TELECOM MEDIA NETWORKS

Mobile Payments in M-Commerce

September 2002

David Buhan
Yu Chye Cheong
Cheng-Lin Tan

CAP GEMINI ERNST & YOUNG

Contents

1. Introduction

We define mobile-commerce payment, or m-payment, as any transaction with a monetary value that is conducted via a mobile telecommunications network (Durlacher).

M-commerce, like electronic commerce, can be business-to-business (B2B), business-to-consumer (B2C), or person-to-person (P2P). In this paper, we focus on B2C m-commerce.

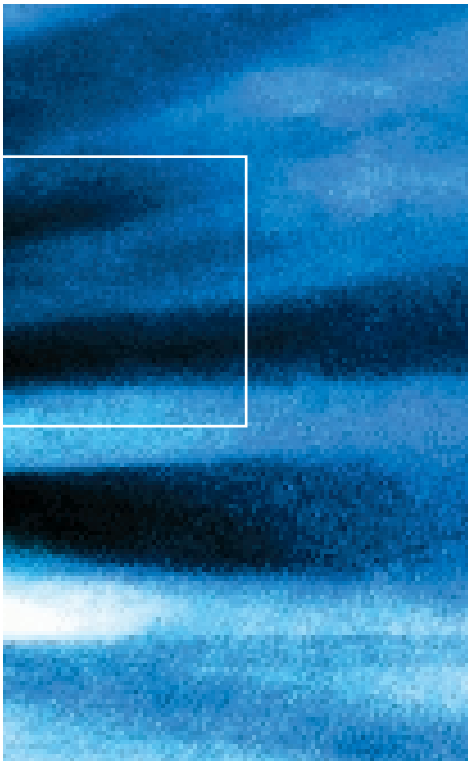
Mobile Payment Expectations

Since the Internet bubble burst, analysts have strongly downsized their initial forecasts regarding the m-commerce market growth. There are many reasons for this slow start, such as device and network limitations, maturity of payment solutions, and customers' lack of interest. But in spite of this, a broad overview of market research indicates that m-commerce remains a huge opportunity:

- In 2001, there were 450 million mobile users worldwide (ResearchPortal.com).
- According to Jupiter (2001), m-commerce should be worth $22.2 billion by 2005 worldwide. Of that, $3.8 billion would come from North America, $7.8 billion from Western Europe, and $9.4 billion from Asia.
- Forrester Research (2001) estimates that mobile payments in Europe should reach €26 billion in 2005.

Yet this represents only 0.5% of customer spending! The real boom in the market will come in the second half of the decade.

Over the following chapters, we will explore the challenges that need to be overcome in order for the m-payment market to meet these expectations. We will then provide a few basics regarding m-payment principles and segmentations. And finally, we will present some of the payment solutions currently available on the market.



2. Challenges Faced by M-Payments

First of all, nobody knows for sure what will be tomorrow's successful business model(s).

Business Challenges

What business model?

What type of services to sell, to which population, what payment schemes to adopt (pre-paid, post-paid, per unit, per view), what type of partners to look for? The telecoms industry has many questions that still remain unanswered. Yet available m-payment solutions are still too new for us to analyze the effect of the choices that have been made. And any answers are likely to differ according to the countries, the cultures, and the interests of the consumers.

One important question is: Should telcos collaborate with banks to address this business opportunity? On the one hand telcos already have direct and privileged access to customers through handsets. Experiences such as minitel's in France show that they are able to collaborate with numerous content and service providers— there are about 8,000 content providers linked to minitel's network. Plus, since telcos already have highly sophisticated billing and accounting systems, they could offer payment services by themselves.

On the other hand, in most countries telcos would need to consider the legal issues before entering this market alone. At the same time, customers are used to paying through banks, and until recently banks have tended to monopolize the payment systems. Plus, studies from Forrester Research show that a most retailers would favor a joint venture including a financial company as a payment provider.

But previous joint experiences between telcos and banks have not really been a success. And such a program would take much longer to become operational than a program launched by a unique player.

The cost

Cost is another issue that could slow the m-payment development process. What is the cost of using the payment method from the consumer's perspective? Is the consumer expected to upgrade his or her existing handset before using the payment method?

How much must a content provider pay to integrate a particular payment method into its existing m-commerce applications? Payment methods with clear Application Programming Interfaces might simplify integration and therefore reduce integration costs. Are the content providers ready to pay for the fees requested from the payment service provider?

Finally, what is the cost of building a successful payment service? These costs include "technical" costs—such as for hardware, software, and integration—and marketing and sales costs (to promote the service to customers or to potential content providers).

A return on investment is not likely to be achieved within the first 2 years. This does not necessarily mean that one should wait for a more mature market—successful early adopters will gain significant competitive market advantages that may be impossible to reach.

Customer apathy

One of the main reasons for m-commerce's slow start is customer apathy. According to

Forrester's research, European consumers are uncomfortable with the idea of mobile payment.

Even though they have no appreciation of the actual security issues involved, they demonstrate "their fear of an unknown medium" and they are not even willing to try paying with their mobile device.

At the moment there are no "killer" applications available that would convince consumers to take the first steps and adopt this new technology. The telcos must therefore stimulate the acceptance of mobile payments with strong consumer value propositions. Applications that enable people to make a payment more efficiently and quickly than what they are used to will be critical. Such premium services could be "personalized," "rush purchase," and "location sensitive."

According to Forrester analysts, "One of the great areas of promise for mobile commerce is to bridge the gap between the touch and feel physical world and the convenient and cost-competitive on-line world."

Technical Challenges

Security

The security of a payment method is undoubtedly crucial if the payment method is to gain widespread acceptance. Security as a whole can be viewed from five angles:

- ***Confidentiality:*** How will the payment method protect against passive monitoring of payment details (e.g. a consumer's personal particulars, password)? Only the sender and receiver of payment details should be privy to them.
- ***Authentication:*** How will the payment method ensure that the consumer and content provider are who they really claim to be?
- ***Integrity:*** To what extent can the payment method protect payment details from being modified from the time they are sent to the time they are received?
- ***Authorization:*** How will the payment method ensure that only authorized consumers are allowed to purchase content? This is a separate concern from just authenticating the identity of the consumer. What are the procedures required to authorize a consumer?
- ***Non-repudiation:*** How will the payment method guarantee that a consumer cannot falsely claim that they did not participate in the transaction?

Security is consumers' primary concern—they will have little confidence in a payment method that cannot provide ways to guarantee authenticity, confidentiality, and integrity. Note that reaching an adequate security level is not enough—more important is to convince the customers that it is actually secure.

Non-repudiation is more important for merchants and payment service providers. This is especially true for hard goods with a value higher than €10 since they are not ready to have high non-payment risks for this segment of products.

Accessibility

We consider this a combination of convenience, speed, and ease of use:

Accessibility also strongly depends on the devices' capabilities and the quality of the network

- ***Convenience:*** To what extent can the payment method be used to pay for any type of content, from any location in the world, using any device? Some payment methods might require consumers to upgrade their existing handsets, or be pre-registered with a company.
- ***Speed:*** Is the amount of time spent using the payment method acceptable to consumers? This is especially true when customers have to pay for the access.
- ***Ease of use:*** Is the payment method easy to learn and use from the viewpoint of a consumer? Ease of use and speed are especially important for micro-payments.

Accessibility also strongly depends on the devices' capabilities and the quality of the network. Will future devices meet expectations?

Standardization

A wide variety of technologies for mobile payments exist today, ranging from simple premium-charged SMS solutions for mobile content to advanced dual-slot phone technology for real-world technology.

New vendors are still emerging every month to launch the "future m-payment solution." Very few of them will achieve acceptable market share, and many of them have already disappeared.

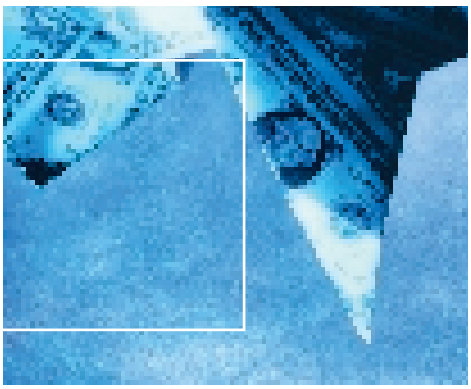
For mobile operators, analysts are predicting a year of "bedding down" technology, where recent technology investments will either "flourish or fail."

Therefore, telcos need to consider the capacity of the solution provider to break through when entering the m-payment market. The good solution providers will be able to interact with other solutions in order one day to build a global m-payment network.

Various initiatives and consortiums are presently working to help meet the above-mentioned challenges. An example is MeT (Mobile Electronic Transactions), an initiative by Nokia, Motorola, and Ericsson that seeks to establish a framework for secure m-commerce. Confidentiality and integrity will be addressed by Wireless Transaction Layer Security (WTLS), while the yet-to-be-implemented Wireless Identity Module (WIM) will ensure client and server authentication. Finally, the WIM will also facilitate the use of digital signatures, which will help ensure non-repudiation.

Another example is the E-Commerce Expert Group (ECOMEG), a working group within the Wireless Application Protocol Forum (W@P). The ECOMEG identifies, describes, and recommends changes to the WAP specification to enable m-commerce and specifically mobile payment, mobile banking/trading, mobile advertising, B2B, and travel and entertainment services.

Technologies play an important role in securing m-commerce. We briefly describe these technologies below and include how each can address the five security concerns: confidentiality, authentication, integrity, non-repudiation, and authorization.



3. Securing M-Payment

While a detailed examination of the security aspects of m-commerce are beyond the scope of this paper, we will briefly provide an overview of some important enablers for secure m-commerce.

Encryption can be used to ensure confidentiality. Encryption is the process by which plaintext data (i.e. direct representation of information in text and numbers) are transformed into unintelligible data. This is achieved using encryption and decryption keys. Understanding any intercepted encrypted data between transaction parties (e.g. consumer and content provider) is almost impossible.

The following mechanisms are based on a public key **cryptosystem**. A cryptosystem defines how encryption and decryption are performed. In a public key cryptosystem, a pair of related keys is used: a public key, which is made publicly known, and a private key, which is kept secret.

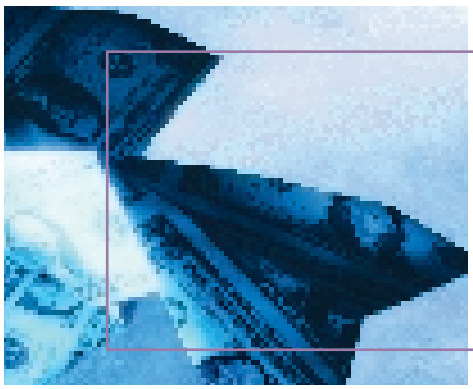
Digital signatures can ensure the authenticity of transaction parties, and the integrity and non-repudiation of transmissions. A digital signature is a data item that accompanies a digitally encoded message (Ford and Baum, 1997). An on-line bookseller, for example, could use a digital signature to verify that a particular book purchase from a Thomas Smith actually originated from Thomas Smith, and not from some prankster. Digital signatures may be produced by encrypting the contents of the data to be transmitted using a private key. This ensures that the digital signatures cannot be forged. Mathematical methods such as hash functions can be used to minimize the size of the digital signature.

To verify digital signatures, we need a copy of the public key of the signing party. It is important to ensure that the public key used is the correct public key, otherwise there are opportunities for a security breach. **Digital certificates** allow us to distribute the public keys in a secure manner that will provide this assurance.

A digital certificate is a collection of information to which a digital signature has been affixed by some recognized authority and trusted by some community of certificate users (Ford and Baum, 1997). A common type of digital certificate is the public-key certificate, which unambiguously binds a particular person, device or entity to a public key. A digital certificate contains four main components (Baltimore, 2000): a public key, information linking this public key to its owner, information about the certificate issuer, and the issuer's digital signature. A Certification Authority issues digital certificates.

A **Public Key Infrastructure (PKI)** is defined by the PKIX Working Group as "The set of hardware, software, people, and procedures needed to create, manage, store, distribute and revoke certificates based on public-key cryptography" (Baltimore, 2000). This is a set of standards that control the lifecycle of digital certificates. A PKI can help address the non-repudiation and authorization aspects of security.

The above-mentioned technologies are instrumental in setting up a secure environment for m-commerce payment. An example of this is **WTLS**, a security protocol in the WAP architecture that includes encryption and digital certificates. WTLS secures communications between the consumer's mobile handset and a WAP gateway1.



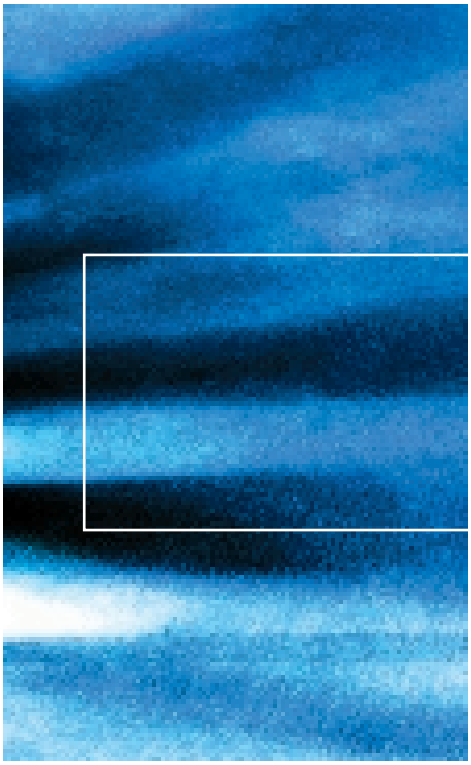
Securing m-commerce is not just an equation involving technology

Another example is **Secure Electronic Transaction (SET)**, a protocol by MasterCard and Visa to support bank card payments. SET is implemented using a PKI.

Future payment methods are likely to rely on a secure environment provided by a comprehensive wireless implementation of PKI under the WAP specification, or Subscriber Identity Module (SIM)-toolkit-enhanced mobile handsets. A hybrid of these two might also be possible. At the moment, the jury is still out as to which of the two is likely to dominate the wireless landscape.

For WAP users of the future, consumers will be able to authenticate themselves to content providers and PSPs using WTLS and a WIM that will store references to industry-standard X.509 digital certificates. These WIMs would be implemented using either smart or SIM cards. Consumers will be able to use their mobile handsets to digitally sign and encrypt outgoing communication. For SIM-toolkit-enhanced mobile users, SIM cards in consumers' mobile handsets serve as a repository for private keys and certificates.

Securing m-commerce is not just an equation involving technology. The process of establishing trust is just as important. A trusted third-party (TTP) can be used to perform the authentication of transaction parties. The TTP can be a telco, bank, or credit card company, for example.



4. M-Commerce Payment Principles

Actors and Roles

The mobile payment value chain is complex and it will take some time before the different roles are assigned to the best actors. Identified key roles to be managed are: content provider, authentication provider, payment authorization and settlement provider, and consumer.

The consumer is the person owning the mobile device and buying content or services from the content provider.

The content provider is someone or some organization that sells either electronic or physical content (products or services) to consumers.

The trusted third party (TTP) is the company used to perform the authentication and the authorization of transaction parties and the settlement. It could be a telco, bank, or credit card (pre-paid account, consumer bill, bank account, etc.).

The payment service provider (PSP) is the central entity responsible for the payment process. It enables the payment message initiated from the mobile device to be routed to, and cleared by, the TTP. This service generally includes an "e-wallet" application that enables payers to store their payment details, such as credit card account numbers and shipping addresses, on a provider's secure server so that they do not need to type in all the pertinent information required for each sale on small and difficult-to-use mobile keypad devices. The PSP may also act as a clearing house to share the revenues between all the partners involved in the payment process. It could be a telco, a bank, a credit card company, or a start-up.

A telco could be positioned at the same time as PSP, TTP, and content provider.

Figure 1 below describes some strengths and weaknesses of different actors to act as PSP or TTP.

Figure 1: M-Commerce Actors and Roles

Criteria	Banks	Credit card firms	Mobile operators	Payment start-ups
Motivation	*Fear of staying behind*	*Add a new channel*	*New revenue and services*	*Business opportunities*
Mobile services skills	○	○	●	◔
Financial services skills	●	●	○	◔
Micro billing capabilities	◔	◔	●	●
Macro billing capabilities	●	●	○	◔
Large end-user base	●	●	●	◔
Large merchant base	◕	●	◔	◔
Move quickly	◔	○	◑	●
Able to expand quickly	◕	●	◕	◔
Sample company	SEB	Visa	Orange	Paybox

Minimal capability ○ ◔ ◑ ◕ ● Robust capability

Source: Forester Research, Inc.

The mobile payment value chain is complex and it will take time before the different roles are assigned to the best actors

In the following chapters, we will review quickly the main phases in the m-payment cycle.

M-Payment Main Phases

Registration

First, the consumer needs to open an account with the PSP to enable the payment service through a particular payment method. During this phase the PSP will require confirmation from the TTP that handles the relationship with the customer.

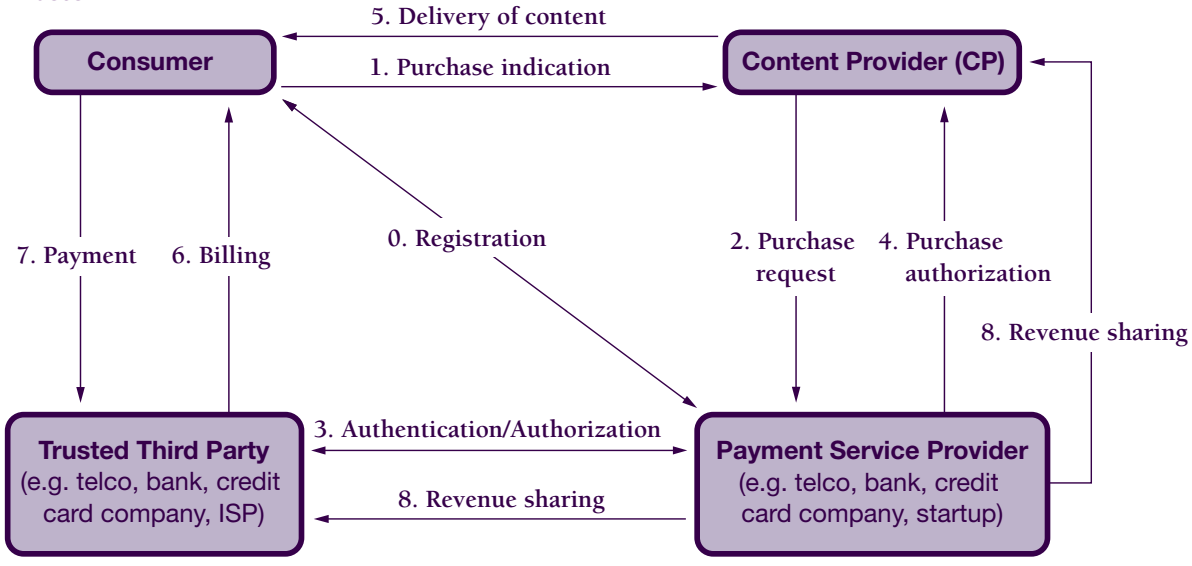
This phase can be seamless for the consumer according to the functional choices made by the TPP and the PSP.

Transaction

An m-payment transaction includes the following steps:

1. Consumer indicates his or her desire to purchase some content. This could take the form of a button press on his or her mobile handset or by sending an SMS to a peculiar number.
2. Content provider forwards the purchase request to the PSP.
3. PSP requests authentication and authorization from the TPP.
4. PSP informs the content provider about the success of the purchase demand.
5. Content provider delivers the purchased content.

Figure 2: M-Payment Main Phases



Clearing and Settlement

Settlement can take place in real time during the purchase or in a post-paid mode. Funds can also be reserved in real time and confirmed later on.

Real-time settlement is carried out during step 4 by the TTP. It can be conducted via a pre-paid account if the TTP is a telco or directly through a bank account if the TTP is a bank.

In post-paid mode, the PSP sends the billing information to the TTP. The TTP sends the bill to the consumers, gets the money back, and forwards it to the TTP.

The PSP is then responsible for computing the revenues of each entity and distributing the funds accordingly.

M-Payment Characteristics

Potential mobile payment falls into several distinct categories:

- Content type
- Content value
- Transaction type
- Transaction settlement method

In this section, we explore some of these important characteristics.

Transaction settlement method

The time aspect distinguishes different settlement methods.

1 – Pre-paid (debit)
Consumers pay in advance to obtain the content they desire. Voice pre-paid cards and electronic "wallets" (stored value wallet) are examples of these kinds of payment methods.

2 – Post-paid (credit)
Consumers receive the content and consume it before paying. For example, a consumer gets a ringtone and pays it through a bill issued by his or her TTP.

Transaction type

1 – Pay Per View (PPV)
The consumer pays once for each view, or increment, of the desired content. An example of this is a consumer paying once to download an entire MP3 file from an m-commerce site. This transaction model is probably the least complex to support in terms of the technical infrastructure required.

2 – Pay Per Unit (PPU)
The consumer pays once for each unit successfully completed with the content provider. A certain number of units (volume or duration units) would have been "spent" for each session, which would be billed to the consumer. An example of where this might be appropriate is a games provider charging fifty cents for every unit that is spent by a consumer participating in an on-line game. This is usually more complex than the PPV model as there is a need to accurately track the consumers' sessions. This model would especially be very complex to implement in an open payment network (e.g. multiple content providers, TTPs, PSPs).

3 – Recurrent Subscription
The consumer pays a recurring periodic amount to access the content on an unlimited basis during the period. For example, a consumer might be charged a flat fee every month in return for unlimited access to a magazine.

Content type

Here are the main content types:

1 – Digital goods (e.g. value-added information, MP3, or downloaded ringtones)
2 – Hard goods (e.g. TV, CD-ROM)
3 – Voting (e.g. vote for TV program)
4 – Ticketing (e.g. book a theatre ticket)

Content Value

1 – Micro-payments
2 – Macro-payments

The limit between micro and macro-payments is usually about €10. For macro-payment, security is much more important than for micro-payments since the non-payment risk has a higher consequence. For micro-payment, the purchase experience should really be easy and quick for the end-user. The operational cost of the purchase should not be too high for PSP and TTP since the margin per purchase will be low.

5. Survey of Payment Methods

In this section, we give a brief non-exhaustive survey of various vendors' payment solutions.

Encorus

Brokat's Mobile Commerce division was recently acquired by eOne Global and is now called "Encorus Technologies."

The following definition applies to the product as it was before the acquisition: Encorus PaymentWorks consists of several components that can be mixed and matched to meet the individual needs of payment and service providers. The key component is the Wallet Server, which offers functionality for consumer and merchant registration, identification, authorization and self-administration. The Wallet Server stores customers' data that is essential for making purchases. It can be thought of as a mobile wallet containing a user's identity, credit information, and (possibly) purchasing limit. User interfaces are provided for consumers and merchants to view and modify their data securely. These user interfaces can be adapted to different languages and corporate identities. The Wallet Server also takes care of payment transaction handling and logging. Multiple currencies are supported.

Encorus eWallet was selected last year by Vodafone to provide its e-Wallet platforms (macro-payment) to Vodafone subsidiaries in Europe.

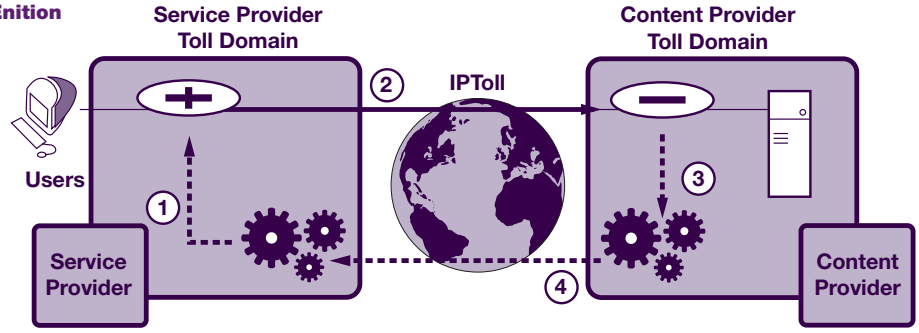
Enition

Enition's patented NetToll™ technology is a network-level product, designed to be integrated within communication service providers' (e.g. broadband ISPs, wireless ISPs, portals) and content providers' network infrastructures. It gives service and content providers a baseline infrastructure for managing compensation for resources delivered via the Internet.

Enition technology integrates transparency and flexibility into compensation calculations, and produces standardized billing tickets that work seamlessly with both Internet-based and legacy billing systems.

Enition technology is located in the Internet Protocol (IP) transport layer, so it has the lowest overhead of any comparable technology used to support value exchange and metering. The technology works by encapsulating and decapsulating data—in essence placing special data "Tokens" in the IP layer and then removing them through Enition's IPToll™ technology.

Figure 3: Enition



Service providers create Tokens that represent the request for the Internet resource that corresponds to the content being requested by the end-user. After traveling across the Internet, the Tokens are extracted from the request by the gateway within the entity that is serving the content (e.g. a content owner, its Web-hosting service, or a cache provider). These Tokens exist only on the network.

Tokens contain data relating to:

- A value expressed in terms of a standard unit of measure (a "Toll Unit"). Each resource request will carry a number of units set in accordance with a Toll Policy created by the content owner.
- The identification of the entity that created the Token, typically service providers.
- A mathematical core that is used to ensure the validity of the Token.

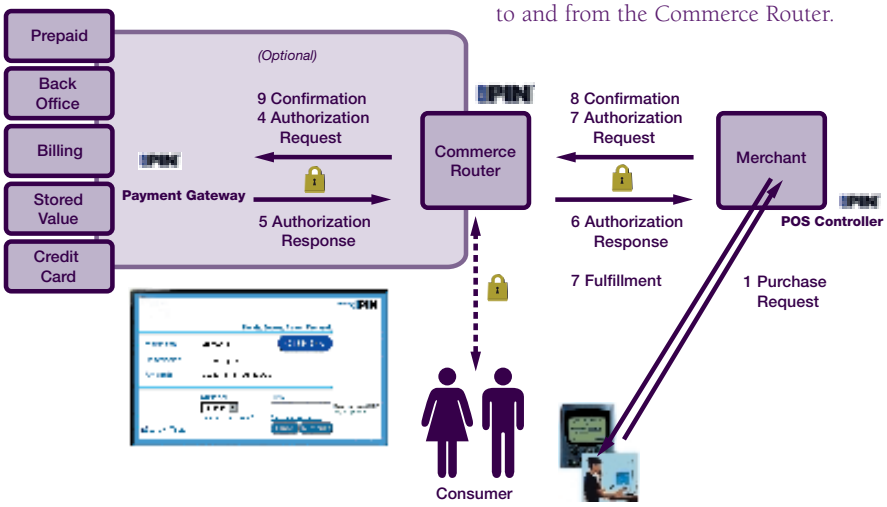
iPIN

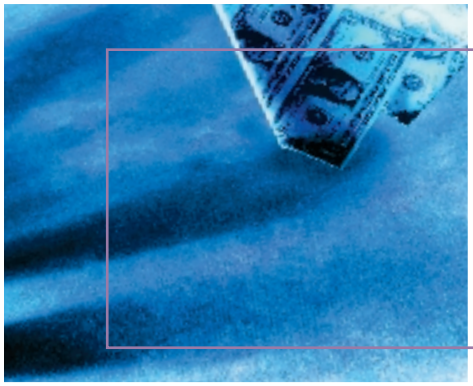
The iPIN Payment Technology is a complete, end-to-end e-Payment platform.

The seven main software components of the iPIN Payment Technology are:

- ***The Commerce Router***—Manages transactions throughout their lifecycle. It serves the user-interface pages, as well as manages all end-user customer-account activity.
- ***The Repository***—Manages the different configurations (currencies, commissioning rules, merchant acquirer, etc.) as well as the merchants provisioning across the network.
- ***The Billing Engine***—Performs transaction fee calculations and transaction aggregation processes. It also produces output to facilitate accounting and settlement of transactions.
- ***The Merchant POS Controller***—The software component that connects to the merchant's in-store or virtual point of sale. It enables the communication of transaction information to and from the Commerce Router.

Figure 4: iPIN





Historically, iPIN has been very strong in micro-payment systems

- ***The Payment Gateway***—The connection to the financial partner's back end.
- ***The Business Intelligent module***—Helps companies track the success and return on investment of their e-payment initiatives.
- ***The iPIN Multiple Payment Instrument Module***—Allows one consumer to manage the usage of multiple funding accounts, such as debit, credit, and pre-paid, within a single application.

iPIN has strong references including France Telecom (Orange France), HSBC, and British Telecom. Historically, iPIN has been very strong in micro-payment systems.

Portal

Portal Software develops billing software for communications (telcos, ISPs) and content service providers. It is currently widely used as a billing system in the IP world. Portal has developed a payment module that interfaces with Infranet software (from release 6.2), the Infranet Content Connector (see figure 5).

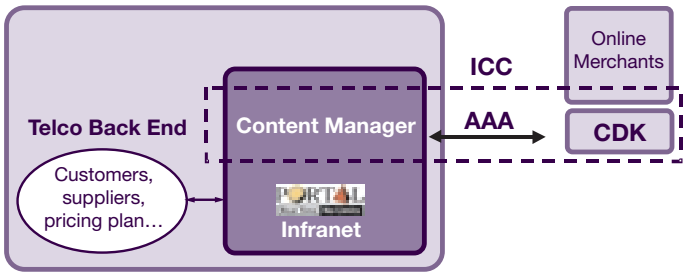
Infranet Content Connector provides a billing interface to link communications providers and value-added service providers in an Internet value chain. These service providers gain access to the functionality of the Infranet platform without having to purchase or support a full-blown system. And providers can increase revenues by easily accommodating a full suite of services—in a way not possible with legacy billing systems.

Infranet Content Connector features a Content Manager on the Telco server side, acting as an interface between Infranet and instances of the Content Developer Kit (CDK), which are distributed among Content Providers through a secure, trusted network connection.

The Infranet CDK set of Java classes enables value-chain partners to perform several key functions against subscriber accounts held in the provider's installation of Infranet, such as authentication, authorization, and accounting (AAA).

The end-customer settlement will be done either through the Infranet bill or through a pre-paid account that may be stored within Infranet. The products' catalog can be located at the merchant side within the CDK or at the Infranet server side.

Figure 5: Portal



Rapsodia

Rapsodia, which is owned by Oberthur Card Systems, proposes the SIMphonIC Application Software Platform. It is a generic, open, and re-usable platform that enables telcos to provide SIM toolkit services.

Above that platform, telcos may add built-in applications proposed by Rapsodia such as m-banking applications or customized applications developed with the SIMphonIC development kit.

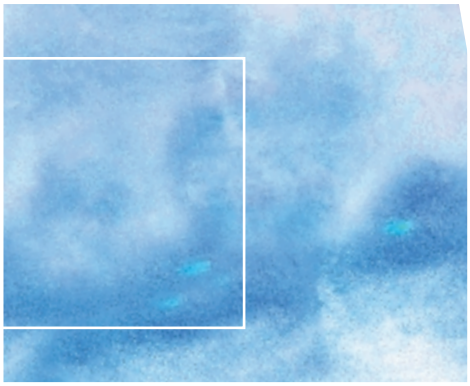
Among these applications, an m-payment application can be easily developed to connect end-users to a bank account or a pre-paid account. Such a solution has been deployed for SMART Communications Inc of the Philippines.

Note: You can also connect Rapsodia SIMphonic ASP with a "pure" payment solution such as iPIN to benefit from iPIN's many functionalities and from Rapsodia's key advantages in the SIM toolkit world.

Others

Other vendors that could provide a payment platform include:

- Mediation solutions such as Narus, XACCT, or Volubill.
- Billing solution providers. Most of them are now adding a payment module within their billing software—this is the case with Geneva and Portal.
- Macalla software whose m-commerce platform was selected recently by the PostBank in Holland.
- Digital Rum, which is currently used by Orange France for macro-payments.
- Trintech.
- 724.
- MoreMagic.



6. Comparison of Payment Methods

We compare in this section some of the solutions described in the previous chapter.

Figure 6: Comparison of Characteristics of Selected Payment Networks

Characteristics		iPIN	Encorus	Enition	Portal	Rapsodia
Transaction criteria	PPV	●	●	◑	◑	◑
	PPU	○	○	●	●	○
	Recurrent subscription	●	◑	◑	◑	◑
	Pre-paid	●	●	◑	●	◑
	Post-paid	●	●	●	●	◑
	Direct debit	●	●	○	◑	●
	P2P	●	●	○	○	◑
Content criteria	Digital goods	●	●	●	●	◑
	Hard goods	●	●	◑	◑	◑
	Tickets	◑	◑	◑	◑	◑
	Votes	◑	◑	●	◑	●
	0-0.1 euro	○	○	●	●	○
	0.1-10 euros	●	◑	◑	●	◑
	>10 euros	◑	●	○	◑	◑
Level of upgrade/ customiz-ation needed	For consumer	Low: need to open/activate an account	Low: need to open/activate an account	None	None	High: May need to upgrade the device
	For content provider	Low: APIs are provided for quick integration	Moderate: APIs to integrate on the CP site	High: need to add an Enition box	Moderate: Java APIs to develop transaction dialogue	Low
	For Payment Service Provider	High: full payment platform to implement	High: full payment platform to implement	High: Enition box to plug to the SI	Moderate: if Infranet 6.2 is already deployed (ICC module included)	High: ASP platform to deploy and customize applications to the needs
	For Trusted Third Party	Moderate: plug to the billing system, bank account or prepaid balance	Moderate: plug to the billing system, bank account or prepaid balance	N/A	N/A	N/A

7. Conclusion

It is useful to consider how some of the newer technologies will affect the design of current and future payment methods.

Technologies such as Java Card and WIMs will allow increasingly sophisticated client applications to be used on a mobile handset. The Java Card specifications enable Java technology to run on smart cards and other devices with limited memory. A WIM will allow consumers to store public keys and digital certificates on their handsets. Applications running on mobile handsets will have a richer user interface and be able to authenticate the consumer to m-commerce transaction parties. Payment method vendors need to exploit these capabilities and yet allow consumers to complete an m-commerce transaction quickly and easily.

Business models are still on trial. The best options will differ according to the scenario: should one go for a closed-garden business model or an open payment network; in the second case, what partners to work with.

It is clear that payment method vendors will be compelled to evolve their solutions continually to keep up with the changing technological and business landscapes. Successful payment methods will be those that can continue to meet the many challenges mentioned in this paper, particularly security. The need for secure, reliable payment methods to be made available to consumers cannot be understated. Without them, consumers potentially risk losing out in the long run.

The success of m-payment will be driven by the success of m-applications (localization, personalization, rush purchase, etc.). The emergence of new devices and networks will drive new services and payment flexibility. The real boom will not come for another few years and it is therefore highly improbable that ROI will be achieved within the next 2 years. However, early adopters of this payment medium who make the right choices will gain significant competitive market advantage that will be hard to match.

8. References

Initiatives/Consortiums

MeT: www.mobiletransaction.org
mSign: www.msign.org
PKIX Working Group:
www.ietf.org/html.charters/pkix-charter.html
WAP Forum: www.wapforum.org

Vendor Products

Digital Rum: www.digitalrum.com
Encorus: www.eoneglobal.com
Enition: www.enition.com
Geneva: www.genevatechnology.com
iPIN: www.ipin.com
Macalla: www.macalla.com
MoreMagic: www.moremagic.com
Narus: www.narus.com
Openet: www.openet.com
Portal: www.portal.com
Rapsodia: www.rapsodiasoftware.com
Trintech: www.trintech.com
Volubill: www.volubill.com
Twister: www.brokat.com
XACCT: www.xacct.com
724: www.724.com

Other References

Baltimore Technologies Ltd., *Telepathy WAP Security Toolkit-Developer's Guide v1.2,* 2000.

Durlacher Research Ltd., *Mobile Commerce Report,* November 1999. Available at http://www.durlacher.com/fr-research-reps.htm

EdgeMatrix, *EdgeMatrix NewsFlash,* 15 November 2000.

Forrester Research, *Mobile Payment's Slow Start,* 2001.

Jupiter Research: *Mobile Commerce, Profiting Despite Customer Apathy,* 2001.

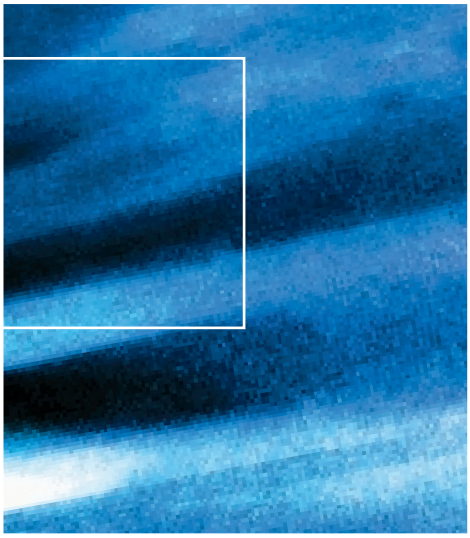
Kalakota, R and Whinston, AB, *Frontiers of Electronic Commerce,* Addison-Wesley Publishing Company, Inc., 1996.

Mott, J, "Secure Payments via WAP", *Ericsson Contact On-line,* 19 November 2000. Available at www.ericsson.com/SE/kon_con/contact/cont19_00/c19_09.shtml.

Hibberd, M, "Mobile Commerce: Who's in Charge?", *Mobile Communications International,* p.35.

"Understanding Security on the Wireless Internet: How WAP Security Is Enabling Wireless E-commerce Applications for Today and Tomorrow", Phone.com, January 2000. Available at: www.phone.com/pub/security_wp.pdf

Simon et al., "Wireless Internet Report: Boxing Clever", *Equity Research, Europe*, Morgan Stanley Dean Witter, September 2000, p.20.



9. About the Authors

David Buhan
Project Manager, Telecom Media Networks

Email: david.buhan@cgey.com

David Buhan has been leading e-payment and m-payment projects for Cap Gemini Ernst & Young's European customers for more than 2 years. He is now part of the m-payment center of excellence developped by Cap Gemini Ernst & Young, in order to assist their customers tackle this very promising but also very complex market opportunity.

David received an engineering degree from the Ecole Centrale Paris and a Master of Science in Industrial Engineering and Operation Research from UC Berkeley in 1996.

Yu Chye Cheong
R & D Engineer, Wireless Internet Centre, Telecom Media Networks

Email: yuchye.cheong@capgemini.com.sg

Yu Chye is a Research and Development Engineer at the Wireless Internet Centre in Singapore. Yu Chye was previously a technology analyst with Andersen Consulting, where he worked primarily on PeopleSoft systems, a major Enterprise Resource Planning system. He specifically worked on Web-enablement of PeopleSoft systems, customisation and handled various aspects of its technical architecture.

Yu Chye is a member of IEEE Computer Society, and his research interests include software architecture, product line development, and mobile commerce. He holds a Bachelor and Masters of Science from the National University of Singapore

Cheng-Lin Tan
Technology Manager, Wireless Internet Centre, Telecom Media Networks

Email: cheng-lin.tan@capgemini.com.sg

Cheng Lin TAN is Technology Manager at the Wireless Internet Centre (WIC). He is responsible for the technical road map within WIC and leads a team of technical consultants working on projects related to m-commerce & mobile services.

Prior to joining Cap Gemini Ernst & Young, he was an Executive R&D Manager in the Centre for Wireless Communications (CWC), a nationally funded R&D centre. He has more than 10 years of experience on wireless projects. His skill set includes people and project management, and technical architecture design and implementation for wireless and Internet projects. He is familiar with various wireless standards such as GSM, WAP, and GPRS.

Cheng Lin has previously worked on projects such as Delphipad (Internet wireless appliance), which was a collaboration project between CWC and Ericsson Cyberlab Singapore. He has also worked on various European ACTS consortium projects, including OnTheMove (mobile middleware) and Cameleon (mobile agents).

Cheng Lin is a member of IEEE & ACM. He holds Bachelor of Engineering and Masters of Engineering degrees in Electrical and Electronics Engineering from the National University of Singapore. His research interests include mobile networking and m-commerce. He has one patent to his name and several other patents pending.

10. About Telecom Media Networks

Telecom Media Networks (TMN) is a global industry practice of Cap Gemini Ernst & Young focusing on the consulting, systems integration, and outsourcing needs of communications service providers and media players worldwide.

TMN is dedicated to implementing strategic solutions that generate sustainable results through leading-edge technology, enabling our clients to thrive in the network economy. Combining expert industry knowledge, strong partnerships, and an excellent set of tested solutions, TMN is in the top tier of global management and IT consulting firms.

For more information visit www.cgey.com/tmn or email tmn@cgey.com

www.cgey.com/tmn

TELECOM MEDIA NETWORKS
HEAD OFFICE
76, avenue Kléber
75784 Paris Cedex 16
France
+33 (0)1 47 54 52 00
tmn@cgey.com

Australia
+61 2 9248 4414

Belgium
+32 2 708 11 11

Canada
+1 416 943 2057

China
+8621 6841 9696

Czech Republic
+420 2 57 32 27 42

Denmark
+45 70 11 22 00

Finland
+358 9 45 26 51

France
+33 (0)1 49 00 40 00

Germany
+49 (0) 211 47068 0

Hungary
+36 23 506 800

India
+91 22 5187 000

Italy
+39 02 42 261

Japan
+813 3279 9210

Malaysia
+60 3 2163 6800

Netherlands
+31 30 689 77 77

New Zealand
+64 9 377 1440

Norway
+47 24 12 80 00

Poland
+48 22 60 60 666

Portugal
+351 21 412 2200

Singapore
+65 6484 3188

Spain
+34 91 732 84 00

Sweden
+46 (0)8 704 50 00

Switzerland
+41 (0)21 620 7100

Taiwan
+886 2 8780 0909

UK
+44 (0)20 7434 2171

USA
+1 314 290 8000