GEMPLUS™

Radicchio®
Information accounted for.

INTRODUCTORY MEMBERS BRIEFING ON

t^2r

TRUSTED TRANSACTION ROAMING

A GLOBAL PLATFORM TO UNLEASH THE POTENTIAL OF WIRELESS DATA SERVICES

Executive summary

There is currently no global network available that would serve as a common platform enabling content and service providers to reach mobile subscribers in a trusted environment. Individual Mobile Network Operators (MNOs) are implementing and piloting projects, but reaching wireless subscribers with sensitive digital content will remain an expensive and confusing proposition until the major parties involved join to build an interoperable framework for Identity, Security and Privacy Management in mobile networks.

As the leading industry forum for trusted mobile services, Radicchio is seeking to establish a trusted infrastructure for wireless data services that will meet fundamental market requirements by enabling:

- Global interoperability
- Reliable identification
- Secure network access
- Secure content access
- Privacy management
- Convenience & benefits (for end users, MNOs and service providers)
- Legal enforcement (EU support)

This Trusted Transaction Roaming Platform will benefit the wireless data services market as a whole and – most importantly – the end users, who will receive a larger variety of services, security, and privacy on an infrastructure that they can really trust.

The operator of such an extensive platform, which would deal with different parties' confidential information, needs to be a neutral entity that is truly trusted and recognized by all the players in the data services market (including financial institutions, MNOs, service & content providers and technology providers). This neutral entity would operate the Global Identity Management on behalf of all GSM MNOs.

Radicchio is now proposing the t^2r (Trusted Transaction Roaming) Project to enable the construction, design, and implementation of a Trusted Platform. The t^2r Project will also lay the foundation for one or many neutral entities to operate such a platform for the benefit of the end users, service providers, MNOs, and various other players in the wireless data services market.

The t^2r Project was presented to the leading Mobile Network Operators at the Carrier Summit held in March 2002 in Bandol, France. Operators present included Hutchinson 3G, MTN, Orange, mm02, Sonera, T-mobile, and Vodafone. The aim of this summit was to reach a consensus on the best way to develop a global framework for trusted mobile and wireless transactions. The feedback was encouraging, and Radicchio believes that this summit has signaled the start of global roaming for secure wireless transactions.

The Trusted Transaction Roaming (t^2r) framework will enable secure identification of all end-users in a wireless network. This allows services outside the home operator network to securely identify end-users as they roam. It also will improve service quality through secure payment

and personalization. For example, the trust platform would make it possible for subscribers to safely purchase services (such as train tickets) while traveling internationally. Given the total worldwide market of wireless end-users, such services and payment process can leverage a common interface and increase revenue. Using the same global identity framework, enterprises and governments could use mobile devices to enhance access control.

Trusted Transaction Roaming makes the mobile device significantly more valuable to the user, defines new revenue streams for the mobile operator and creates a new, managed channel for service providers to extend their services to the nearly one billion global wireless users.

Radicchio has also identified cooperation with international legal and regulatory authorities as an essential step towards ensuring the enforceability of digital contracts signed remotely in wireless networks. Furthermore, it will also seek to make the best possible use of standards written by other organizations to avoid duplicating efforts and to guarantee maximum interoperability.

To ensure that the framework becomes truly global, Radicchio invited the GSM Association and the Liberty Alliance to present at the Operator Summit. Follow-on efforts are planned with other leading industry bodies, such as the European Telecommunication Standardisation Institute (ETSI) and the ICT Standards Board.

Based on the discussions at the Radicchio Operator Summit, the Mobile Network Operators agreed on the following general position:

- Operators recognize the strategic potential of trusted actions based on SIM-card security for current and future services, such as end-user identification, enterprise access control, online payment, etc.
- The operator and services industries need to cooperate to enable the widespread take-up of trusted transaction services.
- The potential of trusted transactions involving third-parties (e.g. banks) can only be successful if operators co-operate to extend a common, global interface that enables secure services.
- The operators will encourage the development of the necessary technical, procedural, and legal standards on a global scale to establish an open and reliable standard that can be implemented by technology providers and used by content and financial service providers.

In the coming months, Radicchio will establish a suitable management structure and technical framework for the t^2r Project based on the input from its member companies and working groups. The results will be published and discussed at the Radicchio Annual members meeting in July 2002.

Copyright and disclaimer

© 2000 Radicchio

All rights reserved. No part of this document may be reproduced or transmitted in any form or by any means without prior written permission from Radicchio.

Disclaimer:

The information contained in this document represents the current view held by Radicchio on the issues discussed as of the date of publication.

This document is provided "as is" with no warranties whatsoever including any warranty of merchantability, noninfringement, or fitness for any particular purpose. All liability (including liability for infringement of any property rights) relating to the use of information in this document is disclaimed. No license, express or implied, to any intellectual property rights are granted herein.

This document is distributed for informational purposes only and is subject to change without notice. Readers should not design products based on this document.

Radicchio is a registered trademark. Other product or company names mentioned herein may be the trademarks of their respective owners.

Contents

CHALLENGES 5
Challenges in an emerging market 5
Challenges faced by Mobile Network Operators 5
From voice to data 5
New business models 5
New ways of accessing the wireless Internet 6
The next generation of wireless networks 6
Leveraging security advantages 7
Challenges faced by Service Providers 7
Challenges facing the industry as a whole 8
Fragmentation 8
Roaming 8
CONCEPTS 9
Trusted Transaction Roaming (t^2r) 9
Objectives 9
Approach 10
Innovation 11
Current m-commerce environment 11
The t^2r innovation 12
Business cases 12
CONCLUSIONS 14
We must work together to build a trusted platform 14
A first step has been taken 14
Next steps 15
Appendix: Enabling Technologies 16
About Radicchio 17

CHALLENGES

Challenges in an emerging market

In three years, there will be one billion cellular phone users worldwide. Half of these will be using their mobile terminals to access the wireless Internet daily.

Mobile communications devices, in whatever form, offer ideal characteristics for undertaking electronic transactions, regardless of location, worldwide. Since personal communications devices contain the capability for transactions based on tamper-resistant hardware, they will enable a huge (and growing) percentage of the world's population to participate in secure e-commerce.

The combination of e-commerce services with the inherent advantages of the mobile device will benefit businesses and consumers alike. Major market players are already in the process of establishing trusted infrastructures that will make secure, high-value transactions from mobile devices across wireless networks a part of everyday life.

Challenges faced by Mobile Network Operators

From voice to data

Mobile Network Operators (MNOs) used to offer their subscribers just one type of service, voice. Slowly, data services made their way into the portfolio, as can be seen in the case of the Short Message Service (SMS), which became a pioneer in its field and a huge success worldwide. Nevertheless, the emerging data features also had a downside: enabling subscribers to access the Internet suddenly meant that other businesses could easily reach the MNO's subscribers through their websites. As was the case with ISPs, MNOs feared being relegated to the role of "pipes" between their subscribers and new service providers. These concerns caused them to take protective action. Many MNOs blocked their subscribers from accessing sites that did not offer the MNO direct business value in terms of revenues. However, several countries' Telecom Regulator Authorities took action and urged operators not to implement such protective measures in order to let end users benefit from a wider variety of services and a healthier price structure.

New business models

The actions of the regulators put Mobile Network Operators back in the awkward situation of not knowing exactly how to leverage their subscriber relationships. Merely offering voice and limited data services (SMS) was no longer a distinguishing factor, since these had become commodity services and were subject to fierce price competition. New competencies and skills are required to offer attractive content and applications to consumers. The MNOs are still in their learning phase and are trying to find new business models based on unmet needs in a changing wireless eco-system.

New ways of accessing the wireless Internet

At the same time, new alternative technologies have emerged on the market to enable wireless connectivity and Internet access: Wireless Local Area Networks (WLANs) connect various handheld devices to a local base station, which in turn is connected to the Internet through a regular landline. The most popular method is the "802.11b" standard, which has already been widely adopted in the United States. Using a compatible handheld device and the 802.11b local area network, the user can, for instance, surf the Net at rapid speeds (up to 11Mb/s) and access a variety of services without any need for a Mobile Network Operator's conventional network (GSM/TDMA or CDMA). For example, a coffee shop can install an 802.11b network on its premises and let its customers connect to the Internet for free as part of its service offering. Using any 802.11b Local Area Network, attractive content and applications can be downloaded when stationary, and then used on the move.

The next generation of wireless networks

In parallel with these developments, Mobile Network Operators have invested heavily in the next generation of wireless networks (3G), which provide higher bandwidth (up to 2Mb/s) and will supposedly enable more compelling content and applications. These wireless networks are designed to be able to deliver mobile multimedia, music and video downloads to handheld devices. However, some analysts question the value of this higher bandwidth on the move, especially when Local Area Networks (LANS), such as 802.11b, offer much higher data throughput speeds.

Mobile Network Operators now have to justify why it is worth accessing the Internet through their networks and not by other means, such as 802.11b LANs. The smart cards already existing in their infrastructure can help them do this. The diagram below illustrates the different options that consumers have for accessing data content.

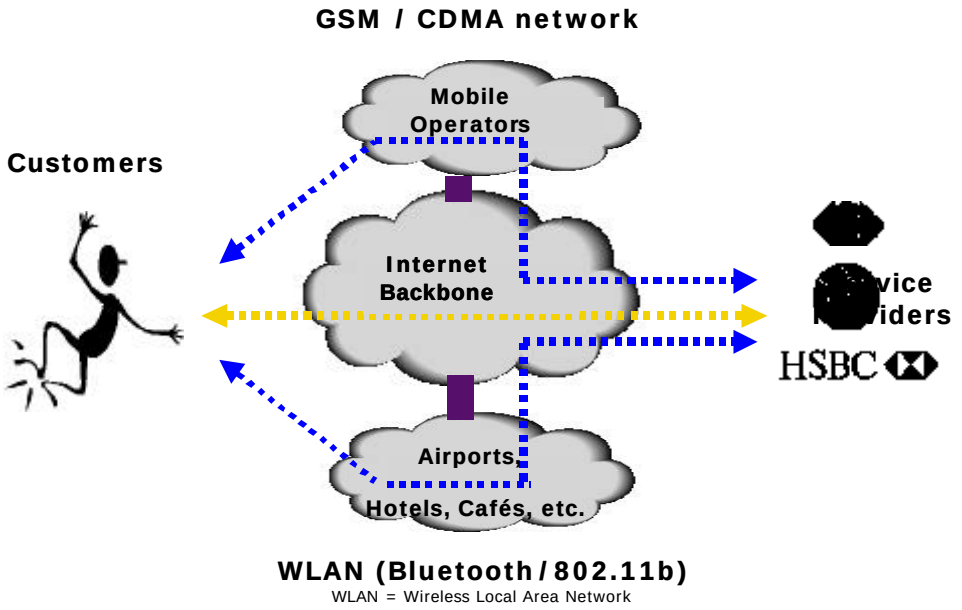

Figure 1: Options for accessing data services

Leveraging security advantages

Security in today's 802.11b networks is poor. The standard does not include a real security mechanism, which makes it relatively easy for a third party to eavesdrop the traffic in the networks. Therefore, using an 802.11b network for accessing the Internet and conducting e-commerce is a scenario that does not currently offer sufficient security or trust.

In contrast to 802.11b, a stable security mechanism was built into the GSM standard from day one in order to enable secure network access. This was achieved by relying on SIMs (Subscriber Identity Modules), which are a type of smart card.

Challenges faced by Service Providers

Service providers, both wired and wireless are looking for better relationships with their customers. When a bank sets up its Internet site using the HTML protocol, it has to go through its Internet Access Provider at some point. However, after that, the bank pretty much has a free hand when it comes to selecting the technology that it wants to use to enable secure transactions. It could, for example, choose to implement a maximum-security system for its customers by using smart cards integrated in its online service through PCs. Nevertheless, this would be a proprietary solution for a limited market and would require new hardware and software for it to take off.

When a Service Provider chooses to make its online services available wirelessly, it faces many questions:

- Which device will be most convenient for the end user?
- What security level do we want to offer our customers?
- Which network and coding protocol do we intend to implement? (GSM/CDMA/802.11b? or HTML/WAP/I-Mode?)

In terms of security, GSM definitely has the advantage, since its architecture offers secure, "tamper-proof" storage. This feature is owed to the removable SIM smart card embedded in the GSM device that enables the subscriber to access the network securely. The same smart card could also be used for a variety of other purposes, such as secure mobile banking, identification, and privacy management. Nevertheless, in today's world, the SIM is the property of Mobile Network Operator (MNO). This means that nothing can be done with it without first consulting the MNO.

In order to utilise the smart cards' capabilities in the GSM devices, many banks have teamed up with Mobile Network Operators to offer secure wireless financial services based on the SIM. Other banks have relied on a lower level of security and have simply set up their own WAP or I-mode site for financial transactions without using the SIM or the experience and help of the Mobile Network Operators.

Those who have relied on the SIM and its capabilities have a very secure solution in place but have also experienced issues relating to the MNO's ownership of the SIM. Having cryptographic keys that enable secure access and identification for a bank's Internet site stored in the MNO's SIM is a sensitive issue.

To counter the ownership issues, some banks and MNOs have made trials using two SIMs (multi-slot) in the handheld device, one belonging

to the MNO and one belonging to the Service Provider. This has meant modifications both for the hardware and software in the handheld device and is clearly not the best option for a future in which a large amount of different services will have to be offered quickly and securely to the end users.

The issues that have been discussed here become even more evident when designing services that extend over national boarders. However, voice services are already offered across national borders, and the same should happen for data services as well.

Challenges facing the industry as a whole

Fragmentation

Rampant credit card fraud continues to weaken consumer confidence in online commerce and drive up the price of transactions. To combat this, many companies are now seeking to enhance security and add trust. This raises several important issues:

- Consumer and retail industry awareness and adoption of the solutions available to address mobile security issues.
- Little or no standardization governing the security practices for establishing, registering, and validating the identity of transacting parties, especially when these parties are mobile and roam internationally.
- A plethora of "island solutions" in security emerging in the wired and wireless world, which is resulting in fragmentation and confusion among consumers, operators, service providers, and content providers.
- Lack of a uniform framework or common foundation for mobile business applications raises the cost of implementation.
- Legal issues surrounding liability (risk management), privacy rights, and the recognition of digital signatures in many countries are too complex for any one company or market sector to solve, especially when the market is global.
- Market development has been hindered by "gridlock" as mobile operators and banks jockey for position in the new economy.

Roaming

Many of the challenges presented by roaming with voice services have already been met. Nevertheless, roaming with data services and transactions brings up another set of challenges as mobile subscribers roam with wireless data services between different networks, countries, and services providers.

For mobile e-commerce services to reach their true potential, it must be possible to exploit the main advantage of wireless devices – *mobility*.

In many markets, these services will soon be in place. But we have to ask: Will subscribers be able to roam with their data services as they already can with voice services?

The next section will examine the proposed approaches for making this possible.

CONCEPTS

Trusted Transaction Roaming (t^2r)

There is clearly a need for a trusted platform that would overcome the inherent weaknesses of the Internet itself when accessing it over a wireless device. The Transaction Roaming Platform would form the base for a global neutral network that builds consumer confidence, offers positive user experience, and ensures a wide array of attractive services across national boundaries.

Such a wireless trust network would be responsible for establishing business architectures, clarifying liability issues, specifying technical standards, facing regulatory challenges, and building bridges to other trust networks.

Many companies have been working with Public Key Infrastructures (see "Enabling Technologies" in the appendix) to generate trust by providing non-reputable authentication. Since the required technologies already exist, Radicchio's t^2r efforts are directed towards defining the business environment for the use of a reliable, interoperable trust framework on a global scale.

In the sections below, we will seek to define the project objectives, describe the approach that should be used to meet the relevant challenges, explain the difference the t^2r innovation will make, and discuss how this will influence the business case for the players involved in m-commerce.

Objectives

The t^2r Platform must meet the following objectives:

- **Global interoperability** - We need interoperability between secure networks that extends across national boundaries to other secure networks. For example, a subscriber who is roaming in a foreign MNO's network has to be able to access familiar services as securely as in his/her home network.
- **Secure network access** – This is a prerequisite for any service in any network. However, many networks (for example: 802.11b) are not secure enough today. In these networks, a third party could eavesdrop on the communication. Networks that rely on smart cards for network access (as is the case with GSM) are considered very secure because the SIMs offer advanced cryptographic capabilities and tamper resistance.
- **Secure content access** – Once a consumer has been able to securely access his/her preferred network, different Service Providers want to make sure that only their appropriate customers can securely access the content/service on offer.
- **Reliable identification** – Just as in the real world, some businesses want to identify you before they serve you. Reliable identification systems are especially important when conducting mobile commerce or dealing with financial or private information.

- **Privacy management** – Relationships between consumers and businesses are sensitive and frequently involve the exchange of private information. Consequently, both parties have responsibilities with regard to handling this information. Here, we need a technology to secure the information exchange and to protect and enable management of the private information wherever it is stored.
- **Convenience & benefits** – ***End-users*** will be offered a vast amount of services conveniently on a global basis. In some cases, data may have to be added, deleted, edited, or updated. This could cause inconvenience. For instance, when a subscriber changes his/her handset to a newer one, all the settings, names, addresses and bookmarks could become lost. The trusted platform has to take this in to account and be constructed in a way that eases the end user experience.
- **Service providers** will be able to conveniently reach a global subscriber base of 600 million GSM users in a trusted environment without having to negotiate separately with each Mobile Network Operator (MNO).
  MNO's will earn revenues in proportion to how their network resources & subscribers have been used. Importantly, the proposed model tackles the business cases for both the MNOs and Service Providers through a revenue sharing model.
- **Legal enforcement** – The relationship between the business and the consumer should take place in a fair way. However, clear dispute resolution authority is required in disputes of any kind. This authority could differ depending on the nature of the service (for example, financial service versus health services). Furthermore, the trusted entity that will operate the proposed platform must obey strict laws and guidelines.

Approach

The t^2r efforts should not try to reinvent the wheel. The participants in the t^2r Project will ultimately drive the construction, design, and implementation of the platform and will leverage the work of existing organizations for specifying functional and technical elements. Here are some examples:

Universal "single sign-on" for online services. The Liberty Alliance is working to construct a universal identification system for online services relying on a "single sign-on" solution. It is promoting decentralized authentication and secure maintenance of personal information. The members represent over a billion customers and include such companies as: American Express, AOL Time Warner, France Telecom, Gemplus, General Motors, Hewlett-Packard Company, MasterCard International, Nokia, NTT DoCoMo, RSA Security, Sony Corporation, Sun Microsystems, United Airlines, Vodafone, etc. Please also see: http://www.projectliberty.org

Privacy Framework. The International Security, Trust, and Privacy Alliance (ISTPA) is a global alliance of companies and technology providers working together to clarify and resolve existing and evolving issues related to security, trust, and privacy. The ISTPA's focus is on the protection of personal information. Its founding members are Gemplus,

Intel, American Express, Motorola, AMD, TRUSTe and NCR. More info at http://www.istpa.org

Legal Framework for online services. The European Union, the US Federal Trade Commission, and several countries' Data Protection Agencies have agreed on common legal aspects concerning online services including privacy. They have settled on what is called "The Fair Information Practice Principles" in order to protect consumers from Privacy violations.

Ties to standardization bodies. The work of The European Telecommunication Standardisation Institute (ETSI) and its subgroups gave birth to the GSM standard. Likewise, it will be important for the consortium that will drive the Network of Excellence Program to establish close links with standardization bodies. This will help in integrating the trusted platform seamlessly into the standards of today's and future network technology (3G and beyond).

The purpose will be to build on the work that already has been done and go even further in terms of integrating it in to one trusted platform. It is important that all the elements in the trusted platform work seamlessly together. Therefore, the integration of various elements (such as identification, secure network & content access, network interoperability and privacy management) will require the most work.

Innovation

Current m-commerce environment

Today, each service provider has to go through each Mobile Network Operator (MNO) to reach the wireless subscribers. The SIM card can be used to enhance the security of these service offerings, but each solution is proprietary and involves a complex implementation process between the MNO and Service Provider.

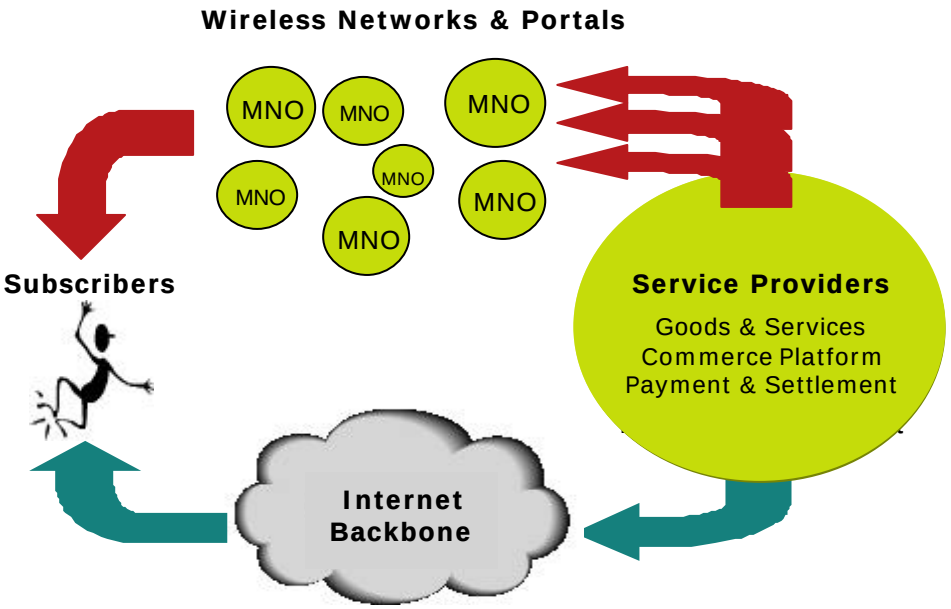

Figure 2: The current m-commerce environment

The t^2r innovation

The key innovation lies in the new architecture that adds a neutral entity to operate a global platform that will use the property of all the Mobile Network Operators in an equal way. It will use their network infrastructure and their SIM - USIM cards globally to create one secure network that can be linked to other secure networks.

The architecture will unleash the capabilities of SIM – USIM cards for everyone's benefit and serve as a common platform enabling content and service providers to reach mobile subscribers in a trusted environment.

One Global Wireless Network
A Trusted Platform for Wireless Data Services

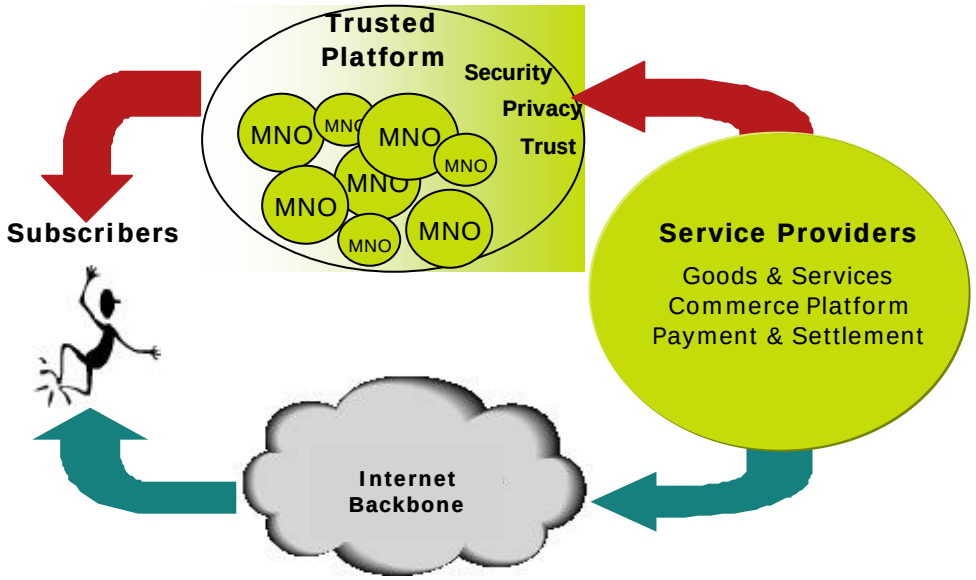

Figure 3: The t^2r innovation: a trusted, global platform

Business cases

The t^2r Platform will solve existing business issues in the wireless data services market. It changes the way that Mobile Network Operators and Service Providers interact with each other as they offer data services to wireless subscribers. The business case is founded on a revenue sharing model that is of mutual benefit to both Service Providers and Mobile Network Operators.

Mobile Network Operators – In today's business environment, the MNO has to negotiate separately with each Service Provider to bring a new secure wireless services offer into place. This includes business model issues, technical solutions, and policies (such as whether or not adult content is allowed). In the proposed Trusted Platform, the entity could take over this costly negotiation operation and offer a stable revenue sharing model to both parties. The MNO would receive revenues in proportion to how its network resources have been used to distribute the services to the subscribers. This should result in a gradual increase of the ARPUs (Average Revenue Per User) for Mobile Network Operators.

Service Providers – It is currently somewhat difficult for Service Providers to offer services to wireless customers by relying on the security provided by smart cards in the mobile networks (GSM). The Service Provider has to enter into specific agreements with the MNO for each network that should carry its service. This is an extremely complicated and slow process, and frequently requires proprietary security solutions. If a Service Provider wants to reach wireless subscribers on a global basis, the process becomes even more complex and costly. The proposed Trusted Platform would enable any Service Provider to benefit from the underlying security infrastructure and access wireless subscribers on a global basis. This would simplify the complex process of providing secure, high-quality services to wireless customers, which is an important prerequisite for a better customer relationship. This revenue sharing model will offer the Service Providers the opportunity to reach the global mass of wireless subscribers and also reduce the set-up and implementation cost of its offers.

Various parties stand to save time and money by using independent entities to operate the proposed platform in a trusted global network. Furthermore, unleashing the security and privacy potential of smart cards will benefit all parties involved. Smart cards are widely recognized secure tokens and are already implemented within the European telecommunication and financial industries.

Since the operator of such an extensive platform will deal with so many different parties' confidential information, it must be a neutral entity that is truly trusted and recognized by all the players in the data services market – such as financial institutions, MNOs, and companies that provide services, content, or technology. This neutral entity would operate the Global Identity Management on behalf of all GSM Mobile Network Operators.

CONCLUSIONS

We must work together to build a trusted platform

Establishing a large, trusted marketplace for mobile e-commerce is too complex, too expensive, and too risky for a single company to accomplish it on its own.

The roaming framework for trusted mobile services must be:

- **Open**: by building a common, neutral platform for global transaction roaming and 3rd party applications.
- **Trusted**: to build consumer confidence.
- **Managed**: to allow content and service providers to reach a large base of mobile subscribers with compelling content without losing control of the networks.

Clearly, such a challenge requires a great deal of coordination between the major players involved, especially the Mobile Network Operators (they have the subscribers and networks) and Services Providers, such as banks (they have the expertise for handling financial transactions).

Once the industry has agreed to build this infrastructure, we must immediately begin the task of installing confidence in the system. Mobile commerce will only become a normal part of everyday life if people know that they can rely on their business partners and are protected against fraud.

A first step has been taken

Radicchio is now proposing the t^2r (Trusted Transaction Roaming) Project to enable the construction, design, and implementation of a Trusted Platform. The t^2r Project will also lay the foundation for one or many neutral entities to operate such a platform for the benefit of the end users, Service Providers, Mobile Network Operators, and various other players in the wireless data services market.

The t^2r Project was presented to the leading mobile operators at the Carrier Summit held in March 2002 in Bandol, France. Operators present included Hutchinson 3G, mm02, MTN, Orange, Sonera, T-mobile, and Vodafone. The aim of this summit was to reach a consensus on the best way to develop a global framework for trusted mobile and wireless transactions. The feedback was encouraging, and Radicchio believes that this summit has signaled the start of global roaming for secure wireless transactions.

To ensure that the framework becomes truly global, Radicchio invited the GSM Association and the Liberty Alliance to present at the Operator Summit. Follow-on efforts are planned with other leading industry bodies, such as the European Telecommunication Standardisation Institute (ETSI) and the ICT Standards Board.

Based on the discussions at the Radicchio Operator Summit, the operators agreed on the following general position:

- Operators recognize the strategic potential of trusted actions based on SIM-card security for current and future services, such as end-user identification, enterprise access control, online payment, etc.
- The operator and service industries need to cooperate to enable the widespread take-up of trusted transaction services.
- The potential of trusted transactions involving third-parties (e.g. banks) can only be successful if operators co-operate to extend a common, global interface that enables secure services.
- The operators will encourage the development of the necessary technical, procedural, and legal standards on a global scale to establish an open and reliable standard that may be implemented by technology providers and used by content and financial service providers.

Next steps

As the t^2r Project moves ahead will seek to:

- Form an **alliance** of mobile operators that can speak with one voice and act in concert when dealing with the other segments of the m-commerce value chain (particularly the Service Providers).
- Further define the **business case** for global interoperability and business architectures for the various industry segments.
- Negotiate contractual **agreements** to establish enforceability and clarify liability and privacy issues.
- Create a common **platform** for identity management systems in the mobile world, for payment processes, and for content/service offerings.

In the coming months, Radicchio will establish a suitable management structure and technical framework for the t^2r Project based on the input from its members and working groups. The results will be published and discussed at the Radicchio Annual members meeting in July 2002.

Appendix: Enabling Technologies

Many technologies are involved in the implementation of such a large-scale project, but here are a few of the most important:

GSM

Global System for Mobile Communications. The most widely used digital mobile phone system and the de facto wireless telephone standard in Europe. GSM is now one of the world's main 2G digital wireless standards, present in more than 140 countries. In fact, GSM uses the basic TDMA technology standard and is implemented on the 900, 1800 and 1900 MHz frequency bands.

GPRS

General Packet Radio Service. A 2.5 G network technology that adds packet switching protocols, shorter set-up time for ISP connections, and offer the possibility to charge by amount of data sent rather than connect time. GPRS promises to support flexible data transmission rates typically up to 20 or 30 Kbps (with a theoretical maximum of 171.2 Kbps) as well as continuous connection to the network. GPRS is a significant step towards 3G, needing similar business model, and service and network architecture.

W-CDMA

Wide-band CDMA. CDMA protocol originated by the Mobile Network Operator NTT DoCoMo and now adopted for third generation networks by ETSI (European Telecommunication Standard Institute) in Europe. W-CDMA supports very high-speed multimedia services such as full-motion video, Internet access, and video conferencing.

SIM - USIM

SIM (Subscriber Identity Module) is a Smart card, which is standard and used in all GSM mobile phones today. The USIM (Universal Subscriber Identity Module) is the equivalent for the next generation of network technology (3G). The Smart card that is embedded in the mobile terminal authenticates the subscriber to the network and can also store a variety of different applications to enable security, trust, privacy and convenience.

Public Key Infrastructure (PKI)

PKI enables the users of an unsecured public network, such as the Internet, to securely and privately exchange sensitive data and conduct financial transactions using a public and a private cryptographic key pair that is obtained from and shared through a trusted authority. The Public Key Infrastructure provides for digital certificates that can identify individuals or organisations and directory services that can store and, when necessary, revoke them. A PKI consists of at least: A Certification Authority (CA), Registration Authority (RA), one or more directories, where the certificates are held and a certificate management system.

The main benefits of PKI-based transactions are strong authentication, confidentiality, non-repudiation, and data integrity.

About Radicchio

Launched in 1999, Radicchio seeks to unleash the tremendous potential of the market for wireless data services, such as mobile e-commerce and mobile e-government.
Guided by a cross industry board of directors including Certicom, EDS, Ericsson, Gemplus, MTN, Sonera Smarttrust and Vodafone, Radicchio is the authority and the industry voice for trusted networks in the mobile world.

Mission

To pave the way for the **mobile revolution**
by facilitating the establishment of a **cross-industry platform**
for **trusted wireless transactions**.

Membership

Radicchio currently represents the interests of:

- Hardware manufacturers (handsets, cards, chips)
- Financial institutions
- Content providers
- Certification service providers
- Systems integrators
- Mobile operators
- Application service providers

Primary tasks

To drive, develop and accelerate market developments, Radicchio seeks to:

- Bring major players together to ensure interoperability.
- Remove bottlenecks.
- Work with international legal & regulatory bodies.
- Publicize the market opportunities.
- Develop mobile transaction solutions with high acceptance among merchants and wireless subscribers.

Working groups

- **Security & Mobile Devices WG** – Seeks interoperable security solutions for the mobile device, including security architectures, secure storage, and user authentication (biometrics).
- **Best Practices WG** – Establishes Radicchio guidelines for best practices, and analyzes successful mobile security implementations.
- **Legal, Regulatory & Governmental WG** – Provides legal support to the other WGs, seeks solutions to the legal challenges specific to mobile applications, and accelerates the acceptance of m-government applications.
- **Marketing WG**– Promotes solutions that will drive the market for trusted mobile data applications.

Deliverables

- Website as a communications platform.
- White papers and guidelines on important industry issues
- Strong conference presence.
- Radicchio Academy as an opportunity to train & learn.
- PR work and lobbying (press releases, by-lined articles, interviews, etc.)

For further information

Please contact: info@radicchio.org or visit: http://www.radicchio.org