Chapter VIII
Identity Management for Wireless Service Access

Mohammad M. R. Chowdhury
University Graduate Center – UniK, Norway

Josef Noll
University Graduate Center – UniK, Norway

ABSTRACT

Ubiquitous access and pervasive computing concept is almost intrinsically tied to wireless communications. Emerging next-generation wireless networks enable innovative service access in every situation. Apart from many remote services, proximity services will also be widely available. People currently rely on numerous forms of identities to access these services. The inconvenience of possessing and using these identities creates significant security vulnerability, especially from network and device point of view in wireless service access. After explaining the current identity solutions scenarios, the chapter illustrates the on-going efforts by various organizations, the requirements and frameworks to develop an innovative, easy-to-use identity management mechanism to access the future diverse service worlds. The chapter also conveys various possibilities, challenges, and research questions evolving in these areas.

INTRODUCTION

Nowadays people are increasingly connected through wireless networks from public places to their office/home areas. The deployment of packet-based mobile networks has provided mobile users with the capability to access data services in every situation. The next-generation wireless network is expected to integrate various radio systems including third generation (3G), wireless LANs (WLANs), fourth generation (4G), and others. One motivation of this network is the pervasive computing abilities, which provide automatic handovers for any moving computing devices in a globally networked environment. Fast vertical handover is considered important for managing continued access to different types of network resources in next generation networks (Li et al., 2005). Such networks will provide ubiquitous service access taking the advantages of each of these forms of wireless communications. Service intake will be increased significantly through the availability and reach of innovative and easy-to-use services. Apart from the remote service access (Web services), the introduction of near field communication (NFC) in use with a mobile phone can enable many new proximity services.

User identity solutions and its hassle-free management will play a vital role in the future ubiquitous service access. Current identity solutions can no longer cope with the increasing expectations of both users and service providers in terms of their usability and manageability. Mobile and Internet service providers are increasingly facing the same identity management challenges as services in both domains continue to flourish. Real-time data communication capabilities of mobile networks will multiply the remote service accesses through mobile networks, if efficient identity management and security is ensured over the wireless access. Personalization through customized user profiles based on their preferences will become an important factor for success of future wireless service access. In more advanced service scenarios, open identity management architecture enables the use of standard user profile attributes, like age and gender, and authorizations for service, such as location, to bring a richer user experience. Users, network operators, and service providers can make use of an open standard technology for identity management to meet their own specific requirements through customizations. There is clearly a need for such a standard for identity management that can be applied to all ubiquitous service access scenarios. As user needs are at the center in the service world from business perspective, identity management mechanism should be user-centric.

The impressive capabilities and reach of emerging next-generation networks, the abundance of services, and on-going development in user device require proper address to the user identity management issues which have yet met the stakeholders' expectations. The main goal of this chapter is to discuss these concerns. The second section discusses the background of identity management. In the third section, requirements and framework of identity management mechanism for wireless service access are given mentioning the current efforts by various organizations. Security issues are also a part of this mechanism. The fourth section provides the future trends. The chapter concludes with the summary of all discussions.

BACKGROUND

In a broadest sense, identity management encompasses definitions and life-cycle management for user identities and profiles, as well as environments for exchanging and validating such information. A service provider issues identity to its users. Identity life-cycle management comprises establish/re-establishment of identity, description of identity attributes, and at the end revocation of identity. Attributes are a set of characteristics of an identity that are required by the service providers to identify a user during service interactions. User authenticates to the service providers as real owner of the identity for accessing services. Authentication is a key aspect of trust-based identity attribution, providing a codified assurance of the identity of one entity to another.

Next-generation wireless network includes state-of-the-art intelligent core network and various wireless access networks. It is expected to offer sufficient capacity, quality of service (QoS), and interoperability for seamless service access remotely. Currently the network and thereby the remote service access are often granted through numerous user identification and authentication mechanisms, such as, usernames/passwords/PIN codes/certificates. Users have to register prior to first usage and publish private information, often more than what is strictly necessary for service access. It hampers user's privacy. There is a growing consensus among the legislators across the world that individual's rights of privacy and the protection of personal data is equally applicable in the context of the Information Society as it is in the off-line world. To address this issue, a user-centric identity management framework is expected where users having complete control over the identity information transmission.

Some services happen in the proximity of users at local access points. These services are accessed through physical interactions with physical cards or devices, for example, payment and admittance. The use of NFC with mobile phones to transfer user information from one device to another boosts the intake of proximity services. The user personal