

FOR IMMEDIATE RELEASE

Contact: Michelle Welch
Telephone: +44 (0) 20 33564886
Mobile: +44 (0) 7901 526883
Email: michelle.welch@goodeintelligence.com

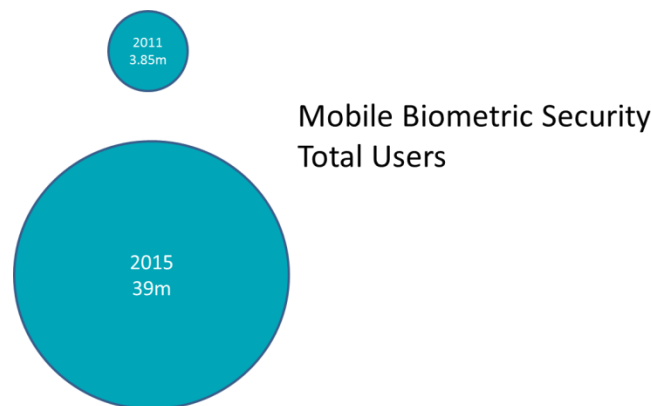
Significant growth expected from mobile biometric security market

New analyst report from Goode Intelligence reveals compelling reasons to utilise the mobile phone for biometric security purposes. Mobile phone biometric security is a versatile third factor to:

- Protect digital assets on the mobile device
- Enhance authentication (as part of multi-modal authentication solutions)
- Protect NFC transactions against fraud

London, United Kingdom – 13 September 2011 – Goode Intelligence (www.goodeintelligence.com), information security research and analysis specialist, has published a new analyst report, *Mobile Phone Biometric Security Analysis and Forecasts 2011-2015*, investigating the market for mobile phone biometric security products and services.

Biometric technology in mobile phones has existed for over ten years but has struggled to establish itself in a suitable use case that results in significant adoption rates. The conditions are now right to create a strong market and Goode Intelligence forecasts that the current global user base of four million users in 2011 is set to grow to 39 million users by 2015.



Source: Copyright © Goode Intelligence 2011

Goode Intelligence predicts that initial growth will come from two technology groups:

1. Embedded mobile biometrics (EMB); including fingerprint sensors embedded by device manufacturers.
2. Third-Factor Authentication; mobile biometrics used in combination with multi-modal authentication solutions, in particular voice-based biometrics.

“There are an estimated 13 million mobile devices around the world that are already benefiting from embedded mobile biometrics in the form of fingerprint sensors” said Alan Goode, author of the report and founder of Goode Intelligence. “A significant number of these are being used in South-East Asia, particularly in Japan where consumers are benefiting from fingerprint-based biometric security to protect NFC payments at the physical point of sale (POS).”

Replicating the Japanese model in other regions in the world

Goode believes that this model could be replicated elsewhere: “2011 is seen as a pivotal year in the adoption of mobile payments using NFC in the rest of the world and there is a strong possibility that the Japanese model of using mobile phone-based biometric security will be duplicated. It may not necessarily replace existing authentication methods, such as chip and pin, as the primary authentication method but could undoubtedly augment it in certain circumstances.”

Embedded mobile biometric (EMB) security becoming mainstream

Goode states in the report that there are indications that more device manufacturers are turning to EMB to enhance security and differentiate their models in an ever-crowded market; “Motorola has been heavily marketing the security benefits of using biometrics (fingerprint sensor) to protect its enterprise-ready Android smartphone, the Atrix, and there are rumours circulating of voice recognition features in the next generation of Apple’s iPhone 5.

“We believe a biometric groundswell is building. The market is currently slow; but pressure is growing. The conditions are ripe for rapid change; for biometrics to move from an ‘interesting concept’ to a ‘must have’ for all smart mobile devices (SMDs).”

The key drivers behind market growth and the adoption of mobile phone biometric security include:

- **Device security protection:** Protecting the device against unauthorised access is the biggest driver for mobile phone biometric security. This includes protection both of apps and the data that resides on the device
- **Mobile Commerce:** The growth of mCommerce and the need to effectively secure the ecosystem on the mobile
- **NFC:** The contactless technology that is reaching tipping point could well be a major driver
- **Convenient alternative to PINs and password:** Swiping a finger on a phone or providing a verbal ‘voiceprint’ can be an easier and far more convenient way to provide authentication than conventional technologies

- **As part of a multi-factor authentication solution:** With the recent attack on RSA, leading to vulnerabilities being exposed in its SecureID token technology, there is a pressing need for strong and agile authentication solutions – mobile phone-based biometric security can be a viable part of this solution
- **Military and law enforcement:** A cost-effective method for capturing biometric data and verifying identity in the field

Further information about the Mobile Phone Biometric Security Report can be found at www.goodeintelligence.com

About Goode Intelligence

Goode Intelligence is a specialist provider of Information Security research and analysis to global technology and telecommunications organisations. For more information about Goode Intelligence please visit www.goodeintelligence.com

For further information contact:

Michelle Welch, Goode Intelligence

Telephone: +44 (0) 20 33564886

Mobile: +44 (0) 7901 526883

Email: michelle.welch@goodeintelligence.com

Issued by:

Goode Intelligence, 26 Dover Street, London, W1S 4LY, UK

Telephone: +44 (0) 20 33564886; **Email:** enquiry@goodeintelligence.com; **Web:** www.goodeintelligence.com