An Access Control System for Home Based Healthcare Information Sharing using Smart Gateway

Daniel Agbesi Dzissah*[1] Hiroyuki Suzuki*[2] Joong-Sun Lee*[3] Obi Takashi*[2] Nagaaki Ohyama*[2]

[1]Interdisciplinary Graduate School of Science and Engineering, [2]Imaging Science & Engineering Tokyo Institute of Technology, [3]ASIST

1. Introduction

As a result of the graying population, home-based healthcare services has seen a rapid demand over the past decade. Home based care and nursing services are a joint service involving a broad range of healthcare services provided by several other individuals and organizations. Mobile computing devices such as smartphones and tablets have been widely recognized as a means for integrating disparate data and computing resources in the pervasive mobile healthcare field. Moreover, mobile devices provide a platform to develop applications on wireless infrastructure to execute healthcare process that in turn can provide remote access to healthcare information exchange services. Such an environment provides ubiquitous and universal access to resources at the point of care, thus improving healthcare quality. In such conditions the ability to provide effective access control environment to ensure the security and privacy of healthcare information are essential [1]. However, traditional authentication scheme adopted in mobile devices such as passwords, digital certificates, secure tokens and biometrics. mainly focus at only user entry-point authentication, which may not suit dynamic healthcare environments. We propose an experimental design of a certificate based context-aware access control method to be used by caregivers and physicians with mobile devices in home-based healthcare environments. In our proposed system, whenever a user visits a patient's home, a gateway authenticates the user's device using certificates and collects context data used for authorizing access to preliminary services using the PKI-based smart card. For accurate context evaluation, the gateway service collects context data and generates certificate credential based on the received context data such as GPS data and user device MAC address for verification and trust assessment of the authenticated user's device.

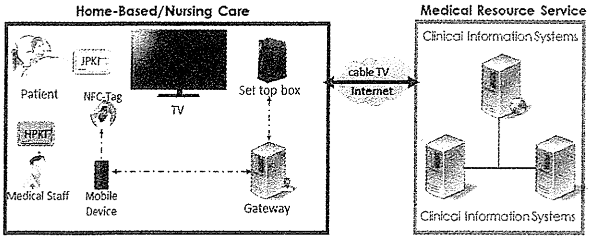

Fig. 1 System architecture

2. Design methods

There are three main elements of the proposed model. First is the application processes running on the mobile device. Second is the gateway, processing authentication requests between remote services and the mobile device.Third is the remote medical resource service, performing duties like authenticating of Japanese-PKI cards and Healthcare-PKI and handle's parsing H-Role privileges of medical staff. When a medical staff requests to access a medical resource service via his/her mobile device, a connection is established with the gateway via a secure NFC-tag as Shown in Fig [2]. By using the application running on the mobile device, a user selects their profile and the resource type. Profile selection allows the mobile application to fetch device's certificate automatically. The application generates a request envelope containing the certificate, the little context data and sends it to the gateway. The gateway receives the request envelope and parses the certificate and returns the generated context. A copy of the context is sent with an authentication request to the medical resource service. A user smart card authentication is required to the medical resource service after authentication between gateway and mobile is confirmed. Context verifies transactions between the medical server and the mobile device, after this verification can the transaction be validated and continue. During this process, a medical staff uses his/her HPKI card to sign a challenge response and enters a PIN code for authenticating card transactions on the mobile phone. According to the validation of the context and the HPKI authentication, the resource authenticates the H-Role of the user. The service is allowed or denied by the system. For a medical staff to access the patient's information, authorization is performed using the JPKI card to sign a challenge response from the medical resource server.

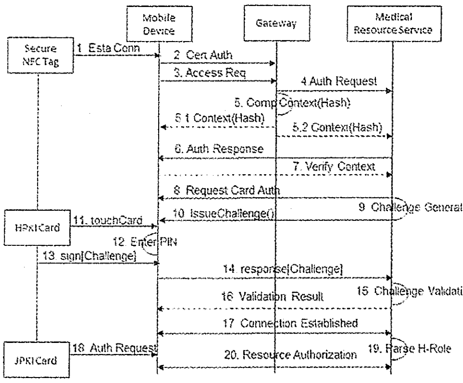

Fig. 2 Activity flow

3. Discussion

The proposed model uses certificates and context as add-ons with PKI-smart cards the aim of providing healthcare resource access to legitimate medical staff. Since relying on a single point, entry authentication cannot be relied on in such setting.

References

[1] He D, Naveed M, Gunter CA, Nahrstedt K. Security Concerns in Android mHealth Apps. *AMIA Annual Symposium Proceedings*. 2014;2014:645-654.