

EXECUTIVE SUMMARY

INTRODUCTION

This report investigates the market for mobile phone biometric security products and services. It provides a market analysis of the use of biometrics on a mobile phone for authentication and identification purposes.

Biometric technology in mobile phones has been with us for over ten years but has struggled to pin itself to a suitable use case that results in significant adoption rates. Mobile phone biometrics, similar to biometrics in other computer devices and keyboards, has so far failed to even become a strong niche yet alone a mass-market product.

Ever since Siemens developed its prototype device back in 1998 (pictured below in Figure ES1) there has been steady stream of handsets being biometric-enabled. The most notable example is the deployment of Fujitsu mobile phones, with embedded fingerprint sensors supplied by AuthenTec, by the Japanese Mobile Network Operator, NTT DoCoMo. The biometrics in these Fujitsu devices were mainly used in conjunction with DoCoMo's mobile payments service (using Sony FeliCa RFID¹ chips for contactless payments).

Figure ES1: Siemens prototype mobile phone with embedded Infineon fingerprint sensor (1998)



Source: Siemens

With the exception of the DoCoMo example there have been few other compelling examples. Nor has there been the 'killer app' or use-case that has propelled the mobile phone biometric security market forward. However, Goode Intelligence believes that the conditions are starting to improve for this market and predicts that larger-scale deployments will be evidence in the five-year period from 2011.

¹ Sony FeliCa is a contactless chip that uses RFID and has been embedded in smartcards, mobile phones and other electronic devices. (<http://www.sony.net/Products/felica/about/index.html>)

Goode Intelligence believes that demand for mobile phone biometric security products and services will be driven by:

- **Device protection:** Many commentators say that protecting the device against unauthorised access is the biggest driver for mobile phone biometric security
- **Government insistence:** Government legislation forcing the adoption
- **eHealth:** Aided by legislation to protect patients' records
- **Military and law enforcement:** Already being widely used with mobile devices
- **Identity – the third-factor:** Led by government identity programs and security issues with document-based id
- **Fraud prevention:** Financial-led and the drive to secure the transaction rather than to simply authenticate the end-user
- **Securing data in the cloud:** Need for agile and secure access to data from anywhere anytime
- **Vendor insistence:** Users 'forced' to use mobile biometrics to protect assets and brand
- **Mobile commerce:** The growth of mCommerce and the need to effectively secure the ecosystem on the mobile
- **Near Field Communication (NFC):** This contactless technology that has multiple uses could well be a major driver
- **Physical access control:** The mobile phone as a component in biometric access control solutions
- **Wow factor:** I want one of those - the Minority Report factor – the “James Bond Phone”
- **Convenient protection:** Easier and more convenient to use than conventional technologies

GI explores these market drivers and their counterbalancing market barriers in later sections of this report.

In addition, GI also investigates the current demand for mobile phone biometric security by examining current activity in this market around the world – there are a number of excellent examples to explore.

By interviewing many of the most important stakeholders in this industry, GI presents a balanced analysis of the current market for mobile phone biometric security. This is supported by an analysis of the major technologies being deployed and five-year market forecasts covering all regions of the world.