GOODE INTELLIGENCE
YOUR PARTNER FOR BUSINESS RESEARCH & ANALYSIS

Putting the Mobile Network Operator at the Heart of Authentication Services with Nok Nok Labs' FIDO Ready™ products

A Goode Intelligence white paper sponsored by Nok Nok Labs

www.goodeintelligence.com

First Edition October 2014

Sponsored by Nok Nok Labs

Published by:
Goode Intelligence

www.goodeintelligence.com
info@goodeintelligence.com

CONTENTS

This white paper from research and consultancy company Goode Intelligence (GI) explores how mobile-based authentication solutions are addressing the needs to conveniently identify consumers. It investigates the role of Mobile Network Operators (MNOs) in modern authentication services and explores how Nok Nok Labs, with their FIDO Ready™ products, are providing the technology to put MNOs at the heart of authentication.

THE NEED FOR INTELLIGENT MOBILE BASED AUTHENTICATION

Mobile and Cloud – legacy authentication is proving inadequate

Two of the inter-connected megatrends of the last few years have been the rise of mobile computing and the delivery of digital services through the Cloud.

The rising use of smart mobile devices (SMD) accessing applications hosted by a variety of service providers for both personal and business purposes has had a profound effect on authentication.

As the smart mobile device becomes the universal smart controller, the way we prove identity on these always connected touchscreen devices becomes critical. Traditional monolithic authentication solutions, both single (largely password) and two-factor (2FA) are proving to be inconvenient, insecure and difficult to scale to services that need to support millions of users on different mobile platforms and devices.

The need to support legacy IT

We also need to ensure that any new authentication solution supports legacy IT infrastructure; an employee accessing enterprise IT through a VPN on a laptop and consumers logging in to a banking website via a desktop computer.

How industry standards and initiatives have facilitated the emergence of intelligent mobile-based authentication

As a result of the combination of these trends a number of agile authentication solutions have been designed and deployed that meet the need of today's service-orientated architecture and protect the privacy of users.

Proprietary mobile-based authentication solutions have been augmented by the development of technology standards, protocols and industry initiatives that focus on a number of inter-dependent technology areas that cover both authentication, and authorization.

Goode Intelligence White Paper

GI's white papers offer analyst insight from research extracted from primary sources including surveys, analyst reports, interviews and conferences.

GI Definitions

SMD: Smart Mobile Device. A term coined by Goode Intelligence to denote a connected mobile device running a mobile Operating System. This includes Smartphones, Phablets and Tablets.

2FA: Two-factor Authentication. Something the user knows and something they own/are (biometrics) or have access to.

VPN: Virtual Private Network creates a private secure network over a public network (Internet).

Organizations that are involved in standardization include the **FIDO Alliance,** The **Organization for the Advancement of Structured Information Standards (OASIS)** and **The OpenID Foundation**.

The FIDO Alliance is an organization that is developing authentication standards and specifications to improve online authentication for both mobile and desktop computing experiences.

FIDO has developed two main specifications, Universal Authentication Factor (UAF), often called the 'Passwordless Experience', and Universal Second Factor (U2F) referred to as the 'Second Factor Experience'.

The **Organization for the Advancement of Structured Information Standards (OASIS)** has been involved in the development of the Security Assertion Markup Language (SAML). SAML is an XML-based open standard data format for exchanging authentication and authorization data between parties and has been around since 2001. SAML enables single sign on (SSO) and has been an important standard in enabling organizations to support SSO both internally and externally with trading partners.

The OpenID Foundation has developed **OpenID and OpenID Connect**, an interoperable authentication protocol based on **OAuth 2.0** authorization specifications.

The OpenID Foundation has also been responsible for OpenID Connect, the third generation of OpenID technology that aims to deliver a more developer friendly authentication protocol. OpenID Connect is at the heart of an industry initiative that is being managed by the mobile industry's body, the **GSMA.**

The GSMA has introduced a program to support the use of mobile devices for authentication purposes. The **GSMA Mobile Connect** initiative aims to provide consumers to securely access a wide array of digital services using their mobile phone for authentication.

Putting the mobile at the heart of authentication and identity provision is a natural choice as the GSMA states that there are over seven billion mobile connections and over 3.5 billion mobile subscribers in the world.[1]

Mobile Connect is an important initiative that is worth investigating in more detail.

The Fast Identity Online (FIDO) Alliance is an organization that has developed authentication standards and specifications to improve online authentication for both mobile and desktop computing experiences.

OpenID Connect: An interoperable authentication protocol based on OAuth 2.0 specifications that lets developers authenticate users across websites and apps without having to own and manage password files.

OAuth: An open protocol to allow secure authorization in a standard method from web, mobile and desktop applications.

SAML: Security Assertion Markup Language is an XML-based open standard data format for exchanging authentication and authorization data between parties.

GSMA: The GSMA Association is an association of mobile operators and related companies.

[1] GSMA Intelligence Global Data, July 2014**: https://gsmaintelligence.com/**

GSMA Mobile Connect – secure authentication for simple mobile online use

GSMA Mobile Connect is an initiative that enables mobile network operators (MNO) to deliver authentication solutions to consumers.

The aim of the initiative is to leverage secure MNO assets such as the network and SIM to allow consumers to authenticate to a variety of connected services and to eliminate the need for passwords.

The MNO provides authentication services on behalf of service providers. A service provider can be a government, a financial services or a healthcare provider that wants a standards-based method of authenticating their mobile-based users.

The GSMA Mobile Connect initiative utilises **OpenID Connect** protocols that supports interoperability across mobile network operators and service providers.

The initiative has developed authentication APIs that are a component of the **GSMA OneAPI Exchange** programme; a programme that focuses on providing consistent access for developers accessing network API services.

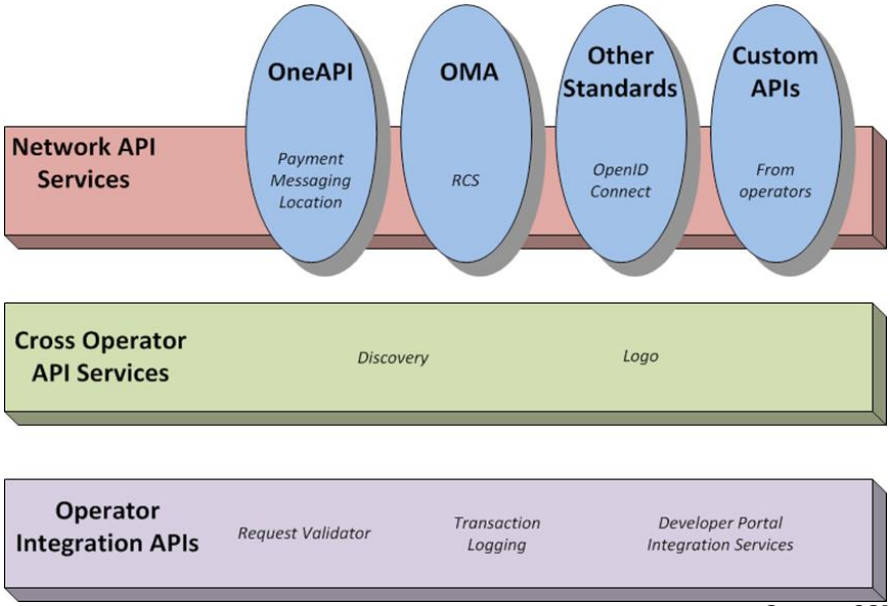
It is an enabling service for MNOs to federate their individual APIs to deliver cross-operator reach.

MNO: Mobile Network Operator.

SIM: Subscriber Identity Module is a chip integrated into mobile devices that stores identity material used by the MNO to authenticate the device onto the mobile network.

API: Application Programming Interface.

Figure 1: GSMA OneAPI Technology



Source: GSMA

Mobile Connect is an important and timely initiative that meets the need for mobile-based identity services. It is built on interoperable standards and leverages the security of the SIM card to offer scalable authentication services that meet the needs of service providers wanting to deliver secure mobile services to their clients and citizens.

The Mobile Connect architecture connects the in-built security of the mobile device with a range of standards-based authentication and identity assurance services. The connection between the mobile authentication client (the first mile of authentication), and network-based authentication and identity assurance services (the second mile of authentication) is vitally important in ensuring security and user privacy.

The Authentication Journey – Linking the first and second miles of authentication

The authentication journey is changing from a simple presentation of a credential that would either result in a "yes you can come in" or a" no do not enter", to one that can involve more miles (steps).

These steps do not have to add complexity and can increase the levels of assurance in the authentication framework being introduced. The choice of what steps to take is dependent on the policy created by the service provider.

The first mile – how FIDO manages mobile-based user authentication

In mobile-based authentication, the first mile involves using a mobile device as an authenticator to enable a user to access an online service or to authorise a financial transaction.

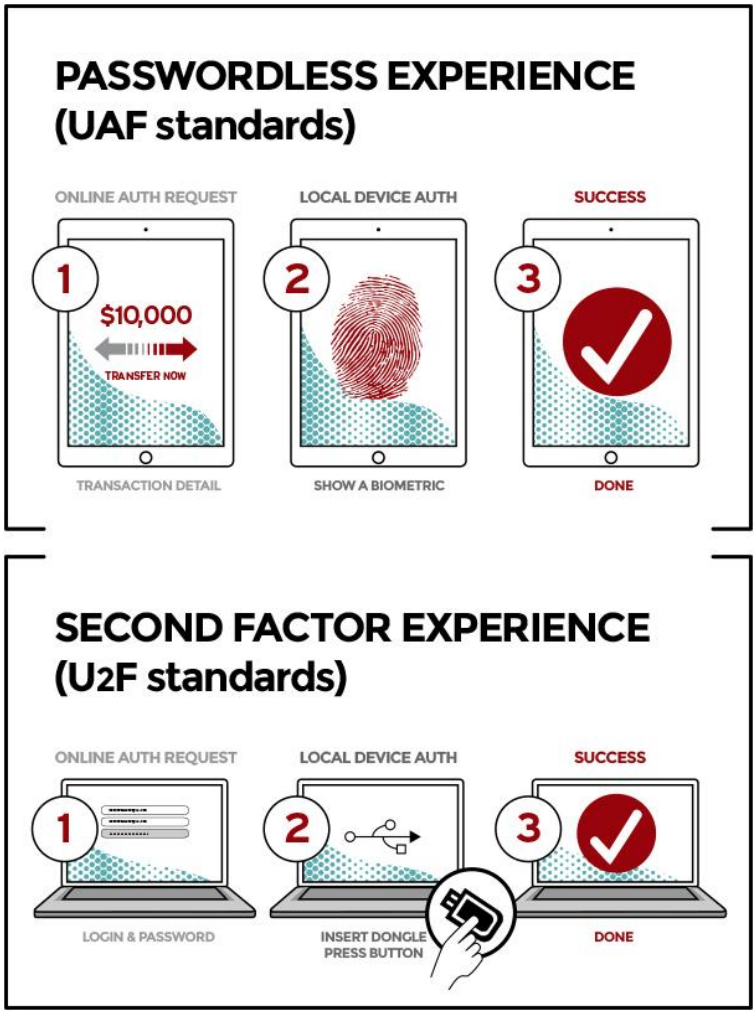
The **FIDO Alliance** is an organization that has developed authentication standards and specifications to improve online authentication for both mobile and desktop computing experiences.

FIDO has developed two main specifications, Universal Authentication Factor (UAF), often called the 'Passwordless Experience' and Universal Second Factor (U2F), referred to as the 'Second Factor Experience' (see figure 2 below).

UAF: The FIDO Universal Authentication Framework allows online services to offer password-less and multi-factor security.

U2F: The FIDO Universal Second Factor protocol supports a second factor for user login.

Figure 2: The FIDO Alliance UAF and U2F Standards



Source: The FIDO Alliance

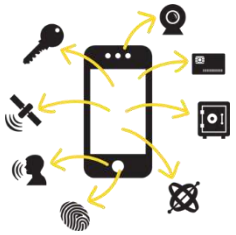
HOW NOK NOK LABS HAS CREATED A FIDO AUTHENTICATION SOLUTION

One authentication vendor that has implemented a solution using the FIDO standards is **Nok Nok Labs (Nok Nok)**. Nok Nok is a member of the FIDO Alliance and was instrumental in creating the first draft of the UAF standards.

Nok Nok has taken both the UAF and U2F standards to create a system that consists of an authentication client installed on the user's device and an authentication server that integrates with a Service *Provider* (SP) application.

Nok Nok Labs has developed the FIDO Ready™ S3 Authentication Suite that is comprised of the following components:

- The Multifactor Authentication Server (MFAS)
- The Multifactor Authentication Client (MFAC) Mobile Edition with support for Android and iOS devices
- The Multifactor Authentication Client (MFAC) Desktop Edition with support for Windows 7 and Windows 8



Service Provider: A Service Provider (SP) is an internet entity that provides a digital service, e.g. an online bank.

MFAS: Nok Nok Labs' Multifactor Authentication Server.

The *MFAC* serves as an UAF endpoint and uses the native capabilities of the device for authentication. The device native capabilities (see figure 3 below) include integrated components such as cameras, microphones, accelerometers, secure elements (*SE*) biometric sensors including fingerprint and GPS sensors. Nok Nok Labs' MFAC's plug-in architecture lets you take advantage of these innovations to authenticate users and can support authentication from both a mobile app or through a browser based on integration via an SDK.

MFAC: Nok Nok Labs' Multifactor Authentication Client for both mobile and desktop.

SE: Secure Element is a tamper-resistant platform (usually a chip) capable of securely storing applications and cryptographic material (keys).

Figure 3: Leveraging the native capabilities of the device for authentication

Source: Nok Nok Labs

ALIPAY AND PAYPAL USE NOK NOK LABS S3 AUTHENTICATION SUITE

The Nok Nok Labs S3 Authentication Suite is being successfully used by two major payment providers, PayPal and Alipay, to provide fingerprint biometric authentication for payments initiated on a range of Samsung devices including the Samsung Galaxy S5 (GS5) smartphone.

The Nok Nok Labs Multifactor Authentication Client (MFAC) is being used on the Galaxy S5 and PayPal has deployed the NNL Multifactor Authentication Server (MFAS) to provide a unified and flexible authentication infrastructure that communicates securely with the NNL client on the Galaxy S5.

Nok Nok powered PayPal payments are currently available in 25 markets, including Australia, Brazil, EU countries including the United Kingdom, Hong Kong, Russia and the United States. PayPal is a major international payment service, available in over 200 markets with 152 million active users and processing 9.3 million payment transactions every day.[2]

China's Alipay overtook PayPal in 2013 to become the largest mobile

[2] Source: PayPal; https://www.paypal-media.com/about

payments platform in the world processing nearly $150 billion in mobile transactions. The Chinese-based payment provider has a reported 300 million registered users, of which 100 million are mobile users.[3]

Both payment providers realise the benefits of moving to a standardised mobile biometric authentication platform to authenticate users for mobile payments. Nok Nok's FIDO authentication technology provides them with a solution that can leverage the integrated fingerprint scanners that are being rapidly deployed to the latest smart mobile devices.

GI Forecasts: By the end of 2015 there will be over 508 million smart mobile devices with fingerprint scanners.[5]

CONNECTING THE FIRST MILE OF AUTHENTICATION TO THE SECOND MILE OF IDENTITY MANAGEMENT

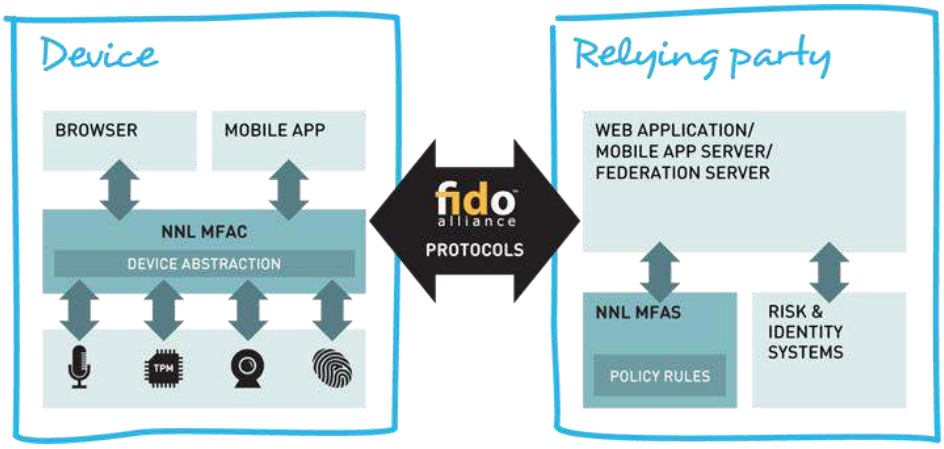
Mobile authentication is not just about what happens on the mobile client; it needs the ability to connect to a wider ecosystem. To meet the demands of today's digital environment a modern authentication solution must support a wide range of devices and provide support for a range of other connected services. Connections to *Identity Federation*, risk management solutions, *threat intelligence* and other associated services are strengthening authentication solutions and making them more business aware.

Identity Federation: The means of linking an identity to multiple distinct identity management services.

Nok Nok Labs' S3 Authentication Suite combines a FIDO mobile client authenticator (NNL MFAC) with a standards-based server (NNL MFAS) that supports connection to third-party services. These complementary third-party services includes Risk Management and Identity Federation solutions (as shown in figure 4).

Threat Intelligence: Evidence-based knowledge about an existing or emerging security threat that can be used to inform decisions about how to deal with that threat.

Figure 4: The Nok Nok Labs S3 Architecture



Source: Nok Nok Labs

[3] Source: Business Insider; http://www.businessinsider.com/alipay-overtakes-paypal-as-the-largest-mobile-payments-platform-in-the-world-2014-2

[5] Mobile and Wearable Biometrics Authentication Market Analysis and Forecasts 2014-2019, Goode Intelligence

An important bridging service for authentication is Identity Federation - the means of linking an identity to multiple distinct identity management services. If you can provide an authentication solution that is standards-based, convenient, secure, and allows the user to connect through to other authorised services without the need to overtly re-authenticate then you have a solution that meets the demands of today's agile mobile computing.

Nok Nok Labs S3 Authentication Suite provides support for federation through connectors in its Multifactor Authentication Server (MFAS). MFAS integrates with federation systems and supports SAML and OpenID-based infrastructure.

GI Forecasts: By 2019 there will be 5.5 billion users of mobile and wearable biometric technology around the world[6]

PARTNERSHIPS WITH IDENTITY FEDERATION PROVIDERS

By partnering with technology providers such as **ForgeRock**, with their Identity Relationship Management (IRM) platform, Nok Nok Labs offers a scalable and interoperable solution for authentication and allows users the flexibility of authenticating once and then having that identity federated to a wide range of connected services.

WHY MNOS ARE A LOGICAL PLACE FOR AUTHENTICATION SERVICES

GSMA Mobile Connect is an initiative that enables Mobile Network Operators (MNO) to deliver authentication solutions to consumers.

The initiative provides them with an opportunity to become a central part of the modern authentication ecosystem and position them at the center of identity management and assurance.

MNOs are logical owners of authentication services in an era where accessing the internet is increasingly being made from mobile devices.

They have long standing relationships with millions of consumers around the world and are considered to be trusted organizations that know how to deliver secure consumer-focused services.

The benefits of MNO-led authentication services include:

- **SIM:** MNOs own and manage a secure hardware chip embedded on mobile devices that can be used to store authentication credentials and cryptographic material
- **Subscriber Data:** The MNO manages a wealth of historical and dynamic subscriber (user) data that can be used as part of an authentication and identity assurance service. As part of a risk-based authentication solution this data can be leveraged to build up a higher level of assurance that a user is genuine and in possession of a mobile device. This includes access to vital location information that is gathered from the cellular network in partnership with GPS location data

[6] Mobile and Wearable Biometric Authentication: Market Analysis and Forecasts 2014-2019

- **Network Security:** As part of its obligations to ensure the integrity and security of both the device and the network, MNOs have designed and built strong security into their cellular and data networks. This designed security can be leveraged as part of a trusted authentication service
- **Regulation:** Most of the world's MNOs are governed by strict telecommunications and data protection regulation that ensure the security and privacy of user data is protected
- **Lost and Stolen Devices:** MNOs have comprehensive policy and processes that support situations when a mobile device is lost or stolen. This is similar to the banking industry's process for managing lost and stolen debit and credit cards. This facility can be used as part of credential lifecycle management to revoke/re-issue authentication credentials

THE BENEFITS OF NOK NOK LABS AS A FIDO-READY™ AUTHENTICATION TECHNOLOGY PARTNER FOR MNOS

MNOs can play an integral role in the delivery of modern mobile-based authentication services and Nok Nok's FIDO-Ready™ authentication technology provides the platform for them to do so.

The benefits of Nok Nok Labs authentication technology for MNOs are:

- First to market with an authentication solution based on FIDO-Ready™ standards
- Chosen by the two largest mobile payment providers, PayPal and Alipay, to provide the technology to enable fingerprint biometric authentication on mobile devices
- Compliments aims and ambitions of GSMA Mobile Connect Programme; can be integrated into Mobile Connect architecture
- Support for both SIM and WiFi-only (SIM-less) smart mobile devices

First to market for FIDO-Ready™ Authentication

The company is the first to market with an authentication solution based on the FIDO-Ready™ standards. The Nok Nok Labs S3 Authentication Suite is the industry's first fully capable authentication suite built from the ground up using FIDO-Ready™ authentication protocols and combines a FIDO-Ready™ mobile client.

Nok Nok Labs S3 integrates with a wide range of FIDO-Ready™ authenticators supporting fingerprint biometrics, voice biometrics, face biometrics, secure elements (SE), trusted platform modules (TPM) and removable tokens.

The Nok Nok Labs S3 Suite comprises of two main components:

- The Nok Nok Labs Multifactor Authentication Client (MFAC)
- The Nok Nok Labs Multifactor Authentication Server (MFAS)

Nok Nok Labs powering fingerprint biometric authentication for Alipay and PayPal

Nok Nok with their FIDO-Ready™ authentication products are already being used in the mobile industry. They have been chosen as the authentication partner for PayPal's mobile payment fingerprint authentication solution found on the latest Samsung smart devices.

Alipay and PayPal are using the NNL S3 Authentication Suite to enable secure mobile payments to be authorised by an integrated *Fingerprint Sensor (FPS)* on both the Galaxy S5 smartphone and the latest Galaxy Tab S Tablet.

FPS: Fingerprint Sensor, usually integrated into a mobile device for biometric authentication purposes.

Figure 5: Using your finger to pay for goods and services on the Samsung S5

Source: PayPal

Nok Nok Labs – A partner for mobile network operator authentication services

The Samsung Mobile Payments (Alipay and PayPal) examples have created a reference model that can be replicated by other organizations; a model where a service provider leverages the built-in capabilities that an OEM has delivered in computer devices (mobile phones, tablets, desktop and laptop computers) and this is then leveraged by a service provider, through a FIDO Server such as Nok Nok's FIDO-Ready™ servers, to enable convenient and agile authentication.

OEM: Original Equipment Manufacturer – the manufacturer of smart mobile devices and computers.

In the Samsung Mobile Payments example, the service provider (PayPal) has deployed their own Nok Nok Multifactor Authentication Server (MFAS).

Other service providers may want to outsource the authentication

server to a trusted third party. MNOs are ideally positioned to be that trusted party and to run NNL FIDO servers as part of a managed service on behalf of service providers.

The GSMA Mobile Connect program shares many of the features of the FIDO Alliance architecture including:

- Putting mobile at the heart of authentication
- Leveraging mobile device secure hardware for storing credential and cryptographic material
- Supporting authentication and identity assurance standards such as SAML and OpenID Connect
- The desire to support Identity Federation to break consumers away from the multiple authentication burden

Support for both SIM and WiFi-only smart mobile devices

There are also scenarios in which FIDO and Nok Nok can enhance operator-led authentication services based on Mobile Connect. The SIM card is at the heart of the Mobile Connect architecture as it offers strong hardware-based security that can be leveraged for authentication purposes. A SIM card will be found in any mobile device that is connecting into the MNO owned cellular network. This means that these devices are a natural fit for any MNO-managed authentication service.

Fast Fact: 9 out of 10 tablets sold in the USA were WiFi only models.

This model does not fit so well for tablet computers and a new range of wearable devices coming to market. Market research informs us that the majority of tablet computers sold will not connect into the MNO owned cellular network and will be WiFi only models. A study from 2012 discovered that nine out of ten tablets sold in the USA were WiFi only models.[4] Goode Intelligence believes that to be successful a modern authentication solution must support devices that do not contain a SIM card. This includes other connected devices including smart TVs, home entertainment controllers and even automobiles.

There are also scenarios where a service provider will not want to deploy a service that resides on a SIM card. They may demand a software-only solution or choose another secure piece of hardware; an OEM integrated Secure Element for instance.

A FIDO-based solution that is closely aligned to the Mobile Connect architecture could offer a comprehensive solution and support devices with and without a SIM card.

[4] Sorry, carriers, 9 out of 10 tablets sold are WiFi, GIGAOM, March 20 2012. Data derived from Chetan Sharma analysis: **http://gigaom.com/2012/03/20/sorry-carriers-9-out-of-10-tablets-sold-are-wi-fi/**

SUMMARY AND CONCLUSIONS

Mobile and cloud computing are two megatrends that are leading to an urgent need to rethink how we authenticate people.

An average person will now have to manage multiple accounts across a wide range of access devices and in the majority of cases have to rely on passwords to authenticate. Passwords are an insecure and inconvenient method of identifying people and there is an urgent need to replace or augment them with secure and convenient solutions.

Fortunately, a combination of activities that include the design and deployment of innovative mobile-based authentication technologies, industry standards / authentication specifications and industry initiatives including GSMA's Mobile Connect are creating a favourable environment for genuine change.

Nok Nok Labs' FIDO Ready™ authentication technology offers service providers the opportunity to deliver standards-based authentication to a large number of digital users and is already being used to provide convenient mobile-based authentication to thousands of Alipay and PayPal mobile payment users around the world.

Goode Intelligence believes it is the ideal platform for Mobile Network Operators to ensure they deliver on the opportunities that the GSMA Mobile Connect program offers them – putting them at the centre of a revolution in authentication services.

For more information on Nok Nok Labs and their authentication solutions for MNOs please visit this **website**.

Nok Nok Labs, Nok Nok and NNL are all registered trademarks of Nok Nok Labs, Inc. FIDO and FIDO-Ready are trademarks of the Fast IDentity (FIDO) Online Alliance.

ABOUT GOODE INTELLIGENCE

Since being founded by Alan Goode in 2007, Goode Intelligence has built up a strong reputation for providing quality research and consultancy services in mobile security, identity and biometrics.

For more information on this or any other research please visit www.goodeintelligence.com.