ID WORLD

THE PLAYERS OF THE AUTO ID INDUSTRY

CARDS - BIOMETRICS - RFID - DATA COLLECTION

Presented by

SUSTAINABLE DEVELOPMENT

Top 50 Suppliers

ePassport technology

- **Artificial intelligence**
  Harnessing technology for inclusive economies
- **Future manufacturing**
  Driving forward the autonomous vehicle market
- **Cyber Security**
  Reshaping enterprise defenses through cloud AI
- **eGovernment**
  Policies and regulations for creating value

Hadrian Media 15 €

JULY 2019

Taryam bld., Industrial Area 18, Maleha Street, Sharjah PO Box 123428, United Arab Emirates, +97165062555

Est.1991
INDUSTRIAL
INNOVATION
GROUP

MegaFlex

ERP

DSS

UnionPay 银联

MasterCard

VISA

www.industrialinnovationgroup.com

Editorial

The era of AI has brought a multiplying factor to the technology evolution stage that sees the visions of today's economists, policy makers, philosophers and sociologists sometimes look like they are way ahead and sometimes miles behind the current industry views about opportunities and challenges related to data intelligence-based innovation.

FaceBook has been fined a dramatic amount of US$5 billion to settle an investigation into the company's privacy violations that was launched following the Cambridge Analytica revelations. This figure is something that seems to beat all records and yet a disappointing amount to those who see the case as a mass manipulation of democratic society will according to democratic standards. In fact, US lawmakers and advocates say the ruling and 'relatively small fine in the light of FaceBook's annual revenues' show federal privacy laws are needed. Labeling it a 'parking ticket', they also say it is the beginning of the end for the Federal Trade Commission's probe into Facebook's alleged mishandling of more than 87 million users' private data during the scandal.

In addition to this, the company has reportedly been struggling under the weight of scandals related to privacy, hate speech, election interference and fake news over the last few years. Indeed, fake news does not support the informed decision making processes of the free citizen imagined by the founders of democratic thinking. Utilized to influence not only consumer but also elector behavior, it jeopardizes the very meaning of the democratic political franchise. Or in other words, the vote many governments around the world rely on when aiming to assert the will of their population to benefit the greater good of each Nation, its values and constitution.

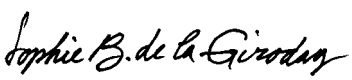
So what is the solution?
Perhaps the first step is redefining privacy as a sphere that does not include only the public or confidential information about each citizen and his or her unequivocal identity from illicit access or fraudulent use, but that first and foremost protects his or her ideas and emotions from being tampered with against his or her interest and according to the agenda of clients of the IT industry itself.

The global effort to protect our privacy and dignity as human beings in the era of artificial intelligence has just started and pressure is mounting. Fake news is among the most difficult challenges - aside from real stories often being called fake by some politicians, actual fake news is used to coerce people into making decisions. Consequently, governments have been putting increasing pressure on sites like Twitter and Facebook to take more responsibility for the content shared on them. But the privacy debate is a double-edged sword with freedom of information being challenged by protection of basic citizen data rights.

In this regard AI while an enabler, is also being seen as a combatant and Twitter has already begun to put safeguards in place. With its recent acquisition of Fabula AI, it reportedly has the ability to analyze large and complex data sets for signs of network manipulation and can identify patterns that other machine-learning techniques cannot. Armed with this, Twitter states it can determine how trustworthy a claim is and hopefully make it visible to others.

It will be interesting to watch what steps the other big processors, handlers and conveyors of data, news and information take in this regard. All this remains to be seen, but is likely - and perhaps regulation or even legislation to make it happen is closer than we think. In any event, all players everywhere need to keep working at it.

Sophie Boyer de la Giroday



FINANCE TRANSPARENCY FORUM

The Sustainability Summit calls for the active contribution of policy makers and of industry leaders worldwide, to drive change in today's finance sector focusing on systems and regulations. Join the Finance Transparency Forum, a dedicated working group debating how policies, technologies and methodologies are to be leveraged and modernized to grant financial inclusion and entitlement, address the analytical divide and define new trust models in the finance sector. Attend FTF Events, restore confidence of investors and support the sustainable development of the digital economy.

SUSTAINABILITY SUMMIT

A ROADMAP TOWARDS OUR GLOBAL GOAL

2019

Brussels • New York • Zürich • Paris • London

Transportation | Resources | Future Cities | Manufacturing | Infrastructures

ORGANIZED BY:

>>> wise media

ENDORSED BY:

FIND OUT MORE AT:

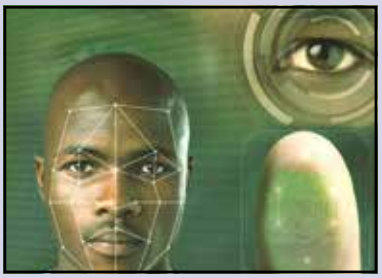
www.financetransparency.org

Contents

An overview of the European Union landscape following the EP May elections and the potential rise of far right anti-European factions in a number of member states.The debate continues as to whether these pose a threat to stability and unity - and what situation the new European President, once elected, will have to face and handle - from issues surrounding Brexit and individual state nationalism to managing migration and cyber frontiers.

A report on how Google is handling the growth of artificial intelligence deployments and how the technology has become a real-world application as part of the fabric of modern life. Harnessed appropriately, Google believes AI can deliver great benefits for economies and society and debates on various systems' potential to transform both industrial and societal processes - as long as governance structures prove to be sufficient if in existence, or are at least being developed if not.

In this section, a study is explored on how digital identification provides a significant opportunity for value creation for individuals and institutions looking at the real and inclusive economic gains. In addition, the rise of the digital signature is examined in terms of its ability as a tool to ensure maximum authenticity and integrity of digital messages or documents. Finally, the rise of devolved regionalised identity systems in Africa is discussed in a wider context in terms of what beneficial takeaways can be gained from the European experience.



ID WORLD
THE SUMMER BUYERS' GUIDE

For the 15th year, our "Top 50 Suppliers of ePassport Technology" features the most active players in the ePassport and eID evolution, who are driving advancements in biometrically enabled, machine-readable identity and travel documents.

Page 31

Top 50 Suppliers
ePassport technology

Matica allies with Canon Fintech

Matica Technologies has announced a strategic partnership with Canon Fintech which includes the joint development of products, largely through the sharing of technology, mainly but not limited to the government and financial markets. The partnership's first joint product is the Matica EDIsecure MC660, a brand new 600dpi high-resolution card printer for high-level security applications based on the highly reliable ID card print engine of the CFN's printer range while also incorporating unique features from Matica's technology and software. Under this alliance, the designed products are manufactured by CFN according to Canon's high standard manufacturing and quality processes, and incorporates unique features not present in the current CFN retransfer printers.

Signicat acquires Norwegian digital ID firm, Idfy

Provider of verified digital identity solutions, Signicat, has announced the acquisition of Idfy, a provider of secure identification and electronic signature solutions. Idfy is one of the fastest growing players within digital trust services in the Nordics, according to the company. The Idfy platform allows companies and institutions to achieve efficient and compliant business processes across a wide range of use cases and security levels. In today's digital society interactions between consumers and institutions are predominantly online and mobile-first. Trust is at a premium, and digital identity is the solution. This creates an incredible opportunity for Signicat and Idfy, with McKinsey describing ID verification as a service as 'the next $20bn industry'. The acquisition enhances Signicat's reach and portfolio of services, and follows the acquisition of Signicat by Nordic Capital earlier in April this year. Idfy has more than 300 clients, with a strong presence in the fintech and real estate sector, with offices in Bergen and Oslo.

Canada–Netherlands biometric program announced for paperless travel

Vision-Box and partners have today signed an agreement to officially launch the Known Traveler Digital Identity service, which will facilitate paperless border clearance between Canada and The Netherlands. The program will allow travelers flying between the two countries to enjoy a seamless journey, whereby a simple face scan will be enough to identify the passengers boarding a plane at departure, and to clear immigration on arrival. They will not need to show their travel documents or go through any further checks. Partners of the initiative are The World Economic Forum and the Governments of Canada and The Netherlands, in collaboration with implementing partners Air Canada, KLM Royal Dutch Airlines, Amsterdam Airport Schiphol, Toronto Pearson International Airport, and Montréal-Trudeau International Airport, and technology partners Accenture and Vision-Box. The pilot will be based on the issuance of a digital identity – a Passenger Data Envelope – for each passenger prior to departure, including the self-service enrollment of their biometrics via a dedicated application. The identity is authenticated by the participating governments and then virtually travels between the two countries.

Idex Biometrics partners with Goldpac

A partnership between Idex Biometrics and Goldpac Group will see the launch of dual-interface biometric smart cards to customers in China and beyond. According to Idex, the market for biometric cards will ramp significantly during 2019 with a vast range of card integrators gearing up their efforts to commercialize biometric cards to provide simple, secure and personal authentication. Goldpace said Smart cards were the preferred means of authentication for billions of people. The partnership reflects the pursuit of innovative technologies for the company's payment products to make them a more secure and convenient means of payment.

HID Global to acquire De La Rue's ID business

Extending its capabilities in the government-to-citizen identification market, HID Global has signed an agreement to acquire the international identity solutions business of De La Rue. Through its identity solutions business, De La Rue delivers identity documents and software solutions for governments around the world. It issues secure identity documents for more than 25 countries, with significant market presence in Africa, Asia, Europe, Latin America and the Middle East. With complementary products, solutions and services that are highly synergistic with HID Global's current offerings, De La Rue's identity solutions business is a strategic fit, according to the company, providing solutions to government departments, working directly with ministries of the interior, immigration departments, police departments, and numerous other government entities and agencies.

eGates opening for Colombo airport

The Sri Lanka's Colombo Bandaranaike International Airport (BIA) is to introduce an eGate system to allow passengers to clear immigration quickly, according to the airport. Around four e-gate machines would be installed at the airport in addition to the existing counters where physical checks are conducted. These systems are expected to be introduced within the next three months and means passengers will have to scan their passport at the e-gate machine in order to pass through. Also the system will be linked to the Interpol database to assist in expediting the process of confirming a passenger's identity.

Polymath teams with Blockpass for blockchain-based digital ID

Security token platform Polymath has entered into a strategic collaboration with digital identity verification solution Blockpass for a streamlined identity verification solution. Through this partnership, Polymath, a decentralized platform that makes it easy to create and manage security tokens, aims to simplify user onboarding and cut down on the required resources in the process. Blockpass is a regtech and compliance platform which leverages blockchain technology and smart contracts and provides digital ID verification as a service. It is creating an ecosystem of pre-verified customers for easy and seamless customer onboarding for any regulated business and industry. Blockpass' KYC Connect products allows businesses to implement the right solution for their needs through the use of an API.

Kudelski and Idemia agree for IoT connectivity

A global partnership that provides manufacturers and service providers a single, fully-integrated solution to manage the network connectivity and security of cellular IoT devices has been announced between the Kudelski Group and Idemia. The two partners say as more companies of all sizes and sectors create new business models and operational efficiencies by connecting their devices, their success depends on their ability to ensure the security of the devices, data and access to both. Ericsson predicts that approximately 70% of all wide-area IoT devices will have cellular connections by 2022. The deal struck integrates Idemia's Dakota IoT (eUICC) and TSM (Trusted Service Management) solutions with the Kudelski IoT Security Platform. Dakota IoT is a secure hardware and operating system that allows device makers to remotely download mobile operator subscriptions to the connected objects deployed in the field and authorise them to use the network. The Kudelski IoT Security Platform provides device security (firmware lifecycle management), data security (transport- and application-level authentication and encryption), access management (token-based feature activation) and active security (monitoring and AI- based anomaly detection) to device manufacturers.

Amadeus pilots biometric boarding for Ljubljana airport

Identity firm Amadeus has said a successful pilot at Ljubljana Airport in Slovenia saw Amadeus take another step towards the creation of a common, centralized industry platform for biometrics. Working with Adria Airways, the airport's home carrier, and LOT Polish Airlines, the pilot saw average boarding times reduced by approximately 75% meaning boarding took just two seconds, rather than the typical five to ten seconds per passenger. The pilot saw passengers enrol using an Amadeus smartphone app that captured a 'selfie' alongside their passport photo and boarding pass, which were all stored securely on a remote server. A photo of the passenger was then captured at the boarding gate and matched against those stored on the server to validate the passenger's identity and flight status. Upon successful matching a message was conveyed to the Departure Control System and the passenger was able to board smoothly. All biometric data was deleted within 48 hours ensuring GDPR compliance.

Sinerix partners with Grey Matter for cloud ID

Cloud technology company Sinerix has signed a deal with channel partner Grey Matter to provide customers with electronic signature and biometric ID authentication software. Developed by Sinerix, the SecureSign platform provides an electronic signature and document exchange platform with built-in authentication and ID verification technology. According to Sinerix, this allows clients to securely manage all kinds of document signing and onboarding processes in just a few minutes. According to the company, Grey Matter has helped more than 4,000 customers to refine their digital infrastructure and modernise their business. Sinerix says its suite of modular software tools is aimed at businesses operating across sectors such as property, financial services, airports, legal, human resources, mortgage providers and security, that rely on safe document exchange, ID verification and a fast and secure onboarding process.

Fragmentation, unity or division? Where does Europe stand?

In the 1950s the original development of the EU was based on the premise of keeping peace in Europe through economic and political stability after two devastating world wars within 20 years of each other. Today there seems to be renewed sabre rattling among the anti-European factions. Should the world worry? The jury may still be out, but the case is definitely altered

It was the founding principle of international unity that would 'make war unthinkable and materially impossible', which led to the establishment of the EEC in 1958 and latterly, the EU, in 1992. Observers say those who are set on tearing down pillars, calling for devolved power and rewriting agreements citing over bureaucracy in Brussels and 'swarming immigration', have forgotten this and that there will be increasing threats to unity and a return to Visas or even visors. If predictions come to pass, there will be drones patrolling the skies above borders, avatars at checkpoints, more data breaches in cyberspace and new nationalistic protocols to unravel.

Following the EU elections in May, far-right parties formed a new group - Identity and Democracy (ID) - in the European Parliament, set on change. The group of 73 MEPs from far-right groups across Europe with Italy's Lega and France's Rassemblement National at its head, wants to devolve power back to EU member states, curb immigration and stop the spread of Islam. Replacing the Europe of Nations and Freedom group, the new ID group also includes far rightists from Germany, Austria, Belgium, Finland, the Czech Âepublic , Denmark and Estonia. Others including the UK Brexit Party and Spain's new Vox party have not signed up to join the ID group but remain a force with 29 MEPs collectively.

According to reports following the launch, the ID group's aims were to prevent the European Union from taking more powers from member states and to block any further harmonization that "undermines of the nation-state". On the other hand members denied the group wanted to destroy the EU – just that it needed to be "limited and reformed". Also, a main difference among the far-right groups in Europe appears to be their attitude towards Russia. The Italians and French reportedly enjoy close ties to Moscow, while Scandinavian and the Baltic parties see Russia as more of a threat.

In this regard, other adviser groups and watchdogs such as the European Council on Foreign Relations (ECFR), say while there are significant divides between the so-called 'anti-European parties' on substance, they could align with one another tactically in support of a range of ideas: from abolishing sanctions on Russia to blocking the EU's foreign trade agenda, to pulling the drawbridge up against migration. This, says the ECFR would put at risk Europe's capacity to defend its citizens from external threats at exactly the time when, given global turmoil, it needs to show more resolve, cooperation, and global leadership.

Yet others say the European Parliament is only one of the EU's governing bodies and, in many ways, the least powerful of them. In its legislative role, the institution cooperates with the Council of the EU (comprising national ministers from EU member states) and bases its work on proposals from the European Commission. So despite having the ability to pass resolutions on a wide range of subjects, the EP has no formal role in foreign policy

Migration

But, apart from providing opinions, the EP has been increasingly active in adopting non-binding resolutions on issues where it lacks a co-decision role – including most aspects of migration. For example, it adopted a resolution on 'the situation in the Mediterranean and the need for a holistic EU approach to migration'. Therefore, watchers say a major threat to the EU's migration policies stemming from the 2019 EP election could result in limiting the capacity of member states and the Council to seek a humanitarian and solidarity-based approach towards migration challenges – instead of securitizing the issue. As on the rule of law and free trade, this would limit the EU's credibility to contribute to the resolution of challenges in other regions of the world and at the global level. With Brexit, the EP election and the end of the current MFF coming in quick succession in 2019 and 2020, all this will soon

fall into the inheritance package of the new president of the Union following the departure of out going president Jean Claud Juncker who himself branded the far rightists as "populist, stupid nationalists who are in love with their own countries" and called for "solidarity with those who are in a worse situation".

Once the Council nominates a candidate for the president of the Commission with a qualified majority, he or she will inherit a landscape fraught with uncertainty – as will the new British Prime Minister in dealing with exiting the EU (or as some hopefuls say, not). But political pundits say if Boris Johnson gets the top job and he does not rule out a No Deal Brexit, the impact (if it happens) will be felt not only in the UK but across Europe - and inevitably fuel more division.

Borders and backstops

As with many of the world's issues surrounding border control, nations and even multinational companies companies are turning to ever more futuristic technologies in order to protect their physical and virtual borders.

In Europe, one of these immediate issues surrounds Britain's borders with questions surrounding the potential hard border in Northern Ireland following Brexit - and the supposed 'technology solutions' mooted by some politicians either still being developed or put under question.

One of these is a satellite system that registers mobile phones as they pass the border, while sensors buried in the ground or radars on flying drones could detect possible unlawful breaches of the boundaries.

Drone swarms

Earlier this year, it was revealed that the UK plans to pay the French £6m for drones, CCTV cameras and night-vision equipment to mount 24/7 surveillance of the North France coast in a new bid to prevent migrants crossing the Channel. Furthermore, it has been reported the European Union are funding a £7.7m project called Roborder, a swarm of autonomous, unmanned ground vehicles, submersibles and flying drones.

The project is made up of a consortium of police agencies, national institutes and private companies, with robotic designer Robotnik. The various drones are equipped with an array of sophisticated sensors, such as radar, emission sensors and thermal imaging, and will be able to patrol land, sea and air. The vehicles can work standalone or as part of a networked swarm, scanning for potential illegal activity --such as unauthorized border crossing, smuggling or even pollutant spills-- and beam back its findings to a manned control hub. Applications for Roborder have allegedly been touted around the Greek island of Kos and the Hungarian-Serbian border.

AI border guards

Another developments, IborderCtrl, is an automated deception detection system, funded by the EU and supported by companies such as European Dynamics and Hungarian biometric firm BioSec. The project has travellers pre-registering at home and asking questions posed by a digital border guard. The avatar will ask questions similar to a human border guard, but the software will use new artificial intelligence techniques --similar to emerging emotion detection technologies-- to ascertain if a subject is answering truthfully. The application will then offer a 'risk score' based on whether it believes its interviewee could be lying and will require a further interview by a human guard before passing over the border. Pilots for iBorderCtrl are being run in Latvia, Hungary and Greece.

According to Unysis, intelligence analysis produced by AI tools will be a great step forward for border security agencies and for our safety. These technology tools hold the possibility of detecting and deterring criminals and threats that have slipped across borders without fear for years. However, the public will support the

use of the tools only if they are assured their personal data and privacy are protected. So ensuring these programs and networks are impregnable must be among implementers first responsibilities, says the company.

Cyber frontiers

In the cyber world with privacy and data constantly under threat from breaches and attack, barriers need to come up rather than down. The past two years have seen cybersecurity turning into a high priority on the Brussels agenda. The Cybersecurity Act forms part of a set of measures across the board intended to promote more robust cybersecurity within the EU by establishing the first EU-wide cybersecurity certification framework across a broad range of products (e.g. the Internet of Things) and services.

The newly introduced European Cybersecurity Act aims to build a safer cyber environment through an EU-wide framework for businesses to achieve cybersecurity certification for their information and communications technology (ICT) products, processes and services. The Act works alongside both the EU General Data Protection Regulation, which requires security measures to be implemented when processing personal data; and the EU Network and Information Security Directive (NIS Directive), which aims to protect critical national infrastructure. In this the Cybersecurity Act encourages all businesses to invest more in cybersecurity and to build it into their ICT devices. Ultimately, the collective framework of legislation is designed to counteract cyber attacks and to raise consumers' and industry players' trust in ICT solutions.

Overall, dealing with divisions and threats rather than celebrating compromise and cooperation seem to be on the European agenda. It remains to be seen which way the world turns this time.

by Victor March

Defending against cyber attacks with cloud AI

Rapid adoption of cloud and SaaS services has transformed the digital business and fundamentally reshaped the challenge of defending the enterprise against advanced attacks. AI-based cloud technologies could combat this threat vector

Driven initially by the need to cut costs and increase efficiency, the transition to the cloud now serves as an essential conduit for digital transformation projects ñ from applying advanced analytics to big data sets, to supporting edge computing and devices that underlie everything from smart cities to connected cars. Yet from a security perspective, these new computing models are expanding the attack surface at an alarming rate, introducing new threat vectors across an increasingly dispersed corporate network.

This trend presents a special challenge for strained security teams, who must now cope with an environment where they have limited visibility and control, and where their familiar on-premise security tools are often not applicable. Additionally, the ease with which developers can spin up a cloud instance and bypass the IT or security team can expose the business to considerable risk, demanding a new DevSecOps approach which may be unfamiliar to teams who have grown up on the traditional on-premise network model. More generally, the security challenges presented by the cloud are largely governed by a Shared Responsibility Model, which delineates the respective areas of the cloud that providers and customers are expected to manage and secure.

While the customer's portion of the Shared Responsibility Model varies across IaaS and SaaS, the general thrust of the Model plainly illustrates that outsourcing certain IT processes to the cloud does not amount to outsourcing your security function altogether. Most organizations recognize this reality but few, if any, are satisfied with the cloud-specific security solutions available on the market, nor can they immediately pivot their teams to a DevSecOps approach as an alternative. While many IaaS and SaaS providers offer native security controls to help customers secure their own portion of the Shared Responsibility Model, these controls are often limited in scope and tend to be useful for compliance, rather than proactive and real-time cyber defense. Even within this limited scope, native security controls can only be effective if they have been adequately deployed by the cloud customer.

Cyber AI technology

Darktrace's cyber AI technology brings a fundamentally unique approach to real-time cyber defense in the cloud. Built on a foundation of unsupervised machine learning and AI, Darktrace Cloud analyzes rich data flows within and across cloud workloads and SaaS applications, learning a normal pattern of life for every user, device, and container. By correlating subtle deviations in behavior in real time, Darktrace Cloud can spot and stop the full range of cyber-threats in the cloud, from malicious insiders and external attacks, through to critical misconfigurations that can expose the business to high-impact compromise across the digital estate. The power of the technology lies in its self-learning approach, which does not rely on pre-defining benign or malicious behavior in advance. Instead, it models the normal behavior of users, containers, and devices in relation to their past, their peer group, and the wider organization, continuously revising its calculations in light of new evidence, and correlating weak indicators to establish an evolving measure of threat probability.

This approach is critical in this new age of cloud-based cyber-threat, where insiders with privileged access and external actors with admin credentials can sweep through an entire cloud infrastructure without setting off alarms. The cloud provider cannot (and should not) be expected to secure the cloud against trusted connections, while

third-party tools with anomaly detection capabilities can only do so in a blunt and flat-footed fashion. By relying on fixed learning periods and pre-defined notions of benign and malicious, these tools can only detect the most obvious threats.

Subtle deviations

In contrast, Darktrace's unsupervised machine learning and AI can go beyond what humans already know or can imagine, and detect subtle deviations that may point to a developing threat. Instead of relying on pre-defined rules and policies, the technology embraces the uncertainty inherent in today's complex digital environment. All significant deviations are seen and correlated, resulting in the detection of genuine threats, without producing floods of false positives. This cyber AI not only detects but can also autonomously respond to in-progress cyber-threats in the cloud. Darktrace Antigena, the platform's autonomous response capability, uses artificial intelligence to take targeted, measured action in response to high-confidence cyber-threats ñ stopping their spread in real time, and giving the security team time to catch up. The types of actions the capability can take vary depending on the specific cloud environment or SaaS application being used, as illustrated in the lists below which are not exhaustive nor definitive across all SaaS or cloud platforms. To neutralize in-progress attacks in cloud environments like AWS and Azure, it can terminate a virtual machine or edit its properties Edit S3 bucket permissions in AWS; temporarily disable a user's programmatic access; reset user passwords to disable management access Edit user permissions; temporarily stop sharing a document.

In SaaS applications like Office 365, Salesforce, G-Suite, and Box, Antigena can kill a user's active sessions. temporarily disable users Restrict or delete file sharing settings from certain files and folders; restrict a user from accessing certain parts of the cloud environment; suspend members from teams and hence their access to certain shared files (in Dropbox, for example).

Visibility and control

Most organizations migrating infrastructure and applications to the cloud struggle with migrating visibility and control along with it. Even security teams that properly configure and deploy native and third-party tools rarely have access to granular, real-time visibility to achieve continuous monitoring for interactive and contextualized threat investigations. To provide this visibility across the digital infrastructure, the solution's graphical Threat Visualizer interface provides a single pane of glass from which anomalous activity in cloud workloads, SaaS applications and elsewhere can be visualized and investigated in real time. The Threat Visualizer is designed for users of all maturity levels, from forensic security experts, to business executives and less experienced members of the IT team. A wealth of information can be variously queried and exposed using the interactive features within the Threat Visualizer, including a dynamic dashboard where users can filter incidents based on their level of severity, and an interactive Play-Back tool which lets users replay incidents and zero in on the real-time context around each event.

Technology deployment

For cloud, edge, and physical deployments, lightweight, host-based OS-Sensors are installed on each cloud endpoint and configured to send intelligent copies of network traffic to a local vSensor deployed in the same cloud environment. The receiving vSensor processes the data and feeds it back to the software in the enterprise, which correlates behavior across the organization's cloud and physical environments. AWS and Azure customers additionally have the option of using Connectors to monitor system administrator activity that may not be seen at the OS-Sensor level, such as logins, file changes or data transfers.

Cloud-Only (IaaS) For organizations that run their infrastructure exclusively in the cloud, Darktrace can manage the deployment as a dedicated service, installing vSensors and OS-Sensors in the organization's cloud environment and feeding data back to a managed cloud instance for analysis. For SaaS deployments, Connectors are remotely installed in the enterprise network and interact directly with the SaaS vendor's security API, via HTTPS requests. This allows user interactions to be processed and monitored within minutes of creation, whether they originate inside the network or from remote locations.

by Darktrace

Future-proofing against AI-led global cyber assaults: 2019 and beyond

As organizations develop their defense deployment plans in advance of coming cyber threats, there are a number of trends and activities most likely to affect their business and systems

In anticipating the major cyber security and privacy trends for the future, there are plenty of clues in the events of the past year. Among the now familiar forms of attack, cyber hacks of major corporate systems and websites continued in 2018 and will inevitably be part of the 2019 cyber security scene. Many well-known organizations around the world suffered significant breaches this year. The single largest potential data leak, affecting marketing and data aggregation firm Exactis, involved the exposure of a database that contained nearly 340 million personal information records.

Beyond all-too-common corporate attacks, 2018 saw accelerated threat activity across a diverse range of targets and victims. In the social networking realm, Facebook estimated that hackers stole user information from nearly 30 million people. A growing assortment of nation-states used cyber probes and attacks to access everything from corporate secrets to sensitive government and infrastructure systems. At the personal level, a breach into Under Armour's MyFitnessPal health tracker accounts resulted in the theft of private data from an estimated 150 million people.

So, what can be expected on the cyber security front in the coming months? Here are some of the trends and activities most likely to affect organizations, governments, and individuals in 2019 and beyond.

Using AI to aid assaults

The long-awaited commercial promise of AI has begun to materialize in recent years, with AI-powered systems already in use in many areas of business operations. Even as these systems helpfully automate manual tasks and enhance decision making and other human activities, they also emerge as promising attack targets, as many AI systems are home to massive amounts of data.

In addition, researchers have grown increasingly concerned about the susceptibility of these systems to malicious input that can corrupt their logic and affect their operations. The fragility of some AI technologies will become a growing concern in 2019. In some ways, the emergence of critical AI systems as attack targets will start to mirror the sequence seen 20 years ago with the internet, which rapidly drew the attention of cyber criminals and hackers, especially following the explosion of internet-based eCommerce.

Attackers will not just target AI systems, they will enlist AI techniques themselves to supercharge their own criminal activities. Automated systems powered by AI could probe networks and systems searching for undiscovered vulnerabilities that could be exploited. AI could also be used to make phishing and other social engineering attacks even more sophisticated by creating extremely realistic video and audio or well-crafted emails designed to fool targeted individuals – or be used to launch realistic disinformation campaigns. For example,

imagine a fake AI-created, realistic video of a company CEO announcing a large financial loss, a major security breach, or other major news. Widespread release of such a fake video could have a significant impact on the company before the true facts are understood.

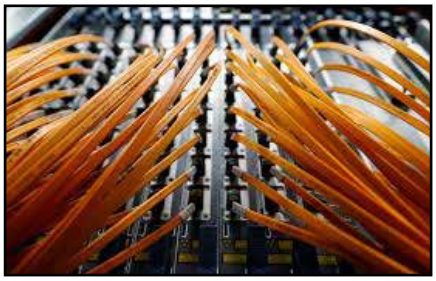
And just as we see attack toolkits available for sale online, making it relatively easy for attackers to generate new threats, it is predicited to eventually see AI-powered attack tools that can give even petty criminals the ability to launch sophisticated targeted attacks. With such tools automating the creation of highly personalized attacks–attacks that have been labor-intensive and costly in the past–such AI-powered toolkits could make the marginal cost of crafting each additional targeted attack essentially be zero.

Counter attacks

The AI security story also has a bright side. Threat identification systems already use machine learning techniques to identify entirely new threats. And, it is not just attackers that can use AI systems to probe for open vulnerabilities; defenders can use AI to better harden their environments from attacks. For example, AI-powered systems could launch a series of simulated attacks on an enterprise network over time in the hope that an attack iteration will stumble across a vulnerability that can be closed before it's discovered by attackers.

Closer to home, AI and other technologies are also likely to start helping individuals better protect their own digital security and privacy. AI could be embedded into mobile phones to help warn users if certain actions are risky. For example, when

AI can assist in home-based digital security and privacy - such as alerts indicating risk on phones or hacked routers



With a number of new infrastructure deployments, 2019 is looking to be a year of accelerating 5G activity

you set up a new email account your phone might automatically warn you to set up two-factor authentication. Over time, such security-based AI could also help people better understand the tradeoffs involved when they give up personal information in exchange for the use of an application or other ancillary benefit.

A number of 5G network infrastructure deployments kicked off this year, and 2019 is shaping up to be a year of accelerating 5G activity. While it will take time for 5G networks and 5G-capable phones and other devices to become broadly deployed, growth will occur rapidly. IDG, for example, calls 2019 'a seminal year' on the 5G front, and predicts that the market for 5G and 5G-related network infrastructure will grow from approximately $528 million in 2018 to $26 billion in 2022, exhibiting a compound annual growth rate of 118 percent.

Although smart phones are the focus of much 5G interest, the number of 5G-capable phones is likely to be limited in the coming year. As a stepping stone to broad deployment of 5G cellular networks, some carriers are offering fixed 5G mobile hotspots and 5G-equipped routers for homes. Given the peak data rate of 5G networks is 10 Gbps, compared to 4G's 1 Gbps, the shift to 5G will catalyze new operational models, new architectures, and–consequently–new vulnerabilities.

Over time, more 5G IoT devices will connect directly to the 5G network rather than via a Wi-Fi router. This trend will make those devices more vulnerable to direct attack. For home users, it will also make it more difficult to monitor all IoT devices since they bypass a central router. More broadly, the ability to back-up or transmit massive volumes of data easily to cloud-based storage will give attackers rich new targets to breach.

Danger of IoT-based events

In recent years, massive botnet-powered distributed denial of service (DDoS) attacks have exploited tens of thousands of infected IoT devices to send crippling volumes of traffic to victims' websites. Such attacks have not received much media attention of late, but they continue to occur and will remain threats in coming years. At the same time, we can expect to see poorly secured IoT devices targeted for other harmful purposes. Among the most troubling will be attacks against IoT devices that bridge the digital and physical worlds. Some of these IoT enabled objects are kinetic, such as cars and other vehicles, while others control critical systems. It is expected to see growing numbers of attacks against IoT devices that control critical infrastructure such as power distribution and communications networks. And as home-based IoT devices become more ubiquitous, there will likely be future attempts to weaponize them–say, by one nation shutting down home thermostats in an enemy state during a harsh winter.

Data in transit

It is likely attackers will also exploit home-based Wi-Fi routers and other poorly secured consumer IoT devices in new ways. One exploit already occurring is marshalling IoT devices to launch massive cryptojacking efforts to mine cryptocurrencies.

In 2019 and beyond, increasing attempts to gain access to home routers and other

A breach into MyFitnessPal health tracker accounts resulted in the theft of private data from around 150 million people

Threat identification systems already use machine learning techniques to identify entirely new vulnerabilities or attacks to systems such as supply chain software

IoT hubs to capture some of the data passing through them are expected. Malware inserted into such a router could, for example, steal banking credentials, capture credit card numbers, or display spoofed, malicious web pages to the user to compromise confidential information. Such sensitive data tends to be better secured when it is at rest today. For example, eCommerce merchants do not store credit card CVV numbers, making it more difficult for attackers to steal credit cards from eCommerce databases. Attackers will undoubtedly continue to evolve their techniques to steal consumer data when it is in transit.

On the enterprise side, there were numerous examples of data-in-transit compromises in 2018. The attack group Magecart stole credit card numbers and other sensitive consumer information on eCommerce sites by embedding malicious scripts either directly on targeted websites or by compromising third-party suppliers used by the site. Such 'formjacking' attacks have recently impacted the websites of numerous global companies.

In another attack targeting enterprise data in transit, the VPNFilter malware also infected a range of routers and network-attached storage devices, allowing it to steal credentials, alter network traffic, decrypt data and launch other malicious activities inside targeted organizations.

It is likely attackers will continue to focus on network-based enterprise attacks in 2019, as they provide unique visibility into a victim's operations and infrastructure.

Supply chain attacks

An increasingly common target of attackers is the software supply chain, with attackers implanting malware into otherwise legitimate software packages at its usual distribution location. Such attacks could occur during production at the software vendor or at a third-party supplier. The typical attack scenario involves the attacker replacing a legitimate software update with a malicious version in order to distribute it quickly and surreptitiously to intended targets. Any user receiving the software update will automatically have their computer infected, giving the attacker a foothold in their environment.

These types of attacks are increasing in volume and sophistication and we could see attempts to infect the hardware supply chain in the future. For example, an attacker could compromise or alter a chip or add source code to the firmware of the UEFI/BIOS before such components are shipped out to millions of computers. Such threats would be very difficult to remove, likely persisting even after an impacted computer is rebooted or the hard disk is reformatted. The bottom line is that attackers will continue to search for new and more sophisticated opportunities to infiltrate the supply chain of organizations they are targeting.

Legislative and regulatory activity

The European Union's implementation of the General Data Protection Regulation (GDPR) will likely prove to be just a precursor to various security and privacy initiatives in countries outside the European Union. Canada has already enforced GDPR-like legislation, and Brazil recently passed new privacy legislation similar to GDPR, due to enter into force in 2020. Singapore and India are consulting to adopt breach notification regimes, while Australia has already adopted different notification timelines compared to GDPR. Multiple other countries across the globe have adequacy or are negotiating GDPR adequacy. In the U.S., soon after GDPR arrived, California passed a privacy law considered to be the toughest in the United States to date. We anticipate the full impact of GDPR to become more clear across the globe during the coming year.

At the U.S. federal level, Congress is already wading deeper into security and privacy waters. Such legislation is likely to gain more traction and may materialize in the coming year. Inevitably, there will be a continued and increased focus on election system security as the U.S. 2020 presidential campaign gets underway.

While upticks in legislative and regulatory actions to address security and privacy needs are almost certain, there is a potential for some requirements to prove more counterproductive than helpful. For example, overly broad regulations might prohibit security companies from sharing even generic information in their efforts to identify and counter attacks. If poorly conceived, security and privacy regulations could create new vulnerabilities even as they close others.

by Dr. Hugh Thompson and Steve Trilling
Symantec

Secure MCU for e-banking and e-ID

ST microelectronics has introduced a secure microcontroller that includes a 13.56MHz RF interface for contactless operation and a serial interface for contact operation. Called ST31P450, it is built on a 40nm flash process and is aimed at contactless and contact applications in banking, identity, transportation and pay-television. The RF interface includes an RF UART for contactless comms up to 848kbit/s compatible with ISO/IEC 14443 Type A, and there is also a serial interface compatible with the ISO/IEC 7816-3. At its heart is a 55MHz dual-core 32bit Arm SecurCore SC000 which meets ISO 7816 and ISO 14443 Type A smart-card and contactless standards, according to ST, and versions are available to supports Mifare libraries including Classic, Plus and DESFire. SC000 is built on Cortex M0, with additional security features to help to protect against attacks.

Cyber security market predicted to top USD 181.77b by 2021

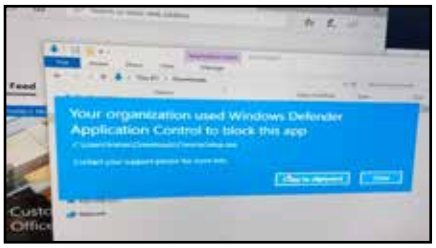
According to a report from Zion Market Research, the global cyber security market valued at USD 105.45 billion in 2015, is expected to reach USD 181.77 billion in 2021. Cyber security is associated with information technology security, which focuses on protecting computers and confidential data stored in it from cyber criminals. The cyber security market offers several advantages including enhanced security of cyberspaces, expanded digital safeguard and quicker reaction time to national crises. These advantages automatically enhance the value of service given to the market end-users. The Internet has given rise to new opportunities almost in every field such as business, sports, education or entertainment and many others. However, the internet has its own drawbacks like cyber crime, where the computer used for various types of thefts and crime. Various types of cyber crimes include hacking, software piracy, denial of service attack, and cyber terrorism. Governments, military, financial organizations, hospitals and several other industries gather and store or transmit a large amount of confidential data on computers. In order to protect this information or data cyber security becomes essential.

Lloyds Bank and Callsign partner to fight cyber crime

A deal between cyber security start-up, Callsign and Lloyds Banking Group is set to help the UK's biggest retail bank by customer numbers to comply with looming antifraud legislation. The lender will use Callsign to provide digital identification and authentication of online payments, as required by an EU directive that takes effect on September 19. The Second Payment Services Directive will require most online payments above Euro 30 to go through an extra level of verification such as entering a code received via a text message. Callsign's technology dispenses with passwords and instead uses multiple real-time data points to help ensure someone is who they say they are. Its software uses artificial intelligence to build a picture of the user and learn how they interact with mobile devices. If they were in an unfamiliar location or swipe in an unusual way, for example, it would trigger an alert. The software can blacklist devices involved in past fraud cases and can be used with other authentication programs.

IT giants release security updates

Microsoft and Oracle have issued security updates with the former patching a single issue in Windows Defender Application Control while Oracle's update covered over 100 products and dozens of vulnerabilities. The issue with Windows Defender, CVE-2019-1167, if exploited would allow an attacker to circumvent PowerShell Core Constrained Language Mode on the machine. However, Microsoft noted to be successful an attacker an attacker would need administrator access to the local machine where PowerShell is running in Constrained Language mode. The update corrects the problem. Oracle's latest critical patch update advisory covered 121 different products with each being associated with multiple CVEs.



Go ahead given for EU Cybersecurity Act

EU Regulation on ENISA (the European Union Agency for Network and Information Security) and on information and communications technology cyber security certification, also known as the Cybersecurity Act, has been passed and will come into force from the end of June 2019. Cyber attacks are becoming more and more sophisticated and most often occur across borders. There is a growing need for effective and coordinated responses and crisis management at the EU level. The Cybersecurity Act aims to build a safer cyber environment through an EU-wide framework for businesses to achieve cybersecurity certification for their information and communications technology (ICT) products, processes and services. ENISA will assume the key role of supervising and advancing cooperation and information sharing across EU member states, EU institutions and international organisations.

Transforming compliance through technology and AI

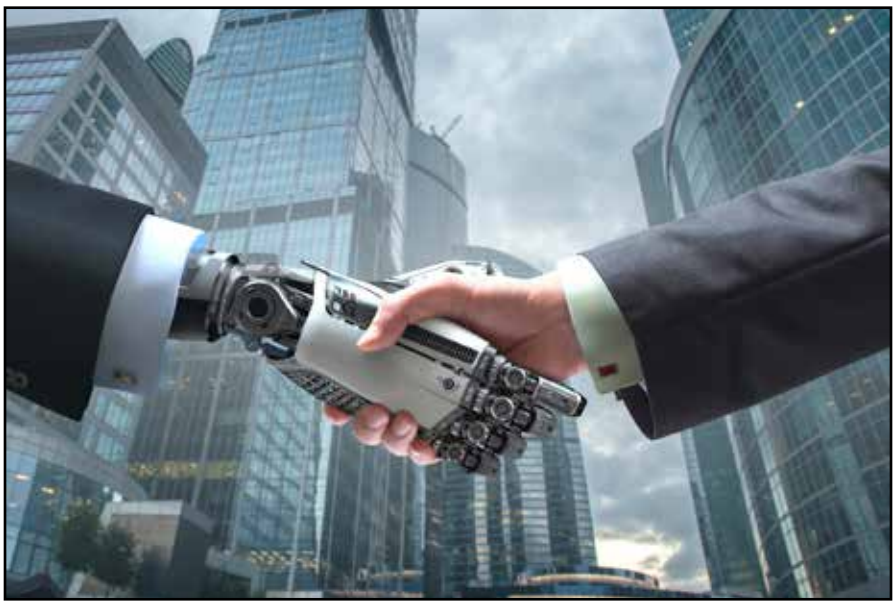
Financial institutions and regulators have realized that by harnessing the power of artificial intelligence (AI) and machine learning (ML) they can now automate compliance functions reducing the burden on compliance staff: regtech is on the rise

As a result of the significant increase in regulatory reporting requirements for financial institutions over the last decade, demand for compliance professionals has surged, but now technology has begun to play a much larger role here with a considerable proportion of the compliance function being automated.

In the UK, the Financial Conduct Authority (FCA) is a pioneer in the regulatory technology (regtech) space, and in collaboration with the Bank of England and a number of financial organisations, the UK regulator began its Digital Regulatory Reporting (DRR) project – a pilot programme designed to evaluate the benefits of machine-readable reporting, and explore how technology (currently RNN and semantic web) can make it easier for financial institutions to meet their regulatory requirements, by making reporting rules less reliant on human interpretation.

The overall aim of this project is to reduce the time and costs involved in interpreting and implementing new reporting requirements, and also reduce the number of individual regulatory reports that firms have to produce. To achieve this, the FCA has been looking at how a regulatory machine-readable framework can interact with a standardised language and be mapped to source data, and it is using semantic web technologies to identify the appropriate approach for the data specification.

Already, the FCA has proved that the concept works, and in a recent presentation, the regulator announced that it had successfully applied machine-reading technology to two different regulations, including one regulation based on capital requirements and another on mortgage lending criteria. Looking ahead,



the FCA plans to broaden the scope of the project in 2019 and apply the technology to a wider range of regulations, which is an exciting development for the industry.

The power of AI

The success of the DRR pilot programme highlights how compliance could potentially be transformed by technology and AI in the years ahead.

While regulatory technology has advanced in recent years, realistically, it's still in its infancy. Where we are situated with regulatory technology right now almost resembles the time that the first vehicles were invented and manufactured back in the early 20th century. Over the next decade, technological advances could completely overhaul compliance as we currently know it, making life considerable easier for financial organisations.

If there's one specific area of technology that has the ability to make a huge impact on compliance, it's AI. It's the latest technology to play a key part in the digital transformation of the financial services industry and the possibilities within compliance and many other industries, going forward, are almost limitless.

Essentially, AI is a series of underlying technologies such as natural language processing, computer vision and ML, that can be brought together within a cloud-based environment to store and process huge amounts of data so that machines can perform sophisticated tasks, without the assistance of humans. Accenture defines AI as a broad term that encompasses a wide range of functions, from simple rules-based algorithms through to natural language processing (NLP) based on deep learning. While AI is not a new area of technology – it has been developed since the 1950s – the technology has advanced significantly in recent years, and newer algo-

rithms are now able to process vast amounts of data and closely imitate human thought processes. As a result, there are now some very interesting AI/ML projects going on in the compliance field, with analysts looking at how AI can solve real-world compliance issues. However, like any other technology, the implementation of AI within the regulatory space needs to be managed carefully.

AI and semantics

One topic that is linked closely to AI is 'semantics', which refers to the meaning of language. In the past, there has been much discussion within the technology world about the possibility of building a "semantic web". This would be similar to the current world wide web but the key difference would be that it would be structured in such a way that data and information could be easily processed by machines. In other words, web pages would be structured and tagged in a way that computers would be able to read them.

The semantic web idea definitely makes sense, however, there have been difficulties in getting it set up. For example, humans were expected to be involved in creating the structured data, and this has made the process time consuming, expensive, and not easy to scale. A paper written by Butler in 2016 suggested completing the semantic system with "knowledge engineers", however, this would still create complications, as the growth of data volumes would most likely outpace the speed of the engineers' effectiveness.
One positive development in this space, however, is the shift towards AI-based cognitive computing systems. The application of AI-based systems could significantly reduce the costs of constructing semantic web systems as it would eliminate the manual work weak point. By using structured data that applies AI-based algorithms, efficiency could be increased significantly.

It is likely that there will be plenty of developments in the years ahead in relation to AI and semantics within compliance, and this could help make banks and other financial institutions far more transparent and manageable for regulators. The work that regulators are currently carrying out in this sphere – with the FCA pioneering the way – is encouraging. With more data becoming available through RDF-based endpoints, regtech will become significantly more effective as it will be able to consume and analyse structured data coming from the regulators.

Embracing technology

ClauseMatch, has embraced technologies such as AI, and has gained experience in semantic-based algorithms. Already, with the help of data scientists and machine-learning experts, they have have developed and tested a system that can identify and compare regulatory paragraphs and grade their relevance to each other based on semantics.

Recently, Clausematch tested its work on the concept of 'whistle-blowing' and the results were quite impressive – significantly outperforming traditional statistical-based approaches. Even when paragraphs had absolutely no words in common but simply discussed the same topics, our system managed to detect relationships, since the machine learned to represent text in a semantic multidimensional space, where phrases such as 'whistle blower' and 'anonymous report' were close to each other. That vector based representation is now playing the key role as a foundation for a deep learning sense extraction solution.

The FCA is implementing regulatory machine-readable framework to source data

Humans vs machines in compliance

Technology will impact many industries in the years ahead, and in some industries, the technology story is about replacing people. Yet while technology is having a profound impact on the compliance industry, the story for compliance is not only about machines. Compliance is a unique industry, and when it comes to implementing technology, it's more about augmenting people. With compliance, it is not about humans versus machines, as both have a vital role to play. The key is to find the right balance between the two and get humans working with machines. The biggest gains are likely to come from the two working well together.

It is important to realise that AI is not a panacea or a magic bullet. Instead, it is a technology that can be leveraged to boost efficiency and improve the culture within an organisation, and better protect consumers on the outside. It should not be forgotten that compliance is about responsibility and ethics, which come naturally to humans. Compliance is evolving at a rapid pace. And that is a good thing.

A decade from now, what is most likely is a three-level compliance structure with humans at the top, AI technology at the bottom, and an automated decision support system in the middle, providing a 360-degree view into the firm's current state of compliance.

At the lower level, AI will assist compliance professionals by offering various solutions to a problem, but it will not make the decisions completely by itself. AI will prompt humans with the right decisions, enabling compliance professionals to do their jobs more efficiently, and with more accuracy.

by Vladimir Ershov and
Anastasia Dokuchaeva,
ClauseMatch

Governing the real world of AI for social economies

Artificial intelligence has become a real-world application technology. It is part of the fabric of modern life. Harnessed appropriately, Google believes AI can deliver great benefits for economies and society

A promise that AI can support decision-making which is fairer, safer and more inclusive and informed will not be realized without great care and effort. This includes consideration of how its development and usage should be governed, and what degree of legal and ethical oversight — by whom, and when — is needed.

To date, self- and co-regulatory approaches informed by current laws and perspectives from companies, academia, and associated technical bodies have been largely successful at curbing inopportune AI use. In the vast majority of instances such approaches will continue to suffice, within the constraints provided by existing governance mechanisms (e.g., sector-specific regulatory bodies). However, this does not mean that there is no need for action by government. To the contrary, governments and civil society groups worldwide need to make a substantive contribution to the AI governance discussion.

Specifically, there are five areas where government, in collaboration with wider civil society and AI practitioners, has a crucial role to play in clarifying expectations about AI's application on a context-specific basis. These include explainability standards, approaches to appraising fairness, safety considerations, requirements for human-AI collaboration and general liability frameworks.

As AI technology evolves and Google's own experience with it grows, the internet giant expects that the global community as a whole will continue to learn and additional nuances will emerge, including a fuller understanding of the trade-offs and potential unintended consequences that difficult choices entail. An observation is that so far much of the current AI governance debate among policymakers has been high level. The 'rules of the road' for AI (be they in the form of laws or norms) will need to evolve over time to reflect thoughtful and informed consideration of economic and social priorities and attitudes, as well as keeping pace with what is possible technologically.

Clarifying expectations

Explainability standards questions can be addressed by assembling a collection of best practice explanations along with commentary on their praiseworthy characteristics to provide practical inspiration. Providing guidelines for hypothetical use cases will allow industry to calibrate how to balance the benefits of using complex AI systems against the practical constraints that different standards of explainability impose. It is also important to describe minimum acceptable standards in different industry sectors and application contexts.

Fairness appraisal will articulate frameworks to balance competing goals and definitions of fairness and clarify the relative prioritization of competing factors in some common hypothetical situations, even if this will likely differ across cultures and geographies.

Safety considerations pose another crucial area for collaboration. Here it will be important to: outline basic workflows and standards of documentation for specific application contexts that are sufficient to show due diligence in carrying out safety checks; establish safety certification marks to signify that a service has been assessed as passing specified tests for critical applications. In the sphere of human-AI collaboration, goals set need to: determine contexts when decision-making should not be fully automated by an AI system, but rather would require a meaningful 'human in the loop'; and assess different approaches to enabling human review and supervision of AI systems.

Finally, liability frameworks can: evaluate potential weaknesses in existing liability rules and explore complementary rules for specific high-risk applications; consider sector-specific safe harbor frameworks and liability caps in domains where there is a worry that liability laws may otherwise discourage societally beneficial innovation; and explore insurance alternatives for settings in which traditional liability rules are inadequate or unworkable.

Transforming processes

AI is a powerful, multi-purpose technology with the potential to transform industrial and societal processes alike. Governments thus have an important role to play in collaboration with industry and other stakeholders to ensure good outcomes. While AI researchers, developers, and industry can lay the groundwork for what is technically feasible, it is ultimately up to government and civil society to determine the frameworks within which AI systems are developed and deployed.

It is important to note that this effort is not starting from scratch. There are already many sectoral regulations and legal codes that are broad enough to apply to AI, and established judicial processes for resolving disputes. For instance, AI applications relating to healthcare fall within the remit of medical and health regulators, and are bound by existing rules associated with medical devices, research ethics, and the like. When integrated into physical products or services, AI systems are covered by existing rules associated with product liability and negligence.

Human rights laws, such as those relating to privacy and equality, can serve as a starting point in addressing disputes. And of course there are a myriad of other general laws relating to copyright, telecommunications, and so on that are technology-neutral in their framing and thus apply to AI applications. Given the early stage of AI development, it is important to focus on laws and norms that retain flexibility as new possibilities and problems emerge. This is particularly crucial given that AI, like many technologies, is multi-purpose in nature.

Overall Google is confident that existing governance structures will prove to be sufficient in the vast majority of instances. In the rare cases where they are not, it is likely that sectoral experts in industry and academia together with practitioners at the forefront of AI application are largely well placed to help identify emerging risks and take steps to mitigate them, in consultation with civil society and government. This multi-stakeholder collaborative approach will allow for the most timely and effective response to concerns about AI without impeding its promise.

Setting international standards and norms would relieve pressure on individual countries and regions to advance a controversial use of technology just because others might be doing so, preventing a race to the bottom. While international treaties cannot in themselves prevent violations, they clarify shared expectations of behavior and thus serve as a metric against which sanctions can be imposed for misuse. Such rules would also acknowledge that the impact of AI transcends borders, setting a level playing field within industry and raising the bar for responsible use.

Governance

AI poses a unique challenge both in formulating and enforcing regulations and norms. There is simply a growing sense that the time has come for a more cohesive approach to AI oversight. Given the open research culture in the AI field, increasing availability of functional building blocks (e.g., machine learning models for image recognition, speech-to-text, translation; processing hardware), and the usefulness of AI to many applications, AI technology is spreading rapidly. If the world waits too long to establish international governance frameworks, we are likely to end up with a global patchwork that would slow the pace of AI development while also risking a race to the bottom. A self-regulatory or co-regulatory set of international governance norms that could be applied flexibly and adaptively would enable policy safeguards while preserving the space for continued beneficial innovation.

AI in healthcare is associated with medical devices, research ethics and similar

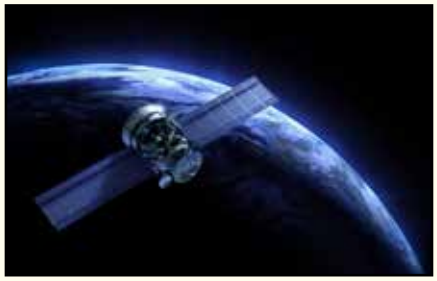
Regulatory approaches

Overall, Google believes the optimal governance regime is one that is flexible and able to keep pace with developments, while respecting cultural differences. It expects self- and co-regulatory approaches will remain the most effective practical way to address and prevent AI related problems in the vast majority of instances, within the boundaries already set by sector-specific regulation. However, Google recognizes that there are some instances where additional rules would be of benefit, and is set to engaging with governments, industry practitioners, and civil society on these topics.

by Google

China to launch AI-powered satellites constellation

A 192-strong constellation of AI-powered satellites, 'Xingshidai', is planned for launch by China, according to reports. The country intends to use the satellites for environmental monitoring, disaster prevention and traffic management as AI will help to process images to avoid sending poor quality pictures back to Earth. Xingshidai satellites will likely use China's Julang-1 booster rockets to reach orbit. Julang-1 can put satellites weighing up to 150kg into orbit at an altitude of 600 kilometres. China's aerospace industry is reportedly growing fast. In January, the nation reported successfully landing a spacecraft on the far side of the Moon. Last month, China successfully launched its Chang Zheng 11 carrier rocket with seven spacecraft on board from a floating launch platform. Next year, the country plans to launch its Mars Global Remote Sensing Orbiter and Small Rover. The application of AI to China's aerospace initiatives has enormous potential. Xingshidai's satellites are being developed by ADASpace, a private Chinese company based in Chengdu.



Samsung Electronics to strengthen neural processing

Plans to expand the reach of artificial intelligence (AI) solutions to fortify the capabilities of neural processing unit (NPU) have been announced by Samsung Electronics. The company will also extend its existing collaboration with globally distinguished research institutes and varsities and support the development of future talent in the AI domain, including deep learning and neural processing. Samsung first introduced the NPU in the Exynos 9820, which is the company's premium mobile processor, in 2018 and plans to continue offering the advanced on-device AI features for high-performance mobile chips. The NPU applications will be further expanding into the automotive industry wherein it will power in-vehicle infotainment (IVI) and advanced driver assistance systems (ADAS), as well as next-generation data centers optimized for big data processing. Samsung's R&D unit – the System LSI Business and Samsung Advanced Institute of Technology – will also work together with the company to extend and evolve the company's present research on NPU into AI hardware technologies, such as neuromorphic processors that will mimic a human brain.

Twitter to tackle fake news using AI

Fabula AI, a UK-based startup employing artificial intelligence for tackling fake news, has been acquired by Twitter. Fake news is among the most difficult challenges of our time. Aside from real stories often being called it by certain politicians, actual fake news is used to coerce people into making decisions. Governments have been putting increasing pressure on sites like Twitter and Facebook to take more responsibility for the content shared on them. With billions of users, each uploading content, manual moderation of it all is not feasible. Automation is increasingly being used to flag problem content before a human moderator checks it. Twitter says its acquisition of Fabula is to improve the health of the conversation, with expanding applications to stop spam and abuse and other strategic priorities in the future. Fabula has developed the ability to analyze large and complex data sets for signs of network manipulation and can identify patterns that other machine-learning techniques cannot. In addition, Fabula has created a truth-risk score to identify misinformation. The score is generated using data from trust fact-checking sources like PolitiFact and Snopes. Armed with the score, Twitter can determine how trustworthy a claim is and perhaps even make it visible to others.

Volvo and Nvidia to partner for self-drive vehicles

A collaboration on AI technology for self-driving vehicle has been announced between Volvo and Nvidia. The deal with Volvo means Nvidia and its AI technology for self-driving cars will now be further developed. Nvidia debuted its 'Xavier' processors for the company's drive autonomous car platform last year. Xavier was in development for over four years, represents the work of over 2,000 engineers, features more than nine billion transistors, and the company claims it is the most complex system-on-a-chip (SoC) ever created. As a maker of powerful GPUs, traditionally for gaming purposes, the company has been increasingly shifting gears into other computation-heavy areas like AI and machine learning.

Danish government injects €200m into AI R&D

Denmark is investing in a range of programs to boost research and development into artificial intelligence and its place in various business sectors, according to AI news. The Danish government is investing more than €200m in digital and artificial intelligence (AI) research and pilot projects. A significant part of the funding is earmarked for ventures that will focus on using AI and digitization technologies to cut costs in mainstream industry sectors such as transportation, energy, construction, and the delivery of healthcare services. The spending programme follows the launch of the Danish government's National Strategy for Artificial Intelligence (NSAI) earlier this year. In Denmark, sectors such as healthcare, energy, transport, construction and agriculture have all been identified as having potential to gain significantly from elevated use of AI and digital technologies.

Major increases in AI, IIoT and ML forecast for next 5 years

Research and Markets have announced rising trends Artificial Intelligence, Industrial IoT and Smart Machines in Enterprise and Industrial Automation in a 2019 - 2024 report. Key findings predict that by 2024 embedded AI in support of IIoT smart objects will reach $4.6B globally, while the hybrid voice and text chatbots market will reach $331.5M USD globally. Researchers say the overall market for AI in big data and IoT will be led by Asia Pac followed by North America and the fastest growing smart machine technology area Neuro-computing, will grow at 22.2% CAGR. In addition, AI in industrial machines is expected to reach $415M globally by 2024 with collaborative robot growth at 42.5% CAGR. In further predicted developments, smart machines and systems will benefit greatly from low latency and localized processing via 5G and MEC. AI algorithms enhance the ability for big data analytics and IoT platforms to provide value to each of these market segments. The report sees three different types of IoT Data: Raw (untouched and unstructured) Data, Meta (data about data), and Transformed (valued-added data). AI will be useful in support of managing each of these data types in terms of identifying, categorizing, and decision making. AI coupled with advanced big data analytics provides the ability to make raw data meaningful and useful as information for decision-making purposes. The use of AI for decision making in IoT and data analytics will be crucial for efficient and effective decision making, especially in the area of streaming data and real-time analytics associated with edge computing networks. Industrial Internet of Things (IIoT) solutions are poised to transform many industry verticals including healthcare, retail, automotive, and transport. For many industries, IIoT will significantly improve reliability, production, and customer satisfaction. While IIoT will initially improve existing processes and augmented current infrastructure, the ultimate goal will be to realize entirely new, and dramatically improved products and services. Smart machines collectively represent intelligent devices, machinery, equipment, and embedded automation software that perform repetitive tasks and solve complex problem autonomously. Along with Artificial Intelligence, IoT connectivity, and M2M communications, smart machines are a key component of smart systems, which include many emerging technologies such as smart dust, neuro computing, and advanced robotics. The drivers for enterprise and industrial adoption of smart machines include improvements in the smart workplace, smart data discovery, cognitive automation and more. Currently conceived smart machine products include autonomous robots (such as service robots), self-driving vehicles, expert systems (such as medical decision support systems), medical robots, intelligent assistants (such as automated online assistants), virtual private assistants (Siri, Google Assistant, Amazon Alexa, etc.), embedded software systems (such as machine monitoring and control systems), neurocomputers (such as purpose-built intelligent machines), and smart wearable devices.

Geisinger AI to target high risk patients

In a move to identify patients at high risk from chronic diseases and provide preventive care, Geisinger will use artificial intelligence (AI) solutions for early detection and prevention of high-burden disease. The technology will allow for better population health management in Geisinger's health system. The company's partnership with Medial EarlySign aims to develop and deploy a suite of machine learning-based solutions to identify individuals at risk for lower gastrointestinal (GI) disorders associated with chronic occult bleeding. The software uses machine learning techniques to analyze medical and electronic health data that is collected as a part of routine care. Patients on a high-risk trajectory are identified through routine lab results (e.g., blood tests) and other early signs of risk.

Autonomous vehicle start-ups snapped up by major players

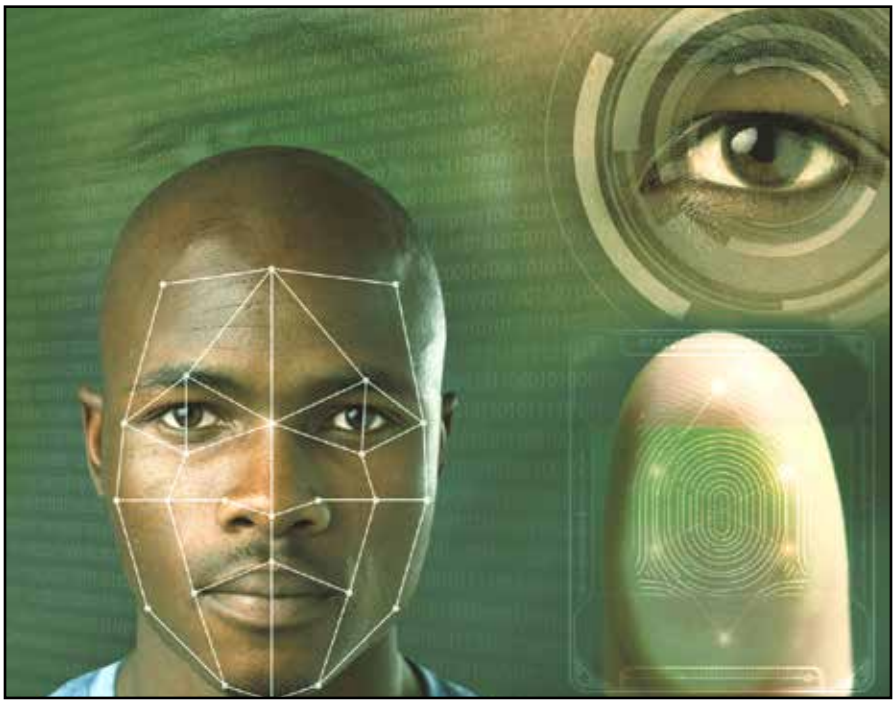
Apple announced it has bought the autonomous vehicle start-up Drive.ai, adding its engineers to the its own self-driving project. Autonomous transportation is one of Apple's biggest research and development efforts, but reports say the company has kept a tight lid on its secretive Project Titan over the nearly five years it has been in existence. It has more than 1,000 people working on the project but recently cut more than 200 jobs. Apple has permits to test dozens of vehicles in California. Drive.ai has been piloting an autonomous shuttle service in Texas. Meanwhile, Uber said it has acquired Mighty AI, a start-up that provides training data for the computer vision models that propel or drive autonomous cars.

Mentor introduces AI/ML toolkit to speed smarter ICs

New software from Siemens business, Mentor, is suing an artificial intelligence/machine learning (AI/ML) development kit and added AI/ML enhancements to two tools to help its customers deliver smarter, AI/ML-powered ICs to market faster. The new Catapult software High-Level Synthesis (HLS) AI Toolkit and HLS ecosystem are designed to help customers jumpstart the development of complex machine learning IC architectures. Meanwhile, Mentor has also announced it is adding AI/ML infrastructure throughout the Calibre platform, and is launching the first two of these AI/ML-powered technologies: Calibre Machine Learning OPC (mlOPC) and Calibre LFD with Machine Learning – both of which leverage machine learning software for faster, more accurate results. These new offerings further expand Mentor's fast-growing portfolio of AI/ML-powered solutions. Last year, Mentor acquired Solido, a pioneer in AI/ML-enhanced EDA tools. Mentor's new Catapult HLS AI Toolkit is designed to help customers developing AI/ML-based accelerators for edge applications get to market faster.

Digitizing Africa for remote government e-services

As the digital world develops, the use of citizen IDs is changing from being used just for physical controls and authenticating documents to wider requirements, such as access to remote services or eServices particularly in the developing world, taking lessons from Europe



EServices are fast becoming a driver of development for sovereign states. Developing countries, such as those across the African continent are learning from the experiences of their European partners when deploying their own modern eServices programs. Traditional services web sites, in which only descriptive information is available, do not allow any on-line transactions. In contrast, eServices provide on-line services enabling internet-based transactions to be managed directly. The three main components of eServices are the service provider, the service recipient and the means of service supply (i.e. the technology). Generally speaking, there are two types of eServices - government eServices or eAdministration, which are offered by a state to its citizens, foreign visitors/residents, or to legal entities such as companies; and private eServices provided by companies and intended for private individuals or legal entities.

The development of eServices offers a number of advantages to a State, such as quicker deployment of its services, reduced operating costs related to the completion of on-line transactions as opposed to manual transactions and reduced fraud related to improved security of transactions. There are also many benefits for citizens and companies, thanks to the set-up of an administration that is more efficient, more easily contactable thereby saving time, and that provides easier access to services. Access to eServices may also present some challenges related to the low penetration of information technologies and communications in certain countries, Internet-based fraud and privacy protection issues, due to the appearance of various types of spy software and security breaches.

The primary driver in the success of eServices is political will - the level of coordination and involvement of governments in integrating governmental services to change their own institutions and develop cooperation between the various authorities in order to meet the requirements of society more effectively. The role of the government can go from that of services regulator (in finances, telecommunications, education, health or a sub-set of these) to one of active coordinator in the deployment of services.

Right combination

Feedback shows that the use of a single document as the key to access governmental or private eServices generally tends to meet with limited uptake by citizens. A digital identity, derived from the core identity contained in the ID document and integrated in mobile devices (PC, tablet, mobile phone, etc.), is the proposal that has met with the most success in Europe: the inclusion of the digital identity in an identification system becomes an essential facilitator, enabling the uptake of eServices by citizens. Of the various identity management systems available, those based on the decentralization of identities offer the greatest security and are most trusted by citizens. In fact, several hundred million new documents are produced each year, without any major attack suffered to date.

The digital identity card, the electronic identification means, contains the core identity of the citizen. Citizens manage the confidentiality of their data and the generation of derived identities in various potential formats through their card:

- pseudonym (anonymization)
- with partial attributes (e.g. over 18 years old)
- full ID where the citizen takes back control of his/her attribute data and his/ her identities with no central database.

Derived identities are directly generated using the digital identity card. This decentralized management of core identities is based on the concept of 'privacy by design'. In contrast, centralized systems have been targeted by identity theft attacks, which has led to mistrust among citizens: Yahoo – 2013-14: 3 billion user accounts; eBay – May 2014: 145 million users; Uber – end of 2016: 57 million users; Sony – 20 April 2011 – 77 million users; Equifax - September 2017 - 147 million customers.

Furthermore, centralized systems are increasingly targeted by system attacks or shutdowns (denial of service attacks) and in the future, quantum computers are likely to become another means of attacking centralized databases.

Regional ID systems in Africa

There are various levels of security for digital identity. One of the main issues involved in digital identity is the level of certainty that you can have about a digital identity: how confident can we be that the person using the identity is really who they say they claim to be? It is in the digital space that each citizen is most exposed to cybercrime, regardless of their proximity to digital practices.

Each new internet service potentially requires a new identity: a citizen may need to manage many digital identities enabling him/her to access these services, in addition to their own personal identity. The increasingly widespread use of digital identity solutions, a crucial defense against digital crime, is now a priority matter. Secure digital identity is beginning to become a true reality for the majority of states. The security level of a digital identity depends on the entire life cycle management process of this identity: from creation until expiry.

Citizens manage the confidentiality of their data in various potential formats

Three assurance levels for electronic identification means are set out in the regulation:

- low level: the electronic identification means utilises at least one authentication factor. The electronic identification means is designed so that the issuer takes reasonable steps to check that it is used only under the control or possession of the person to whom it belongs.
- substantial level: the electronic identification means utilises at least two authentication factors from different categories. The electronic identification means is designed so that it can be assumed to be used only if under the control or possession of the person to whom it belongs.
- high level: the electronic identification means protects against duplication and tampering as well as against attackers

The electronic identification means is designed so that it can be reliably protected by the person to whom it belongs against use by others. Give priority to the inclusion of citizens and system interoperability (e.g. France Connect in France)

Studies are currently underway in France regarding the reference identity ('high' level digital identity) that may be protected in a digital identity card. If this system is chosen, it is expected to enable its use by third-party operators to create and manage a 'substantial' level digital identity. These operators are identity providers (IP) according to the ecosystem defined by France Connect, a 'Platform State' program. The establishment of a national digital identity ecosystem based on IPs is important for ensuring freedom of choice for users; maintaining a simple and practical servic; ensuring the interoperability; providing full compliance with the eIDAS system; monitoring market evolutions and ensuring the appropriate balance between the various parties.

Inclusion

The ways in which identity is used are changing, from simple identity checks to the inclusion of services. The first deployments in Europe show that the inclusion of digital identities is a key factor in the inclusion and therefore uptake of eServices. The needs for simplified use and security drive the creation of derived identities (composed of part or all of the attribute data making up the citizen identity), based on the citizen's core identity contained in their national ID card.

The complementary nature as regards utilization and security between the digital identity card and its various mobile derived identities enables the best value proposal to be offered to citizens. Simplification: the citizen takes control of his/her data and his/her identities: He/she controls the data that he/ she wishes to share and make visible in each of his/her digital identities. Security: the centralization of identities in a database may be targeted by identity theft attacks, shutdowns of the central system containing the identities and in the future, attacks from quantum computers. The decentralization of identities provides the highest possible level of security.

African countries are taking tips from Europe for their eServices deployment programs

by IN Groupe

Achieving inclusive growth through 'good' digital ID

According to a recent study, digital identification provides a significant opportunity for value creation for individuals and institutions. But what are the real and inclusive economic gains?

Nearly one billion people globally lack a legally recognized form of identification, according to the World Bank ID4D database. The remaining 6.6 billion people have some form of identification, but over half cannot use it effectively in today's digital ecosystems. Individuals can use digital ID to be verified unambiguously through a digital channel, unlocking access to banking, government benefits, education, and many other critical services. Programs employing this relatively new technology have had mixed success to date—many have failed to attain even modest levels of usage, while a few have achieved large-scale implementation.

Yet well-designed digital ID not only enables civic and social empowerment, but also makes possible real and inclusive economic gains—a less well understood aspect of the technology. The political risks and benefits of digital ID are potentially significant and deserve careful attention but are beyond the scope of this report. The McKinsey Institute has developed a framework to understand the potential economic impact of digital ID, informed by an analysis of nearly 100 ways in which digital ID can be used, with deep dives into seven diverse economies: Brazil, China, Ethiopia, India, Nigeria, the United Kingdom, and the United States.

Creating value

Digital ID is a foundational set of enabling technologies that can be pivotal in a wide range of digital interactions between individuals and institutions. Digital ID technologies are also akin to 'dual use' technologies that can be employed both to benefit society and for undesirable purposes by governments and other institutions, as well as individual actors. The research focuses on how good use of digital ID can create value and societal benefit, while being clear-eyed about the possibility of misuse and associated risks and challenges, and the need to mitigate them.

The technology enables individuals to unlock value and benefit as they interact with firms, governments, and other individuals in six roles: as consumers, workers, microenterprises, taxpayers and beneficiaries, civically engaged individuals, and owners. Individuals benefit most as consumers from wider access to services, and as taxpayers and beneficiaries from time saved interacting with government. For example, digital ID could contribute to providing access to financial services for the 1.7 billion plus individuals who are currently financially excluded, according to the World Bank ID4D Findex survey, and could help save about 110 billion hours through streamlined e-government services, including social protection and direct benefit transfers. For institutions, gains could come from higher productivity, cost savings, and fraud reduction; for example, improving customer registration could reduce onboarding costs by up to 90 percent, and reducing payroll fraud could save up to $1.6 trillion globally. F

In the seven focus countries, researchers found extending full digital ID coverage could unlock economic value equivalent to 3 to 13 percent of GDP in 2030—if the digital ID program enables multiple high-value use cases and attains high levels of usage. The potential varies by country based on the portion of the economy with bottlenecks that digital ID can address as well as the scope for improvement in formalization, inclusion, and digitization over current levels. The estimates include the full value from use cases of digital ID, assuming high levels of adoption by 2030, the necessary digital infrastructure and ecosystems to enable usage, and complementary investments required.

Economies and policies

For emerging economies, while the share of the economy that digital ID can address tends to be modest, scope for improvement can be sizable, leading to average potential per-country benefit of roughly 6 percent of GDP in 2030,

based on our modeling. Much of this value can be captured through digital ID with authentication alone. For mature economies, many processes are already digital, so the potential for improvement is more limited and largely requires digital ID programs that enable additional data-sharing features. Average per-country benefit of 3 percent could be possible, assuming high usage rates.

Just over half of the potential economic value of digital ID could accrue to individuals, making it a powerful key to inclusive growth, while the rest could flow to private-sector and government institutions. Beyond quantifiable economic benefits, digital ID can offer non-economic value to individuals through social and political inclusion, rights protection, and transparency. For example, robust identity programs can help guard against child marriage, slavery, and human trafficking.

Capturing the value of good digital ID is by no means certain or automatic. Careful system design and well-considered government policies are required to promote uptake, mitigate risks like those associated with large-scale capture of personal data or systematic exclusion, and guard against the challenges of digital ID as a potential dual-use technology. User adoption of digital ID will be accelerated if it provides value, engenders trust, and protects privacy. Institutions will be drawn to digital ID uses that lower costs, improve customer experience, or, in the case of public institutions, improve welfare. The right digital ID technology, designed with the right principles and enforced with the right policies, can protect individuals from the risk of abuse and enable the safe inclusion of billions in the digital economy. As the landscape evolves, more work will be needed to understand the opportunities and commensurate challenges and to comprehend how stakeholders can respond.

Legal identification

It is easy to take identification for granted, particularly in mature economies. However, close to one billion people in the world have no form of legal identification and may be denied access to critical government and economic services. The rest of the world's inhabitants, about 6.6 billion people, either have some form of identification but limited access to the digital world, or are active online but face growing complexity that makes it hard to keep track of their digital footprint securely and efficiently. Digital ID could help all three groups verify their identity through a digital channel, unlocking access to the digital world in the economic, social, and political realms.

Indeed, good digital ID programs, implemented thoughtfully, offer significant inclusion benefits and higher standards of privacy and security with limited costs. When scaled to high adoption rates across multiple use cases, the economic value to individuals and institutions can be significant. Despite its mixed success so far, digital ID can represent an important key to unlocking inclusive growth.

High assurance

Unlike a paper-based ID such as most driver's licenses and passports, a digital ID can be verified remotely over digital channels, often at a lower cost. Regardless of whether the issuer is a government or nongovernment entity, digital

ID has the following attributes.

It is verified to a high degree of assurance that meets both government and private-sector institutions' standards for initial registration and subsequent acceptance for a multitude of important civic and economic uses. A range of credentials can be used to achieve unique high-assurance authentication and verification, including biometrics, passwords, QR codes, and smart devices with identity information embedded in them.

Digital ID is unique and established with individual consent. With a unique ID, an individual has only one identity within a scheme, and every scheme identity corresponds to only one individual. This is not characteristic of most social media identities today, for example. Consent means that individuals knowingly register for and use the digital ID, with control over what personal data will be captured and how they will be used.

Furthermore, digital ID can form the foundation of a host of applications in many aspects of an individual's life, work, and social interactions. The potentially pervasive nature of digital ID makes it akin to dual use technologies—like nuclear energy and GPS—that are designed to generate benefit but are also capable of being used for harmful or undesirable purposes. For example, a government might misuse digital ID programs by deploying them for political and social control, while a private-sector firm might misuse digital ID for commercial gain by influencing consumers in ways that they do not understand or desire.

The attributes of good ID, including high assurance and consent-based creation and use, promote trust and protect privacy. The design and governance of digital ID programs should incorporate these attributes and guard against the potential for misuse, to avoid outcomes contrary to the best interests of users.

by McKinsey

Signing up for protected identities

Digital signatures verifying the authenticity of digital messages or documents, have become widespread tools for authentication and integrity. How do the benefits outweigh those of traditional identity methods?

Document signing certificates enable organizations to digitally sign Adobe, Microsoft Office and other document types, marking them with visual trust indicators that verify the publisher's identity — an indication that the document has not been altered. With document signing certificates, organizations can authenticate documents, allowing for secure and efficient electronic transmission of official papers, including legal documents, invoices, engineering plans and diagrams, diplomas, and charters while reducing costs associated with printing and maintaining paper files.

In the modern computerized world, signatures have gone digital, with the United Nations officially recognizing digital signatures in 1996. Through the use of digital certificates, people are now able to sign emails, documents and all other kinds of digital media. This not only improves efficiency, it is also the most secure method of authenticating documents in human history.

Certification authority

Document signing certificates support digital signature for Adobe, Microsoft Office and other documents to secure legally binding documents. Document signing certificates can be created on any desktop to create trusted document verification in real time. Visual trust indicators show recipients that the sender's identity has been verified by a trusted certification authority (CA) and the document has not been altered during transmission.

While paper signatures provide static proof of a document's authenticity, digital document signing certificates provide real-time assurance throughout the document's lifetime, as any changes made after a document is digitally signed are indicated and render the original signature invalid. Many large governments and organizations depend on digital signatures to sign, protect and transmit official documents.

As a result of their dynamic nature, digital document signing certificates have become the standard of digital-signing efficiency, and they have proven to be a reliable tool since their introduction to the world as a feature of the enterprise email software Lotus Notes 1.0 in 1989. Over the last few decades, technology and software have advanced.

Examples of this is when Microsoft Word became the most widely used word processing software in 1990 and Adobe introduced the Portable Document Format (PDF) in 1993. As Word documents and PDFs became more prevalent, the need to sign documents — and not just emails — started to grow.

Adobe approved

Aligning the development of digital signature technology with the makers of the software for which they are designed to sign plays a pivotal role in improving the effectiveness of document signing certificates and the overall user experience of digitally signing Adobe PDFs and Microsoft documents. The Adobe Approved Trust List (AATL) is one such program that improves the effectiveness of document signing certificates on Adobe PDFs. CAs are qualified and then added to a Trusted Identity List (TIL) maintained by Adobe. The CA submits an application along with their root certificates to Adobe so that Adobe Acrobat and Reader can check that the signed PDF is secured by a valid certificate that is chained up to the corresponding root certificate on the (TIL).

The requirements to become a member of this program are extensive, which promotes the values of digital security, authentication and trust, including generating and storing key pairs in a medium that prevents exportation and duplication, demonstrating the use of strong identification and authorization procedures, and passing a certification authority third-party audit (such as the WebTrust audit for CA) within 18 months of applying to join the program.

Physical tokens

Public key pairs are generated on hardware security modules (HSMs) that store the private key. HSMs are highly secure so that the private key cannot be exported or used by another party to make a signature.

Timestamping is critical when it comes to supporting signature revocation

The Adobe Approved Trust List improves the effectiveness of document signing certificates

Some CAs provide Crypto-as-a- Service by offering hosted HSMs, or an HSM can be purchased and managed on-premises. Certificate signing keys can also be stored on a USB token, which are often used for low volume use cases.

The minimum requirement for storing signing certificate keys has been established at FIPS (Federal Information Processing Standard) 140-2 Level 2 which requires that the hardware has features such as tamper-evident coatings or seals (that would need to be broken to access the plaintext cryptographic keys) and security parameters inside the module. Document Signing Certificate Types Document signing certificates can support a variety of digital signing scenarios, including signatures for individuals, groups or organizations. Additionally, document signing certificates can also support manual or automated signing, making them both a flexible and efficient digital signing option.

Digital signatures have three main features - identity assurance, data integrity and non-repudiation Any recipient of a document signed with a valid digital signature gains trust and confidence that the document is authentic and its contents have not been altered. Digital signatures are legally binding due to this identity assurance and data integrity. The non-repudiation of digital signatures is of enormous benefit to those who wish to use digital signatures in place of traditional, handwritten signatures because it means the authenticity of the signature cannot be denied.

Data Integrity

Think of digital signing like putting a stamp or seal on a traditional document. Centuries ago, you could tell if a message had been tampered with if a seal was no longer intact. The invention of digital signing and hashing offers a similar, but much improved way to ensure that a document has not been altered. The signatory, in both cases, is the person putting their final stamp of approval on the document.

But how does this process work? The publisher cryptographically hashes the document into a fixed length number (i.e., 160-bits, 256-bits, etc.).

The length is fixed for efficiency so that the hash for books such as Jack & Jill and War and Peace will be the same length. The hash is encrypted using the private key. The document, encrypted hash and certificate string are provided to readers. The readers decrypt the hash with the public key, which is in the document signing certificate(s). The reader also hashes the document. The reader then compares the two hashes. If they match, the publisher has signed the document and the reader verifies that the document content has not changed.

Software displaying the signature acts as third-party verification in the root chain

Trusted Identity

Most publicly trusted digital certificates, including document signing certificates, require third-party identity verification, which is usually carried out by a CA. In order for the document signing certificate to establish trust, the CA generates a root certificate, which software developers embed into their applications. The root certificate acts as the link in the chain of trust between the CA and the software developer's software. In the case of document signing, a signature may contain an identity — the organization name, department, and an email address of the individual or group that will be signing the documents. When signed, the identity will be displayed on the document to let the recipient know who signed it and when it was signed.

The software displaying the signature acts as the third-party verification and is embedded within the certificate root chain. The signature display provides assurance to the end user that they can trust in the information they are reading in the document, that the information comes from the expected source and, combined with the data integrity aspect, the information contained in the document is what was written by the signatory. Any organization can set up their own public key infrastructure to issue digital certificates for signing. However, privately issued certificates will not be trusted by other public devices. This means that you need to use a third-party CA if you want to get automatically, publicly trusted digital signatures.

Non-Repudiation

The digital signature in document signing certificates must be undeniably authentic in order to be legally binding. Such a state of signing authenticity is known as non-repudiation meaning the legitimacy of the digital signature cannot be repudiated or refused. Thus, if someone signs a document using a digital signature, we need to be able to show that only that person could have had control over that signature at the time. With digital signatures, the most important way to prove non-repudiation is to ensure that only the signing party has control over the private key that is used to establish the identity. Document signing certificate private keys are stored and generated on FIPS 140-2 Level 2 tokens. These hardware devices protect the private key. Once a private key has been generated on the device, it cannot be removed. The devices are protected with pins and possibly even more complex authentication requirements to make sure that if the hardware is stolen or compromised, only the person with the authentication code can access the private key.

Hardware devices such as tablets protect the private key, safeguarding the signature

Lifetime Authentication

CAs are able to equip their document signing technology with the ability to maintain the validity of digitally signed documents for the document's life time. Any changes made to the document will render the digital signature invalid, signaling that the document has been changed and making any agreements and digital signatures in the previous document also invalid on the newly changed document.

Digital certificates can be revoked if the user thinks their identity or the certificate's private key has been compromised. Revocation will invalidate the signature from any future use. Software that supports digital signatures will perform a revocation check when the document is opened. The signature will contain a link where the software can go and perform the check. If the revocation service returns a response that the certificate and signature have been revoked after the signature was applied to the document, the signature will appear as invalid with a number of visual indicators in the document.

When a digital signature is applied to a document, a digital timestamp may follow. The timestamp will show the exact time and date that the document was signed. Timestamping is critical when it comes to supporting signature revocation and making sure that signatures are valid well after the certificate has expired. When revoking a signature, the user is likely saying that they do not want their signature to be used in the future to sign any documents. If their previously signed documents have been timestamped, those signatures will remain valid - allowing for long term digital signatures to be used on documents a digital certificates have validity periods and do expire.

by Entrust Datacard

Digital ID to be used by 5bn people in 2024

A new report from Juniper Research has found that the number of people using government-issued digital identity credentials will grow by over 150% from an expected 1.7 billion in 2019 to over 5 billion in 2024. Emerging economies in Asia and Africa are some of the biggest markets, as countries leapfrog analogue identities to benefit from the efficiencies digital registration and management bring. However, with simpler apps being quick to develop and almost indistinguishable from a user perspective, companies and operators will need to be the ones to drive the use of self-sovereign identity forward, according to Juniper. The report, Digital Identity: Technology Evolution, Regulatory Analysis & Forecasts 2019-2024, shows that those countries unencumbered by legacy systems are following Estonia's lead of rapid digital identity development. For example, almost 12 million people in Malawi are expected to have digital identities in 2022, with Nigeria and other countries supplying digital identity to over 420 million people on the continent on both cards and apps. Governments typically provided such cards, which many people in more developed countries have previously rejected. Juniper Research anticipates that markets across Europe and North America will be led by the financial services sector and digital driving licences, rather than formal government identification. Juniper Research believes mobile single sign-ons will be a large part of several digital identity platforms, with over 1 billion users by 2023; generating over $5 billion in revenues that year.

HID launches credential management service

Identity solutions provider, HID Global, has announced it has added its Credential Management Service to the growing offering of cloud-based identity solutions. The service simplifies the issuance and management of trusted Public Key Infrastructure (PKI) certificate-based credentials. The PKI credentials can be used by a broader range of organizations for convenient and secure multifactor authentication and converged physical access to facilities, as well as digital signing and encryption of emails and documents. The HID Credential Management Service includes everything needed to issue and manage the lifecycle of digital identity and high-assurance credentials using a cloud delivery model. It removes PKI complexity and enables a wider set of authentication use cases than nearly any alternative in the Identity and Access Management (IAM) market. Most operating systems and browsers automatically recognize these certificates, ensuring the digital identity issued by the HID Credential Management Service can be used as a foundation for achieving zero trust security. Endpoint authenticator options include smart cards and USB tokens, mobile app authenticators and converged badges for accessing facilities and IT systems.

UK govt delivers on expanded ePassport gates

The UK government has delivered early on the commitment made in its spring statement to allow nationals from seven countries to use ePassport gates from June 2019 onwards. The gates, which use facial recognition technology to check passenger identity and maintain the UK's border security, are now available to visitors from Australia, Canada, Japan, New Zealand, Singapore, South Korea and the United States. ePassport gates have been available to British and EU nationals since 2008. EU nationals will remain eligible to use them once the UK leaves the EU. The move has been designed to speed up border controls for low-risk countries with a new global immigration and border system will improve security and fluidity for passengers coming to visit or work in the UK.

Idemia embarks on 3D for Royal Caribbean Cruises

Announcing the expansion of Royal Caribbean's debarkation process using Idemia's MFace high speed 3D face capture technology, the companies said with the successful completion of trials at Cape Liberty, New Jersey, and the Port of Miami, the program is now moving into commercial production at these ports. Idemia's facial recognition technology has enabled the Royal Caribbean passenger debarkation process to be both more secure and efficient with technology playing a key role in enhancing the passenger experience by completing the process significantly faster than the manual verification method previously used. The MFace technology by IDEMIA streamlines the process by comparing the facial identities of individuals disembarking with the identities of ticketed passengers who boarded the ship at the start of a cruise, matching against images in the U.S. Customs and Border Protection's (CBP) Traveler Verification Service (TVS). No images are stored by Royal Caribbean, CBP or IDEMIA after the trip is completed to ensure that passenger privacy is maintained.

India working on advanced ePassports

India's ministry of external affairs has announced that it is working on a chip-enabled ePassport as it pursues reforms to deliver citizen-centric services. The Ministry said it has initiated discussions with the India Security Press regarding the project for the issue of chip-enabled e-passports to the citizens in order to pursue the manufacture of e-passports on priority so that a new passport booklet with advanced security features can be rolled out in the near future. India Security Press in Nashik will be working on the chip-enabled e-passports which will have security features. The ministry is also opening a new Post Office Passport Seva Kendras (POPSK).

Digital ID transforms as biometrics comes of age

With an estimated 120 countries now deploying electronic passports incorporating highly secure features and over 70 countries implementing eID cards, in 2019, digital identity technologies such as smart cards and biometrics have come of age. National ID cards have undergone a huge transformation; simple paper documents designed for single identification applications have given way to smarter documents in the form of a credit-card. These citizen ID cards or eIDs include a microprocessor for stronger document verification but also on-line authentication and signature. As they contain the portrait of the cardholder and very often fingerprints, they can be used for biometric identification and biometric authentication when needed.

Regulation

Last year, the European Parliament proposed a new regulation to implement security features of ID cards aligned with those of passports. In April 2019 the European Parliament approved the regulation and it still needs to be ratified. Member States and Iceland, Norway and Liechtenstein will need to start to issue these new cards with a secure contactless chip and the holder's photo and two fingerprints in the 2021-2022 timeframe as the directive comes into force 12 months after publication and States have two years to comply.

This new generation of national ID card offers one of the best identity theft protection. These eID cards also enable governments to implement on-line applications such as eGovernment solutions giving citizens access to public services with the reassurance of robust security. The development of these government issued IDs means a single card can offer a host of applications – from acting as a driver's license, enabling the user to file their taxes or giving him/her access to state benefits.

Global adoption

It is estimated that 3,6 billion citizens will carry a national eID card by 2021, but while some nations have been reticent in adopting eIDs, other countries have been far more bullish with implementations in Asia with China, Malaysia and Indonesia to name a few, or across Africa in countries like the Republic of South Africa, Nigeria and more recently in Algeria and Cameroun. Added to that are deployments across large parts of Europe, in the Gulf and in parts of Latin America. All provide interesting examples of the potential of eIDs to affect millions of ordinary lives throughout developed and emerging economies.

Annual issuance is expected to peak in 2019 at 679 million state-issued IDs with a chip. According to research company Acuity Market Intelligence, the number of electronic National ID cards in circulation will reach 3.6 billion citizens by 2021. This rapidly evolving dominance of electronic IDs reflects the global drive towards eGovernment and eCommerce services enabled by electronic identities. This move, according to Acuity, will provide substantial opportunities as national, regional, and global transaction infrastructures secured by a trusted digital identity scheme emerge over the next five years.

Economic empowerment

The case for eID cards and ePassports is quite straightforward for most people in the eID industry. In the business world, they play a key role in enabling financial services firms and telecoms companies to fulfil Know Your Customer (KYC) requirements and carry out Know Your Employee checks. They allow government departments to interact with their citizens more effectively around the clock. In the border control environment, combined with facial recognition and biometric authentication systems, they boost security and improve passenger throughput, giving authorities the confidence that the person standing in front of them is who he or she claims to be.

Emerging economies see the value of eID credentials in general, because they promote economic empowerment, drive democracy and aid economic development as highlighted by the World Bank Group initiative named ID4D.

They show the rest of the world that they are modern, secure and trustworthy states, able to implement new technologies and standards – and very much open for business. Furthermore, secure ID technology that can be used cross-border is important as it promotes regional integration and stability and makes economic development more likely.

And there are similarities with the European Regulation put in place in September 2018. A framework of digital trust will allow European citizens of 31 countries to free themselves from uncoordinated and separate infrastructures. One of the most innovative aspects of the Regulation is the possibility of accessing many services throughout Europe using the same national digital identity, whether public or private, provided it has been officially recognized by the authorities of the country where it is currently in use.

by Gemalto

15th edition!
The most authoritative directory in the industry

Presented by
SUSTAINABLE DEVELOPMENT

2019 Top 50 Suppliers

ePassport technology

National ID cards have undergone a huge transformation and digital identity technologies such as smart cards and biometrics have come of age. It is forecast that the number of electronic National ID cards in circulation will reach 3.6 billion citizens by 2021. More than 120 countries are now issuing electronic passports with 1 billion ePassports currently in circulation. Unlike conventional passports, the electronic passport has a microprocessor which stores a digital version of the ID photo as well as all of the ID data found on the first page of the paper passport.

For 15 years, our "Top 50 Suppliers of ePassport Technology" features the most active players in the ePassport and eID evolution, who are driving advancements in biometrically enabled, machine-readable identities and travel documents (MRTDs).

» Manufacturing digital eIDs
» Growing ePassport issuance

Top 50 Suppliers

ePassport technology

		Components						Equipment		IT Systems		Services	
		Security Paper	IC Chips	Operating Systems	Inlays / Antennas	Cards / Passports	Prelaminates	Card Manufacturing	Data Capture and/or Personalization	Software / Applications	Readers/ Hardware	System Integrator	Value Added Reseller
3M	www.3M.com/security					✔			✔		✔	✔	
Access IS	www.access-is.com					✔		✔			✔		
ASK	www.ask-rfid.com				✔	✔					✔		
Atlantic Zeiser	www.atlanticzeiser.com					✔		✔	✔	✔		✔	
Austria Card	www.austriacard.at			✔		✔			✔	✔			
Bundesdruckerei	www.bundesdruckerei.de					✔		✔	✔	✔	✔	✔	
Cetis	www.cetis.si					✔				✔		✔	
Cognitec Systems	www.cognitec.com									✔			
Crossmatch	www.crossmatch.com									✔	✔	✔	
Cryptovision	www.cryptovision.com			✔		✔				✔		✔	
De La Rue	www.delarue.com	✔	✔	✔	✔	✔		✔	✔			✔	✔
Dermalog	www.dermalog.de								✔	✔	✔		
Diletta	www.diletta.com					✔		✔	✔	✔	✔		
Entrust Datacard	www.entrustdatacard.com			✔					✔	✔			
Gemalto	www.gemalto.com		✔	✔	✔	✔		✔	✔	✔	✔	✔	
GET Group	www.getgroup.com					✔			✔	✔	✔	✔	✔
HID Global	www.hidglobal.com				✔	✔		✔	✔	✔	✔	✔	
IAI	www.iai.nl												
Idemia	www.idemia.com			✔	✔	✔			✔	✔		✔	
Industrial Innovation Group	www.industrialinnovationgroup.com	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
Infineon Technologies	www.infineon.com		✔										
Integrale Solutions	www.integralesolutions.com	✔		✔	✔	✔		✔	✔	✔	✔	✔	
Iris	www.iris.com.my		✔	✔	✔	✔		✔	✔	✔	✔	✔	✔
Ixla	www.ixla.it								✔	✔			
JDSU	www.jdsu.com	✔											
Kugler-Womako	www.kugler-womako.com										✔	✔	
Landqart	www.landqart.com				✔	✔							
Linxens	www.linxens.com		✔		✔	✔			✔	✔			
Lumidigm	www.lumidigm.com								✔		✔		
MaskTech	www.masktech.de			✔					✔	✔			
Melzer	www.melzergmbh.com				✔	✔		✔					
Monet+	www.monetplus.cz								✔	✔		✔	✔

		Components						Equipment		IT Systems		Services	
		Security Paper	IC Chips	Operating Systems	Inlays / Antennas	Cards / Passports	Prelaminates	Card Manufacturing	Data Capture and/or Personalization	Software / Applications	Readers/ Hardware	System Integrator	Value Added Reseller
Mühlbauer	www.muhlbauer.de							✔	✔	✔	✔	✔	
Multipolaris	www.multipolaris.hu	✔		✔	✔	✔		✔	✔	✔	✔	✔	✔
Nadra	www.nadra.gov.pk					✔		✔	✔	✔		✔	✔
Nagra ID	www.nagraid.com		✔	✔	✔	✔							
NBS Technologies	www.nbstech.com					✔		✔	✔		✔		
NetSeT Global Solutions	www.netsetglobal.rs					✔			✔	✔	✔	✔	✔
NXP	www.nxp.com		✔	✔	✔								
Oasys	www.oasys.uk.com					✔		✔	✔				
On Track Innovations	www.otiglobal.com		✔	✔	✔	✔		✔	✔	✔	✔	✔	✔
Optaglio	www.optaglio.cz	✔				✔							
Orell Füssli	www.ofs.ch	✔	✔	✔	✔	✔	✔		✔	✔	✔	✔	✔
Otto Künnecke	www.kuennecke.com								✔	✔	✔		
PAV Card	www.pav.de	✔			✔	✔		✔	✔				
ruhlamat	www.ruhlamat.com		✔		✔	✔		✔	✔		✔		
Secunet	www.secunet.com					✔			✔	✔		✔	
Secure Tech Consultancy	www.securetech-consultancy.com			✔		✔			✔	✔	✔	✔	✔
Sicpa	www.sicpa.com	✔							✔	✔		✔	
Smart Packaging Solutions	www.s-p-s.com				✔		✔						
Speed Identity	www.speed-identity.com					✔			✔		✔		
Supercom	www.supercom.com		✔			✔			✔				
Suprema	www.supremainc.com					✔			✔		✔	✔	
Thales	www.thalesgroup.com					✔				✔		✔	
UL Transaction Security	www.ul-ts.com					✔			✔	✔	✔	✔	✔
Unisys	www.unisys.com			✔					✔	✔		✔	
Veridos	www.veridos.com	✔		✔	✔	✔		✔	✔	✔	✔	✔	
Vision-Box	www.vision-box.com		✔	✔		✔	✔		✔	✔	✔	✔	
Zetes	www.zetes.com			✔		✔		✔	✔	✔	✔	✔	

LEGEND

COMPONENTS
SP = Security Paper
IC = IC Chips
OS = Operating Systems
INL = Inlays/Antennas
CARDS = Cards/Passports
PL = Prelaminates

EQUIPMENT
MF = Card Manufacturing
PERS = Data Capture and/or Personalization

IT SYSTEMS
APP = Software/Applications
HW = Readers/Hardware

SERVICES
SI = System Integrator
VAR = Value Added Reseller

3M Security Systems Division — **CARDS, PERS, HW, SI**
www.3M.com/security
1545 Carling Ave., Suite 700, Ottawa, Ontario – Canada Tel. +1 613 720 2070 Fax +1 613 720 2063

3M Security Systems, Identification & Authentication security solutions from one of the world's most trusted and innovative companies. Industry experience. Global reach. Ingenious technologies. Integrity. Credentials that have made 3M a leading provider of security solutions. Serving customers in over 200 nations, you not only get the personal attention of a local company, but also benefit from the strength of an experienced, reliable, global organization. 3M™ ePassport Readers, 3M™ Identity Document Issuance Systems, 3M™ Border Management Systems and 3M™ Confirm™ Laminates offer proven security.

Access IS — **CARDS, MF, HW**
www.access-is.com
18 Suttons Business Park, Reading, Berkshire, RG6 1AZ – UK Tel. +44 7748 770 632 Fax +44 118 926 7281

Access IS designs and manufactures innovative e-Passports, e-IDs, and e-DLs readers for Governmental and Commercial applications. From the world's smallest OEM OCR reader to our compact desktop Full-Page passport reader, we have a broad range of scanners to answer all your needs (i.e.: Border control & Immigration, ID Document Issuance, Law Enforcement, Hotel Check-in, Banking and Retail, Gaming, KYC, etc.). All our products are designed to be fast, accurate and highly reliable to endure years of heavy duty frontline use.

ASK — **INL, CARDS, HW**
www.ask-rfid.com
info@ask.fr
2260 route des Crêtes, BP337, 06906 Sophia-Antipolis – France Tel. +33 4 97 21 40 00 Fax +33 4 92 38 93 21

ASK, with over 200 million contactless products in circulation in 50 countries, including more than 15 million ePassport inlays, is a worldwide provider of a full range of contactless devices including smart cards, smart tickets, smart adhesive labels, readers and inlays for electronic passports, eID documents and contactless smart cards. The ASK e-Identity range includes SPiD eCovers for ePassports, and CoreLam, for eID inlays. ASK has been selected by major clients worldwide to provide e-identity inlays to several governmental bodies.

Atlantic Zeiser — **CARDS, MF, PERS, APP, SI**
www.atlanticzeiser.com
thorsten.tritschler@atlanticzeiser.com
Bogenstraße 6-8, 78576 Emmingen – Germany Tel. +49 7465 291-0 Fax +49 7465 291 166

Atlantic Zeiser is a world-leader in industrial high-security identification, coding and personalization solutions, offering total system solutions to governments and industries such as security printing (passport and banknote production), commercial printing, plastic card, telecom, pharmaceutical, banking, packaging, labels and cosmetics. The company specializes in card personalization systems and digital & security printing solutions by printing sensible variable data onto various products to create product identity – whilst ensuring full data and process integrity. AZ supports its customers through 11 subsidiaries as well as distribution and support offices in some 50 countries.

Austria Card — **CARDS, OS, PERS, APP**
www.austriacard.at
isales@austriacard.at
Lamezanstrasse 4-8, 1230 Vienna – Austria Tel. +43 1 610 65-0

Austria Card is a market leading and internationally operating company in the field of secure communications for payment, government and industrial applications. High standards, quality of life, innovation, and personal attention are the driving values of the company. Austria Card provides government authorities with national identity cards, driving licenses, digital tachograph cards, police identification, and passport data pages. The compliance with international standards shows that Austria Card meets the customers' demand for high levels of security: periodical audits of production processes and product quality as well as a continuous innovation process ensure that latest standards are met..

Bundesdruckerei **CARDS, MF, PERS, APP, HW, SI**

www.bundesdruckerei.de
info@bundesdruckerei.de

Oranienstraße 91, 10969 – Berlin Tel. +49 30 2598 0 Fax +49 30 2598 2205

Berlin-based Bundesdruckerei is one of the world's leading companies engaged in the development and supply of systems solutions for secure identification applications. In addition to full-scale passport and ID-card systems, the company provides national and international customers with ID documents, high-security cards, document verification hardware, security software along with trust center services. Bundesdruckerei also produces banknotes, postage and revenue stamps as well as electronic publications. Subsidiaries of the Bundesdruckerei Group are: BIS Bundesdruckerei International Services, D- TRUST, Maurer Electronics and iNCO.

Cetis - High Security Printing House **CARDS, APP, SI**

www.cetis.si
info@cetis.si

Copova 24, 3000 Celje – Slovenia Tel. +386 3 4278 500 Fax +386 3 4278 817

With its smart ID management solutions Cetis offers competent partnership to governments and companies. Cetis answers the questions of HOW TO provide cutting edge identification documents and identity management solutions taking into account demands of customers. System integration accompanied by security printed matter is Cetis's turnkey service. We have patented solution for e-passport with polycarbonate data page and have a nationally awarded innovation – Nanotech intaglio lamination plates. Highest security standards are self-evident: ICAO/ISO, CWA 14641, FSCC (Facility Security Clearance Certificate), EMV & CQM.

Cognitec Systems **APP**

www.cognitec.com
info@cognitec.com

Grossenhainer Str. 101, D-01127 Dresden – Germany Tel. +49 351 862 920 Fax +49 351 862 9210

Cognitec develops market-leading face recognition technology and applications for enterprise and government customers around the world. Various independent evaluation tests have proven the premier performance of the FaceVACS® software. Cognitec's portfolio includes products for facial database search, video screening and analytics, border control, ICAO compliant photo capturing and facial image quality assessment. Corporate headquarters are located in Dresden, Germany; other offices in Miami, FL; Rockland, MA; and Sydney, Australia.

Crossmatch **APP, HW, SI**

www.crossmatch.com
sales@crossmatch.com

3950 RCA Boulevard, Suite 5001, Palm Beach Gardens FL 33410 – USA Tel. +1 561 622 1650 Fax +1 561 622 9938

Crossmatch, an HID company, helps organizations solve their identity management challenges with market-specific biometrics technologies. We empower governments, law enforcement agencies, banks, retailers and other enterprises to mitigate risk, drive productivity and improve service levels. Our solutions are built on consultative expertise, refined best practices and the application of advanced biometrics technologies. Crossmatch understands the forces of change in the markets we serve and we develop solutions that anticipate customer requirements. Our network of consultative and technical service experts collaborate with customers in more than 80 countries worldwide.

LEGEND

COMPONENTS
SP = Security Paper
IC = IC Chips
OS = Operating Systems
INL = Inlays/Antennas
CARDS = Cards/Passports
PL = Prelaminates

EQUIPMENT
MF = Card Manufacturing
PERS = Data Capture and/or Personalization

IT SYSTEMS
APP = Software/Applications
HW = Readers/Hardware

SERVICES
SI = System Integrator
VAR = Value Added Reseller

Cryptovision
www.cryptovision.com
info@cryptovision.com

CARDS, OS, APP, SI
Munscheidstr. 14, 45886 Gelsenkirchen - Germany Tel. +49 2 09 1 67 24 50 Fax +49 2 09 1 67 24 61

Cryptovision is a world-leading specialist for cryptography and electronic identity solutions. The Germany based company has been specializing in this field for 15 years, with hundreds of successful projects delivered. More than 100 million people worldwide make use of cryptovision products every day in such diverse sectors as defense, automotive, financial, government, retail and industry.

De La Rue
www.delarue.com
identity.systems@uk.delarue.com

SP, IC, OS, INL, CARDS, MF, PERS, SI, VAR
De La Rue House, Jays Close Viables, Basingstoke, Hants RG22 4BS – UK Tel. +44 1256 605000 Fax +44 1256 605299

De La Rue's intelligent Government solutions, now part of HID, ensure the integrity of every individual's identity, today and tomorrow. A reliable and trusted partner of governments worldwide, De La Rue has implemented over 100 projects in 65 countries in the last 6 years alone, focusing on the provision of passport, ePassport, national ID, eID, driving license and voter registration schemes. A specialist identity systems integrator, we pride ourselves on the ability to deliver complete identity solutions with the highest possible levels of end-to-end security.

Dermalog
www.dermalog.de
info@dermolog.de

PERS, APP, HW
Mittelweg 120, 20148 Hamburg – Germany Tel. +49 40 4132270 Fax +49 40 41322741

DERMALOG

As the name - derived from the Greek terms "derma" (skin) and "logos" (mathematical logic) - suggests, Demalog is active in the fields of biometric identification technologies. Dermalog's technology, based on more than 20 years of experience, is employed in border control, access control, civil and criminal AFIS (automatic fingerprint identification system), smart card and biometric logon applications. The company has its head office in Hamburg and a branch office in Kuala Lumpur, Malaysia, with further branches planned in the most important markets and continents.

Diletta
www.diletta.com
contact@diletta.com

CARDS, MF, PERS, APP, HW
Industriestrasse 25-27, D-64569 Nauheim – Germany Tel. +49 6152 18040 Fax +49 6152 180422

For more than five decades DILETTA has been engaged in the development and production of identity products and security systems for governments and other national institutions. DILETTA offers complete systems for centralized and decentralized personalization of high security travel documents which support all safety criteria, contactless chip technology and machine readable features. With over 30,000 installations in more than 100 countries we have gathered an amazing expertise and ample experience.

Gemalto
www.gemalto.com
info@gemalto.com

IC, OS, INL, CARDS, MF, PERS, APP, HW, SI
6, rue de la Verrerie 92190 Meudon – France Tel. +33 1 55 01 50 00

Gemalto, part of Thales, is a leader in digital security solutions and dedicated to making personal digital interactions more convenient, secure and enjoyable. The company provides end-to-end digital security solutions, from the development of software applications through design and production of secure personal devices such as smart cards, SIMs, ePassports, and tokens, to the management of deployment services for its customers. Gemalto has operations in about 100 countries and over 10,000 employees including 1,300 R&D engineers.

Entrust Datacard — **MF, PERS, APP**

www.entrustdatacard.com
1187 Park Pl, Shakopee, MN 55379 – USA Tel. +1 952 933 1223

Entrust Datacard offers technologies that empower governments to enhance service levels while strengthening security, mitigating risk and controlling costs. Solutions range from citizen enrolment and document issuance to physical and digital credentials.The company provides identity-based solutions that streamline and safeguard access — to facilities, networks and the cloud — for employees and other authorized users. The scalability of our identity-based solutions allows enterprises to respond quickly to changing security needs.

HID Global — **INL, CARDS, MF, PERS, APP, HW, SI**

www.hidglobal.com
15370 Barranca Pkwy, Irvine, CA 92618 – USA Tel. +1 949 732 2000 Fax +1 949 732 2120

HID Global is the trusted leader in products, services and solutions related to the creation, management, and use of secure identities for millions of customers worldwide. Recognized for robust quality and innovation, HID Global is the supplier of choice for OEMs, integrators, and developers serving a variety of markets that include physical access control; IT security, including strong authentication/credential management; card personalization; visitor management; government ID; and identification technologies for technologies for a range of applications.

IAI industrial systems — **PERS**

www.iai.nl
info@iai.nl
De Run 5406, 5504 DE Veldhoven – The Netherlands Tel. +31 40 254 24 45 Fax +31 40 254 56 35

IAI designs, builds and supplies passport personalization equipment. Functionalities include chip encoding, laser engraving, inkjet printing and lamination, perforation of the passport number through the visa pages, perforation of the holder's photograph (ImagePerf) and the application of a label on the back cover. IAI offers high volume passport systems for centralised personalization (BookMaster One) and low volume systems for decentralised personalization (BookMaster Desk). The BookMaster One has recently been redesigned to offer a more flexible choice in configuration and speed.

Idemia — **OS, INL, CARDS, PERS, APP, SI**

www.idemia.com
info@idemia.com
Boulevard Lénine, BP 428 76805 Saint-Etienne-du-Rouvray – France Tel. + 33 2 3564 5346

Idemia is a leader in trusted identities for an increasingly digital world placing the client, consumer or citizen at the heart of everything it does, combining security, convenience, the human factor and continuity within a single proposition.The company places augmented identity at the center of its actions and conceives security in a global way, upstream of technological developments, by factoring in the customer's environment and how they specically use technology.

LEGEND

COMPONENTS
SP = Security Paper
IC = IC Chips
OS = Operating Systems
INL = Inlays/Antennas
CARDS = Cards/Passports
PL = Prelaminates

EQUIPMENT
MF = Card Manufacturing
PERS = Data Capture and/or Personalization

IT SYSTEMS
APP = Software/Applications
HW = Readers/Hardware

SERVICES
SI = System Integrator
VAR = Value Added Reseller

Infineon Technologies — **IC**

www.infineon.com/chip-card-and-security
SiliconIdentity@infineon.com

Am Campeon 1-12, 85579 Neubiberg – Germany Tel. +49 800 951 951951

Infineon Technologies AG offers the industry's most comprehensive product portfolio of semiconductor-based security products for a wide range of chip card and security applications including electronic ID documents, mobile payment and system security. With more than 25 years experience in security ICs and core competences in the fields of security, contactless communication as well as integrated microcontroller solutions (embedded control), Infineon is helping to augment data security in an increasingly connected world.

Integrale Solutions — **SP, OS, INL, CARDS, MF, PERS, APP, HW, SI**

www.integralesolutions.com
magali.notot@integralesolutions.com

Route du haut marais, 77320 Jouy sur Morin – France Tel. +33 1 64 75 69 84 Fax +33 1 64 20 37 95

Integrale Solutions, a subsidiary of Arjowiggins Security SAS, specializes in both digital and physical security for the e-ID and secure documents market. Integrale Solutions is your trusted solution partner to deliver a complete end to end e-Document solution. We benefit from more than 15 years of e-ID implementation experience and expertise in high security document, advanced electronic technologies and system solutions. Integrale Solutions products are a perfect fit for a wide variety of official e-documents: e- passport, national e-ID cards, e-health cards, e-driver licenses, e-tickets, e-vouchers.

Iris — **IC, OS, INL, CARDS, MF, PERS, APP, HW, SI, VAR**

www.iris.com.my

Smart Tech. Complex, Tech. Park, Bukit Jalil, 57000 Kuala Lumpur – Malaysia Tel. +603 89960788 Fax +603 89960441

Founded in 1994, IRIS the inventor of the world's first ePassport and multi-application smart card, has more than 20 years of experience as a technology innovator and leading provider of secure electronic identification documents for all trusted identity solutions. Recognized for excellence in ID technology, IRIS understands the importance of secure authentication, authorization concerns and standardization to the nation.

Ixla — **PERS, APP**

www.ixla.it
renzo.eterno@ixla.it

Via Ponte Chiusella 28, 10090 Romano C.se (Torino) – Italy Tel. +39 0125 719286 Fax +39 0125 718455

IXLA ID LASER SYSTEMS

With desktop laser systems for personalization of eID and ePassport, IXLA fully owns its technology and has more than 1.100 systems installed in 37 Countries. Thanks to these successes, IXLA has become a benchmark for the industry and a qualified partners of the upmost important players for the ID documents GSP.

Jdsu — **SP**

www.jdsu.com

2 Applegate Drive, Robbinsville, NJ 08691 – USA Tel. +1 609 632 0800 Fax +1 609 632 0850

Jdsu's Authentication Solutions group, now including ABNH, offers a market-leading set of overt and covert security solutions for authentication and brand protection, including counterfeiting protection of identity documents. The company's unique color-shifting technologies, such as OVP, SecureShift, MetaSwitch and Phantom, along with its Charms microstructured taggants, can be provided as integrated solutions, including printing on a variety of substrates for labels and packaging. And with the addition of ABNH, options now include holographic hot stamp foil, HoloMag, demetalized holographic laminates, and tamper-apparent holographic labels. Jdsu provides custom solutions for customer-specific authentication needs.

Linxens — **MF, IC, INL, PERS, APP**

www.linxens.com | 6 Rue Marius Aufan, 92300 Levallois Perret – France | Tel. +33 1 41343450 | Fax +331 47576492

Linxens is a world-class provider of component-based solutions for the security & identity market. We design and manufacture Microconnectors and RFID Antennas and Inlays. With 8 production facilities in Asia, Europe and North America, 4 R&D Centers, and over 3000 employees, Linxens makes its large-scale production capacity available to its customers, and delivers guaranteed product and technical reliability. Linxens technology gives users the best connection possible. Linxens crafting the future of connections.

MaskTech — **OS, PERS, APP**

www.masktech.de | Masktech GmbH, Nordostpark 16, 90411 Nuernberg – Germany | Tel. +49 9119 551490 | Fax +49 9119 551497

MaskTech is the leading independent provider of high security multi-application operating systems and customized Flash/ROM masked products for electronic identification applications. Our core product - MaskTech Chip Operating System (MTCOS) - is a high performance OS, especially designed for secure semiconductors with powerful crypto co-processor and RFID, dual interface or contact interface. MTCOS is available and certified Common Criteria EAL4+ on a unique variety of microcontrollers of different silicon vendors. MTCOS is a fully open standard compliant (ISO/IEC) multi-application system, used in over 60 country's travel, ID documents and authentication solutions worldwide. MTCOS is fully compliant to the ICAO DOC9303 (ePassport) standards, to BSI TR-03110 and the eDL specification ISO/IEC 18013.

Melzer maschinenbau — **INL, CARDS, MF**

www.melzergmbh.com
sales@melzergmbh.com | Ruhrstr. 51-55, Schwelm, 58332 – Germany | Tel. +49 2336 929280 | Fax +49 2336 929285

For more than 60 years MELZER has been internationally recognised and established as the leading equipment supplier for the production of the most advanced ID documents, Smart Cards, DIF Cards, RFID Inlays and e-Covers for Passports. Customized solutions, the modular machine system and the lean production approach ensure and maintain unsurpassed yield rates, flexibility and profitability. The MELZER product portfolio also includes a broad range of versatile RFID converting equipment.

Mühlbauer — **MF, PERS, APP, HW, SI**

www.muehlbauer.de
info@muehlbauer.de | Josef-Mühlbauer-Platz 1, 93426 Roding – Germany | Tel. +49 9461 952 0 | Fax +49 9461 952 1101

For over 30 years the Mühlbauer Group has been a reliable turnkey solution partner for private companies and the public sector in the areas of plastic- and chip cards, passports and various RFID applications around the world. The primary reason: our thinking and execution of a solution goes far beyond the ability of other suppliers. Especially for Government projects with applications such as ID cards, passports or driver's licenses we provide our clients an enormous array of options which save valuable time and resources.

LEGEND

COMPONENTS
SP = Security Paper
IC = IC Chips
OS = Operating Systems
INL = Inlays/Antennas
CARDS = Cards/Passports
PL = Prelaminates

EQUIPMENT
MF = Card Manufacturing
PERS = Data Capture and/or Personalization

IT SYSTEMS
APP = Software/Applications
HW = Readers/Hardware

SERVICES
SI = System Integrator
VAR = Value Added Reseller

INDUSTRIAL INNOVATION GROUP

Target/Product

Tax stamps
IDs, cards &
secure document

Sector

Government & Public Sector
Manufacturing & Retails

Technology

RFID
Holograms
Biometrics
Security printing
Software
Taggants
Track&Trace

Taryam bld., Industrial Area 18, Maleha Street, Sharjah PO Box 123428, United Arab Emirates, info@industrialinnovationgroup.com Tel.: 97165062555
www.industrialinnovationgroup.com

Nadra
www.nadra.gov.pk
abdul.baqi@nadra.gov.pk

CARDS, MF, PERS, APP, SI, VAR
Shahrah-i-Jamhuriat, G-5/2, Islamabad 4400 – Pakistan Tel. +92 90392597 Fax +92 9108143

NADRA is one of the leading organizations in providing cutting edge technology in system integration and ID solutions in Pakistan. NADRA has one of the largest centralized databases of the world and offers ID solutions and services which keep secure national, social and cultural factors in mind to provide customized solutions for any country. The multiple product & service based applications include issuance of Citizen Registration Cards, Chip based Smart ID Cards, Travel Documents, Biometric based Border Control System, Motor Vehicle Registration System, e-Toll Collection System, Online Verification System, Biometric Verification System, Personnel & Access Control System and e-Commerce platform.

Nagra ID
www.nagraid.com

IC, OS, INL, CARDS
Crêt-du-Locle 10, 2301 La Chaux-de-Fonds – Switzerland Tel. +41 32 924 04 04

NagraID (Switzerland), expert advisor and technology provider for the digital & ID security industry, offers tailor made products like secure smartcards, Display Cards, inlays, prelaminates, e-Covers with gold printing and security features, etc with value-added services and transfer technologies for citizens ID's, corporate ID's, financial and e-Consumers ID's markets. NagraID's advanced technologies and product families are the results of 35 years of experience in micro-electronic product development, crowned by Swiss high precision, quality methodologies and heritage. NagraID's products are Certified ISO 9001:2008 & Security environment according to EMV and CCEAL5+. Established in 1976, NagraID joined the Kudelski Group in 2001.

NBS Technologies
www.nbstech.com
info@nbstech.com

CARDS, MF, PERS, HW
703 Evans Avenue, Suite 402, Toronto M9C 5E9 – Canada Tel. +1 416 621 1911 Fax +1 416 621 8875

NBS Technologies has remained a leading developer and provider of equipment for card personalization, EMV compliance/ migration, smart card manufacturing and semiconductor handling equipment. Governments are clearly the most sensitive and aware of security and access control issues – National Security has never been more important. At NBS, we can deliver card personalization and card printing systems to governments that meet the needs of virtually any specific application. In either an instant, on-the-spot issuance scenario, remote/distributed/branch issuance or via a centralized card production facility, NBS has the solution that fits.

NetSeT Global Solutions
www.netsetglobal.rs
office@netsetglobal.rs

CARDS, PERS, APP, HW, SI, VAR
Osogovska 10, 11030 Belgrade – Serbia Tel. +381 11 3058612 Fax +381 11 2547492

NetSeT Global Solutions is a trusted solution provider and system integrator for complex, national level projects - eID, eHealth, eDL/VL and ICAO ePassport. With more than 15 years of experience and 12 national projects worldwide, NetSeT is the leading eID/ ePass company in SEE region. Flagship products and services: Central Identity Management System, CAMS, Enrolment, Perso Data Management, Smart Logistics, Secure National Registers, eGovernment PKI, EAC PKI, eID and PKI Applets, Secure Middleware, Strong Authentication and Encryption, Border Control, Entry/Exit Management System.

LEGEND

COMPONENTS
SP = Security Paper
IC = IC Chips
OS = Operating Systems
INL = Inlays/Antennas
CARDS = Cards/Passports
PL = Prelaminates

EQUIPMENT
MF = Card Manufacturing
PERS = Data Capture and/or Personalization

IT SYSTEMS
APP = Software/Applications
HW = Readers/Hardware

SERVICES
SI = System Integrator
VAR = Value Added Reseller

NXP
www.nxp.com

IC, OS, INL
Mikron-Weg 1, A-8101 Gratkorn – Austria Tel. +43 3124 2990 Fax +43 3124 299330

With 2 billion chips sold to date, NXP Semiconductors is the world's leader in the design and manufacturing of contactless chips used in smart cards, smart labels and tags as well as in automotive systems and the corresponding reader components. NXP has been awarded over 80% of all ePassport projects globally, including the US, France, Germany and Singapore. Furthermore NXP is supplying its technology for major national ID, health card and driving license projects.

Oasys Technologies
www.oasys.uk.com
sales@oasys.uk.com

CARDS, MF, PERS
3 Stratton Bus. Park, Montgomery Way, Biggleswade, UK, SG18 8UB Tel. +44 (0)1767 600232

Passports and ID Card production lines now form the basis of the latest range of high quality production equipment from Oasys Technologies. On passports and ID Cards, Oasys now has an established track record on machinery to produce the full E-Data Page product covering the key steps of collation, lamination and guillotining/punching operations.

On Track Innovations
www.otiglobal.com

IC, OS, INL, CARDS, MF, PERS, APP, HW, SI, VAR
ZHR Industrial Zone, P.O. Box 32, 12000 Rosh Pina – Israel Tel. +972 4 686 8000 Fax +972 4 693 8887

Since 1990, OTI provides secure contactless smartcard technology for a wide variety of markets. OTI's offerings include products/solutions for ePassports, national IDs, electronic payments, petroleum payments, medical, and automatic parking and ticketing systems. OTI provides an end-to-end turnkey, interoperable, ICAO/ISO compliant solution for national ID/ePassports, driving/vehicle licenses, voter registration programs, ranging widely from data enrollment through population registry, biometric screening, and documents production, to eVisa and border control applications, including security printing, raw materials, smart inlays/covers/stickers, chips, operating system, readers and personalization systems.

Optaglio
www.optaglio.cz
jan.bitman@optaglio.cz

SP, CARDS
Rež 199, 250 68 Husinec-Rež – Czech Republic Tel. +420 220 941 075 Fax +420 220 941 077

Optaglio helps governments tackle identity theft and illegal migration by delivering authentication solutions of the highest standards. We develop and innovate our protective solutions for both national and international ID documents in order to keep ahead of counterfeiters. Optaglio delivers advanced security for multilayer polycarbonate documents. The top solution for ID protection - OVMesh™ presents a superior alternative to hot stamping foils with high refractive index in terms of tamper resistance and design versatility and the ease of application.

Orell Füssli Security Printing
www.ofs.ch
info@ofs.ch

SP, IC, OS, INL, CARDS, PL, PERS, APP, HW, SI, VAR
Dietzingerstrasse 3, CH-8036 Zürich – Switzerland Tel. +41 44 466 77 11 Fax +41 44 466 79 01

Founded in 1519, Orell Füssli Security Printing is a leading provider of security technology, products and solutions for identification documents and systems, banknotes, and secure documents. Nowadays, travel documents must meet toughest security standards, and the development, production and issuing of passports, visa and other identification documents has become a complex and demanding task. Since we know how to meet these standards in a customized way, we are the ideal partner for such projects.

Otto Künnecke
www.kuennecke.com
contact@kuennecke.com

PERS, APP, HW
Bülte 1, 37603 Holzminden – Germany Tel. +49 5531 9300 0 Fax +49 5531 9300 903

Otto Kuennecke has set a mark with handling of ID projects. In 2014, Otto Kuennecke received the ICMA "Elan Award" for the most innovative machine in the business – the DCS, a high-end storage and commissioning system for ID documents for just in time mailing management. With machine solutions by Otto Kuennecke, ID documents can be verified, sorted and packed in different kinds of packages – banderoles, post boxes, secure envelopes etc. Otto Kuennecke creates the right solution for your special requirements.

PAV Card
www.pav.de
timm@pav.de

INL, CARDS, MF, PERS, SP
Hamburger Strasse 6, 22952 Luetjensee – Germany Tel. +49 41 54 7 99 0 Fax +49 41 54 7 99 151

PAV is a well-established company with a rich tradition and employs about 250 staff members. Our epassport inlays made from polycarbonate or synthetic paper are suited for further processing in every standard passport production. The inlay from PAV can be integrated smoothly into the cover or the data page of the passport. The RFID technology makes it possible to read-out the data wireless. Today we serve several countries with their ePassport inlays and eID cards.

ruhlamat GmbH
www.ruhlamat.com

IC, INL, CARDS, MF, PERS, HW
Sonnenacker 2, 99819 Marksuhl, Germany Tel. +49 36925 9290 Fax +49 36925 929111

ruhlamat is an innovative engineering and machine building company with its headquarters located in Germany. Activities are focused on smart card and passport processing technology, e.g. passport production and personalization, card production and personalization, module preparation as well as Inlay/RFID solutions and special machinery. ruhlamat branches and representations throughout the world create an ideal basis for a professional and area-spanning service network.

Secunet
www.secunet.com

CARDS, PERS, APP, SI
Kronprinzenstrasse 30, 45128 Essen – Germany Tel. +49 201 54 54-1234 Fax +49 201 54 54-1321

Secunet Security Networks offers solutions and know-how for the complete life cycle of electronic passports, identity documents, residence permits, and visas. secunet experts support public authorities, organisations in the industrial sector and system integrators in their projects concerning biometrics and eIDs. The Federal Government of Germany as well as many other European countries trust in our expertise as a pioneer and reliable partner.

LEGEND

COMPONENTS
SP = Security Paper
IC = IC Chips
OS = Operating Systems
INL = Inlays/Antennas
CARDS = Cards/Passports
PL = Prelaminates

EQUIPMENT
MF = Card Manufacturing
PERS = Data Capture and/or Personalization

IT SYSTEMS
APP = Software/Applications
HW = Readers/Hardware

SERVICES
SI = System Integrator
VAR = Value Added Reseller

Secure Tech Consultancy
www.securetech-consultancy.com
info@securetech-consultancy.com

CARDS, PERS, APP, SI, VAR, HW, OS
Software Technology Park, Sector I-9/3, Ind. Area, Islamabad – Pakistan Tel. +92 51 111 111 782 Fax +92 51 443 6480

Secure Tech Consultancy is the perfect partner for both public & private sector organizations seeking success in planning and implementing IT Solutions. Our expertise covers implementing ID cards, e-Passports, border control, data integration, biometric technologies, RFID systems, access Control, Office Automation and e-Governance projects. We are experienced in enrolment & integration of iris, facial and fingerprint identification. Our success stems from many successful on ground implementations.

SPS INL, PL

Providing secure and high added value components for card and document manufacturers

SPS has delivered several million epassport inlays and e covers based on its unique ebooster technology to Asian, African, and European countries. The Teslin based inlay uses an inductive coupling technology, where there is no physical connection between the antenna and the chip's module enhancing the durability of the passport. SPS' technology is designed to accept all chip and OS suppliers on the market, offering a highly reliable and cost effective solution to passport manufacturers. SPS offers unique security features which gives the final passport a unique added value. SPS also proposes a complete offer for Polycarbonate data pages from finished datapage to hinge inlay and electronic components.

The company is specialized in the design, manufacture and sale of contactless solutions based on inductive coupling technology and dedicated to ID cards, e-passport and dual interface banking cards. Headquartered in Rousset, France, with a subsidiary in Singapore, SPS employs 180 people. Part of IN Groupe, one of the global leaders in secure identity solutions, the company specializes in contactless and dual-interface products, with a recognized micro packaging expertise. SPS has filed over 120 patents supporting its exclusive technologies.

As a world leader in secure and electronic components for banking and government markets, the company brings value to its customers by pre-certifying the performance of cards using its technology and guaranteeing card functionality in the field.

SPS
85 avenue de la Plaine
ZI de Rousset-Peynier
13790 Rousset – France
Tel. +33 442538830
Fax +33 442538448
www.s-p-s.com
contact@s-p-s.com

SICPA
www.sicpa.com

SP, PERS, APP, SI
Av de Florissant 41, 1008 Prilly – Switzerland Tel +41 21 627 55 55 Fax +41 21 627 57 27

Sicpa is a provider of security inks and integrated security solutions that protect most of the world's banknotes, as well as the security documents of over 100 countries, including passports, visas, ID documents and access cards. We are the trusted partner of governments, central banks and security printers, providing cutting-edge technologies to address specific needs in the domain of document security.

Speed Identity
www.speed-identity.com
info@speed-identity.*com*

CARDS, PERS, APP, HW, SI
Slakthusgatan 9, SE-121 62 Johanneshov – Sweden Tel. +46)8 702 33 50

Speed Identity is a leading global provider of high performance biometric enrollment and data capture solutions. The company pioneered live biometric enrollment in the early 2000. To date we have successfully delivered thousands of systems to more than 120 countries worldwide. Our customers include government departments and agencies such as ministries of foreign affairs, ministries of interior, law enforcement agencies, tax agencies, road authorities and immigration agencies. a leading global provider of high performance biometric enrollment and data capture solutions.

Supercom
www.supercom.com
info@supercom.com

IC, CARDS, PERS, HW, SI
1 Arie Shenkar Street, Herzliya 4672501 – Israel Tel. +972 9 889 0880 Fax +972 9 889 0814

Since 1988 SuperCom has been a global leading provider of traditional and digital identity solutions, providing advanced safety, identification, and security products and solutions to governments as well as private and public organizations around the world. SuperCom has been inspiring governments and national agencies, to design and issue secured multi-ID documents and robust digital identity solutions to its citizen and visitors, using SuperCom e-government platforms and innovative solutions.

Suprema
www.supremainc.com

CARDS, PERS, HW, SI
16F Parkview Office Tower, Jeongja-dong, Gyeonggi, 463-863 – Korea Tel. +82-31-783-4502 Fax +82-31-783-4503

Suprema is a leading global provider of biometrics technology and identity management solutions. The company's range of products includes fingerprint modules, biometric access control systems, e-passport readers and live-scanners. Suprema's solutions are featured by integration of the excellent embedded system design capability and the strong backgrounds in theories and algorithms backed by a number of experts having the rich experience and extensive knowledge in the field of biometric solutions, embedded system design and signal processing.

Thales
www.thalesgroup.com/security

CARDS, APP, SI
45 rue de Villiers, 92526 Neuilly-sure-Seine Cedex – France Tel. +33 1 57 77 80 00 Fax +33 1 73 32 20 22

Thales is one of Europe's leading players in the security market. Identity management systems play a major role in a country's economic and social development. They help simplify relationships between administrations and the citizens they serve, providing easier access to elections, job vacancies and social services.Thales produces identity documents and operational control systems in over 25 countries. More than 250 million secure identity documents have been generated by Thales - a long-standing supplier of identity systems, biometric systems and secure documents both in France and around the world..

LEGEND

COMPONENTS
SP =Security Paper
IC =IC Chips
OS =Operating Systems
INL =Inlays/Antennas
CARDS =Cards/Passports
PL = Prelaminates

EQUIPMENT
MF =Card Manufacturing
PERS =Data Capture and/or Personalization

IT SYSTEMS
APP =Software/Applications
HW =Readers/Hardware

SERVICES
SI =System Integrator
VAR =Value Added Reseller

SUSTAINABLE DEVELOPMENT

Publisher
Roberto Dell'Acqua

Editor in chief
Sophie B. de la Giroday

Editorial Staff
Victor March, Gaia Steden
idpublications@onpublishing.com
John Matthews, Andrew Fielding
sd@hadrianmedia.net

Advertising
Karina May
karina.may@hadrianmedia.net

Issue: June/July 2019

Hadrian Media AG
Baarerstrasse 10
6304 Zug (ZG),
Switzerland

CH – 170.3.038.475-4

www.sustainabledevelopmentmagazine.com
www.id-world-magazine.com
www.onboard-technology.com

People and organizations featured in this issue

Page	Name	Page	Name	Page	Name
7	Amadeus	18	Google	15	Oracle
21	Apple	7	Grey Matter	7	Polymath
7	Blockpass	6, 29	HID	21	Research & Markets
15	Callsign	7, 29	Idemia	29	Royal Caribbean
6	Canon Fintech	6	Idex	20	Samsung Electronics
20	Chinese Government	6	Idfy	21	Siemens
16	Clausematch	40	IIG	6	Signicat
7	Colombo Airport	22	IN Groupe	7	Sinerix
20	Danish Government	29	Indian Government	44	SPS
10	Darktrace	20	Invidia	15	ST Microelectronics
6	De la Rue	29	Juniper Research	12	Symantec
21	Drive AI	7	Kudelski	47	Thales
15	ENISA	15	Lloyds Bank	20	Twitter
26	Entrust Datacard	6	Matica	21	Uber
8	European Commission	24	McKinsey	29	UK Government
3	FTF	48	Melzer	6	Vision-Box
21	Geisinger	21	Mentor	20	Volvo
30	Gemalto	15	Microsoft	15	Zion MR
6	Goldpac	21	Mighty AI		

ID WORLD BUYER'S GUIDE – a well of information

Sustainable Development is proud to present the world's leading reference on auto ID technology solutions and component suppliers, bringing together a comprehensive review of players in the fields of Cards, Biometrics, RFID and Data Collection. Drill deeper into essential information about who supplies which products in relation to the key auto ID technologies, which role each company plays in the value chain, as well as product specifications and categories. ID WORLD connects our industry. Key players provide us with their direct input and the Buyer's Guide is sent out to the qualified mailing lists of end users who receive the ID Community publications.

Vertical directories published throughout the year

Top Suppliers - Access Control Technologies
Systems, components and total solution providers in the production and deployment of projects in physical and logical access control. Reach key decision makers at end-user level as well as system integrators in safety and the wider security systems industry.

Top Suppliers - ePassport Technologies
Players involved in the production and deployment of ePassport and eID projects. Reach key decision makers at government level and potential industry partners interested in the digital wave of personal ID.

Top Suppliers - Anti-counterfeiting and Product Security Technologies
Component and solution providers in the field of anti-counterfeiting and product security technologies active in the fields of advanced solutions for instantly validating product authenticity.

Top Suppliers - Mobile Authentication Technologies
Key players involved in the deployment of mobile authentication projects focusing on vertical market segments of advanced biometrics authentication, innovative applications for mobile transactions, NFC and credentialing via mobile.

Top Suppliers - Animal Identification Technologies
Component and solution providers in the field of animal identification active in the fields of advanced technologies for livestock tracking, pet identification and the monitoring of marine and endangered species.

Request your copy or update your profile at idpublications@onpublishing.com

Solutions for the smart city.

Better decisions deliver better outcomes.

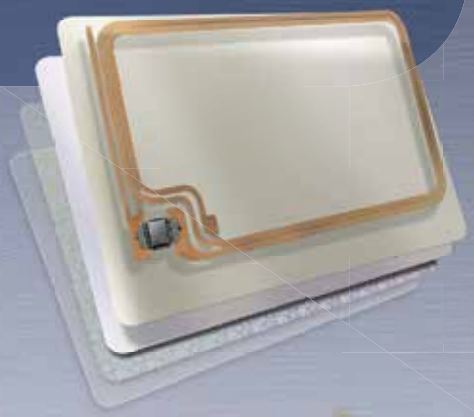
The smart city concept is a vision shared by major cities as they make the decisions today that will shape their future. More services, greater efficiency and a focus on sustainable development are key and Thales is helping governments and public authorities to answer the challenge. By providing greater integration, interconnectivity, and leveraging existing infrastructure, Thales has an unrivalled capability of providing powerful city-wide management systems. Our solutions for the smart city are backed by a proven track record spanning more than 25 years in over 30 major cities and help administrators, operators and citizens arrive at timely decisions that deliver better outcomes.

To learn more about our solutions for the smart city, scan the QR code or visit **thalesgroup.com/smartcity**

THALES

Together • Safer • Everywhere

High Speed Inline Production of RFID Inlays



- All types of antennae
- Plated, wire embedded, printed, etched
- Up to 2,400 inlays/hour
- Including lamination and cover application

INNOVATIVE MACHINERY SOLUTIONS SINCE 1956

MELZER®

Please visit us at: IDENTITY WEEK · London, United Kingdom · Booth: S98 |
ID4AFRICA · Johannesburg, South Africa · Booth: B3 | **ICAO TRIP** · Montreal, Canada · Booth: 50 **more** ▷

www.melzergmbh.com