# In-Air Signature: Security verification on smartphones

## Software based solution to verify people through performing an identification hand movement holding a Smartphone

*Biometrics, Biosignal and Security Group (GB2S), located within the integrated Domotics Center (CeDInt) of the Technological University of Madrid (UPM), has developed a biometric verification system of people through their smartphones. For verification, people have to make a gesture in the air while holding mobile phone in hand. This gesture identification can be invented by people, who can also select their handwritten signature made in three dimensions. The results obtained by this method achieved accuracy rates close to 98% against forgery in several experiments in which was recorded and analyzed a person performing his signature in the air. This result greatly improves current verification systems for mobile phones, where, if it were to record a person writing his PIN, the verification system would break.*

**Technology solution supported by the Technical University of Madrid**

## Technology solution

This technology provides a software solution for the verification of people using a Smartphone. The only requirement is a mobile phone with an accelerometer, through which capture the movements of the repetition of signatures in the air. **In-Air Signature achieve**. Having a low computational cost and an architecture where all processing is done on the mobile device, resulting in real-time verification.

On the other hand, this technology with reduced deployment cost has a wide range of application to different sectors and combination with other technologies.

## Areas of application

- **Sector 1**: Security
- **Sector 2**: ICT applied to network services and infrastructure.
- **Sector 3:** ICT applied to digital content.

*"The proposed technological solution is a big improvement in security verification systems on mobile phones"*

## Market demands

- **Security**
  - Current Capture and biometric verification systems are high-cost and mainly applied to security on military and government sectors.
  - It has been widely demonstrated the vulnerability of current solutions based on two-facto authentication (typically the mobile pone, “what you have”, along with the PIN number)
- **ICT applied to network services and infrastructure**
  - The development of protocols for mobile payment, such as NFC, and the strong involvement of multinationals suggests that mobile payment is near a reality.
  - The market for mobile payments, with a wide variety of companies, partnerships and initiatives, is extremely fragmented and competition is intense. In this market biometric security is presented as a plus applicable to them all and an added value to their products
- **ICT applied to digital content**
  - High penetration of smartphones, chosen by many users as their personal electronic device.
  - The technology for the protection of smartphones is not very advanced, as well as user authentication and identification for the use of applications and network services.

*“The mobile payment, as well as, applications and adoption of smartphones are a high growth market in which this solution presents low cost, easy integration with other applications and high security”*

## Market potential

- **Security**
  - Biometric security on mobile device market revenues will increase from $ 30 M in 2011 to $ 161 M in 2015.
  - The number of users will experience an increase of 4 million in 2011 to 39 million in 2015.
- **ICT applied to network services and infrastructure**
  - Payments by Mobile ranks first in the ranking of the budget for technology leading financial institutions
  - The annual growth rate for mobile payments is estimated at 54%, from 49,000 million to 426,000 millions in 2015.
- **ICT applied to digital content**
  - The number of smartphones will grow from 1,500 million in 2011 to 2,000 million in 2015.

## Competitive advantages

- The realization of the signature is unique to each individual. The imitation of the firms with recorded material is very difficult (about 2% accuracy), similar to handwritten signatures. Falsification has a 100% success after having seen a PIN code, and also it can say, guess, copy, etc.
- No additional hardware required except an accelerometer, which usually comes included in today’s mobile phones.
- Lower cost to the existing market solution with a similar level of biometric security. Ease of integration with the systems of the organization. High interaction with mobile applications and wide versatility of application to different needs (mobile games, mobile payments, etc.).
- Expandable to other devices with accelerometers (TV remotes, pointers, etc.)
- Users accustomed to a written signature, so it is not required to invent a new pattern. Minimally invasive technique.

## References

- Extensive research career and business collaboration. Commercial interest in this technological solution have been shown at national and international level.
- Second prize of the ninth edition of the awards actúaUPM (Business Creation Competition of the UPM) for the best business idea.

## IPR

- Registration software M-005532/2013

## Development stage

- ○ Concept
- ○ R & D
- ○ Lab Prototype
- ⊕ Industrial Prototype
- ○ Production

**Contact GB2S**
Javier Guerra Casanova.
Cármen Sánchez Ávila.
e: {jguerra,csa}@cedint.upm.es
w: http://www.gb2s.es

**UPM contact**
Innovation, Commercialization and Entrepreneurship Area
Centre of Support for Technological Innovation – UPM
e: innovacion.tecnologica@upm.es