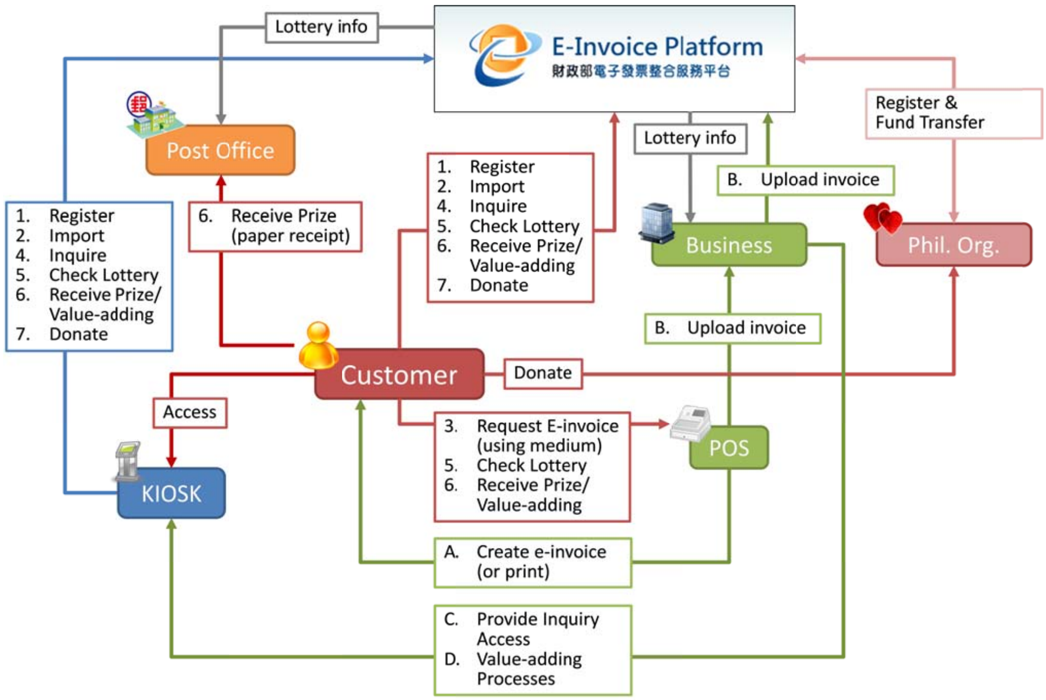

Fig. 2: B2C Data Flow

is associated with cellular phone number, it is also dubbed a "cellphone barcode". When a General Carrier is generated in the e-invoice platform, an account is created for the carrier so that they can use the account to manage their invoices, as well as to use the services provided by the platform. To access the account, a 4-digit PIN number is required. The user receives the PIN along with the serial code of the carrier via e-mail when they apply for a General Carrier. The PIN can be changed later on.

手機條碼：/-KX7+4Q

Fig. 3: Sample General Carrier

Each General Carrier is distinguishable by the confluence of the cellular phone number and e-mail address, meaning that a single cellular phone number can apply for multiple serial codes just by supplying different e-mail addresses. Similarly, multiple serial codes can be linked to a single e-mail address, enabling the management of separate purchase routines. This design also allows a user to have multiple accounts in the e-invoice platform, so as to increase privacy protection. With this design, the number of serial codes generated under high usage may be extremely large, but the code space is large enough for the entire Taiwanese population and all phone-mail pairs[6].

To use a General Carrier, a consumer can print the barcode onto a label and include the code at the bottom (see Fig. 3). The electronic file for this label is automatically generated as an image for ease of printing. Another viable option is to save the barcode image onto a mobile device with a display. During a purchase, the POS scans the barcode to link an e-invoice to the carrier.

IV. Issues in The Current Implementation

Having described Taiwan's e-invoice system and the carrier concept, we now discuss issues in the current implementation that require further attention. All of them are related to the use of carriers.

A. *No e-Invoice Data for Immediate Review*

Currently, consumers are still given a paper copy of an invoice containing transaction details (see Fig. 1) even if they use carriers to collect e-invoices in a transaction. The main reason for providing paper e-invoices is to allow consumers to review the details immediately after a transaction for possible errors. Clearly, this paper version of e-invoice can be omitted if a consumer believes that the purchase record is free of errors or there are digital alternatives for reviewing a purchase. Reviewing an e-invoice might be done at an on-site kiosk or via a user's mobile device connecting to the e-invoice platform.

[6]According to [27] the total number of cellphone numbers in Taiwan is 29.36 million. If only alphanumeric characters are used (case-sensitive), 62^7 is already many orders of magnitude beyond that.

Unfortunately, the e-invoice data may not be there in timely fashion.

According to [6], businesses should upload e-invoices to the e-invoice platform within 48 hours after transactions occur. This policy is different from countries such as Mexico, where government servers process and store e-invoices in real-time [28]. In Taiwan, businesses can choose to implement a real-time process (i.e. upload an e-invoice immediately after a transaction) or a delayed batch upload. At present, all companies opt for the latter.[7] Uploading e-invoices as fast as possible would require setting an extremely small interval between two consequent batch uploads, or uploading them immediately after each transaction. Typically, businesses would prefer to avoid doing so as it creates too much overhead for their IT infrastructure. Moreover, the current e-invoice platform is not optimized to serve a large number of individual uploads simultaneously.

Since no businesses upload in real-time, consumers cannot review e-invoices electronically and immediately after purchases because no data is available online. Although the process may become real-time in the future, giving consumers abbreviated form receipts appears to be the only option that enables an instant review of a transaction—unless a consumer has a device to receive an e-invoices during a transaction.

B. Limited Readability of Carriers by POS

In the current implementation of B2C e-invoices in Taiwan, a carrier does nothing with the POS other than giving it a string of identification code. However, even just reading carriers could sometimes pose a problem to an existing POS. As discussed before, several mediums can be used as carriers. For store-issued carriers (e.g., membership and loyalty cards), their POS systems can surely read the cards and thus retrieve the carrier IDs. For non-store-issued carriers, this is not necessarily true, even if the carriers are meant to be “universal”.

For example, recall the General Carriers discussed in Section III-C. Since they are generated via mobile phones, a natural medium to carry a General Carrier is a consumer’s smartphone, so that it can be displayed as a barcode on the smartphone’s screen to be scanned by a POS reader. However, depending on the technology used, existing barcode scanners may not be able to read a barcode displayed on a smartphone’s screen [29]. Specifically, if the scanner is laser-based (as opposed to LED-based), reading the barcode from a screen is highly likely to fail because laser scanners read by sensing the reflection of an emitted laser. Mobile device screens, such as those of smartphones, have layers of glass and filters that refract instead of reflecting light, making it difficult for sensors to read them. In contrast, LED-based scanners illuminate objects to be scanned and use CCD image sensors to read.

[7]Every business that wishes to upload e-invoices to the platform can download “Turnkey” software, which helps convert and validate e-invoice files to appropriate XML format, packages and signs them, and schedules the auto-upload interval.

While switching to LED-based scanners would solve the problem, businesses might still favor laser-based scanners because they can scan with higher precision from greater distances, regardless of the orientation of barcodes. Consequently, it falls upon consumers to print the barcode on labels as a fail-safe.

Note that the above issue could also have far-reaching implications for emerging O2O (Online to Offline) services, as consumers might have difficulties using digital coupons issued to their smartphones in a purely digital format. This, in turn, could undermine consumers’ purchase experiences.

C. Lack of Seamless Integration into Purchase Behaviors

Currently, the use of carriers is not seamlessly integrated with consumer purchase behaviors in the sense that the former are used just to associate e-invoices with specific buyers; payment is accomplished separately by another medium (e.g., credit/debit cards). For example, paying with General Carriers involves a two-step process: presenting a carrier barcode to be scanned by a POS reader, and then presenting a credit/debit card or using cash to pay for the goods. Some may consider this extra step to associate e-invoices a nuisance, and prefer paper invoices instead.

Some type of carriers may avoid the aforementioned problem. In Taipei, EasyCards are quite popular as they are the default pass card for public transportation services (MRT and buses). Over 29 million cards beenwere issued between 2002-2011 (compare this to the population of the island, which is 23 million) [22]. The company operating the EasyCard payment system has also successfully promoted the cards to university campuses and companies for use as an ID card and a security pass, as well as to convenience stores for payment of small amounts. The EasyCard is based on MIFARE’s contactless smart card technology, allowing a transaction to be completed by simply placing the card close to a reader. Since each EasyCard has a unique ID, it naturally became one of the first carriers supported by Taiwan’s e-invoice system. Shopping with EasyCards can seamlessly integrate the use of carriers into the payment process. The problem is that only small amount payments are allowed by EasyCards. Besides, the medium does not provide an immediate transaction review of the type mentioned in Section IV-A, as it is simply a plastic card with no display.

D. Carrier Traceability

The e-invoice platform processes and stores e-invoice data under the government’s supervision. With the massive amounts of data this generates, Taiwan’s government recognizes it’s potential in the big data realm. For example, businesses and research facilities could use B2C e-invoice data in a number of ways, such as market analysis, trend detection, consumer expenditure analysis, etc. The value of the data itself, along with the global trend toward e-government and open data [30] is pushing the government to seriously consider opening the e-invoice data to the public. However, if the data are stored as they are, people may conceivably consider such a move to be a privacy threat.

First, it should be noted that any transaction via a carrier produces an e-invoice that is directly linked to the carrier, meaning that using a carrier precludes an e-invoice's, and thus a transaction's, anonymity. A non-anonymous e-invoice stored on the e-invoice platform could be easily traced by the government to a specific carrier. As such, every time this carrier is used, its transaction data will be exposed and can be monitored by the government. If a consumer imports this carrier to their CDC account, the government can easily track the citizen's transaction records.

Moreover, unregulated, controversial applications may emerge at the expense of consumer privacy. For example, a large database of individual consumers' private information and purchasing records could be produced through data mining. It would be disconcerting if the public could access an unofficial, but highly detailed, profile of every consumer. It is conceivable that personally-tailored advertisements may become overwhelmingly pervasive, businesses could screen employees by examining their daily activities, and an individual's purchasing power might no longer remain a secret.

Fortunately, on Oct. 1, 2012, the government enacted the *Information Protection Act*, which restricts personal data from being elicited, processed, or used without the person consents or unless a case falls under specific exceptions, as stated in law. Nevertheless, the law functions passively as a discouragement of such privacy-invasive acts. A more proactive approach would be to implement carriers in a way that eliminates the traceability of e-invoices.

V. Possible Solutions

In the previous section, we have identified four problems related to carriers in the current e-invoice implementation environment in Taiwan, namely: (1) no e-invoice data for immediate review; (2) limited readability of carriers by POS; (3) lack of seamless integration into purchase behaviors; and (4) carrier traceability.

The first problem can be solved if the medium for carriers possesses some communication capability and storage capacity to allow it to receive invoice data from POS systems during transactions. A consumer could then review transaction details regardless of whether the corresponding e-invoice has been uploaded to the e-invoice platform or not. The second problem clearly relates to how a carrier medium communicates with a POS. The third problem is also tied to this issue because if the medium can communicate with a POS to process a payment, then no extra medium is required to store the carrier ID. Therefore, we begin this section by discussing possible communication methods between carrier mediums and POS readers.

The last problem can be overcome through a cryptography technique known as "blind signature". We propose an algorithm based on the technique to prevent carriers from being traceable. Finally, we discuss the possibility of integrating e-invoice carriers into the concept of a "digital wallet" to enhance user experiences.

A. Communications between Carrier Mediums and POS

The fact that smartphones have become the norm[8] suggests that they are an appealing medium for carriers. In fact, the General Carriers discussed in Section III-C were also meant to be supported by consumers' smartphones. Although currently they can only be displayed as barcodes on screens to be scanned by POS readers, as technology evolves, more convenient ways for using General Carriers via smartphones will emerge. Therefore, we focus on technologies in smartphones with the potential to facilitate communication between carriers and POS systems. We review three technologies: QR Code, Bluetooth, and NFC.

1) QR Code: A QR Code, short for Quick Response Code, is a two-dimensional barcode originally developed by Toyota's subsidiary Denso Wave in 1994 to track vehicles during manufacture [32]. Since then, numerous types have been proposed, but here we will refer to the ISO/IEC 18004:2006 standard for "automatic identification and data capture techniques" [33] or, namely, the type of QR Code most commonly seen today.

QR Codes can be easily generated by inputting the text message to be encoded to a program to produce the code. They can also be easily read using a phone's camera equipped with appropriate software to decode the image taken by the camera into the original text message. In the e-invoice scenario, the POS can encode transaction details into a QR Code and display the latter on a screen to allow the consumer to capture the image and decode it to plaintext. Although this approach requires consumers to scan the QR codes in order to view transaction details, it requires minimal intervention in the POS system, as no communication connection between consumer's devices and the POS system is needed.

However, the QR Code itself has some limitations. The volume of data a QR Code can hold is determined by its dimensions: the higher the dimensions, the denser the code. Among the 40 versions of QR Codes, a higher version number means it is larger and can store more characters [33]. Each version supports four levels of error correction: L (7%), M (15%), Q (25%), and H (30%), and a higher level reduces available storage for actual data. At maximum, version 40 L can store up to 4,296 characters or 2,953 binaries. In practice, however, version 40 is too large to be printed or displayed. In addition, an extremely high-resolution camera is required for an acceptable recognition rate at this density. Instead, smaller versions that hold less than 100 characters are much more common, such as the QR codes used in Taiwan's e-invoices.

Unfortunately, transaction details vary in length and can easily surpass the storage limit. Although it is theoretically possible to display multiple QR Codes in succession to allow transmission of data fragments that can be reassembled, that approach would greatly increase both the recognition time and

[8]According to eMarketer [31], six countries had smartphone penetration rates above 50% in 2012, and the worldwide smartphone penetration was projected to approach 50% in 2017.

the probability of error. To guarantee a high recognition rate and fast decoding, it would be wise to transmit not the actual data, but a URI string instead. This means an intermediate portal would have to be implemented by businesses, third-party service centers, or the government.

2) Bluetooth: Bluetooth is a wireless technology for data exchange standardized as IEEE 802.15.1 [34]. Created by Ericsson in 1994, it is currently maintained by the Bluetooth Special Interest Group, which consists of numerous firms in the telecommunications, computer, and other related industries. Bluetooth is frequently compared with IEEE 802.11 (branded as Wi-Fi), which is also a wireless technology. Both Bluetooth and Wi-Fi utilize radio waves of short wavelength in the 2400 to 2483.5 MHz band to transmit data, but Wi-Fi has a higher transmission rate and distance, albeit at the expense of higher power consumption, cost, and hardware/software requirements. As a result, Bluetooth is better suited for close (1 to 100 meters, depending on class), low-power, and low-bandwidth transmissions, such as transmitting an e-invoice's transaction details to a consumer's phone.

However, Bluetooth requires POS to actively choose the correct device within range to connect; a process known as pairing and bonding. If POS utilizes Bluetooth to transfer data, some degree of user interaction is necessary, such as vocally identifying the correct device name from among a list of possible pairings. In contrast, the NFC technology (see next section) has a transmission range of only around 10 centimeters. Thus, cashiers can easily determine whose device the POS is communicating with.

Assuming complete pairing and bonding, both software (i.e. an app) and an underlying protocol must be present to facilitate data transfer. In its most basic form, the POS simply sends an XML or JSON document, which the corresponding software on a phone can then save and display in a more user-friendly format. If transmission time is critical, the POS may also choose to send a URI string that links to an intermediate portal to read the transaction details.

3) NFC: NFC, or Near Field Communication, is a wireless communication technology based on existing RFID standards, or, more technically speaking, on magnetic field induction. Invented and defined in 2004 by a joint organization of Nokia, Philips, and Sony named the NFC Forum, NFC promotes interoperability among devices and developments in related products. NFC is standardized in ISO/IEC 18092 and ISO/IEC 21481, or NFCIP-1 and NFCIP-2, respectively. These standards detail modulation, encoding, transfer speeds, data format, protocols, and operation modes for NFC-enabled devices.

NFC can be roughly divided into two communication modes: passive and active. In the passive mode, an "initiator" provides a magnetic field to a "target" (e.g. NFC tag), which responds with a fixed message by drawing power from the provided field. In the active mode, both the initiator and target are powered, enabling them to generate their own magnetic fields to send messages. Since we are more concerned with communication between the POS and consumers' mobile devices, we shall focus on the active mode.

To facilitate inter-device communication, a common data format must be in place. The NFC Forum proposed the NFC Data Exchange Format (NDEF), which specifies how data should be encapsulated and segmented. Sending an NDEF message requires a peer-to-peer transfer protocol, so the NFC Forum provides the Simple NDEF Exchange Protocol (SNEP) as an answer. SNEP defines how a SNEP client should send requests and how the server should respond. Additionally, SNEP relies on an underlying data link layer named the Logical Link Control Protocol (LLCP) to achieve reliability. The LLCP has two service types: connectionless and connection-oriented. The first requires minimal setup but provides no guarantee of reliability or flow control. The latter, used by SNEP, enhances functions stated in NFCIP-1 to allow reliable, orderly delivery of data. Connection-oriented LLCP faciliates small-size file transfers, such as e-invoice transaction details.

By default, SNEP only requires the server side to respond to PUT[9] request messages with an information field up to 1024 octets, or 8-bits. Support for messages larger than 1024 octets is left as an implementation choice. In the scenario of sending/receiving transaction details, we can reasonably assume that the consumer plays the role of client while the POS plays the role of server. First, the consumer's mobile device issues a PUT request to the POS to upload carrier information, such as a General Carrier's serial code. The POS then accepts the request, receives the message, and responds SUCCESS back to consumer's device. However, when it comes to the transaction details, the default server implementation has no method to send information. Two options can rectify this:

1) The POS implements both the server and the client roles. To send transaction details, the POS has to assume the client role and issue a PUT request to the consumer's device. Depending on whether the consumer's device (now assuming the server role) supports information over 1024 octets, the POS either uploads the transaction details in their entirety, or a URI, to the transaction details via an intermediate portal.
2) The POS's server implementation has to support GET[10] requests from clients. After a consumer's device has uploaded carrier information, it issues a GET request to the POS, which will then respond with transaction details encapsulated in an NDEF message. Since the 1024-octet limit only applies to the server, the consumer's device should have no problem receiving the transaction details in their entirety. There is, however, an option to receive a URI instead, in order to reduce transmission time.

Modifications to SNEP, as described above, should be implemented on the POS since it would be easier to modify a POS than to modify consumers' mobile devices. If compatibility is an issue, sending a URI will ensure all NFC-enabled devices will correctly receive transaction details.

[9]Request to upload an NDEF message
[10]Request to retrieve an NDEF message.

Fig. 4: A practical NFC-based circumstance

Bluetooth, NFC, and QR Code are all valid mediums for communication between a consumer's mobile device and a POS. Unlike Bluetooth, NFC does not require device pairing. In addition, both Bluetooth and QR Code require some level of training on the consumer's side, which increases perceived complexity and may discourage adoption. Communication by NFC requires minimal configuration and simply requires placing the device close to a sensor—a step that a consumer does when they use the device to pay for a transaction, thus allowing the use of carriers to be seamlessly integrated into the consumer's purchase behavior.

B. A practical NFC-based scenario

Followed by the above discussions, we present a NFC-based scenario as a possible solution for communications between carrier mediums and a POS. An i-phone 8 (with iOS 13.0 beta 4) is simulated as a mobile device, while a Raspberry PI 3 (with Raspbian Buster Lite 4.19.57-v7+, NXP LibNFC NCI for Linux R2.4, and a PN7150 NFC module) acts as a mobile POS connected to an e-invoice management server. All of the experiment is programmed using Swift. The simulated POS and mobile device are as shown in Fig. 4. The following scenario is performed. First, the mobile device (i.e. the i-phone) sends a 12-byte unique number of an e-invoice in APDU (application protocol data unit)-defined format as a request to the POS (i.e. the Raspberry PI 3 embedded with a PN7150 NFC module). Note that the Raspberry PI 3 is operated in the card emulation mode. Upon receiving the request, the POS retrieves the corresponding e-invoice and send it back to the mobile device. Table I shows the response time for retrieving e-invoices with various sizes through NFC.

C. Blind Signature

There are several possible approaches for tackling the traceability and privacy issue surrounding e-invoice carriers, including generalization of data (i.e. removing private, identifiable information before releasing data to the public), legal regulations such as the *Personal Information Protection Act*, and obfuscation of the carrier information. Here we

TABLE I: Response time for retrieving an e-voice through NFC

Size of e-invoice retrieved	**Response time (ms)**
300	78.4
600	123.8
900	172.2
1200	225.6
1500	278.1
1800	380.4
2100	426.2
2400	475.2
2700	531
3000	585.3

TABLE II: List of variables in the proposed algorithm

Term	**Definition**
ID$_x$	Consumer's original carrier ID
TID$_x$	Consumer's temporary carrier ID
Timestamp	A timestamp
R	Random number generated by consumer
eINV(TID$_x$**)**	E-invoice associated with carrier **TID**$_x$
S	Signature value
(e, d)	e-invoice platform's public and private key pair, where $\mathbf{e} \cdot \mathbf{d} \equiv 1 \pmod{n}$
Encry$_k$**(Msg)**	Message Msg encrypted by key k. This is equivalent to computing $(\text{Msg})^k \pmod{n}$

focus on obfuscation of the carrier information, which avoids consumers' invoice data being traceable, while still allowing consumers to be able to complete transactions and enjoy the usual services offered by the e-invoice platform.

This notion of untraceable transactions, or untraceability, was first discussed by David Chaum, and was realized through a technology called *blind signature* [35]. Blind signature is a cryptosystem that prevents any third party from determining a data provider's information, while granting the ability to prove data provider's identity under certain circumstances. In brief, blind signature works as follows. A user first obfuscates private information using a random blinding factor. The blinded information is then sent to a signing agent to be signed, who, not knowing the blinding factor, cannot know the content of the blinded information. The signed information is sent back to the user, who can un-blind it to reveal and verify the signature of the signing agent. In this way, a piece of information can be signed (i.e., approved by authority) without letting the signing agent know anything about it. Blind signature can be implemented with an RSA signature scheme, which provides asymmetric key encryption. For instance, the signing agent signs with its private key, and the user decrypts with the public key to verify.

Below we present an algorithm to adapt the blind signature technique to Taiwan's e-invoices. We assume that consumers use mobile devices that are able to communicate with the POS via, for example, NFC. The variables and their definitions are shown in Table II. Operations such as '+' and '·' are modulo n unless otherwise specified, where n is the modulus used in the RSA scheme.

When a consumer places an NFC-enabled smartphone close to a POS reader, the phone produces a random blinding factor **R**, encrypted with **e**, and blinds the concatenation of $\mathbf{ID}_x$ and **Timestamp** to produce the temporary carrier ID $\mathbf{TID}_x$.

$$\mathbf{TID}_x \equiv (\mathbf{ID}_x + \mathbf{Timestamp}) \cdot \mathbf{R}^{\mathbf{e}}$$

The reader receives $\mathbf{TID}_x$, and the POS generates the e-invoice $\mathbf{eINV}(\mathbf{TID}_x)$, which is then uploaded to the e-invoice platform. The platform, upon receiving the e-invoice, uses its private key **d** to sign $\mathbf{TID}_x$, producing signature value **S** as follows.

$$\begin{aligned} \mathbf{S} &= \mathbf{Encry_d}(\mathbf{TID}_x) \\ &\equiv (\mathbf{ID}_x + \mathbf{Timestamp})^{\mathbf{d}} \cdot \mathbf{R}^{\mathbf{de}} \\ &\equiv (\mathbf{ID}_x + \mathbf{Timestamp})^{\mathbf{d}} \cdot \mathbf{R} \end{aligned}$$

A copy of e-invoice $\mathbf{eINV}(\mathbf{TID}_x)$ and its corresponding signature value **S** are stored in the platform's database. The platform then transmits **S** and $\mathbf{eINV}(\mathbf{TID}_x)$ back to the consumer through the store's POS.

The consumer has to verify if ***S*** is indeed sent by the e-invoice platform to ensure that the purchase is genuinely processed. To do so, the smartphone uses ***R*** to un-blind $\mathbf{TID}_x$ and public key ***e*** to verify **S** as follows.

$$\begin{aligned} (\frac{\mathbf{S}}{\mathbf{R}})^{\mathbf{e}} &\equiv \left(\frac{(\mathbf{ID}_x + \mathbf{Timestamp})^{\mathbf{d}} * \mathbf{R}}{\mathbf{R}}\right)^{\mathbf{e}} \\ &\equiv (\mathbf{ID}_x + \mathbf{Timestamp})^{\mathbf{de}} \\ &\equiv \mathbf{ID}_x + \mathbf{Timestamp} \end{aligned}$$

If the resulting $\mathbf{ID}_x$ and **Timestamp** match the originals, the consumer can be sure that the e-invoice is indeed signed by the platform and is correctly stored in database.

Later on, if the consumer needs to prove ownership of e-invoice $\mathbf{eINV}(\mathbf{TID}_x)$, they can present $\mathbf{eINV}(\mathbf{TID}_x)$, $\mathbf{ID}_x$**+Timestamp**, and **R** to a verification agent. The agent computes a signature $\mathbf{S'}$ using the above process and compares it with **S**. A match then proves the ownership.

Note that without the blinding factor **R** and the **timestamp**, it is virtually impossible to reverse-calculate the true carrier ID $\mathbf{ID}_x$ from $\mathbf{TID}_x$. Thus, during the entire transaction process, both the business (POS) and the e-invoice platform know nothing about the consumer's true carrier, and so no entity other than the consumer can access their private information and purchase records. Moreover, by varying the timestamp, the temporary carrier ID $\mathbf{TID}_x$ will be different for each transaction, which then makes tracing a certain $\mathbf{TID}_x$ meaningless.

An experimental implementation is done with an NFC-enabled Android-based smartphone (i.e. Nexus S) and a simulated POS on a Windows 7 PC equipped with the ACR 122U NFC reader. Due to the fact that Nexus S does not support NFC peer-to-peer communication, the NFC reader has to fall back to passive mode through card emulation[11] in order to "send" data back to the smartphone. Average throughput by this method has been tested and found to be 12Kbits/s.

[11]An NFC device emulates a contactless card containing data to be "sent" to another NFC device, which will read the emulated card and receive data.

D. Digital Wallet

A mobile device can further integrate a consumer's e-invoice experiences into a digital wallet. A digital wallet is an electronic device that supports electronic commercial transactions. This electronic device can be a physical device such as a smartphone, or a virtual device such as a PayPal account. Both types of device support the same basic function of enabling electronic payments, which translates to storing consumer credentials, credit/debit cards, bank accounts, gift cards, tokens, or any kind of virtual currency. Here, we focus on the physical representation of digital wallets.

Currently, using General Carriers to perform transactions requires an extra step to present the carrier barcode in order to link the e-invoice to the consumer. This medium is physically separated from the other medium (e.g., credit card, digital wallet, etc.) that is necessary to complete a transaction. As discussed earlier in this section, with mobile devices and wireless communication technology such as NFC, carrier information can be transferred electronically to the POS, which can also return data including, but not limited to, transaction details. However the act of paying has not yet been integrated together as a single step. With the combination of the digital wallet and communication with the POS, we can finally complete a transaction in one step, greatly simplifying the process. Reliable communication also opens the door to other services such as digital coupons, whose data can be transmitted digitally rather than read by a laser scanner at a POS (which can be problematic, as described in Section IV-B).

However, in the case of NFC, not all mobile devices support this technology. To this end, service providers have several ways to enable the necessary capability for consumers [36]:

1) Tray extension: A tray casing with smart chips and a NFC antenna embedded within that can be fitted onto a smartphone. A similar idea puts the chip and antenna onto a sticker, which can be pasted onto the back casing of a smartphone. This solution may prove costly, however, and would require changing the hardware extension itself to replace the chip inside.
2) UICC card, or, more commonly, a SIM card: A SIM card with a built-in smart chip and NFC antenna. Mobile operators may prefer this method since it ties a phone number to the NFC service.
3) Micro SD card: A Micro SD card that provides both storage and NFC capabilities. Any device that has a Micro SD slot can become NFC-compatible.

In 2011, the largest mobile operator in Taiwan, Chunghwa Telecom, partnered with EasyCard, MasterCard, Cathay United Bank, and other entities to offer a tray extension built for iPhone [37]. It also established a TSM service to provide authentication and security for future transactions conducted with NFC. In 2012, the Hami Digital Wallet application was introduced, along with a special SIM card that houses consumer credentials, although it requires an NFC-capable smartphone [38]. It should be noted that these services have not yet offerred direct support for carriers and related e-invoice services.

The idea of the digital wallet has been partly realized through several commercial solutions such as Google Wallet and Square Wallet [4], [39]. Although they have been expanded to only a limited number of countries outside the United States, other countries have made efforts to achieve the same goal. For example, in Japan, "digital money" is a common payment method. One very popular payment method is the Osaifu-Keitai (literally the "Wallet Phone") [40], which is based on a RFID smartcard named FeliCa. The technique has not yet supported paperless e-invoices, but recent efforts by some Japanese firms may change this [41], [42]. On the other hand, Korea has made great strides in realizing the digital wallet through NFC due to the joint efforts of numerous Korean mobile operators, card providers, government organizations and other related industries [43]. These firms come under one roof, known as the Grand NFC Korea Alliance. Special zones have been equipped to showcase a large range of NFC services including payments, loyalty programs, digital receipts, and more. The Alliance is also finding partners overseas, such as the Japanese mobile operator DOCOMO, to provide a hybrid environment in which both NFC and FeliCa can function.

The Korean implementation of digital wallet platforms via NFC-enabled smartphones most closely approaches Taiwan's e-invoice goals. However, the requirements set by Taiwan's e-invoices and the Uniform Invoice are unique; solutions will have to take problems such as transmission of carrier information, transaction details, and UIL procedures into account. As such, integration of existing digital wallet applications, carriers, and e-invoice services are imminent in the future.

We conclude that in order to solve the problems of communication, integration, and security/privacy that are involved when implementing full solution B2C e-invoicing, carriers should become active entities that facilitates the transmission of data. Mobile devices such as smartphones represent the kind of medium that will undoubtedly become inseparable from the modern implementation of e-invoicing. By borrowing smartphones hardware capabilities, not only can technical difficulties be overcome, but the possibility of developing applications such as O2O commerce is also realizable.

VI. Conclusions

Carriers, which were originally just meant to store or link e-invoices, are destined to become connected with other services to create a more complete environment for e-invoicing in the cloud computing era. A carriers system can stand alone by itself, but it is only the integration of such systems that can continuously generate value. It is also apparent that mobile devices are important enablers that give consumers the ability to utilize these services electronically. Without mobile devices, wireless communication would not be possible, making information transfer less easy, less secure, and less eco-friendly (because of paper consumption). The possibilities of these technologies are great; for instance, a consumer can read a NFC tag to purchase an item with the carrier information and payment options automatically sent to a portal hosted by a service provider. Digital coupons may be transferred wirelessly, rather than scanned, and subsequent payments and e-invoicing can be automatically completed.

Although Taiwan's Uniform Invoice system imposes unique specifications and challenges on carrier implementation, such as proof of ownership, inability to duplicate, confidentiality of private information, etc., the general problems of communication, integration, security/privacy are all issues that must be taken into consideration when building an e-invoice system. Multiple technologies can help to overcome these issues but as we have analyzed, mobile devices coupled with NFC technology are by far the better solution among available options. The future of e-invoicing should be built upon an infrastructure that facilitates innovative applications and services, and that is precisely what our solutions aim to accomplish.

References

[1] B. Koch, "E-invoicing/e-billing opportunities in a challenging market environment," Billentis, Switzerland, Tech. Rep., 2012.

[2] European Commission Informal Task Force on e-Invoicing, "European Electronic Invoicing (EEI) Final Report," European Commission, Tech. Rep., 2007.

[3] European Commission, "Council Directive 2010/45/EU," 2010.

[4] Google Inc., "Google Wallet FAQ," 2013.

[5] Council for Economic Planning and Development, R.O.C., "Accomplishments of e-invoicing project within last 5 years (translated)," 2010. [Online]. Available: http://www.cepd.gov.tw/m1.aspx?sNo=0014254&ex=4&ic=0000007

[6] E-Invoice Platform, Ministry of Finance, R.O.C., "Operation guidelines for trial implementation of e-invoicing in consumer channels (translated)," 2011. [Online]. Available: https://www.einvoice.nat.gov.tw/wSite/ct?xItem=1354802&ctNode=2350&mp=1

[7] E. Ho, S. Apostu, F. Michahelles, and A. Ilic, "Digital receipts: Fostering mobile payment adoption," in *Ambient Intelligence. AmI 2013., Lecture Notes in Computer Science*, vol. 8309. Springer, Cham, 2013, pp. 140–149.

[8] K. T. Wadsworth, M. T. Guido, J. F. Griffin, and A. Mandil, "An innovation in paper receipts: the electronic receipt management system," in *Proceedings of the 2010 IEEE Systems and Information Engineering Design Symposium*, 2010.

[9] S. Tokunaga, S. Matsumoto, and M. Nakamura, "Implementation and evaluation of consumer-oriented lifelog service using daily receipts," in *Proceedings of the 13th International Conference on Information Integration and Web-based Applications and Services*, 2011, pp. 337–340.

[10] V. Vadde, C. H. Nithya, and A. P. Surhonne, "An nfc based innovation for paperless retail transactions and digital receipts management," in *Proceedings of the 2015 Annual IEEE India Conference*, 2015.

[11] M. H. Hasan and A. Khalid, "Development of multimedia messaging service (mms)-based receipt system for mobile banking," in *Proceedings of the 2010 International Symposium on Information Technology*, 2010.

[12] Z. Shen and Y. Tijerino, "Ontology-based automatic receipt accounting system," in *Proceedings of the 2012 IEEE/WIC/ACM International Conferences on Web Intelligence and Intelligent Agent Technology*, 2012.

[13] M. Altmeyer, P. Lessel, and A. Krger, "Expense control: A gamified, semi-automated, crowd-based approach for receipt capturing," in *Proceedings of the 21st International Conference on Intelligent User Interfaces*, 2016, pp. 31–42.

[14] A. Suponenkovs, A. Sisojevs, G. Mosns, J. Kampars, K. Pinka, J. Grabis, A. Locmelis, and R. Taranovs, "Application of image recognition and machine learning technologies for payment data processing review and challenges," in *Proceedings of the 2017 5th IEEE Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE)*, 2017.

[15] K. J. Lee, J.-I. Ju, and J. M. Jeong, "A payment & receipt business model in u-commerce environment," in *Proceedings of the 8th international conference on Electronic commerce: The new e-commerce: innovations for conquering current barriers, obstacles and limitations to conducting successful business on the internet*, 2006, pp. 319–324.

[16] F. Paci, N. Shang, S. Kerr, K. Steuer Jr, J. Woo, and E. Bertino, "Privacy-preserving management of transactions receipts for mobile environments," in *Proceedings ofthe 8th Symposium on Identity and Trust on the Internet*, 2009, pp. 73–84.
[17] C. Lin, "An appraisal of business tax reform in taiwan: The case of value-added taxation," in *The Political Economy of Tax Reform, NBER-EASE*, T. Ito, A. O. Krueger, and editors, Eds. University of Chicago Press, 1992, vol. 1, pp. 137–155.
[18] Y.-J. Joung, Y.-C. Tseng, S.-C. Cha, N.-W. Lo, G. Chung, and S.-H. Hsu, "Motivations, deployment, assessment, and prospects of taiwans e-invoicing system: An overview," in *Proceedings of the 47th Hawaii International Conference on System Sciences*, 2014, pp. 2200–2209.
[19] A. C. Hsueh and J. Hsu, "Taiwan Convenience Stores 2010," Global Agriculture Information Network, Tech. Rep., 2010. [Online]. Available: http://gain.fas.usda.gov/RecentGAINPublications/TaiwanConvenienceStores2010_TaipeiATO_Taiwan_6-30-2010.pdf
[20] Data Processing Center, Ministry of Finance, R.O.C., "Message Implementation Guideline Ver: 3.0.1."
[21] President Chain Store Corporation, "iCash user guide." [Online]. Available: http://www.icash.com.tw/howtouse.asp
[22] EasyCard Corporation, "What is EasyCard?" 2013. [Online]. Available: http://www.easycard.com.tw/english/easycard/index.asp
[23] National Taxation Bureau of Taipei, Ministry of Finance, R.O.C., "Get a card reader with cdc card, starting 5/1 with limited quantities (translated)," 2013. [Online]. Available: http://www.ntbt.gov.tw/etwmain/front/ETW118W/CON/952/6655640052411628180
[24] Certificate Authority of MOI, Ministry of Interior, R.O.C., "About MOICA: History." [Online]. Available: http://moica.nat.gov.tw/html/cover05_1.htm
[25] Directorate-General of Budget, Accounting and Statistics, Executive Yuan, R.O.C., "Year 2011 Average Family Income and Expenditure per Household by Areas." [Online]. Available: http://win.dgbas.gov.tw/fies/doc/result/100/a11/49.xls
[26] eTax Portal, Ministry of Finance, R.O.C., "[Fiscal Information Agency] new method of acquiring e-invoice: Cellphone barcode releases on March 1 (translated)," 2012. [Online]. Available: http://www.etax.nat.gov.tw/etwmain/front/ETW118W/CON/444/5128976699419695483?tagCode=
[27] Innovative DigiTech-Enabled Applications & Services Institute, Institute for Information Industry, R.O.C., "2012 Q3 observations on mobile network (translated)," 2012. [Online]. Available: http://www.find.org.tw/find/home.aspx?page=many&id=350
[28] F. M. Coss, "E-invoicing in Mexico," in *EXPP Summit*. Barcelona, Spain: SAT, 2011.
[29] TAL Technologies, Inc. (2011) Reading Barcodes Directly from a Computer Screen. [Online]. Available: http://www.taltech.com/support/entry/reading_barcodes_directly_from_computer_screen
[30] S. M. Lee, X. Tan, and S. Trimi, "Current practices of leading e-government countries," *Commun. ACM*, vol. 48, no. 10, pp. 99–104, Oct. 2005. [Online]. Available: http://doi.acm.org/10.1145/1089107.1089112
[31] eMarketer Inc. (2013) Smartphone Adoption Tips Past 50Worldwide. [Online]. Available: http://www.emarketer.com/Article/Smartphone-Adoption-Tips-Past-50-Major-Markets-Worldwide / 1009923
[32] Denso Wave Incorporated, "History of QR code," 2013. [Online]. Available: http://www.qrcode.com/en/history/
[33] ISO/IEC 18004:2006, "Information technology – automatic identification and data capture techniques – QR code 2005 bar code symbology specification," Geneva.
[34] IEEE Standards Association, "802.15.1-2002 - IEEE Standard for Telecommunications and Information Exchange Between Systems - LAN/MAN - Specific Requirements - Part 15: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANs)."
[35] D. Chaum, "Blind signatures for untraceable payments," in *Crypto*, vol. 82, 1982, pp. 199–203.
[36] C. Ping, "Financial Supervisory Commission loosens restrictions: the beginning of mobile payment (trnslated)," 2013. [Online]. Available: http://www.digitimes.com.tw/tw/dt/n/shwnws.asp?CnlID=13&id=0000319946_B3Z830FT574376507SXIL&ct=1
[37] H. Tang, "NFC digital wallet has comeCWT debuts iPhone tray for easy payment (translated)," 2011. [Online]. Available: http://www.nownews.com/2011/12/09/11490-2764873.htm
[38] U-3C.com, "CWT NFC pilot program begins, introduces hami smart wallet service (translated)," 2012. [Online]. Available: http://phone.u-3c.com/article2248.htm
[39] Squareup Pte. Ltd., "Square Wallet (Japan)," 2013.
[40] NTT DOCOMO, INC., ""Osaifu-Keitai"," 2013. [Online]. Available: http://www.nttdocomo.co.jp/english/service/convenience/osaifu/
[41] PAYMENT NAVI, "Japan NCR's digital receipt by integrating with FSP (RETAILTECH JAPAN) (translated)," 2013. [Online]. Available: http://www.paymentnavi.com/?s=%E6%97%A5%E6%9C%ACNCR%E3%81%AEFSP
[42] Toshiba Tec Corporation, "Hakuhodo and Toshiba Tec, develops electronic proof of purchase service with us of electronic receipt system "Smart Receipt" (translated)," 2013. [Online]. Available: http://www.toshibatec.co.jp/page.jsp?id=3625
[43] GSM Association, "Korea Blazes Global Trail for NFC," GSM Association, Tech. Rep., 2012. [Online]. Available: http://www.gsma.com/mobilenfc/wp-content/uploads/2012/11/Korea-Case-Study-Nov-2012-FINAL.pdf