Enhancing Security and Trust in WAP in Mobile Commerce Part 5
Singapore, Fri November 10 2000
By the editorial team of e-Cop.net

Enhancing Security and Trust in WAP on M-commerce
In order for e-commerce and m-commerce (mobile commerce) in the area of consumer business to flourish, the most important factor is that the consumer uses these services. Therefore there is a need to give the consumer confidence and trust to use m-commerce on their wireless mobile equipment e.g. WAP enable phones or PDAs. Many WAP phone subscribers do not take advantage of the WAP service simply because they are worried that their personal data and important information; like credit card number, are disclosed to fake merchants and untrusted WAP Gateway providers when doing m-commerce on the untrusted public network - The Internet.

Another reason is that the connection speed is extremely slow so the costs of accessing the Internet and m-commerce are very high. In order to give trust to the consumer, solution like Wireless Public Key Infrastructure can be implemented.

Public Key Infrastructure (PKI)
Public-key infrastructure (PKI) is the combination of software, encryption technologies, and services designed for secure communications and business transactions on the Internet. Public-key infrastructure is basically made up of public key cryptography, which consists of shared secret key and public key. A PKI thus fulfils the four basic principles of a secure Internet; Confidentiality, to keep information encrypted and secure; Integrity, to prove that information has not been tampered with during transmission; Authentication, to identify a user and Non-Repudiation, to assure the origin of a transaction.

Third Party Trust
Third-party trust refers to a situation in which two people implicitly trust each other even though they do not have a personal relationship. Two strangers can trust each other if they each have a relationship with a common third party, and that third party vouches for the trustworthiness of the two people.

The need for third-party trust is fundamental to any large-scale implementation of a network security. When establishing third-party trust among a large number of people, one authority is needed to ensure the trustworthiness of the others.

public key cryptography, third-party trust is in part human and in part automated. A trusted human authority must decide the rules regarding who is and is not to be trusted. Automation can manage the actual trust relationships.

Certification Authority (CA)
The role of the CA has become a crucial component within the networked economy. Used across a variety of e-business and m-commerce applications, from online banking to shopping, the growing need for digital certificates is opening up enormous opportunities for Certification Authorities (CAs), those organisations responsible for the issuing and management of user Certificate.

Registration Authority (RA)
The Registration Authority (RA) consists of the following 3 components.

Registration Authority Console
Registration Authority (RA) Console is a server being set-up for the Registration Authority Officer to submit Certificate request. It can communicate with the Certification Authority (CA) Server to handle digital certificate request in a Certification Process. It is typically installed on different machine from the Certification Authority Server that it serves and will be under surveillance. Biometrics-based protection mechanism, like verifying fingerprint of the Registration Authority Officer, in accessing this Registration Authority Console will be used.