BIOMETRIC SUMMIT NEW YORK 2019

BIOMETRIC SUMMIT NEW YORK 2019

Hosted by
rise new york
Created by
BARCLAYS

GOLD SPONSORS

iproov zwipe

SILVER SPONSORS

AWARE PRECiSE

acuant B-Secur Connecting Your Heart BehavioSec nok nok ID R&D IRIS ID typingdna

Thursday 4 APRIL 2019

MEDIA PARTNER
BIOMETRIC UPDATE.COM

STRATEGIC PARTNER
IBIA International Biometrics+Identity Association

BIOMETRIC SUMMIT NEW YORK 2019

Alan Goode

CEO and Chief Analyst,Goode Intelligence

A very warm welcome to the second Goode Intelligence Biometric Summit. Building on last summer's success in London, I'm delighted to bring this event to the USA in New York City.

Biometrics continues to be one of the hottest technology areas with increasing investment activity bringing more technology providers to a growing market. Financial services, payments, transport and governments continue to be at the vanguard of adoption but other vertical sectors are increasingly turning to biometrics to support a range of use cases – some of which are breaking out of security and identity applications. Emotion and wellbeing detection are two areas that biometric technology enables, allowing developers and service providers to leverage a single biometric sensor or application for multiple uses.

So what's in store today? The summit starts with a keynote speech on "Biometrics, Creepy or Convenient?" We often talk about the balance between convenience and security but what about the balance between convenience and creepiness? When does the balance tip to a technology being a little too creepy? This is an incredibly important subject as it directly affects user adoption and government regulation. It is both an ethical and a trust debate.

These themes of ethics and trust are explored further in the two *Innovation* panels. We have seven companies taking part in the *Showcasing Innovation in Biometrics* sessions representing behavioral biometrics, biometric authentication, heart (ECG) biometrics, identity and document verification, iris biometrics and voice biometrics.

The morning *Innovation* session brings together B-Secur, ID R&D, Iris ID and TypingDNA. B-Secur develops heartrate (ECG) biometric algorithms that are destined for use in a wide range of solutions from auto to supporting first-responders in the field. TypingDNA has been part of the Techstars accelerator program here in New York and provides behavioral biometric technology. ID R&D is a science-driven authentication vendor that focuses on biometrics for mobile login and conversational interface developing facial liveness detection in combination with behavioral and voice biometrics. Since 1997, Iris ID has been a key developer and driver of the commercialisation of iris recognition technology with its product, IrisAccess, now in its sixth generation, and is considered to be the world's most deployed iris recognition platform.

Our afternoon *Innovation* session promises to be the perfect way to end the day with presentations from three identity and biometric vendors: Acuant, BehavioSec and the award-winning Nok Nok Labs. Biometrics is being leveraged to support digital onboarding while complying with anti-money laundering (AML) and know-your-customer (KYC) regulations. Acuant is one of the leading companies in supplying identity and document verification technologies. BehavioSec is a pioneer in behavioral biometrics working with DARPA in its continuous authentication programs and we are fortunate to have their CEO, Neil Costigan joining us. Biometrics for user authentication has been one of the great success stories for this technology and Nok Nok Labs, a founding member of the FIDO Alliance, has millions of consumers globally using biometrics on mobile devices to eliminate passwords and reduce friction. Their S3 Authentication Suite recently won the 2019 GSMA Global Mobile Award (GLOMO) for mobile security and authentication.

Gold sponsors, iProov and Zwipe will be on hand to demonstrate the opportunities of biometric technology for financial services. Biometric payments are on a tremendous growth path with adoption across both traditional and new digital payment channels. Today, contactless payment cards are driving cashless transactions at physical locations, reducing the friction of the PIN or signature but have a low transaction limit (approximately $40). The introduction of fingerprint sensors on payment cards has the potential of allowing higher value transactions at physical locations without the inconvenience of a PIN or signature. Zwipe is a Norwegian technology vendor that is paving the way for biometric payment cards and is working with all parts of the payment infrastructure including Mastercard to bring this technology to market. iProov's patented facial recognition technology was awarded a contract with the US Department of Homeland Security in 2018 and has also seen success in financial services. On the subject of the Creepy or Convenient debate iProov's CEO, Andrew Bud, states that "done well, biometrics are neither creepy nor convenient. They are world-changing – for the better, of course. Trust will become the most precious asset in the online economy, and biometrics can be the only non-shareable, non-repudiable, non-destructible way to assert trust. But only if they are done well – usable by the widest range of the population, and carefully implemented to assure genuine presence." This certainly resonates with me and I encourage you to join Andrew for his Birds of a Feather session during lunch.

Aware and Precise Biometrics join us as Silver sponsors and bring many years of biometric experience between them. Aware's Dave Benini believes that "biometrics for authentication improves security and convenience and this shouldn't be seen as creepy or invasive". Dave will be on-hand to provide us with his views on spoof detection for mobile biometric authentication – an increasingly important topic for biometrics. If you have a fingerprint sensor on your Android smartphone it is very likely you are using software provided by Precise. Building on its success in the smartphone fingerprint market, the company has utilized its expertise in biometrics to develop a new platform – YOUNiQ – for the verification of digital identity. Precise's CEO, Stefan Persson, will share more about making everyday life easier and more secure in his session How biometrics will transform digital identity authentication.

I hope you enjoy this summit and look forward to meeting and talking with you throughout the day. And, I hope you'll also join us in London for the third Biometric Summit on 20th November.

Alan

AGENDA

09:15 Registration

09:35 Auditorium: Opening welcome from the Chair and Rise

09:50 Auditorium: Keynote Address: Alan Goode, CEO and Chief Analyst, Goode Intelligence

Biometrics – Creepy or Convenient?

10:20 Auditorium: *How biometrics will transform digital identity authentication*

Stefan K Persson, CEO, Precise Biometrics

10:45 **Break – refreshment area**

11:05 Auditorium: *Showcasing Innovation in Biometrics – Part I*

Presentations by B-Secur, ID R&D, Iris ID and TypingDNA, followed by a moderated panel.

12:15 Auditorium: *Genuine Presence Assurance - securing banks and customers*

Andrew Bud, Founder & CEO, iProov

12:50 – 13:40 **Lunch – refreshment area**

13:00 – 13:30 Auditorium: *Birds of a Feather lunch - led by iProov*

Join Andrew Bud with your lunch to continue the conversation around Genuine Presence Assurance

13:40 Auditorium: *How biometric payment cards and biometric enabled wearable devices will make contactless payment even more prevalent*

André Løvestam, CEO, ZWIPE

14:20 Auditorium: *Biometric Authentication - Rethinking the Blink: an update on Spoof Detection for Mobile Biometric Authentication*

David Benini, VP Marketing and Product, Aware

14:50 Auditorium: *Showcasing Innovation in Biometrics – Part II*

Presentations by Acuant, BehavioSec and Nok Nok Labs, followed by a moderated panel.

15:50 Auditorium: *Closing remarks from the Chair*

16:00 Close

SPEAKERS

David Benini,

VP Marketing and Product, Aware

David Benini is Vice President of Marketing & Product at Aware, Inc., where his responsibilities include driving marketing and new product development efforts towards growth of Aware's biometrics software and solutions business. Dave's current areas of focus are Aware's Knomi™ mobile authentication framework, its AwareABIS™ biometric identification platform, and its Indigo™ biometrics-as-a-service offering.

Andrew Bud,

Founder and CEO, iProov

Andrew Bud is founder and CEO of iProov, the world's leading provider of Genuine Presence Assurance for online face authentication and ID verification. He has led the prize-winning London-based business since 2013, and customers for its patented technology now include the US Department of Homeland Security, UK Home Office and ING. Previously, he was the founder, CEO and then Executive Chairman of mBlox Inc., which grew to become the world's largest provider of enterprise-to-consumer SMS services and payments, processing six billion transactions a year when it was sold in 2016.

His earlier experience includes the role of Marketing Director of Europe's largest Cisco distributor, the founding CTO of what is now Vodafone Italia, and the founder of Europe's first wireless LAN business. He has a degree in Engineering from the University of Cambridge.

Ben Carter,

CCO, B-Secur

Ben's Experience spans a number of local and global leadership roles in major technology players including Microsoft, Nokia, Pace and Sony.

Specialising in the mobile industry, with experience across global and European operator, retail and distribution channels, Ben manages B-Secur's commercial strategy and GTM, building strong customer relationships.

Dr. Neil Costigan,

CEO, BehavioSec

As CEO of BehavioSec (www.behaviosec.com), Neil Costigan leads the company's work delivering innovative behavioral biometric technology protecting consumer transactions, payments and financial firms from fraud and theft. He has more than 25 years' of entrepreneurial and technical leadership experience in venture-backed startups, and global technology corporations spanning the U.S., and EU.

A cryptographer by training, his career expanded to include software development, executive leadership and entrepreneurship. He holds an extensive portfolio of patents and serves as Principal Investigator for BehavioSec's U.S. DOD DARPA projects. Prior to BehavioSec, Neil was VP for R&D at Smart Card manufacturer Gemplus (now Gemalto) and Co-founder/CTO at PKI specialists Celo Communications (Celo).

Neil holds a PhD (2009) for his thesis on Elliptic Curve Cryptography on Modern Processor Architectures and has developed a number of commercial security applications. He frequently presents on innovation, cryptography and network security.

Alan Goode,

CEO and Chief Analyst, Goode Intelligence

Alan Goode is the CEO, Chief Analyst and Founder of Goode Intelligence, a world-leading identity and biometrics research and consulting organisation founded in 2007 and based in London. With 13 years of research and analysis experience and 17 years of senior management and technology consultancy including strategy and deployment, Alan is an expert in biometrics, authentication/identity, fraud management and cyber security. His previous roles include Head of Information Security at T-Mobile UK, Security Practice Manager at Atos Origin, Head of Digital Security at De La Rue Identity Systems (including biometric passports) and Security Analyst for Citibank (Payments).

Alexey Khitrov,

CEO and Co-founder, ID R&D

Alexey Khitrov is the CEO and Co-founder of ID R&D – a science-driven authentication vendor that focuses on biometrics for mobile login and conversational interface. Before co-founding ID R&D, Alexey held key executive positions with various biometric companies and pioneered new products and award-winning deployments with government institutions and top US banks, such as the Government of Mexico and Wells Fargo. He has over 10 years of experience in the biometrics space, mostly in executive positions, and is a subject-matter expert in behavioral, voice, and facial recognition. Through Alexey's leadership, the ID R&D team has won numerous awards and recognitions, including being selected as a Top-10 AI start-up in America by Microsoft, Top Pick at Tech Crunch's Disrupt, and many others.

André Løvestam,

CEO, Zwipe

Leading Zwipe on its mission to make convenience secure, André Løvestam joined Zwipe as CEO in March 2018 and has led the company through a milestone year, including a successful MUSD 14 fund raising and public listing on the Oslo Stock Exchange, Merkur Market in January 2019. Prior to Zwipe his career features several chief executive officer and senior executive positions at prominent and publicly listed Nordic ICT and FMCG companies, including companies like Orkla, Telecomputing and Tomra.

André holds a Bachelor of Science (B.Sc.) (Hons) from the University of ManchesterInstitute of Science and Technology.

Dr. Rolf Lindemann,

Senior Director Products & Technology, Nok Nok Labs

Rolf Lindemann brings more than 15 years of experience in product management, R&D and operations from the IT security industry. He works for Nok Nok Labs, Inc. as Senior Director Products & Technology. Prior to Nok Nok Labs Rolf Lindemann worked as Senior Director Product Management in the user authentication group at Symantec where he was responsible for research and product strategy on device authentication in smart grids and mobile networks. Before Symantec's acquisition of TC TrustCenter, he was Executive Director Product Strategy at TC TrustCenter GmbH. Earlier, Dr. Lindemann headed up the Betrusted research team and was development manager at TC TrustCenter GmbH. In that position he was responsible for the architecture and ITSEC evaluation of the PKI core components.

Tim Meyerhoff, Director, Iris ID Systems

Tim has been involved in new technology launches since 1989, and spent 22 years with Panasonic. Since 2000 Tim has focused on the Iris and Face modalities at Iris ID and he has participated in many projects which use multiple biometric modalities. With more than 17 years in the biometric and identity management industry he is highly proficient in the technical and application attributes of the key modalities, namely Iris, Face and Fingerprint. As a biometric SME Tim has experience with multiple vendors in the arena. His expertise is in both technical and business development areas.

Raul Popa,

CEO and Co-founder, TypingDNA

Raul Popa is the Co-founder and CEO of TypingDNA and is dedicated to the cause of bringing frictionless authentication through typing biometrics to the world. With a multi-disciplinary background including software engineering, social-psychology, product management, and data science, he co-founded two other startups and has 15 years of experience in the software business. His passion for AI-based technology contributed to building TypingDNA as an award-winning business with state of the art technology in typing biometrics.

Stefan K Persson,

CEO, Precise

Stefan Persson has more than 16 years' experience from various product management and product development roles in Ericsson, Sony Ericsson and Sony Mobile Communications. His latest role was as COO at Bang & Olufsen where he was responsible for Product Management, Research & Development, Quality, Design, Operations and Supply Chain Management.

He has managed product development in China, Sweden, USA and Japan as well as being responsible for Sony Mobile Communications' mobile accessories business.

In his role as CEO of Precise Biometrics, Stefan Persson is responsible for outlining the strategic direction of the business and daily operations.

AWARE

As a leading provider of solutions for biometric identification and authentication, Aware offers biometric systems built on granular software component products for fingerprint, face, iris, and voice enrolment and matching; mobile liveness detection and authentication; an ABIS with forensic face and fingerprint examination applications; and a biometric services platform. The company has provided government-grade biometric software products and solutions since 1992. More recently it has been leveraging its products for private-sector applications, such as for mobile biometric authentication in financial services and enterprise security. We spoke to David Benini, Vice President of Marketing & Product to find out more about Aware and the company's vision for the future.

What changes are you expecting to see over the coming year?

We have seen facial recognition algorithm performance improve substantially in recent years, as noted by NIST recently. Looking forward, we expect to see a similar trajectory for attack detection approaches and algorithms. The result will be vastly improved usability and performance in terms of matching and attack detection performance for mobile authentication. This will drive further adoption for customer and employee facing applications, particularly where biometric security features native to the device are insufficient or undesirable for the particular use case.

Where are you seeing the greatest demand for biometrics?

Aware is seeing continued demand in our traditional markets, particularly where government agencies must update their legacy biometric systems and improve their connectivity. We are seeing the most growth in demand for authentication solutions, both for financial services and for enterprise security.

What's the most exciting innovation you're seeing in biometric technology?

Machine learning has had a massive impact on facial recognition and attack detection algorithm performance, which has made facial biometrics an ideal approach for newer use cases such as mobile authentication. It's hard to overestimate its impact on the growth of the potential market for biometric solutions.

Standards continue to be critical to the industry. FIDO has also been a critical catalyst for biometrics gaining a foothold for authentication applications. The standards have been expertly crafted and adoption is beginning to ramp.

Looking forward a bit, we are in early stages of adoption of decentralized, self-sovereign identity models that utilize digital credentials and claims. This is an exciting area to watch.

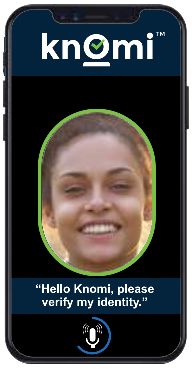
From your perspective, how will Machine Learning augment biometric technology solutions?

Machine Learning will continue to drive improvements in performance of algorithms for voice and facial matching and attack detection. These in turn improve usability, which is the biggest driver of adoption.

For those looking to deploy biometric technology in their organization, or in their products, what are the key things that you would advise them to consider?

Biometric algorithms can be very difficult to test and compare, in part due to the large amount of data that is needed and the challenges around replicating realistic conditions and a breadth of attack modes. Fortunately, organisations like FIDO are beginning to define performance requirements, and a few labs are now providing certification services. Without decades of algorithm testing work done by NIST, the world would be largely in the dark about how biometric matching algorithms actually behave and perform.

But organizations should avoid outsourcing their algorithm assessment efforts completely. Those that do what they can to perform their own testing with their own data benefit greatly from learning where the performance boundaries lie for their own specific use case. Every biometric algorithm has a unique personality that is hard to truly know without a hands-on approach.



iProov

We caught up with Andrew Bud, founder and CEO of iProov and, experienced entrepreneur, to talk about innovation and what the future holds in the biometrics industry.

Tell us about how your business has grown over the past few years.

From our launch in 2013, it took us a number of years to develop, prove and perfect our technology. Our first patents were granted in 2015, and since then we have been awarded 11 others. In 2017 we won many prizes, from organisations such as SINET, Citi and the UK NCSC then in 2018 we saw our commercial lift-off, with contracts with the US DHS, UK Home Office, ING, Rabobank and others, and very rapid growth to large numbers of users, transactions....and attacks. More recently we received confirmation of conformance of our performance metrics with ISO 30107-3 from NPL, the UK National Standards Laboratory and launched our new device-independent, contactless Palmprint verifier.

What are you expecting to see change or evolve over the next 18 months?

The market is rapidly recognising the primary importance of genuine presence assurance in biometrics. That is new and growing rapidly – we expect it to become a dominant feature of the market. As world leaders in this specific expertise, we welcome this timely and necessary development. Regulatory change is driving banks and financial institutions worldwide to tighten up identity verification and authentication, while making the mobile user journey easier. That can only be done with biometrics, especially face biometrics. So we are expecting very rapid growth in uptake in the near future. We also expect to see governments make much wider use of self-service biometrics for border crossing, visa and immigration and national identity schemes.

What do you feel the most exciting innovation is for biometric technology at the moment?

Machine learning is transforming biometric technology right now and delivers incredibly good results. 5G will also bring the ability to ship very large amounts of data off a user's device into the cloud, enabling entirely new classes of server-side biometrics. However, the next big thing will be large scale attacks by deepfake videos...

From your perspective, how will Machine Learning augment biometric technology solutions?

Everything is changing. Machine learning is a performance-enhancing drug for biometrics, but also for attackers. Generative Adversarial Network attacks represent a real peril for the old way of doing biometrics. Convolutional neural networks can find the deepest, most hidden patterns. We are in a new arms race.

Where are you seeing the greatest demand for biometrics?

Automated, self-service identity verification for onboarding is a terrific market for our genuine presence-assured face biometrics right now. It improves customer conversion while cutting costs, and it demands the combination of very strong security and great usability that we deliver. I am also impressed by the speed and confidence with which governments are innovating in travel, visa and immigration and other applications.

Looking beyond the use of biometric technology solutions for authentication, what other use-cases and applications will be transformed by this technology?

I think we have to be careful about using biometric technology beyond authentication in its broadest sense. Authentication is a voluntary, deliberate act of consent by a user, to attain an outcome beneficial to them. Other applications of biometrics may lack that consent, or lack the user benefit. That may sometimes make them problematic to public opinion.

Biometric technology continues to innovate rapidly with new uses appearing to make the process of authentication and verification more convenient and secure to support the increasing use of digital identity.

We caught up with three leading companies – B-Secur, ID R&D and Typing DNA to find out about their innovative biometric technology products and solutions, and their thoughts about trends for the future.

Tell us about how your business has grown with some of your recent highlights and how you're expecting to evolve.
Raul Popa, CEO and Co-founder, TypingDNA:
We started TypingDNA committed to improving our technology and providing the best typing biometrics authentication solutions. Joining organisations such as the International Biometrics + Identity Association (IBIA) and the European Association for Biometrics, along with our participation in the prestigious Techstars NYC accelerator gave us the opportunity to be closer to our customers in the USA. Over the past year, our dedication to seamless and frictionless integration of typing biometrics authentication solutions has helped us reach one million users, an achievement we're really proud of.

Our mission is to improve security without compromising user experience. Most importantly we are currently working on complementing our range of multifactor biometrics solutions with products which are easy to use and to integrate within already existing business systems.

Ben Carter, CCO, B-Secur:
In the last four and a half years we've had a rapid journey from a deep R&D university-lead project through to now having around 40 full-time employees, working across technology, science, commercial and operations. This growth has been driven by the development of 'HeartKey', a world-first, next generation biometric product. I'm excited to see that ECG technology is moving into the mainstream something just recently underlined by the announcement of ECG technology within the Apple Watch Series 4. We are seeing increasing demand for ECG technology coming from industries including automotive, healthcare and health and wellness. We believe we are on a precipice of seeing ECG technology coming out of the hospital and into the home, within everyday devices.

Alexey Khitrov, CEO and Co-founder, ID R&D
The past year has been one of tremendous growth for us. We doubled both our number of signed contracts and the size of our staff, opened a West Coast headquarters and we launched the first biometric authentication solution for messaging. We also released an update to our IDVoice, which uses a new generation of technology called x-Vector to deliver the fastest and most accurate text-independent verification solution on the market. Lastly, we saw great reception from the industry, including being named a Top Pick for Fintech by TechCrunch and a finalist in Microsoft's Innovate AI competition, as well as being accepted into the Plug antd Play Accelerator program, the Google Cloud Startup Program, and the Microsoft IoT and AI Insider Labs program.

Over the next 18 months we expect to see a huge growth in demand for the conversational interface (CI). Customers are used to talking to Alexa at home, to Siri or Google on their mobile, to their car radio etc, and consequently want that kind of experience across all their technological interactions. Voice has become king of the UI, and businesses are rushing to offer it. But enterprises want to ensure that a more seamless user experience is still highly secure. The ability to combine these two counter-directional trends of robust security and a user-friendly UX is where ID R&D sees the opportunity to apply our scientific and technical capabilities and change the way customers engage with the enterprise.

Where are you seeing the greatest demand for biometrics?
Alexey Khitrov: The greatest demand thus far has been in financial services, not surprisingly because they have so much at risk and want to use all the tools available to improve security. However, the conversations we're having across a number of verticals, such as healthcare and telco show that biometrics appeal to them as well. And the fact that voice is now king is obviously driving strong interest in a whole range of voice activated devices, like smart speakers, and also anything where voice is a desirable interface, like in cars and TVs.

For those looking to deploy biometric technology in their organisation, or in their products, what are the key things that you would advise them to consider?

Alexey Khitrov: Best practices would mean that organizations should deploy a multi-modal biometrics solution. With just one modality, bad actors can still figure out ways to trick the system. Second, you must think about spoofing and build in an anti-spoofing layer. Third, you are far more secure against fraudster attacks if you implement continuous verification. This is where everyone wants to be and eventually needs to be. If you're starting out now, design for multi-modal, continuous verification from the beginning.

Ben Carter: Understanding the potential of each biometric modality and their corresponding use cases is essential alongside the benefits for implementing each e.g. comprehending the impact of stress in the workplace or reducing staff absence and turnover. And of course, the efficient management and security of health data – something that is often sensitive and personal.

Raul Popa: As Alexey says, this is in the financial system due to its higher vulnerability to cyber-attacks. As much as users try to strengthen their passwords and memorable information it is not quite enough to be protected online. The banking sector has been shaken up by the emergence of challenger banks, which focus on app-based online activity, as well as by regulations like PSD2 which mean that banks need to implement stronger authentication for their customers. The solution is simply to apply multifactor authentication (MFA) to transactions, accounts and generally to customers' digital activity. But to be able to compete with newer online financial institutions, banks must also ensure seamless and frictionless integration of MFA. We can now do this without impacting user experience. It is interesting to look at behavioral biometrics as the answer to the simple question: Who are you?

We are often so caught up in our day to day business that we might forget passwords or pincodes and we can even lose phones and other devices which might be required during authentication. However, who we are remains the same. And importantly, behavioral biometrics can be used as an MFA option which does not affect user experience, since this is implicitly done in the background

Ben Carter: We're also seeing a growing and significant ecosystem where all devices have IoT connectivity and consumers will be able to access their ECG health and wellness information all day, every day. We believe this will be a fundamental development in how individuals manage their health.

So looking at how the use of biometrics technology can improve our everyday lives, what do you think the future has in store?

Ben Carter: Machine Learning (ML) and AI technology will unlock new insights into the data we're collecting. When applied to biometric tech we can rapidly increase the security of our systems by utilising features that would not have been obvious or recognised with traditional methods. As biometrics become more accepted multi-modal solutions are becoming more popular to further increase security; ML and AI provides a reliable method of collating and integrating these technologies into a seamless experience for the user, managing the system inputs to determine the appropriate modalities and parameters to use.

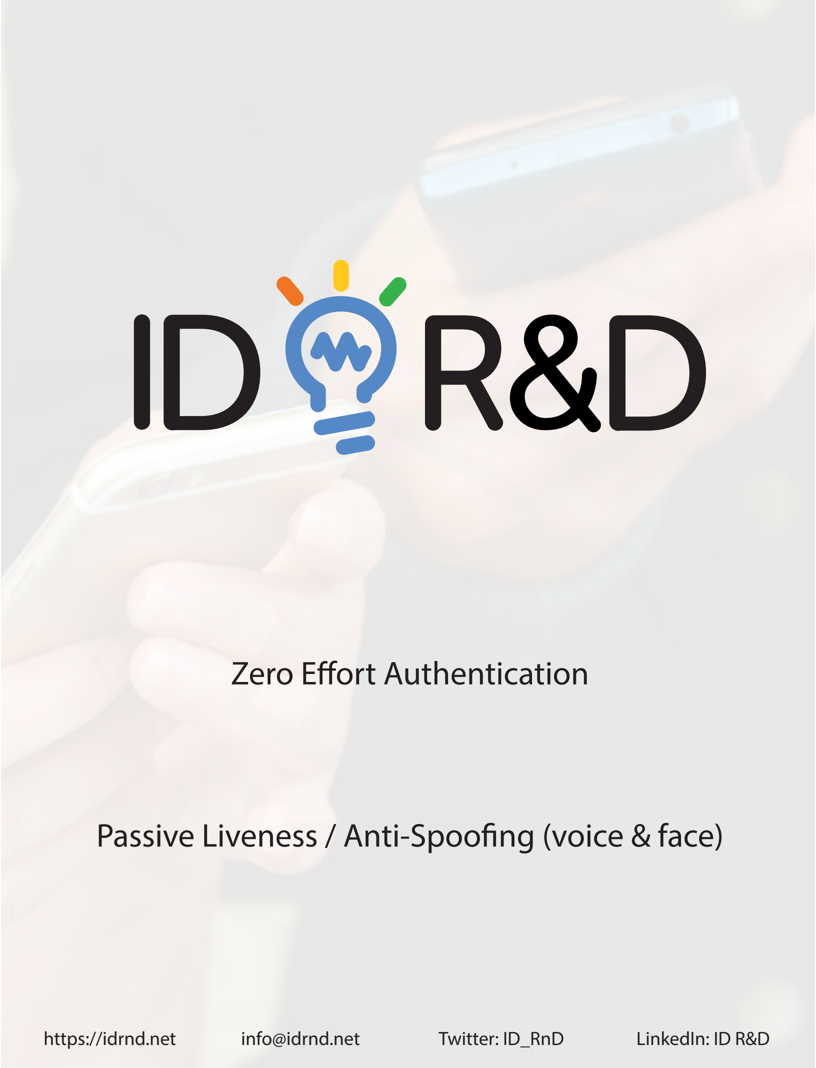
The data collected during a biometric authentication doesn't necessarily need to be limited to security. Some biometrics can reveal more information about a person e.g. ECG can give us heart health and stress data, facial recognition gives us basic emotional mapping which can feed into a wider IoT system – for example smart cities that can predict when and where people will be more stressed due to external events or more tired and therefore may be more likely to be involved in an accident. There's a wealth of information and data coming from the human body that we're beginning to collect, and machine learning and AI are the tools we can use to ensure we're getting the full benefit. So your car, your phone, your watch etc. will be helping you live a longer and healthier life.

Alexey Khitrov: Without a doubt, I see biometrics as absolutely changing our lives for the better. Imagine a day when your technology knows you as well as your friends and family do. You don't have to constantly verify yourself for transactions, but can go through the day with all of your technology delivering a personalized and secure experience.

Your phone, your ATM, your car, your thermostat, your doctor's office, etc – biometrics enables all industries, applications, and devices to know you automatically without any effort on your part.

What do you feel the most exciting innovation is for biometric technology at the moment? And what do you think the next 'big thing' will be?

Raul Popa: It is crucial to look at the development of even more seamless and frictionless behavioral biometrics solutions which follow the authenticated user throughout the entire session. People are moving towards a more digitalized life and this implies that the need for online security is bigger than ever before. Hence, we believe innovation in our field lies at the heart of continuous authentication, as with the use of multiple devices and accounts, it is no longer enough to only ensure that the person who logs in is who they say they are, but it is also necessary to constantly check their identity. Typing biometrics are key to behavioral biometrics and we are optimistic that the level of product adaptation to users' needs and the demand for typing biometrics are ascending.


ID R&D
Zero Effort Authentication
Passive Liveness / Anti-Spoofing (voice & face)
https://idrnd.net
info@idrnd.net
Twitter: ID_RnD
LinkedIn: ID R&D

Zwipe

Following his appointment as CEO of Zwipe in March 2018, André Løvestam has led the company through a milestone year, including a successful MUSD 14 fund raising and public listing on the Oslo Stock Exchange, Merkur Market in January 2019. We spoke to him to find out what the future holds for Zwipe and the wider biometrics industry.

Tell us about how your business has grown over the past few years and what you are expecting to see change or evolve over the next 18 months.

In the last 12 months Zwipe has had its most successful fundraising round, topping up a B-Series fundraising effort with 14 million USD in fresh capital, in addition to securing a European Union "Horizon 2020" grant valued at 2.3 million EUR. The new funds will enable the company to strengthen its strong position in the rapidly emerging biometric payment cards marketplace.

We have also initiated 12 different market-leading biometric payment card pilots, supported by both VISA and Mastercard payment networks, across Europe and the Middle East, most notably with Banca Intesa Sanpaolo in Italy.

The market is moving towards commercialization and over the next 18 months we expect to see the first volume deployments in the global biometric payment card marketplace, as well as the development of the biometric enabled wearable payments segment.

Where are you seeing the greatest demand for biometrics?

In the context of payment cards, it looks like biometrics will be first adopted in the so-called high net worth individuals and corporate card segments. As volumes increase, and product costs go down, we expect biometric payment cards to proliferate all segments over time. In terms of geographies, the greatest demand seems to come from the Middle East, then Europe, Asia and Latin-America, but, again, over time biometrics will be a global phenomenon.

Looking beyond the use of biometric technology solutions for authentication, what other use-cases and applications will be transformed by this technology and how do you see biometrics improving our everyday lives?

Our emphasis has been on securing convenience. We are focusing on eliminating the unnecessary trade-off between security and convenience in the payments space, and we believe our secure, fast and easy-to-use biometric authentication solutions can be applied across different verticals - such as payment, access control and government identification – and different form factors, such as smart cards and wearables.

Utilizing biometrics for primary authentication makes security seamless. This same user experience is rapidly being adapted to the internet of things and increasingly becoming a core element of any transactional activity.

In terms of improving everyday lives, the simplest example we have today is our mobile phone. Not too long ago we used to walk around with unlocked phones because it was inconvenient to lock them and enter PINs or passwords that were difficult to remember as you had to change them every so often. Today we utilize biometrics hundreds of times a day, to access our smart phones. The gateway for many of us is the fingerprint and that convenience is being adapted to the checkout experience, both physically and digitally, where your biometric information is used to authenticate your transactions in a much faster and more frictionless manner then what has been the norm in the past.

For those looking to deploy biometric technology in their organisation, or in their products, what are the key things you would advise them to consider?

Biometrics is not just a security tool. Biometrics at its heart is an excellent means of identifying and authenticating people, and it is increasingly proving to be an ideal tool for driving a better user experience. UX has never been more important and the brilliance of biometrics in delivering a more frictionless and secure user experience is why it is being so widely adopted in so many of the devices and products that people cannot live without. This capacity will only grow as more companies join the likes of Zwipe in driving innovative offerings to the market.

The key consideration should revolve around how and where to store biometric data. With the threats of hacking and data and identity thefts having a self-contained system is, in my opinion, of paramount importance. Zwipe's biometric payment card solution, for instance, stores the biometric data solely on the card itself, and the matching is done on the card. So there is no need for a central database that criminals could find it worthwhile to hack.

zwipe

There has always been an unnecessary trade-off between security & convenience...

Thanks to Zwipe's unique technology consumers can have the best of both

SPONSORS AND PARTNERS

Our thanks to all our sponsors and partners:

Gold Sponsors:

iProov
iProov creates a safe digital environment with our strong authentication solutions. Our patented Flashmark technology achieves unmatched security through resistance to all known forms of identity spoof attack, including photo-realistic artificial video. iProov offers a highly intuitive, hardware and platform independent solution that places no demand on the end-user. Our technology has been used for secure customer onboarding, strong customer authentication and KYC. We have gained wide recognition globally and our products are being used in production by governments and top-tier banks. Our clients include the UK Home Office, the US Department of Homeland Security, ING and Rabobank.

Zwipe
Zwipe is a technology solution provider that enables battery-less, ultra-low-power, self-contained biometric authentication solutions. Together with an ecosystem of partners including global brands within security, financial services and ID applications, Zwipe is "Making Convenience Secure™" for banks, merchants and consumers. Using advanced fingerprint recognition while protecting personal information, Zwipe's solutions address the data theft pitfalls inherent in traditional authentication methods. Headquartered in Oslo, Norway, Zwipe has spent the last 10 years developing its unique power harvesting technology platform in combination with security solutions based on international infrastructure standards. To learn more, visit http://www.zwipe.com

Silver sponsors:

Aware
Aware is a leading provider of software products and solutions for biometric identification and authentication. We provide biometric systems built upon our more granular software component products for fingerprint, face, iris, and voice enrolment and matching; mobile liveness detection and authentication; forensic examination applications; and a biometric services platform, among others. Our solutions are used globally for a variety of applications in government, financial services, and enterprise security. Aware is a publicly held company (NASDAQ: AWRE) based near Boston.

Precise
Precise provides market leading solutions for verification of people's identity using biometrics, making everyday life easy and more secure. Our solutions are used hundreds of millions of times every day, worldwide. For more information, visit https://precisebiometrics.com

Innovation Sponsors:

Acuant
Acuant's next gen Identity Platform is powered by AI with human assisted machine learning to reduce fraud while providing a seamless customer experience and increasing conversions in the digital economy. Built to scale and meet KYC, AML and GDPR regulations, Acuant achieved ISO certification and has the industry's highest speed and accuracy rates. Award-winning products include AcuFill ID capture, AssureID authentication, Facial Recognition Match, Chip and Ozone ePassport authentication. Solutions are omnichannel allowing businesses to establish identities on premise or remotely via the cloud and mobile devices. Completing more than three billion trusted transactions worldwide, partners include Fortune 100, FTSE 350 organizations and start-ups in all industries. For more information please visit www.acuantcorp.com

B-Secur
B-Secur are experts in ECG technology. Using the heart to enable secure health & wellness insights in the connected world.
We've invested over 15 years of scientific research in ECG to become a world leader in the development and integration of ECG technology, partnering with some of the world's leading technology companies.

We've harnessed the power of ECG to create HeartKey®, a suit of powerful offering user identification and advanced physiological monitoring with intrinsic data protection. HeartKey® brings world class expertise in ECG; combined with powerful, flexible integration and configuration possibilities to create the optimal product, with a competitive edge.

BehavioSec
BehavioSec is the most proven vendor in Behavioral Biometrics. The company's Behavioral Biometrics platform is widely deployed across Global 2000 companies for its proven ability to dramatically reduce account fraud and data theft. Founded in 2008 out of groundbreaking academic research, BehavioSec technology allows companies to continuously verify digital identities with superior precision in real-time.

BehavioSec's enterprise grade solution is used in global deployments by many of the world's largest companies, reducing manual review while safeguarding millions of users across billions of transactions. BehavioSec investors include Forgepoint Capital, Cisco, ABN AMRO, Conor Ventures and Octopus Ventures. BehavioSec is headquartered in San Francisco, CA and has global operations throughout Europe and Asia Pacific.

ID R&D
Based in New York, NY, ID R&D's award-winning scientists and engineers focus on research in the science of biometrics to produce the most advanced and highest performing biometric technologies. Our approach is to combine best-in-class biometrics to transfer the authentication burden from the user to the technology, thus enabling a zero effort authentication experience. Using the very latest in artificial intelligence methods, we develop and deliver voice biometrics, voice anti-spoofing, facial liveness, and keystroke behavioral biometrics. Recent awards and recognition include being a 2018 TechCrunch Top Pick, 2018 Microsoft AI Top 10, and inclusion in Gartner's Market Guide for Authentication.

Iris ID Systems
Iris ID Systems Inc. has been active in iris recognition research, development and production since 1997. The company's IrisAccess® is the world's leading deployed iris recognition platform used in thousands of locations daily authenticating the identities of millions of people. More public and private organizations look to IrisAccess for iris-based authentication than to all other iris recognition products combined. For more information, visit http://www.irisid.com

Nok Nok Labs
Everything authenticates on the Internet. User frustration over legacy authentication methods, increased fraud due to compromised credentials and the need to support regulations like PSD2 and GDPR will continue without a more convenient approach. The ability to protect organizations and users in the digital world is at risk if we don't solve the authentication problem.

Nok Nok Labs helps global organizations provide simple, secure, scalable methods to authenticate users and devices that prevent fraud and other security risks. By reducing the reliance on weak, phishable passwords and other broken legacy authentication methods, Nok Nok empowers business leaders to improve the user experience to access digital services, while meeting the most advanced security and regulatory requirements.

TypingDNA is a cybersecurity company, launched in 2016, committed to providing the best typing biometrics and authentication solutions on the market, currently based in New York, USA and Romania, EU.

The company's mission is to strengthen security without compromising user experience and to create seamless, frictionless, scalable and easily deployable security solutions. TypingDNA really shines at providing the most available, state of the art online biometric technology - it can be used with any keyboard, on any device, works passively behind the scenes, and it starts performing with only one previous sample.

Media Partner: BIOMETRIC UPDATE.COM

BiometricUpdate.com is the leading news property that publishes breaking news, analysis, and research about the global biometrics market.

Host Partners:

rise
new york

PRECISE

Active in the biometrics industry for over two decades, Precise is well known for its leadership in developing high quality fingerprint solutions, initially with hardware for physical access and more recently, software for mobile devices and smart cards. Alongside the natural evolution of biometric technology, Precise is readying itself for new opportunities and has used its extensive experience in biometrics to develop a platform for verification of digital identity. This new platform – YOUNiQ – combines multiple biometric technologies with other types of smart technology to provide convenient and secure verification of digital identity which in turn, enables modern, everyday life to be easier and more secure. Stefan K. Persson, CEO of Precise explains more...

"Biometrics is becoming a natural part of our lives, it is expanding beyond our smartphones into new applications, such as smart cards, wearables, cars and door locks to mention just a few. This year we expect to launch our first contactless biometric payment cards and we've already moved our biometrics solutions into automotive. Recently Hyundai announced that in one of its new models the driver will be able to use fingerprint biometrics to unlock the car, start the engine and adjust settings in the vehicle and we're delighted to be part of this innovation.

"As we constantly strive to make our everyday lives easier and more carefree, convenience has become one of the key factors when choosing a product or service. Often however, when convenience is prioritized then the security is compromised or vice versa; the challenge is to find the right balance between these two factors – using biometrics you can get both. Security can easily be enhanced by using multiple biometrics such as face, fingerprint, voice etc. without affecting convenience.

"As a wide range of devices are increasingly being equipped with sensors and smart technology, this opens up the opportunity to create very strong digital identities. By gathering data of what makes you unique, for example your fingerprint, face or voice together with how you behave and where you are, it becomes possible to create an identity profile that is extremely hard to replicate and spoof. And in the future, we'll become even more digital, as for example our digital IDs will replace our current ID documents such as passports. Machine Learning and Artificial Intelligence will further improve the 'digital identity' system over time, making it even safer, with fewer possibilities for fraud and other attacks.

"Looking to the future, the way we use biometrics today is just the first step. As with all new technology it will take time to adopt – but we can't stop the evolution! Soon biometrics will be everywhere, in our homes, cars and work places. They will not only be used for authentication but also for personalization and interaction with our daily interfaces. And they will help to improve our lives, for example in health care where biometrics will be used to predict and detect health issues."

Biometrics has become an increasingly important tool in the fight against fraud in almost all payment channels. Biometric solutions can be used to ensure a convenient and secure authentication regardless of whether it is cash retrieved from a cash machine, card or mobile payments. Payments have become the main driving factor for adoption of biometrics at the consumer level. Today, approximately 575 million use biometrics for payments on a daily basis, a figure that is expected to increase to 1.2 billion users in 2020 according to research from Goode Intelligence.

Find out more about YOUNiQ at **https://precisebiometrics.com/products/youniq/**

Biometric technology is proving to be an important tool to accurately identify people and aid the fight against fraud. We spoke to experts at Acuant, BehavioSec, Iris ID and Nok Nok Labs who represent some of the exciting technologies in this space to discover more about their innovative products and solutions and how they are set to improve everyday life both now and in the future.

Dr. Neil Costigan, CEO, BehavioSec

The last few years have been very exciting for us as we've brought Behavioral Biometrics from being a research subject to it being part of the core infrastructure for some of the most prestigious companies in the world. Looking forward, while demand is strongest from the financial sector, as ransom and malware are expanding the need for security across verticals, we're also seeing increased interest from new areas, like the healthcare industry. I think we'll continue to see exciting innovation with passive biometrics and continuous authentication over the coming years.

Machine Learning (ML) and Artificial Intelligence are very important for augmenting biometric technology solutions.These are the very techniques that made Behavioral Biometrics commercially viable, and without them we wouldn't have a product. Looking beyond the use of biometric technology solutions for authentication, I believe that a lot of the technology can probably be used for many cool health and productivity solutions. We've already seen how biometrics are used to simplify our everyday lives, removing burdensome physical tokens and other taxing 20th century solutions. As a Behavioral Biometrics company, we're also spared most of the fears associated with static biometrics, so we see biometric technology to be convenient, rather than creepy.

If you are planning to deploy biometric technology in your organization or products, then my advice is to make sure you don't get left behind; attackers prey on the weak. While most companies already know that they need to increase security, they're sometimes holding back out of a perceived safety of having little or nothing to lose in a cyberattack. Today, even the least mature enterprise holds a lot of information in CRM systems, email and internal communication tools. A leak could very well be catastrophic. Deploying a modern multilayer security system is a cheap way of reducing that risk.

Stephen Maloney, Executive VP of Business Development & Strategy, Acuant
Acuant has grown rapidly over the past few years with our cloud and mobile offerings leading the way and we've been recognized for our product innovation, including being named a Gold Winner for both the Stevie® Awards and Info Security Product Guide's Global Excellence Awards®. Importantly, our identity verification is increasingly being called upon to augment or replace traditional methods of identification such as passwords, knowledge-based authentication and data.

In our experience companies are looking for thoughtful, well designed and fully integrated solutions to solve their problems. In identity verification, proving the identity of a user, especially those not present, is becoming a business imperative. But these solutions must strike a balance between risk and friction as well as protecting personally identifiable information (PII) and regulatory compliance. We see use cases and scenarios requiring different solutions. For Acuant it is about using robust document authentication and biometrics like facial match to create trust anchors. The balance of risk and friction will then determine how it is used in onboarding good, new customers, providing people and machines with access, meeting regulatory requirements and fighting fraudulent transactions. Additionally, the use of blockchain and other cryptographic methods will allow us to carry out digital transactions while revealing only the amount of PII absolutely required for that specific transaction.

Machine Learning (ML) and Artificial Intelligence are augmenting biometric technology and aid in both big data analytics and behaviour biometrics. Our document authentication is curated machine learning with new improvements being routinely developed. We see that various use cases, guided by the level of risk and assurance required along with how much or little friction can be tolerated in the transaction, determine which technology is appropriate and how often ML or AI is utilized. We see the emergence of cloud-based AI technology will continue to make it easier and less expensive.

Looking beyond the use of biometric technology solutions for authentication, we see these technologies entering into everyday life by helping with school attendance, voice technology in automobiles and in the living room, advances in healthy living and lifestyles, near real time language translation as well as many other applications. When looking at the use of biometrics to improve everyday life, the use case helps to separate creepy from convenient. When it protects me, reduces my friction and alleviates risk, it is convenient. When it predicts or assumes things for me, follows or anticipates, it can be creepy. When it is convenient it will be used and when creepy, it will need to be regulated or dissolve.

Acuant's Next Gen Identity Platform is powered by AI with human assisted machine learning to reduce fraud while providing a seamless customer experience in the digital economy. Built to scale and meet KYC, AML & GDPR regulations, Acuant has the industry's highest speed and accuracy rates. Solutions are omnichannel allowing businesses to establish identities on premise or remotely in seconds while protecting customer data.

Contact Acuant and mention you attended the Biometric Summit for a customized identity proofing consultation.

For more information
Visit: acuantcorp.com
Email: info@acuantcorp.com

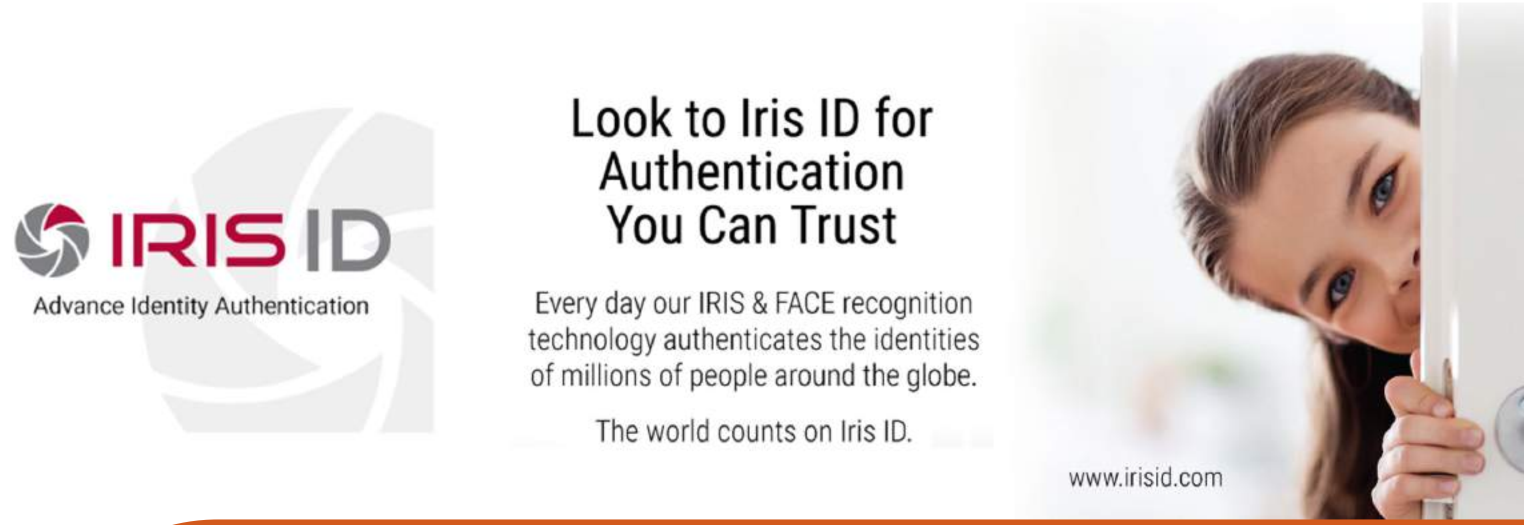
acuant

Tim Meyerhoff, Director, Iris ID

Over the past years we have seen most of our growth at Iris ID in the ID markets, specifically border patrol interdictions, legitimate border crossings, National ID and election defence applications. This year's highlight was the one thousandth system install with US Border Patrol, along with our flagship product the new E Gates being installed for Privium at Schiopl Airport in The Netherlands. There has been a lot of attention to facial recognition recently and it is an important market trend for the future. Face is part of our repertoire and although it still has issues at scale, we expect to see many more programs which will be collecting iris along with face.

Looking at what the next 'big thing' will be, in domestic US I would say it is the Air Exit pilot programs which are certainly getting a lot of attention in the media. Plus the CLEAR expansion with Hertz – biometric checkout for car rental is pretty cool. We see that there will be a lot of growth in the healthcare field along with workforce management and Access Control. Civil ID applications are on the rise globally, but slower to grow in US domestic markets. In Law enforcement & corrections we're seeing multimodal solutions now being used. For example, Face was officially implemented in the FBI database just last year and the iris pilot instituted in 2015 will be an officially supported modality at CJIS sometime in 2019.

My advice for those of you deploying biometric technology is that the overall security of the system and its ability to protect PII is paramount. Then think about the convenience of the modality, achieving a low false rejection rate, and ease of enrolment. There will be cases where a person cannot use the biometric sensor for various reasons. So accommodating ADA requirements or an alternate means of authentication should be considered. Cost is a factor of course, and the rule of 'you get what you pay for' certainly applies here.


IRIS ID
Advance Identity Authentication
Look to Iris ID for Authentication You Can Trust
Every day our IRIS & FACE recognition technology authenticates the identities of millions of people around the globe.
The world counts on Iris ID.
www.irisid.com

Dr. Rolf Lindemann, Senior Director Products & Technology, Nok Nok Labs
Back in 2012 we set out a vision to transform the way authentication works, and over the subsequent years invented the concept for FIDO, recruited allies, created the FIDO Alliance and shipped the first versions of our product. Not long afterwards our vision was embraced and joined by every part of the computer industry from chips and systems to devices, authenticators and operating systems. We then created the first secure fingerprint sensor based FIDO authenticator with Validity/Synaptics, Samsung and Qualcomm and proved that FIDO could work at scale by deploying with PayPal, NTT Docomo and AliPay.

By 2018 we were the market leaders in shipping FIDO standards-based solutions with our industry-leading S3 Authentication suite. Our customers authenticate more than 150 million active users and over 4.5 billion transactions – a scale that no other standards-based authentication vendor can claim for their solutions. Our clients include four of the largest banks and four of the largest telcos in the world, and we have doubled our revenue year over year. Building on all this success, over the past year we have seen significant adoption of our technology. Some recent examples include:

- Successful launch of our S3 Authentication Suite at Japan's largest bank, MUFG Bank, Ltd
- Nok Nok S3 Suite is now used by four out of the five world largest banks
- Achieving the GSMA GLOMO Award for the "Best Authentication and Security Solution" for our S3 Authentication Suite

We're continuing to innovate around our standards-based backbone and have deployed use cases ranging from physical security and IoT applications to commerce, payments, healthcare and cloud access. And, to enable next generation authentication, we have now integrated risk signals into our product.

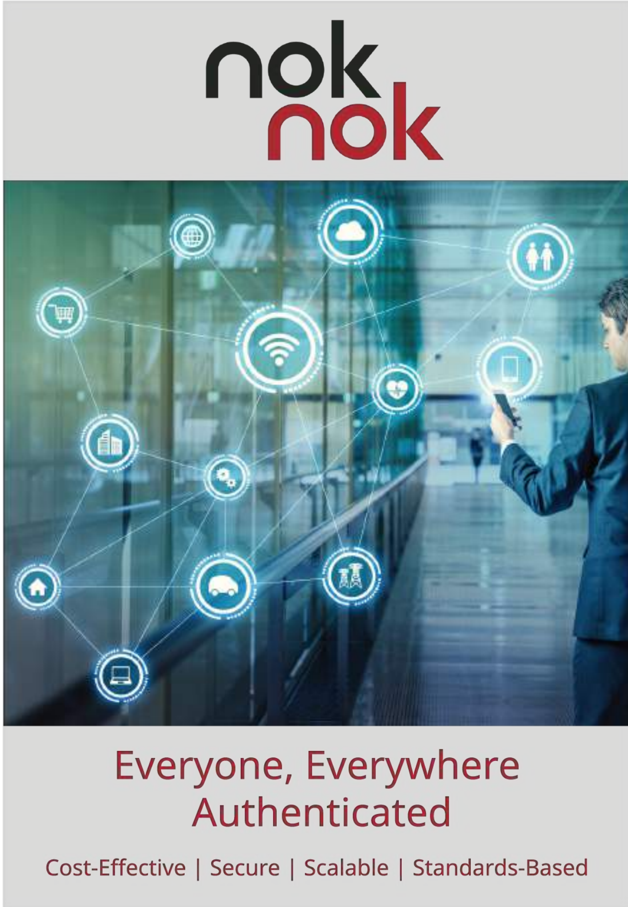
The future looks very exciting. We monitor developments in biometrics on three fronts: sensing technology, form factors/usability and security. We're pleased to see all three going through an explosive growth period and expect to see more biometrics, in more factors than ever before. FIDO of course allows these biometrics and tokens to be used for more than just opening your phone, it allows for secure online and privacy-respecting authentication.

Current biometric implementations already prevent scalable attacks nicely. We're particularly excited by continuing improvements in the underlying security architecture for biometrics to prevent spoofing and other targeted (non-scalable) attacks. For example, Apple and Samsung have both demonstrated careful attention to detail here using both hardware and software to innovate past previous limitations and to raise the bar for attackers. Going forward, we expect biometric vendors to put even more emphasis on presentation attack detection, given that false-accept-rates are already sufficiently low. Then, on the form factor side, we expect to see more wearables using biometrics for authentication, e.g. the rings from Motiv. It will be interesting to see if consumers will broadly accept these form factors...

Today, we are still in the early days of the post-password era. Visionary customers and early adopters are leading the way and we're now entering an era where people can trust that modern authentication is secure, scalable, easy to use and allows for privacy. We see pretty much every online interaction for consumers being transformed to use biometrics as the primary method of authentication in the next five years. Companies like Cigna, TMobile, Bank of America, PayPal and others are already doing this, and their peers in the banking, payments, commerce, cloud, media and healthcare areas will also be moving to use modern authentication based on FIDO. That brings a diversity of use cases and integrations which we are very well equipped to handle as the leading vendor in this area. For example: MasterCard Europe has been speaking about making biometrics mandatory for 3DS v2 (card not present) transactions, PSD/2 is driving a need for FIDO, NIST 800-63 which influences federal procurement is deprecating SMSOTP in favor of non-phishable authentication like FIDO. All these trends create a demand for our solutions across sectors and we have partnered with companies like Ericsson, Fujitsu, Hitachi, and OneSpan to extend our reach as this growth continues.

Other use cases and applications are set to be transformed by biometrics technology. We see demand for remote identity verification that is stronger than knowledge-based authentication (KBA). This is especially the case in countries without electronic identity cards, but even in some countries with electronic identity cards, practical alternatives to KBA are rare. As a result we see a demand for remote identity verification using biometric technology (like face recognition with appropriate presentation attack detection) typically combined with other technologies like document- scanning and document verification. If you are thinking of deploying biometric technology then I recommend you start with technologies that consumers are familiar with, and whose technology performance and security characteristics are well known. Make sure you create a threat model and understand the security and privacy model of your biometrics implementation. Consider using a mature platform that implements the FIDO specification as a shortcut to get the security, quality and privacy implementation of biometrics versus "rolling your own". An added benefit of FIDO is that it respects user preferences so both various biometric and non-biometric modalities are supported.

Finally, remember that biometrics are great to use in the case of 'local' interactions. For securing remote interactions, cryptography also needs to be part of the solution, combined with biometrics. FIDO combines both.



NOTES

JOIN US AT BIOMETRIC SUMMIT LONDON 2019

Thank you for joining us today, we hope you enjoyed this unique event and that you'll join us again later this year at Biometric Summit London 2019 on Wednesday 20 November at Rise London where we'll be extending our focus on innovation to include new sessions and engagement on biometrics for Digital Identity and Electronic Know Your Customer (eKYC).

Find out more and register at
www.goodeintelligence.com/london-2019/

BIOMETRIC SUMMIT

Hosted by
rise london