Pipeline
Knowledge Is Power

www.pipelinepub.com Volume 4, Issue 1

Finding Your Identity: Fixed-Mobile Convergence and ID Management

by Bohdan Zabawskyj and Jeff Popoff

The market readiness of fixed-mobile convergence (FMC) technologies is still an open question. Home zone technology is the least disruptive and fully market-ready, while the introduction of mainstream IMS-based SIP services remains at least 3-5 years away. Regardless, the transition to total FMC is inevitable. It is only a matter of when, not if.

According to research from Heavy Reading, differences in the core networks of fixed and mobile technologies will all but disappear by 2012. Operators are in varying stages of integrating their fixed and mobile networks and services to drive operating and capital cost efficiencies, to leverage economies of scale and to provide competitive bundled offerings and complementary distribution channels for content and services. In an FMC environment, operators will be able to leverage their respective brands while simultaneously tailoring product packages to meet the specific requirements of subscribers.

One key strategic enabler underlies the successful consumer adoption of FMC: subscriber identity management across multiple services and networks. FMC services, such as UMA and SIP-based dual-mode services are making possible the convergence of subscriber services across multiple access networks.

However, federation of subscriber identity across all networks brings with it significant challenges. Mobile operators must address regulatory concerns over identity privacy; they must evaluate the commercial value of "follow-me" service personalization, including availability management; they must coordinate the bandwidth policy management of so-called "free-rider" IP services such as P2P file exchanges. This article addresses the ways in which operators can seamlessly adopt and bring to market FMC technologies while protecting subscriber privacy and preferences.

The authors explore best practices for subscriber identity management and present a straightforward examination of the fixed-mobile convergence space as it stands today.

Current market readiness of FMC technologies

Initial FMC attempts were based on Intelligent Network (IN) architectures but experienced limited successes due to operational complexities and costs resulting from an absence of end-to-end approaches for provisioning and operational management of subscribers and services. Some limited successes led to wireless identity management such as Home Zone for consumers and Tiered Billing for enterprises. However, the underlying SS7 protocol of IN architectures was connection-oriented and designed predominantly for voice services, and by the mid to late 90's, it was soon recognized that IN approaches fell well short of expectations.

This shortcoming was rectified in the early 2000's with the development of open architectures such as Parlay, IMS, SIP, eTOM, and SOA. These technologies provided a more highly integrated and end-to-end view of subscribers, and furthermore were designed to be amenable to multi-media and Internet services. Many operators today are well underway in deploying IMS, which will be the key core network technology underpinning FMC. Additionally, the rapid evolution of 'smart phones' has helped to realize mobile delivery of multimedia services using FMC networks by placing sufficient features, bandwidth, and processing power directly into the hands of subscribers.

How subscriber identity management is proving a key enabler for FMC

FMC has the potential to do for communications what Apple did for mobile music, TiVo did for television, and Amazon did for books. Lest there be any doubt about the business value of identity management, consider the example of three companies that sell identical underlying commodities (books in this example). One company offers identity management and personalization, the other two do not. As a result, between 2004 and 2005 Amazon's sales grew 18% compared to 3% for Barnes & Noble Bookstores and 5% for Borders/Waldenbooks (Source: www.fonerbooks.com/booksale.htm).

The personalization of FMC is defined by total subscriber freedom: the freedom to control their privacy, multimedia preferences, permissions and identity; the freedom to control their availability, location, presence and call-handling; and the freedom to control opt-ins, opt-outs, notifications and memberships, be they contacts, buddies or groups.

Privacy management is essential to promoting user confidence when adopting privacy-sensitive services such as advertising, Location-Based Services (LBS), and personalized broadband services. In a public opinion poll by Forrester Research, 43 percent of respondents felt that LBS would threaten their privacy. In some jurisdictions such as the US, there are even regulations requiring that LBS demonstrate compliance, the FCC Customer Proprietary Network Information (CPNI) rules for instance.

The role of GUP and HSS standards

Numerous industry initiatives like Microsoft Passport and Liberty Alliance were started to address the issue of user profile data management. A telecom-based initiative 3GPP Generic User Profile (GUP) aims to aggregate user profile information relevant to network operators. The HSS (Home Subscriber Server), or User Profile Server Function (UPSF), is the master user database that supports the IMS network entities actually handling the calls/sessions. Similar to the GSM Home Location Register (HLR), the HSS contains subscription-related information (including the IMPU, IMPI, IMSI, and MSISDN), performs authentication and authorization of the user, and can provide information about the physical location of user.
While HLRs enabled the mobility of services outside the home network, services are generally restricted to a fair degree within visited networks. HSS improved on this by enabling most home services to be available in visited networks. However, a shortcoming of GUP, HLR, and HSS is that they do not provide accommodation for user preferences, privacy, or context sensitive services.

The core of personalized service delivery will be the ability to collect, analyze, and use information about subscribers and their preferences. Unfortunately, the Internet experience demonstrated that personal data is a valuable asset that can be used incorrectly or fraudulently, and therefore subscribers are reluctant to give it away for reasons ranging from simple inconvenience (i.e. unsolicited ad messages or spam) to real threats such as identity theft. Thus the GUP, HLR, HSS constructs require augmentation to both securely and permissively handle subscriber identity management aspects.

Policy Management for FMC Networks

Consistent and predictable Quality of Service (QoS) levels will also form a crucial part of the end-user experience across access technologies. It will therefore be important to regulate and guarantee QoS levels on a per-service and per-subscriber basis. In particular, given the varying nature of next-generation media services, the 'best effort' delivery of services will almost guarantee inferior service levels irrespective of the access technology used, resulting in dissatisfied subscribers. It will therefore be important to both regulate bandwidth in a manner that allows carriers to mitigate costly capacity build-outs for low-value traffic, and to provide a means to optimize the generation and delivery of content and services in a manner that meets the contextual requirements (e.g. fixed vs. wireless) as well as the preferences of the subscriber as stored in a subscriber repository.

Best practices for subscriber identity management

Based on our firsthand experiences with Tier 1 network operators in Western Europe and the United States, we have observed the following best practices for subscriber identity management in wireless and FMC networks:

- Give subscribers simple and convenient control of their privacy, preferences, and permissive identify sharing
- Offer secure and trusted protection of subscriber data by refraining from disclosing it easily or incorrectly to third parties
- Leverage user-data analytics to proactively identify their persona to discover and permissively offer new services that are relevant and valuable to them
- Create one common point of federated subscriber privacy and preference data across networks for use by all FMC services and third party applications
- Leverage the consolidated and federated subscriber data to support the advent of next-generation services by ensuring that appropriate subscriber-centric QoS levels are applied proactively

Conclusion

Clearly, FMC brings with it significant benefits, chief among them the ability to supply communication services ubiquitously while supporting nomadic and mobile capabilities. To remain competitive, however, FMC network providers must be able to differentiate their service offerings by delivering compelling features (e.g. guaranteed QoS levels) and capabilities (e.g. the ability to enable 3rd-party service and content providers to deliver optimized services) quickly and efficiently while maintaining subscriber privacy. Only those FMC providers that are able to deliver the greatest convenience and value, and create the most efficient value chains will succeed in attracting the top content providers and the most loyal and profitable customers.

If you have news you'd like to share with Pipeline, contact us at editor@pipelinepub.com.