Project profile

Cluster for Application and Technology Research in Europe on NanoElectronics

CA202 | What you touch is yours [eGo]

PROJECT CONTRIBUTES TO

Communication	✔
Automotive and transport	✔
Health and aging society	
Safety and security	✔
Energy efficiency	
Digital lifestyle	✔
Design technology	✔
Sensors and actuators	✔
Process development	✔
Manufacturing science	
More than Moore	
More Moore	
Technology node	

HIGH QUALITY, HIGH SPEED USER-CENTRED COMMUNICATIONS SYSTEMS

Partners:

ATOS Worldline
CIT
Continental
Cork Institute of Technology
Decawave
Gemalto
IDEX
INRIA
Lincor Solutions
Precise Biometrics
STMicroelectronics
Tyndall Institute

Project leader:

Jean-Pierre Tual
Gemalto

Key project dates:

Start: July 2010
End: June 2013

Countries involved:

France
Ireland
Norway
Sweden

The eGo project proposes an innovative way to establish secure, bidirectional wireless communications between objects or individuals in the future 'Internet of things'. This is based on a touch-and-use scheme exploiting the electrical conductivity over human skin and will open up intuitive ways of establishing ownership of items used in electronic transactions. The concept proposed embeds innovative sensors and batteries, ultra low power receivers, chip cards, memory and high-speed wireless emitters in a small system-in-package device. The feasibility of the approach will be demonstrated in applications including automotive, electronic payments, access control and consumer electronics.

With the fast growing number of electronic transactions over Internet and product features such as keyless control of vehicles, electronic security has become vital. Positive identification and authorisation levels have to be addressed to prevent illegal use of services and/or physical devices.

The CATRENE CA202 eGo project aims to develop hardware and embedded software devices which comply fully with the next wave of computing and integrate in both ambient-intelligence and Internet-of-things scenarios. It will develop new ways to establish high-speed, secure bidirectional wireless communications channels supporting intuitive and simple context-sensitive interactions between people and objects. These interactions will preserve the security and privacy of the transactions.

New items – eGo and eGo-compliant devices – will integrate very low-power over-body communication to enable immediate touch-and-use interaction between persons and objects. Objects with which the user wants to interact will be provided with small eGo-compliant integrated devices which emit a code that can be carried over the human skin. The code contains essential data to bootstrap a wireless communication based on ultra wide band (UWB) technology.

Over-skin communications

The first communication channel will be based on ultra short distance and low speed, and use the human skin to carry a unidirectional bundle of data from the eGo-compliant device such as a door handle, digital camera, handset or car to the eGo device carried by the end user. The operating distance for this contactless communication is about 12 mm with a data rate as low as 8 Mbit/s. The channel would require an ultra low power transceiver.

The code emitted by the eGo-compliant device would be collected by the user's eGo device working in a permanent listening mode and incorporating an over-skin receiver. Such a receiver can be designed with ultra low power capability; it will have no impact on health as no signal is injected into the user's body.

The over-skin receiver would wake up a second wireless transceiver which opens a second short distance and high speed, bidirectional channel providing a high data rate – up to 30 MBit/s – over a short distance of less than 40 m.
The perfect candidate appears to be the UWB (IEEE 802.15.4a) or pulse-radio technique enabling measurement of distance between the eGo devices. This is essential to prevent some security attacks, allow the start of a transaction or terminate an application. Wireless technologies such as ZigBee and Bluetooth do not allow accurate measurements of such distances – less than 200 mm accuracy.

A secure channel equivalent to a virtual private network (VPN) would be established between the eGo-compliant device and the eGo device worn by the user, exploiting the received code as a session key. As soon as the code is used while establishing the VPN, the eGo-compliant device would generate a new code according to classical cryptographic protocols.

Securing transactions

The goal is to establish a virtual and private connection over the second channel between the user's eGo device and the eGo-compliant device. This would be established when the user explicitly touches the eGo-compliant device using a hand, finger, etc.

The eGo and eGo-compliant devices will support secure transaction characteristics, including:

- **Portability**: Services may be anywhere and eGo device must be able to carry all user credentials;
- **Connectivity**: Service vectors must be able to communicate with a wider system which participates in the complete transaction;
- **Security**: Credentials must be protected – that is available only to those for whom they were initially intended – and must also be impossible to clone;
- **Non-repudiation**: Service vectors must be able to complete a transaction without any risk of repudiation from the original user;
- **Data-storage capability**: Service vectors may need to carry large amounts of data which may be private, public, protected and/or verifiable;
- **Autonomy**: The eGo device must be provided with an efficient, long-life integrated power source;
- **Privacy**: The eGo procedure will, in an environment with supporting infrastructure, make it possible to replace external user biometric verification with faster, privacy-enhancing verification of digital certificates that can also be adapted to multiple levels of assurance and security;
- **Efficiency**: To facilitate this new interaction principle, the project will develop integrated MEMS or sensor devices to enhance the efficiency of the eGo device with use of biometric sensors, inertial sensors and 3D thin-film batteries; and
- **Anonymity**: Cryptographic principles will be embedded within eGo to perform authenticated transactions without disclosing the identity of eGo holders or allowing their traceability.

Reinforcing Europe

The project will demonstrate the feasibility of this over-skin communications capability, demonstrating several eGo form factors, first in discrete components and subsequently in an economic large scale integrated chip approach for mass markets. It will also develop application demonstrators in domains such as automotive with a human/car interaction, electronic payment, access control and identification, peer-to-peer communications and consumer electronics.

Hardware and embedded-software components pioneered in eGo will enable industry to reinforce Europe's position in the development of critical micro- and nanoelectronics components as essential enablers for the future digital economy. These will include chips for body area or personal area networks, and integrated sensors and actuators for many embedded applications.

Necessary security and privacy issues will be addressed, including pervasiveness of wireless interfaces, use of intelligent sensors, context-aware transactions, biometric identity verification and assertion of identity. All necessary embedded software, including Java Card 3.0 and provisions for credentials download, will be developed as will secure synchronisation of eGo devices owned by the same user.

The resulting technology will provide innovative enablers for high-value business segments such as mobile payments, identification and access control, machine-to-machine and device-to-device communications, and device and service personalisation in areas such as cars or travel. It will also make it possible to define appropriate propositions for intuitive, efficient, easy-to-use ways to interact and perform secure transactions in the future Internet of things.

CATRENE Cluster for Application and Technology Research in Europe on NanoElectronics

CATRENE Office
9 Avenue René Coty - F-75014 Paris - France
Tel.: +33 1 40 64 45 60 - Fax: +33 1 43 21 44 71
Email: catrene@catrene.org
http://www.catrene.org

CATRENE (Σ! 4140), the EUREKA **C**luster for **A**pplication and **T**echnology **R**esearch in **E**urope on **N**ano**E**lectronics, will bring about technological leadership for a competitive European information and communications technology industry.

CATRENE focuses on delivering nano-/microelectronic solutions that respond to the needs of society at large, improving the economic prosperity of Europe and reinforcing the ability of its industry to be at the forefront of the global competition.