

### TECHNOLOGY

#### INTRODUCTION

This section defines the major technologies that are being adopted to enable the mobile phone to be transformed into an authentication device.

For the end user, there are plenty of options, both in the type of technology adopted and in the number of vendors that are offering their products and services – a healthy sign of a vibrant and growing area of technology.

This section includes interviews with the key vendor stakeholders in this market. GI has interviewed many of the most important players from the key technology vendors within this industry to learn first-hand, their views and insight into the market for mobile phone-based authentication products and services.

The vendor profile section highlights important information about the key technology enablers in this market and includes information on company history, management teams, financial status, strategy and, where available, sales figures.

There are many ways in which a mobile phone can be turned into an authentication device. GI's research has identified these as the key technologies:

- One-Time-Password (OTP) sent as an SMS text message to a mobile phone
- Mobile soft token
- Mobile PKI
- Other (including technologies such as Voice and Mobile TAN)

Before detailing the mobile phone-based authentication technologies it is worth spending some time to understand the current authentication landscape in terms of what is currently being used and what the dominant technologies are.

#### CURRENT DOMINANT AUTHENTICATION TECHNOLOGIES

For the majority of users today, one-factor authentication – something a user knows, e.g. a User-ID and a Password or PIN – is still king. This is especially so in the consumer market where cost and distribution issues mean that the User-ID and Password combination is the easiest, but not the securest, form of authentication around the world.

Even within the enterprise, where the risk is often perceived to be greater – with higher levels of sensitive information to protect – the User-ID and Password still dominates.

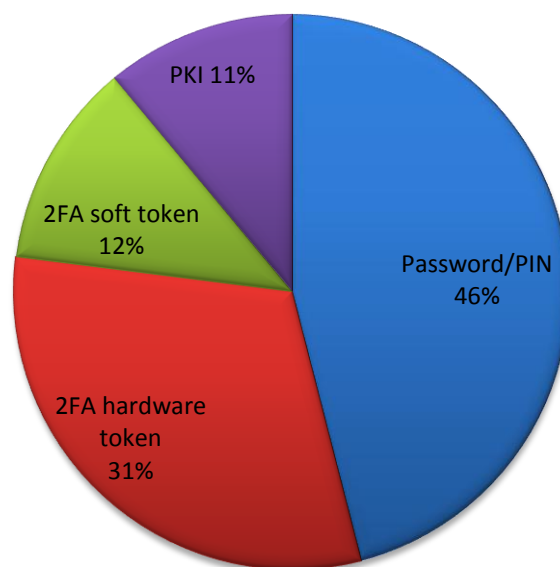
## The Mobile Phone as an Authentication Device 2010-2014

**Local network authentication in the enterprise:** In research carried out by GI in September 2009, 46 percent of enterprise users were still using User-IDs and Passwords (see figure 6 below) to authenticate at a local network level.

For those organisations that have strengthened their authentication solutions, 31 percent have chosen to deploy a 2FA hardware token with a further 11 percent using the soft token equivalent. This is unsurprising as 2FA is prevalent in Finance and the survey elicited its highest response rate from those working in this sector (33 percent of respondents). The remaining 11 percent of organisations have adopted PKI certificate-based authentication as their strong authentication method. PKI certificate-based authentication can be Two-Factor, hardware-based, where the certificate is stored either on a smart card or USB device, or One-Factor, software-based, where the certificate is stored in a secure area of the PC or laptop.

**Figure 6. Enterprise authentication of non-mobile devices onto a local network**

**How do you authenticate local users (non-mobile phones, e.g. PCs and laptops) onto the network?**



*Source: Copyright © Goode Intelligence 2009*

**Remote network authentication in the enterprise:** Mobility is changing the way that we do business. It has become common business practice to allow employees to access enterprise networks remotely, either at home or whilst travelling on business.

GI polled the information security community on how they are currently authenticating remote network users, predominantly over the internet using some sort of VPN technology. Findings show that authenticating authorised users over the Internet is a challenge and organisations still heavily rely on the inherently weak User-ID and Password/PIN combination with 42 percent of those polled using this method to authenticate remote users (See figure 7 below).

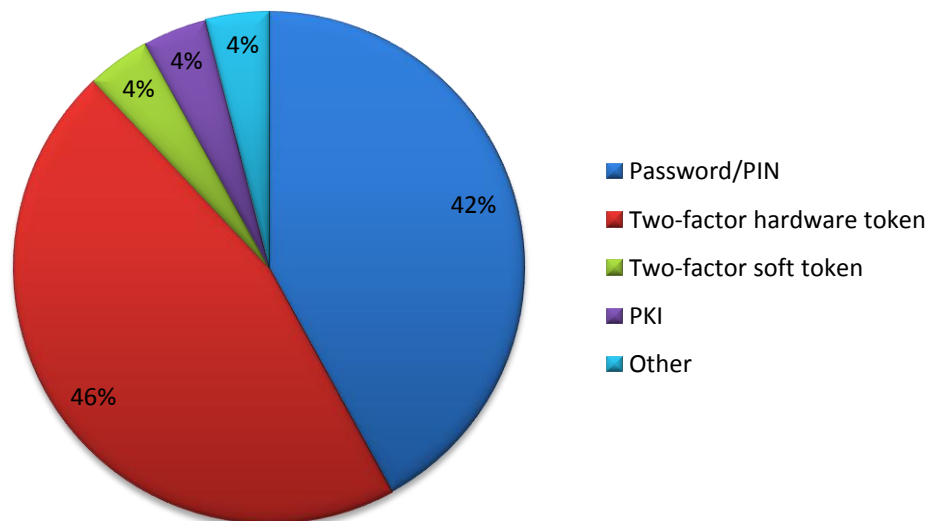
## The Mobile Phone as an Authentication Device 2010-2014

Driven by industry regulation and information security policy, 2FA technology has a stronger presence for remote network access. 46 percent of organisations use a 2FA hardware token to authenticate their remote workforce.

Only four percent use the Soft Token version of the 2FA One Time Password (OTP) solution and a further four percent use PKI certificates. The remaining four percent is made up of other authentication solutions.

### Figure 7. Enterprise authentication of non-mobile devices onto a remote network

How do you authenticate remote users (non-mobile phones, e.g. PCs and laptops) onto the network?



Source: Copyright © Goode Intelligence 2009