BioConnect

The Identity Division of EnterTech Systems

A white paper from BioConnect

THE FUTURE OF "BRING YOUR OWN IDENTITY" IN IDENTITY RELATIONSHIP MANAGEMENT

By Robert Douglas - January 2015

BioConnect
The Identity Division of EnterTech Systems

TABLE OF CONTENTS

BioConnect
The Identity Division of EnterTech Systems

THE EVOLUTION OF IDENTITY METHODS

Access control solutions have certainly evolved over time, but no matter how advanced, keys, PINs, cards (Prox, EM, etc.), fobs and smart cards (Mifare, iCLASS, etc.) all have one thing in common: they are approximations of identity. They provide users with an identity that can be used to access secure areas, but there is nothing in their design that can stop users from borrowing, forgetting, losing, or even stealing them. And that is their inherent weakness. Biometrics solves that problem very simply; by eliminating non-secure approximation, it forces users to use their own identities to gain access and boosts security and accuracy dramatically.

The tragic events of 9/11 ushered in a new era in identity management; to combat terrorism, the US government invested billions into true identity technologies. This spawned a biometric industry that saw technology companies with a heavy emphasis on technical engineering expertise enter the government space.

By 2007, most of these biometric technology companies had either been acquired or gone out of business, with tremendous consolidation occurring as everyone tried to build out identity platforms. By this time, the federal government was ready to adopt those identity platforms, but most other large-scale operational organizations such as enterprises, healthcare, educational institutions and state/local government agencies were not. They continued to use traditional access control systems such as cards and smart cards, and did little with biometric access technology beyond high-security entryways. Typical deployment at the time was biometric readers on high-security doors and card readers everywhere else.

MOVING FORWARD, ONE STEP AT A TIME

While there was still low adoption of biometric technology by 2007, you could see that change was on the horizon. With improving technologies and increasing acceptance, biometrics was gaining traction. "Big brother" oversight and privacy concerns became less of an issue in light of user convenience and stronger security, and the need to see who was at the door trying to get in.

TODAY'S CHALLENGES FOR IDENTITY ADOPTION

Until recently, biometrics was still seen as too expensive and too complex to implement, so use remains limited. This perception persists even with some critical infrastructure facilities such as data centers, control rooms and utility sub stations found in communications, utilities, hydro and gas industries. Here's what one such facility said in a recent interview, a Data Center Operations Manager with a data center co-location provider:

''We're about to replace our access control system and so far we have disregarded biometrics as too expensive.''

The four main obstacles preventing mainstream adoption are:

1. Complexity. Biometrics is perceived as too complicated to install and use.
2. Expense. Biometric readers cost significantly more than basic card readers.
3. Difficulty onboarding users.
4. Significant lack of education.

Obstacle #1: Biometrics is too complicated
Each biometric technology company has their own biometric administration system that is separate from the access control manufacturer's software system; to use biometrics, an administrator must manage two different systems, which adds complexity.

Globally, access control systems providers have their research and development resources focused on building their core security functionality, leaving integration to biometric devices a lower priority. Of the top 30 global access control manufacturers, very few have integrated their systems into biometric devices since 2000. And even those who did initially integrate haven't been able to keep up with the quickly changing technology; almost none have stayed current.

As a result, as new biometric technologies entered the market, there were no certified release-level integrations between the systems and readers, and access control manufacturers and end users were unable to take advantage of the latest advances.

Obstacle #2: Biometric readers are too expensive
Due to high initial development costs and initially lower volume sales, biometric technology companies

tried to recoup their investments with aggressively high price points and premium positioning in the marketplace. The price gap between biometric readers vs card readers left many to opt for card readers.

Obstacle #3: Difficulty onboarding users

There have been no diagnostic tools to measure the quality of initial user enrollment, help troubleshoot issues, or tune performance. In essence, installers for system integration firms have been flying blind. Plus, most deployments have taken a "card plus biometrics" approach rather than just using biometrics on its own. This piecemeal solution, commonly referred to as a 1:1 match, means a user has to use a card and a finger to verify their identity.

So why would you move to biometrics and still use cards? It's an approach that was initially necessary because of technology limitations; on-site, local reader matching capability was constrained to the hardware capacity in a specific device. However, these days, 1:1 matching is no longer required in many access control applications. Server matching would allow 50,000 to 500,000 users to have identity verification at any given time throughout a connected biometric system.

Obstacle #4: Lack of education

A significant lack of training for the security integration community means they simply don't have the knowledge they need to ensure the successful installation, provisioning and go-live of biometric systems. The result? Disappointing deployments and a lack of profitability for systems integration firms.

Overcoming barriers

Listening to the needs of the security community including access control manufacturers, systems

integrators, installers and end user enterprises is the key to getting past these barriers. BioConnect is a great example of just that. The technology allows for biometric readers and other devices and applications to be easily integrated with access control systems. By simplifying installation, deployment, enrollment and management of biometrics with an access control system, costs and complexity are drastically reduced while user onboarding and system management become much easier.

Training and biometric certification programs are another way to foster biometric uptake. Biometric technology companies must take responsibility for ensuring people in the security community have the technical knowledge and capabilities to install their products easily in the field. If systems integrators, installers and enterprises lack the knowledge to execute, then they will keep choosing card readers or other technologies like PINs that are only approximations of a person's identity, leaving everyone vulnerable to unauthorized identity sharing or theft. BioConnect has taken on this challenge with a monthly biometric certification program.

BioConnect

The Identity Division of EnterTech Systems

THE ROAD TO 2020 – EXPECT MONUMENTAL CONSUMER UPTAKE

In a fascinating twist, today the #1 biometrics company isn't even in the biometrics industry. With its launch of the iPhone 5s in the fall of 2013, Apple introduced the watershed technology that will bring about mainstream adoption of biometric access control.

"Apple has shown the market how to deploy biometrics into consumer electronic devices with its Touch ID fingerprint solution on the Apple 5s," said Alan Goode, founder of Goode Intelligence. "Apple's flagship smartphone has proved a very popular device with consumers, outselling the less expensive iPhone 5c that ships without Touch ID."[1]

By 2015 – The rise of smartphones and wearable technology

Goode Intelligence forecasts that by the end of 2015 there will be 619 million people using biometrics on mobile devices.[2] And according to Gartner, by 2016, biometric sensors will be integrated into 40% of smartphones, with fingerprint scanning as the main biometric feature due to the technology's intuitive and unobtrusive usage.[3] This will change societal acceptance of biometrics dramatically, making the technology ubiquitous quite quickly.

[1] Author Adam Vrankulj, February 4, 2014 Biometricupdate.com article: http://www.biometricupdate.com/201402/619-million-people-using-biometrics-on-mobile-devices-by-the-end-of-2015-goode

[2] Author Adam Vrankulj, February 4, 2014 Biometricupdate.com article: http://www.biometricupdate.com/201402/619-million-people-using-biometrics-on-mobile-devices-by-the-end-of-2015-goode

[3] Author Stephen Mayhew, December 11, 2014 Biometricupdat.com article: http://www.biometricupdate.com/201412/30-of-wearables-will-be-unobtrusive-to-the-eye-by-2017-gartner

Other forecasters point to the global use of biometrics as a verification method that will move quickly from millions to trillions of transactions. Additionally, there are early signs of biometrics being used to conduct financial transactions, at border crossings, and for access to buildings, schools and homes. We are at the dawn of a new wave of "biometric everything."

New wearable technologies, commonly referred to as "wearable IDs," are emerging based on true identity. You can now get smart digital bracelets that monitor your heart rate, eye verification for your phone, and even clothing with biometric technology incorporated into the fabric. And one day, we will even be able to have microcapsules placed under our skin to emanate an identity signal, giving us streamlined access to everything we need. And the future promises tremendous strides that will take us far beyond today's biometric solutions. More technologies will emerge far beyond finger, face, iris and vein recognition, changing the landscape dramatically.

Gartner believes wearables will feature biometrics as coupling devices to smartphones, but will mostly be used as a means to collect biometric data to be transmitted to smartphones where the majority of intelligence and authentication will occur.[4]

Besides Apple, another example of a market leader adopting biometrics is Google. As speculated in a report by Quartz, the next version of Google Glass could enable wearers to access websites by using biometric data, scanning their fingerprints or eyes instead of entering a password.[5]

[4] Author Stephen Mayhew, December 11, 2014 Biometricupdat.com article: http://www.biometricupdate.com/201412/30-of-wearables-will-be-unobtrusive-to-the-eye-by-2017-gartner

[5] Author Stephen Mayhew, December 5, 2014 Biometricupdate.com article: http://www.biometricupdate.com/201412/google-wants-biometric-authentication-over-passwords-for-glass

BioConnect

THE PATH TO ADOPTION MAY NOT BE SO EASY

With those rosy market trend predictions, everyone will be adopting the technology. Or will they? The industry faces a number of challenges, not the least of which is marrying biometrics to existing systems, which represent huge investments for their users. How will companies incorporate all these different biometric technologies into their access control systems? And how will they work with access control systems that communicate through cards and smartcards, and simply don't understand the language of biometrics? Fiscally-conscious companies won't be keen to scrap their investments to start from scratch.

To achieve those adoption forecasts, the industry must deliver value – and solutions that ensure fast, easy deployment. We need technology that can control and manage all devices, manages users' true identities, and provide simple single sign-on for all devices and applications. BioConnect is one such technology. It's taking the lead by becoming the central identity management platform that facilitates communication between biometric technologies, access control systems, card readers, mobile devices, ID wearable devices, enterprise applications and more. BioConnect Enterprise Server (BES) is the platform enabling a "Bring Your Own Identity" future.

By 2020 – A world of ''Bring Your Own Identity''

By 2020, we will be in a world of "Bring Your Own Identity" (BYOI). A decade ago, "Bring Your Own Desktop" (BYOD) was an emerging trend in the business world. Where enterprises once provided standard desktop technology for all employees, BYOD allows employees and third parties to come to the office with their own technology and work seamlessly and securely. Another example of the influence of consumer technology on the enterprise was the adoption of personal mobile device usage, including smartphones and tablets. These personal devices made its way into the enterprise by the consumer and companies had to figure out how to securely integrate them into the enterprise communication platform.

A similar trend is on its way for social applications and biometrics. One example is Facebook at Work, the much-rumored business version of the consumer product. Designed as a business tool, it's a social application that will allow employees to engage inside the enterprise, connect with other people in their professional network, and collaborate on work projects.[6] And, essentially, bring your own work tools to the (real or virtual) office. This is just one of the many emerging social applications for the enterprise and it could be hitting the market soon.

The same is true for biometrics. With so many biometric choices and biometric ID wearables on the horizon, we can foresee a day in the near future where employees will use their own personal biometrics to gain access to company property, both physical and virtual. Like the desire to use your own laptop or mobile device at work, personal biometrics give individuals control over the biometric, allowing them greater privacy and convenient one-size-fits-all use.

We believe society will respond positively to this trend, and companies will need to establish concrete plans to incorporate it into their operations. BioConnect Enterprise Server is an enabling platform that enables personal biometric identification into the secure enterprise environment.

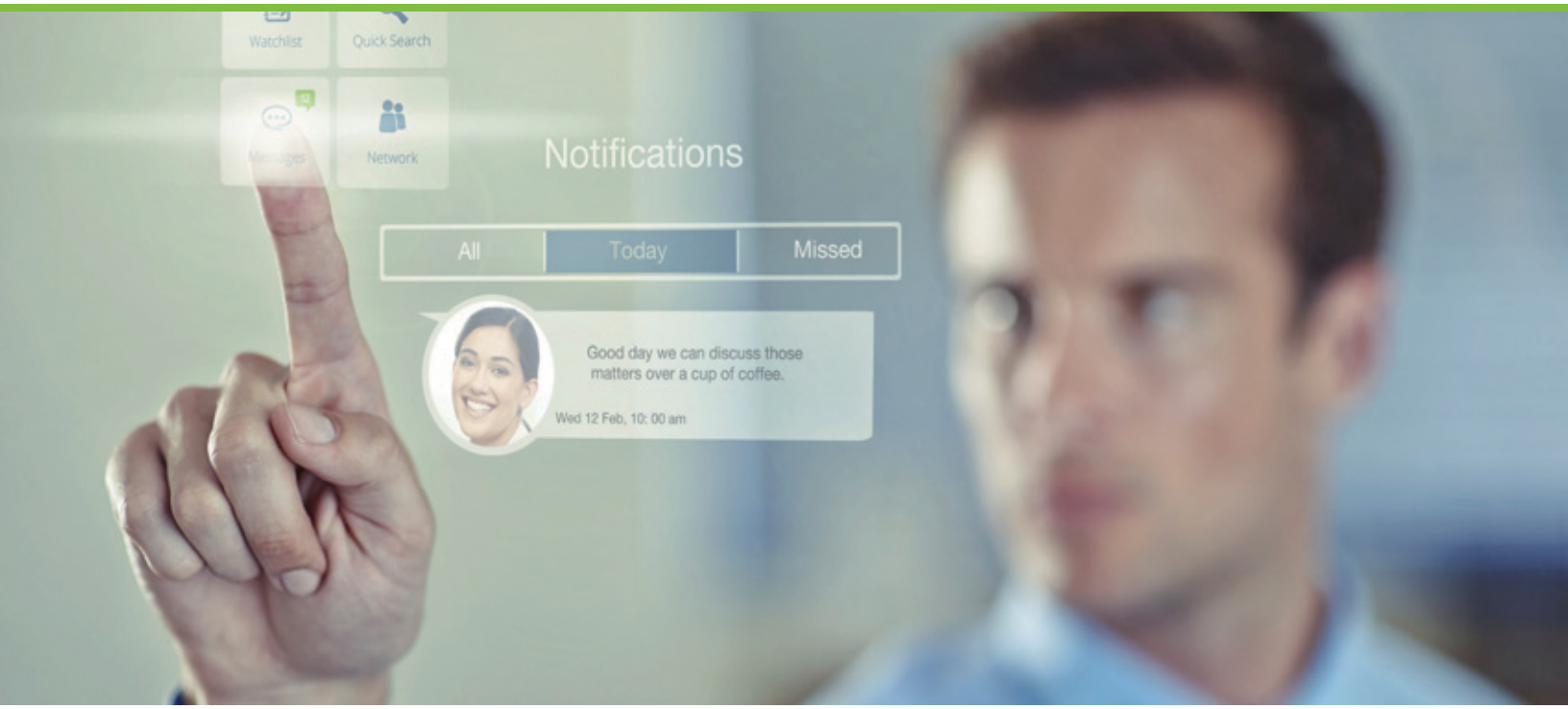
''The Identity of Things (IoT) is forcing an inflection point in the industry that manages assets and user identities. It will generate a lively debate around the Identity of Things and ultimately will result in an updated view of identity management. Perhaps we will even see a day when the Identity of Things will evolve into a form of identity relationship management. The future is full of possibilities.''[7]

[6] Author Issie Lapowsky, October 17, 2014 Wired article: http://www.wired.com/2014/11/facebook-at-work/

[7] Earl Perkins, Research VP, Gartner, August 4, 2015 Blog: http://blogs.gartner.com/earl-perkins/2014/08/04/the-identity-of-things-for-the-internet-of-things/#comments

BioConnect

The Identity Division of EnterTech Systems



WHERE TO NEXT? IDENTITY RELATIONSHIP MANAGEMENT

Gartner Research uses the term Identity Relationship Management (IRM) to describe the plan to incorporate a wide array of identities into your corporate strategy for both logical and physical access.

Momentum is gathering behind IRM. Another proponent of IRM is Kantara Initiative, who accelerates identity services markets by developing innovations and programs to support trusted on-line transactions. With a membership roster that includes international communities, industry, research and education, and government stakeholders – they too will help drive adoption of IRM. Here is Kantara's perspective on the future:

"Identity and Access Management (IAM) services were traditionally built for a company's internal use, to assist with manual on and off boarding, and establishing access privileges to company data and systems behind the firewall. Today a company must implement a dynamic IAM solution that serves employees, customers, partners and devices, regardless of location. This is the evolution of IAM to IRM: Identity Relationship Management." [8]

[8] December 2014, Kantara Initiative website: https://kantarainitiative.org/irmpillars/

CONCLUSION: IRM WITH BYOI AT THE CORE

As new technologies enter the market, BioConnect's Enterprise Server offers an identity management platform to build on. By 2020, "Bring Your Own Identity" (BYOI) will be in the workplace. This new IRM+BYOI paradigm will incorporate an array of identities into your corporate strategy for both logical and physical access. Our vision is IRM with BioConnect at its core, eliminating all barriers to secure access to devices and applications, and creating a seamless, interconnected, highly productive workplace.

Where do we go from here?

If you are the CSO or CIO of your company, think about using an identity platform that gives you the flexibility to incorporate different biometric modalities, ID smartphones and ID wearables into your access control system. Move away from point solutions where one biometric is only connected to one access control system and work towards an identity architecture that can accommodate flexibility – both for BYOI and for leveraging multiple access control systems over time.

If you are an access control manufacturer, engage with an identity platform provider that will serve all the biometric identity types in your current system – and will be able to accommodate your future technology roadmap.

About Robert Douglas

Robert Douglas is the founder and CEO of ENTERTECH SYSTEMS. He was formerly President and CEO of Bioscrypt Inc from 2003 to 2009 (BYT. TO), which was successfully sold to L-1 Identity Solutions (NYSE:ID) in 2008. Over the last twelve years, Robert has been providing global market leadership in the biometric physical access control market. Prior to that, Robert was President of Psion Teklogix Americas, where he led a $140 million corporate turnaround and growth plan in the wireless handheld market.

He has extensive experience in emerging segments of the IT industry, including Identity Management, Biometric Access Control, Enterprise Hardware, ERP, CRM and wireless solutions in a wide range of private and public industries. He has helped build market-leading companies including Pivotal Corporation, Siebel Systems, Oracle Corporation and IBM.

Robert holds a Bachelor of Business Administration degree from McMaster University and completed the Queen's University Executive Program. He is a past non-executive board member of MKS Inc, Bioscrypt Inc. and is currently on the boards of Survalent Technologies, Actual iD and ENTERTECH SYSTEMS.

About BioConnect

BioConnect is the identity division of ENTERTECH SYSTEMS, purpose-built to make biometrics for IP access control systems for mainstream adoption. Our systems approach removes three main obstacles to mainstream adoption: cost, complexity and on-boarding users. Our highly responsive, results-driven technical services team works with our certified partner network to ensure complete customer satisfaction.

suprema partnered with ENTERTECH SYSTEMS

ENTERTECH SYSTEMS is Suprema's official operating partner in the United States, Canada, United Kingdom, Ireland and Puerto Rico. The company offers Suprema's family of #1-rated biometric devices (finger, face, card and PIN), next generation IP access control system, biometric algorithm and SDK, and software products.

www.bioconnect.com | info@bioconnect.com