The next wave.

And why you are the one surfing it

The battle to rid ourselves of the password is in the end game. The long lasting battle has made numerous victims and it will take some more before we have finally defeated the evil password. However the war is in its final stage and there is hope for all those who are struggling daily to gain access to systems or execute transactions by typing in passwords or token/phone generated time codes.

Recap of the war to date

It's fair to say our continuous battle against the passwords was at its peak when the Internet matured. More and more password protected websites and web applications started appearing. In order to improve user convenience "(web)single sign-on" became popular. The downside risk of this approach however was an expanding security gap.
We tried to close the hole with one time password tokens, smartcards, fingerprints scanners, iris camera's and the like, you name it, we tried it.

Only over the last few years we began exploring the possibility of using the (smart)mobile phone as a security token or use "to phone pushed" SMS codes to gain access to systems and applications.
The speed in which these kinds of authentication methods have been adopted by the corporate and consumer market is astonishing.
The moment the key players such as Google, Facebook, Apple, Twitter, LinkedIn etc. realized their weakest link was their data and not the functionality, they attempted to close the door with "two-step" authentication techniques. Consequently flooding the market with a mix of SMS, passphrase (mothers name, favorite color) and/or location based security measures. Offered for free by the way.

What took RSA and Vasco more than 20 years to reach their present market shares with buyable solutions such as SecureID® and Digipass®. The majority of today's internet population only needed 2 years to accept and adopt strong authentication as an access method solution "for free".

So what's the next wave?

The next wave isn't difficult to predict. The starting point being the Apple acquisition of Authentec in the summer of 2012. Setting the example for mobile device manufacturers to embed fingerprint technology into mobile devices. The iPhone 5S will have a fingerprint sensor built in, most likely in the 'Start' button. Samsung and the others will be sure to follow suit.
The mass acceptance of (embedded)biometric fingerprint technology is ready to take off.
In the next 3-18 months the market will be flooded with mobile phones, tablets and phablets that not only have biometric fingerprint readers built-in, but also come with improved sensitivity camera's, NFC and various other sensor technologies as well.

All efforts are to ensure that the mobile device becomes the most trusted piece of equipment ever. The user will have a sophisticated, electronically advanced, wireless, strong authentication device that can outsmart every single existing authentication technology that is available today.

It is man's final attempt to kill the password and……..he shall succeed.

So how will this work?

Biometrics first

First let's make something clear. The Biometric fingerprint technology that will be embedded in the mobile (smart phone) devices, differs from the technology used in Government run ID installations/projects.
Even though the sensors in both scenario's do the same, the output for the electronic passports is a full fingerprint image whereas the output of the fingerprint enrollment for the ICT-world is a so called fingerprint template. This is a mathematical representation of certain parts of the fingerprint. Meaning that every time a fingerprint is scanned the calculated number (sum) has to come close to the one that is stored. Resulting in fewer privacy issues so to speak.

Apple will leverage the technology that Authentec (former UPEK) developed.
Meaning that the fingerprint template will be stored in a secure chip. This chip then handles the enrollment and fingerprint matching. When the verified result is positive, the chip will issue a One-Time Passcode that performs the actual logon or low level authentication.
The huge advantage being that the fingerprint is uniquely stored in the mobile device. The user has control and as it is just a template that is stored on a tamperproof chip, privacy is guaranteed.

The login process is as follows; you place or swipe your finger, a matching is done, if verification is positive, a one-time passcode is issued. Simple, elegant and secure.

The possession of the phone and the fact that biometric verification has taken place; something you have and something you are, is strong authentication in its purest form.

So be on the lookout for the next wave of smartphones. We will love and want them all just because they absolve us of the fact that we don't have to type those annoying passwords anymore.

NFC is more than payment

Nowadays NFC readers or tags are built into smartphones. NFC, Near Field Communication, is a secure contactless protocol that enables two-way communication. It's an enhancement compared to the "old" RFID technology where the chip functionality was static.

The payment industry wants to use this technology to facilitate contactless payments by phone. However not everybody in the industry is very excited by the idea. PayPal for instance do not think NFC is the way forward.
There are numerous other applications suitable for NFC. Imagine programing your NFC enabled television or pay per view just by holding your phone in front of the television, would be nice to have. The other application that is very intriguing is to have secure access to computer networks and websites by leveraging biometric technology and NFC in a mobile device.

It's a killer app, no passwords are needed anymore, not even at the low level. The ability to always logon securely to systems and sites. Making it possible to get rid of the password systems once and for all.

What will change?

Embracing the mobile device as being the personal completely trusted security device/token is a concept that is still disruptive to the current authentication industry.
An industry that now leverages (sms)tokens, cards, card readers, biometric scanners and all kinds of other technological solutions, is on the eve of becoming extinct. Where today they are considered as being high tech top notch technology, the fact remains that they are the dinosaurs of tomorrow.

"Why connect a reader to a desktop or other device when you have an intelligent reader in the palm of your hand? Why am I forced to enter codes or user-ids when my phone can say it for me?"
All these questions and more you, as a user, will throw at IT departments or ask your bank or demand of other corporations and institutions that want to deal or do (financial)business transactions with you.
They will be swift to adopt your demands and turn them into useable IT solutions in order to save costs and increase security, but above all to make the user happy. He started the wave by bringing his own device and now continues by bringing his own electronic identity. What more direction can you want as a business?

The weakest link

The vendors of operating systems will have to switch to SAML like protocols on the low-level. The old Microsoft adagio; requiring users to have user ID and password/certificate on the entry-level is an old-fashioned concept, soon to be outdated. It is simply to vulnerable and easy to crack.
Apple on the other hand has chosen to centrally store usernames and passwords of the user in iCloud, thus creating a Single-Sign-On like functionality. But in my honest opinion that option can raise severe security issues too. For the sake of argument, let's assume that Apple's decision to launch an iCloud Keychain is just a first step in an evolutionary phase to liberate the user of passwords.
It is becoming clear however that the software vendors might turn out to be the weakest link in the password battlefield. Because of their structure, their speed of innovation is disappointing and their architectural decisions are sometimes questionable and under par.

With smart innovative solutions developed by startups, that with thanks to the current social networks are quickly adopted by the general public, the power of the masses might strengthen the vendors weaknesses. Encouraging them to incorporate products like Authasas as part of the solution that enables vendors to join the wave.

It's the last hurdle to take on the road to finally having secure and user controlled networks.

Bio on mr. van der Drift

Mr. van der Drift founded Authasas in 2009. Mr. van der Drift has been a leader in the ICT industry since 1984, concentrating his efforts on improving strong authentication methods since 1997. As an entrepreneur, Mr. van der Drift's leadership has resulted in the foundation of several companies with their core business being to expand and further develop the biometric and smartcard industry in Europe, the USA, and Asia.

Mr. van der Drift is a recognized leader, visionary and public advocate for the continued innovation and evolution of strong authentication technologies. As a public representative of the industry, you can often find Mr. van der Drift participating at conferences, in the media and open forums.