

AUTOPILOT

Integrated System for Automatic Personal Identification and Indoor Localization and Tracking¹

R. Alesii, F. Graziosi, L. Pomante, F. Santucci: Center of Excellence DEWS, University of L'Aquila, ITALY - (roberto.alesii/fabio.graziosi/luigi.pomante/fortunato.santucci@univaq.it)

S. Tennina: CISTER Research Center, ISEP/IPP, PORTUGAL - (sota@isep.ipp.pt)

M. Di Renzo: L2S, UMR 8506 CNRS - SUPELEC - Univ Paris-Sud Laboratory of Signals and Systems (L2S) French National Center for Scientific Research (CNRS) Ecole Supérieure d'Electricité (SUPELEC) University of Paris-Sud XI (UPS), FRANCE - (marco.direnzo@lss.supelec.fr)

Introduction – Future wireless communication systems will have to enable and provide a multiplicity of services for an increasing number of mobile users. In this context, it is very important that wireless technologies might provide these services in a secure and robust way to the final user, by guaranteeing the privacy of users regardless of the specific and requested service. Moreover, future services are expected to be more and more specialized to the user personal needs, as well as user's current location in space on a given time.

Objective – The main aim of this demo consists in providing a solid proof-of-concept of a networked embedded systems, which provide localization and tracking services to control, in a distributed fashion, the access to restricted areas. More specifically, the demo will show that a wireless biometric badge represents an efficient integrated solution for localization and tracking in radio-navigation applications, as well as for automatic personal identification in realistic GPS-denied environments.

Badge Description – Our embedded biometric badge is a “system-on-badge”, which can perform four main tasks: i) localize people, ii) scan and verify fingerprints, iii) check if a user is the badge's owner, and iv) send related outcomes wirelessly to the system, without the need to transmit biometric data of the user over the wireless medium. It is equipped with:

- a System-on-Chip used for wireless medium-range communications as well as localization operations;
- a fingerprint sensor reader with its embedded companion chip. This chip is the key element for handling biometric data: it allows to authenticate people based on fingerprint information, as well as store data in a memory protected from physical external attacks. Moreover, only this chip and the infrastructure's gateway know how to decode the messages they send to each other;
- a RFID tag based on the ISO15693 standard and its companion chip;
- a rechargeable battery, its driver to monitor the charge status, and a user interface with 8 leds and a push-button.



Demo Description – The aim of the demo is to show via experiments two main functionalities of the badge. On the one hand, we will show that a badge-provided user can be localized in a simple way by resorting to a *Location Service* built upon a novel location algorithm, which runs in the badge's microcontroller unit. Localization is performed in a distributed and decentralized fashion by receiving data from fixed nodes, which are called anchor/reference nodes. On the other hand, we will show that when a user approaches an area with restricted access the system can activate the authentication procedure of the user, thus either allowing or denying the user to get access to the area depending on the authentication outcome. This latter authentication procedure takes place via fingerprint matching. However, the system is designed to avoid any wireless transmission of critical user's data.

¹ This work has been supported by WEST Aquila, an spin-off of the University of L'Aquila, and by the ERC Starting Grant VISION (Contract n. 240555).