FRAMEWORK FOR THIRD GENERATION (3G) CELLULAR NETWORK DEPLOYMENT AND SERVICES OFFERING IN SINGAPORE

RESPONSE FROM GEMPLUS

Answer to TAS Consultation on 3G cellular network deployment & services

1 The services for the 3G

- In one hand, for existing 2G operators going to third generation, 3G offers an extension of the radio spectrum and voice could still be a central service for the beginning. This will be enhanced by video, but it is likely that this service will be expensive, therefore many users may still use voice-only communication.

- In the other hand, new services emergence, based on the broadband access for data that 3G offers, will be triggered by the need for differentiation of both existing 2G operators and 3G new entrants.

- Many applications will come from adaptation of successful internet applications. These wireless internet applications can be listed in domains as: entertainment, messaging, transactions…
  - Entertainment : e-gaming, e-gambling, e-commerce, e-book, e-music,
  - Messaging : e-mail, e-chat, instant messaging
  - Transactions : e-bank, e-trade, e-commerce, e-auction, ..

- Another way to divide applications into categories is to look at the interlocutors :
  - Person to person, e.g. voice, video or data exchange between users
  - Person to machine, e.g. consultation on a server
  - Machine to machine, e.g. control

- Some applications will be specific to the mobile context, we can expect for instance:
  - Services based on the location : positioning, localized advertisement,…
  - proximity services: the handset will probably have the ability to communicate locally with the environment through short range radio like Bluetooth. This will allow "proximity services" as home remote control , synchronization with other information devices (PC, palmtops,…), local transactions with merchants.

Some operators in the world have definitely identified specific services (i.e. without any equivalent in the 2G or 2.5G) relying on the possibility to have pictures on the move.

On a general basis, the business model to which 3G shall be compared is more the one of internet rather than the one of 2G : 3G is more an open system, in which users can choose their applications. In this respect, 3G will satisfy individual needs. Therefore, it is difficult to define who is "the" typical 3G user.
As usual, the demand from business users should drive the emergence of high speed multimedia services and emergence of wireless intranet.
Another consideration is the fact that 3G will extend to "non person" subscribers.

2 The 3G actors

Favoring new entrants is beneficial to the end user. On the other side, favoring the transition of existing 2G operators to the 3G is also beneficial to the end user. For this reason the scheme of allocating spectrum for both existing and new players appears to be a good scheme.

Compared to 2G, which is voice-centric, the different roles of the operator are more visible in 3G. And these different roles may be in fact played by different actors.
Roughly :

- Carrier/ISP: the entity which transports the data from/to the user. Early stages in the 3G standardization process shown the will to favor a 2 layers model for the basic service provision: pure carrier and service/connection provider. This model has lived and it is now foreseen that carriers will still be the main subscription provider as in 2G.
- gateway/portal : the entity which is a central node to a range of services. Looking at the situation in 2G, it is not clear yet if it will be controlled exclusively by the carrier.
- Content provider : In any case, the number of contents providers should be greatly increased, compared to 2G
- Bank : The role of banks in 3G's e-commerce is not clarified, mainly because mobile e-commerce infrastructure is still in the evaluation phase for 2G
- Certification authority : this is the entity which guaranties the transactions, including the origin and the destination (trusted third party)

A regulation authority may desire to define the rules, regarding the combination of these different roles, according to national laws. For instance, it may be allowed or not in a specific country that an operator owns a bank, and that access to some 3G services are subject to opening an account in this specific bank.

3 3G Applications will need smart cards

In the standard defined by 3GPP, a smartcard, called the USIM (UMTS Subscriber Identity Card), is mandatory in every terminal in order to make calls. We list below what functions will be assumed by the USIM.

- security by shared secret Key : this is used to verify the subscription of the user to a specific operator (carrier, portal, content provider, bank). The secret key is stored securely

in the card, and the user is authentication is carried through a challenge/response exchange (e.g. what is done is the authentication scheme defined by 3GPP and 3GPP2)
- Personal Information Manager (phonebook, bookmarks, URL) : the smart card offers a convenient place to store all the personal information. This place is secure (protected by a PIN code) and transportable.
- SIM Toolkit applications will certainly permit to have a smother transition from GSM to 3G, as it permits to extend some capabilities of GSM terminals towards 3G. This is in particular the case with m-commerce.

Additionally, the USIM is a platform for other applications, or features, such as:

- Public key security, in which the card is used to store the secret key used for public key generation, and to check the certificates from the third trusted party. This is in particular the features which are provided by the WIM (WAP Identity Module) which is used in transactions build on the WAP protocol.
- copyright control for content : high-value contents (such as books, videos, music, games) will be downloaded on the 3G terminal, thanks to the high throughput offered by 3G and to the multimedia abilities of the terminal. Then, copyright control may be offered by an application embedded in the smart-card (USIM).
- provisioning (& cookies) : today's world need to remember a lot of parameters (network, password), e.g. in order to connect to its email mailbox. The card offers a secure way to store all these information, which can be populated by the operators themselves.
- cache for data or application that would need too much time to download at every use. Therefore, USIM storage would allow local browsing and a good protection of these data.
- user authentication based on biometrics. The card offers a convenient way to store the biometrics parameters of the user and to perform the check of the identity (comparison between the stored and the measured parameters)
- plastic roaming. The USIM offers a convenient way to offer global roaming to the user between the different IMT-2000 sub-modes, and with preceding systems (GSM, CdmaOne, PDC…)

All these applications will require smart cards with high EEPROM memory (256k to a few megabytes), in order to meet the application requirements.

4 Regulation in the smart-card area

As seen before, the smart-card is a link between the user and the service providers. In GSM, the service provider is the GSM operator, therefore the SIM is his property. In 3G, there are many service providers. We see here some possible schemes :
- the 3G operator keeps the property of the card, and this implies that other actors need to agree with the 3G operator in order to have their parameters/programs downloaded into the card
- either the user becomes the owner of the card, which is seen as a execution platform on which the user chooses freely to download applications. In this case, there is a reserved area for the operator.
- in some cases, a dual-slot terminal (which means that the terminal accepts 2 smart-cards at the same time) may be useful. This might be the case when 2 different smart-card

applications cannot share the same smart-card, for security, psychological, or legal reasons (e.g. credit card and SIM).

More precisely, we see these different fields in which some rules may be defined :

- security on the application level (e.g. for m-commerce, m-banking)
- service profile & portability (roaming between networks, between terminals which can be achieved by smart-card roaming)
- common criteria of certification of the security of the card (ex: anti-DPA). This is specially the case as some security mechanisms are not fully standardized.
- confidentiality of the data : phonebook, sensible data (e.g. medical data), cache for local browsing shall be protected from unauthorized access.
- size of the storage space allocated to the user. Some applications are user-centric and will be probably loaded by the user himself on his card. Thus, the user might be freely allowed to choose the capacity of the smart-card.
- user data versus operator's ownership : shall the operator be authorized to fetch information that were stored by the user ?

Anyway, it is a field where a regulation authority might desire to arbitrate between all the players, in order to guarantee the user a free choice, and a good privacy.

5 3G WW time-frame for 3G frequency licensing.

Outside Asia, 3G frequency licensing policy will be as follow :

- In Europe, all licenses will be allocated at the end of Y2K. The 3GPP standard is mandatory (note that the USIM is mandatory in this standard). The principle of allocation : beauty contest or auction, depending on countries
- in the USA, there will be a problem because part of the IMT-2000 spectrum is already allocated for 2G systems. So, 3G systems are not likely to be deployed before 2002. The choice of the standard will probably be left to the operator.