ID WORLD

THE PLAYERS OF THE AUTO ID INDUSTRY

CARDS - BIOMETRICS - RFID - DATA COLLECTION

2019
BUYER'S
GUIDE

❯ **Transforming digital connectivity**

❯ **Technology and industry trends**

❯ **Profiling leading players in auto ID**

❯ **53** **product categories**

Hadrian Media 15 €

DECEMBER 2018

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

High Quality Equipment
Made in Germany
by MELZER Schwelm
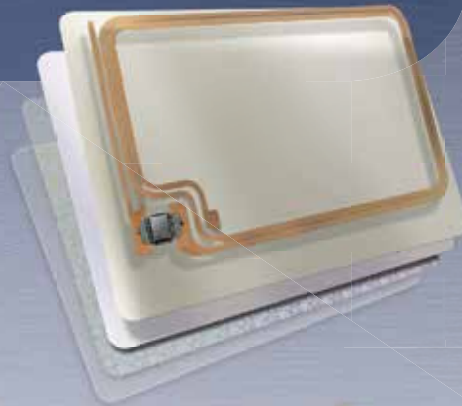
MELZER®

▷ **www.melzergmbh.com**

As we begin the very last of this century's teenage years it is worth reflecting on the transformation the world of advanced ICT has seen in recent times and what lies ahead.

It has been a period of digital revolution, motivated by global needs on a human level in developing countries, in consumerism, connectivity, the vast amounts of data and emerging technologies created to control, analyze and process it. Digital transformation in all organizations is being driven by business needs with the realization of the necessity to embrace an ever more tech-savvy workforce and public. Whether in the service industries, manufacturing, finance or government, institutions and companies need to know more than ever before what their clients' needs are, what their customers want and what their citizens expect. This brave new world is being pervaded by emerging technologies such as artificial intelligence, robotics, cloud computing, chatbots and Internet of Things.

Devices too are evolving. The smart phone, now commonplace and in the hands of almost every person in the developed world, is being enhanced by tools such as Alexa and other digital assistants. In the UK, for example, people use Alexa to report crime. Several governments are using chatbots as 'artificial conversational' systems for communicating their services. One of many is in Mississippi, where 'Ask Missi' allows citizens to access government information. Furthermore, digital assistants and cognitive computing facilitated by mobile, are being deployed in both the public service sector and the manufacturing industry.

In business, identity and trust are key enablers for policy and governance as demonstrated by the introduction of the European General Data Protection Regulation (GDPR) and the giant steps being taken to protect against cybercrime and data breaches.

Similarly, what has been coined as the Internet of Everything, machine learning and AI have become the focus of businesses and institutions in their drive to ally employees and customers with better productivity, increased data monetization and profits. An example of this level of interconnectivity can be seen in the automotive industry with the introduction of Connected Autonomous Shared and Electrified (CASE) strategies. Online networks with 5G performance targeting high data rates are powering vehicles, drones, robots and sensors, while autonomous vehicles themselves are no longer the stuff of science fiction.

While this new digital world and the phenomenal and rapid growth of new technologies continues apace, the building blocks of ICT and identification still hold true and form the very basis of the innovations the world of data and ID is experiencing today. So these core technologies – Cards, Biometrics, RFID and Data in the Internet of Things are as relevant as they were 20 years ago. In fact, biometrics has, as predicted, taken the high ground in all sectors from finance to government, with smart cards still at the heart of ID and security, whether as a hard token or as the key component for integrated mobile logical and physical access.

In this issue, we once more probe into these new and emerging technological innovations and provide a focus on technology suppliers who play a major role in their development and implementation.

Enjoy!

Sophie Boyer de la Giroday

Sophie B. 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

Contents

Viewpoint: with the UK on course to end its EU membership, this report investigates how the status quo may change. It looks at how personal data can flow freely throughout the European Union's member states through the intra-EU data transfer arrangements organisations in place, subject to EU data protection laws, as well as EU data protection restrictions on the transfer of personal data outside the European Economic Area (EEA), and what arrangements exist surrounding the EU-US data shield.

A broad look at how European countries are taking a leading role in understanding the value that can be derived from open data and are making strategic steps to capture and nourish this potential – paving the way for open government across Europe and a better participation of citizens in the decision-making processes of their country.

With growing complexity in eGovernment ecosystems due to connectivity, mobile productivity and interoperability, this report asks whether traditional credentials, such as passwords and smart cards, are keeping up and if mobile is the answer to the challenge. As the proliferation of mobile devices, the Internet of Things and other elements of increasing connectivity impact everyday life, the view is that trends are rapidly changing the landscape for eGovernment as more agencies than ever before leverage advanced applications to deliver citizen services.

2019 BUYER'S GUIDE

ICT technologies are constantly evolving and as the digital era sees widespread adoption in all sectors, auto ID still lies at the ehart of the industry. Our publications regularly update government buyers, end-users in all vertical sectors, as well as integrators with essential tools to support their decisions. Since the year 2000, the **ID Community Publications** offers the prime reference to access the best product portfolio to date in terms of stable and proven auto ID technologies, ideal compromise between functionality, economy and compliance, as well as smart choice for business continuity. As a global directory of the players of the automatic identification industry, it is a unique platform highlighting the market and technology trends in the world of advanced automatic identifcation. The full Annual Buyer's Guide is the world's leading online reference on auto ID technology solution and component suppliers, bringing together a comprehensive review of players in the fields of Cards, Biometrics, RFID and Data Collection.

Adequacy in data exchange: safeguarding flows

With Brexit still high on the world stage and the European agenda, how does the EU determine if a non-EU country, which the UK is on course to become, has an adequate level of data protection? What will really apply if and after the UK leaves and becomes a non-member state: waiver, inclusion, shield or reform?

Currently, personal data can flow freely throughout the European Union's member states as the intra-EU data transfer arrangements organisations put in place, are subject to EU data protection laws. That is set to change with the UK on course to end its EU membership.

EU data protection law places restrictions on the transfer of personal data outside the European Economic Area (EEA). Businesses are prohibited from transferring personal data to non-EEA countries unless they have in place one of a number of safeguards to ensure EU data is adequately protected when processed in those 'third' countries.

One mechanism which has helped to facilitate the free flow of personal data between organizations in the EU and non-EEA jurisdictions is the adequacy framework. That provides the European Commission with powers to designate non-EEA territories as having data protection standards in place that are essentially equivalent to those provided for in the EU.

To-date, the Commission has issued adequacy decisions for 12 territories, including the US, Canada, Switzerland and New Zealand, and it is in the process of adding Japan and South Korea to that list.

UK PM Theresa May and European Commission President, Jean-Claude Juncker

In this regard, the European Commission has the power to determine, on the basis of article 45 of Regulation (EU) 2016/679 whether a country outside the EU offers an adequate level of data protection, whether by its domestic legislation or of the international commitments it has entered into.

Adequacy decisions

The adoption of an adequacy decision in the European Union involves:
- a proposal from the European Commission
- an opinion of the European Data Protection Board
- an approval from representatives of EU countries
- the adoption of the decision by European Commissioners

At any time, the European Parliament and the Council may request the European Commission to maintain, amend or withdraw the adequacy decision on the grounds that its act exceeds the implementing powers provided for in the regulation.

The effect of such a decision is that personal data can flow from the EU (and Norway, Liechtenstein and Iceland) to that third country without any further safeguard being necessary. In others words, transfers to the country in question will be assimilated to intra-EU transmissions of data.

Michel Barnier, Chief European Negotiator for the UK exiting the EU

Brexit and data protection

Following the UK Government and the European Commission's announcement that the UK and EU27 countries had reached a draft agreement on the terms of the UK's withdrawal from the EU, part of the agreement included an outline of the political declaration on the future EU-UK relationship with regard to data protetion.

According to this declaration, the Commission will assess UK data protection standards on the basis of the EU's 'adequacy framework' with a view to adopting an 'adequacy' decision 'by the end of 2020'. Over the same period, the UK will 'take steps to ensure comparable facilitation of personal data flows to the Union', it said.

While the political declaration indicates that a mutual EU-UK 'adequacy' arrangement could facilitate the flow of personal data between the EU and UK after 2020, the draft withdrawal agreement outlines what protections should apply to the UK's processing data about data subjects outside of the UK prior to the end of the Brexit transition period and after that period in circumstances where a future adequacy arrangement is not in place.

Cyber security

According to media giant, Forbes, set against this backdrop of Brexit political uncertainty, is a cybersecurity industry increasingly worried about the post-Brexit threatscape.

According to its own research, Forbes says whether the UK crashes out of the EU with or without a Brexit deal, the impact upon cybersecurity is likely to be considerable and immediate for business and industry. Some

European Commissioner for Digital Single Market, Andrus Ansip

EU and US shield

At the time of its implementation, approval of the the Privacy Shield preserved a key legal mechanism for EU-US data flows, according to the Future of Privacy Forum (FPF). Continuing challenges were also mooted - surveillance reform needs continue on both sides of the Atlantic - but the Privacy Shield is seen as a much needed certainty for American companies that rely on the EU-US framework to pay and manage their EU-based employees, as well as for the 150 plus EU companies that use the framework to transfer data to their own US subsidiaries.

The Safe Harbor agreement ceased amid concerns regarding US government surveillance programs. The Privacy Shield approval was also implemented in the wake of surveillance reforms and additional commitments by the US government. The FPF detailed more than two dozen significant reforms to US surveillance law and practice since 2013. A previous study revealed that Safe Harbor included 152 companies who are headquartered or co-headquartered in European countries, which span a wide range of industries and countries.

The 152 companies include some of Europe's largest and most innovative employers - many from the world of advanced digital information and ID, doing business across a wide range of industries and countries. According to its raison d'etre, EU-headquartered firms and major EU offices of global firms depend on the Privacy Shield program so that their related US entities can effectively exchange data for research, to improve products, to pay employees and to serve customers. FPF also found that more than 3,700 companies have signed up for Privacy Shield – a nearly 70 percent increase from 2017.

Meanwhile, the European Commission recently published its second annual review of the EU-US Privacy Shield, finding that the US continues to ensure an adequate level of protection for personal data transferred under the Privacy Shield from the EU to participating companies in the US. This is good news for business, supporting transatlantic trade and ensuring meaningful privacy safeguards for consumers. It is also good news for EU employees and companies, many of whom rely on the agreement to retain and pay staff. The Commission's review highlighted a key next step to support the Privacy Shield arrangement – urging the U.S. government to appoint a permanent Ombudsperson by the end of February 2019.

industry experts say opinion is divided into three main areas of cybersecurity concern: employment, regulatory compliance and information sharing.

International transfers

According to further reports, enforcement of GDPR matters will change under any withdrawal agreement. The Information Commissioner' Office (ICO) will no longer be part of the European Data Protection Board, and will no longer be able to act as a lead authority in cross-border processing issues affecting more than one EU country.

Businesses that process personal data in the UK and in EU countries may have to deal with the ICO for the UK processing activities and designate a 'main establishment' in an EU country for their EU processing activities.

In the wider world, looking west to data

transfer between Europe to the United States, frameworks seem to be in place but reforms are constantly on the table.

In 2016 the EU-US Privacy Shield, a renewed framework for transatlantic data flows, replaced the EU-US Safe Harbor arrangement. The EU-US and Swiss-US Privacy Shield Frameworks were designed by the US Department of Commerce and the European Commission and Swiss Administration to provide companies on both sides of the Atlantic with a mechanism to comply with data protection requirements when transferring personal data from the European Union and Switzerland to the United States in support of transatlantic commerce, subject to privacy safeguards and commitments.

The Swiss-US shield framework was approved by the Swiss Government in early 2017, complying with Swiss requirements.

by Victor March

EU perspectives on digital technology for economic development

Stefano Manservisi, Director General of the European Commission DG DEVCO, looks at how the EU is supporting partner countries in addressing the key challenges brought about by the '4th industrial revolution'. How is AI and the broader spectrum of digital technology adoption transforming the lives of citizens?

According to the European Commission, the EU's Digital Single Market is the second biggest contributor to Europe's economy. It is not only an enabler for constant innovation, but if used and developed properly, it can also be a key driver for inclusive growth and sustainable development.

Following the EU's strong effort over the past years to mainstream digital services and technologies into its development policy, it is now looking to replicate this success in other regions. In this exclusive interview, Stefano Manservisi, Director-General for International Cooperation and Development at the European Commission, discusses this aim to support partner countries outside of the EU — and particularly those suffering economic hardship — in addressing the key challenges that digitalization and the technical revolution will bring, and how digitalization will play a central role in improving people's lives.

How important is the massive rise in digital technology adoption in terms of transforming economies and cultural development?

We are entering the fourth Industrial Revolution — the digital one — based on information technology and artificial intelligence. This is hugely important and transformational as these technologies are connecting people with institutions, people with markets and people with ideas. I believe this is something which embraces a deep cultural revolution as well, in order to grasp all the benefits — which are many. In fact, there is a need to invest in technology and in knowledge, as well as a requirement to transform culture and literacy.

All this can be done throughout the world — in developing and developed countries alike. It is a powerful moment to unify and therefore requires cooperation, as this revolution has no boundaries — only shared opportunities.

What are some of the challenges for empowering people with digital strength, based on the lessons already learned by the European Commission?

The main lesson is that one can control not only the technological application, but provide powerful impetus for more cooperation and collaboration. This positive aspect of the new industrial revolution is linked to digital inclusion, information technology and artificial intelligence. It can also ultimately lead to increased democracy because it shortens the path and narrows the gap between citizens and public sector institutions, making them much more transparent.

While everyone can be more empowered, this change must still be subject to a deep societal transformation in order to create an inclusive society without any group or individual feeling excluded from the huge opportunities that present themselves.

What experiences can the EU share with other parts of the world, which are embarking on strategic digital developments?

The European Union has developed digital skills and policies within its own internal market and we are now ready to share our knowledge and experience with the rest of the world. This is the basis of our international cooperation. This fourth Industrial Revolution is a powerful game-changer for our societies and for our industry. Because information technology connects people with institutions and markets and turns ideas into opportunities, the European Commission has been building IT as a strength for its own internal market.

Digital-for-education projects are advancing to reach people in remote areas

Today, we are all confronted with the challenge to create jobs for youth that are sustainable, so IT, digital technologies and artificial intelligence are perfect drivers to help realize this goal.

While the EU is ready to share its own experience via international cooperation and policy, we also know that this will not be realized without effort. The first consideration is to protect rights of people, to protect identity and data; second is to allow democracy to grow and not to be dependent on new technology. This means we have to drive technological advancement and not to be driven by it. All this requires good governance by a powerful and credible institution with regulatory frameworks which are clear and enforceable.

As it eventually leads to a new way of participating, the requirement is for all to be active protagonists of change. If people are closer to an institution through digital applications, it also means that they need to take more responsibility because they have increased leverage and are therefore able to take meaningful decisions. So the European Union is using this not only as a driver for international cooperation in a new style, but also to promote its agenda of better governance to empower people and to have more transparency in public finance. International cooperation is about people and a better life for citizens - this is the ultimate challenge.

What are some of the specific digital strategies already being introduced or put forward - particularly in developing countries?

Digital-for-development is a new avenue which has already been opened. It is something which is unifying and not just available for the more privileged sections of society. In fact, digital technology can lead millions of people out of poverty. In this regard, the European Commission is working to apply this in the Horn of Africa - an area which is poor, unstable and still emerging from wars. The aim is to bring together different stakeholders across the region to realize new technology as not only a 'ready-made' product, but a way to train people and build a culture to create jobs.

Meet Stefano Manservisi

Stefano Manservisi is Director-General for International Cooperation and Development at the European Commission, a post he has held since 2016. He previously served as Head of the Private Office of Federica Mogherini, High Representative of the Union for Foreign Affairs and Security Policy and Commission Vice-President. In 2014, he was the Head of the Delegation of the European Union to Turkey. Before that, he held different positions at the Commission, including as Director-General for Migration and Home Affairs, and Director-General for Development and Relations with African, Caribbean, and Pacific States. He has also headed various Private Offices of senior figures in the Commission.

What about other sectors that are impacted by this transformational technology?

In healthcare, we are collaborating with the Bill and Melinda Gates Foundation for financing the Foundation's project of a digital platform for health across Africa. This is intended to empower and allow poor citizens in African countries to have access to basic knowledge and services on health. Another sector is digital-for-education — an area in which we are already advancing — reaching people in remote areas far from cities or educational and cultural institutions.

Similarly, the Commission has recently launched a major program in order to create literacy and a new profile of employability for young people. So 'digital' is something which is not only the future but also the present in our work for Africa, in our work for the poor - and in our efforts to reach sustainable development goals across the continent and in other countries of the world, where poverty is rife.

Evaluating gateways to open data maturity in Europe

New reports show a number of European countries that have taken a leading role in understanding the value that can be derived from open data, have made strategic steps to capture and nourish this potential – paving the way for open government across Europe
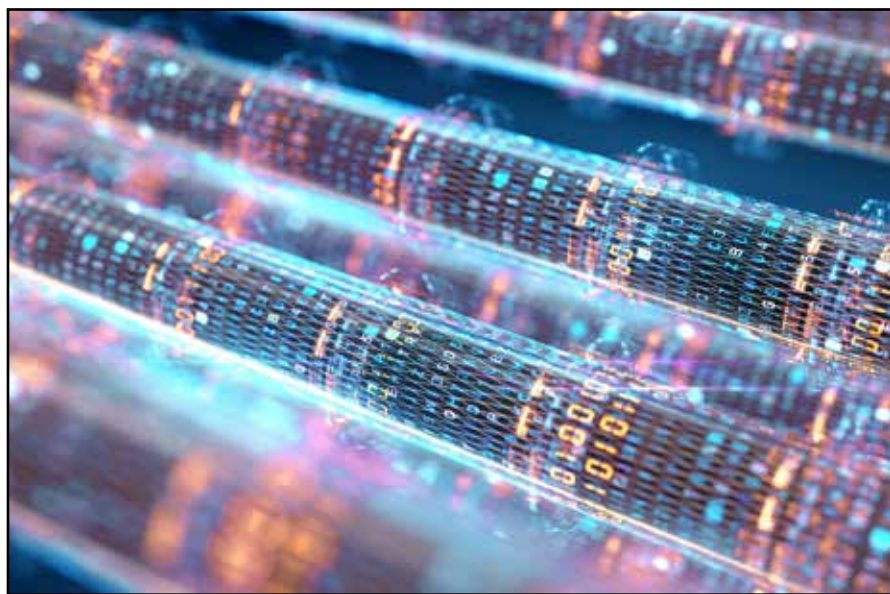
With the emergence of data-driven innovation hubs and smarter cities across Europe, the potential of data has become beyond dispute. In particular, the value of the data collected by the public sector has gained in relevance and attention in the past years. This translated in an intensification of efforts to ensure the publication of government held data at national, regional and local levels.

Open data has served as means to foster open governments across Europe and a better participation of citizens in the decision-making processes of their country, to increase transparency of public spending and political handling. Open data has sustained the development of data- driven processes and activities in the context of smarter mobility and connected cities. It has enabled civil society's watchdog function by making data on public spending, ownership, public officials' wages and public spending, and led to the flourishing of a new kind of investigative journalism that is data-driven. In short,

open data has become an enabler for innovation and knowledge in today's world.

Shedding light into the European countries' progress with regards to their open data activities, the EU Portal's 2018 landscaping provides a tool for benchmarking this progress against the past and in the years to come. The key findings of the year's assessment summarize Europe's maturity levels on four relevant open data dimensions: policy, portal, data quality and impact. The findings emphasize the leading role of a few European countries that have timely understood the value that can be derived from open data and have taken strategic steps to capture and nourish this potential.

New benchmarking

The 2018 report introduces deeper granularity in how open data maturity at country level is assessed. It captures the finer elements of the previous assessments' dimen-

sions - policy and portals - and complements them with two new ones: impact and quality. In terms of policy maturity, the new benchmark sets a stronger focus on updates to and scope of national open data strategies, and on what can be described as an enabling type of coordination activities – that enables the local and regional levels to develop their own open data initiatives, according to their own needs and at their own pace. Additionally, the policy dimension highlights the activities that foster reuse of open data by both the public and private sector.

In terms of portal maturity, the new benchmarking focuses on advanced portal features that help drive interaction between the supply and demand sides of open data and enable a more strategic publication of data. The updates capture the level of sophistication of national portals to include advanced functionality, usage analytics, variety of data available on the portal, and a strategy to ensure the portal's sustainability in time.

Strategic transformation

With its newly introduced dimensions – impact and quality, the benchmark aims at incentivizing European countries to enhance their open data efforts in new strategic areas. Increasing the quality of both metadata and data is the natural next step to ensure that value can be derived from published open data. By capturing and measuring this value, the virtuous circle around open data publication and reuse will be strengthened and the ecosystem of advocates increased. At the same time, it will help reduce the circle of sceptics as it will provide evidence of the positive effects that open data can have. Working on both quality and impact represents the two natural next steps for those
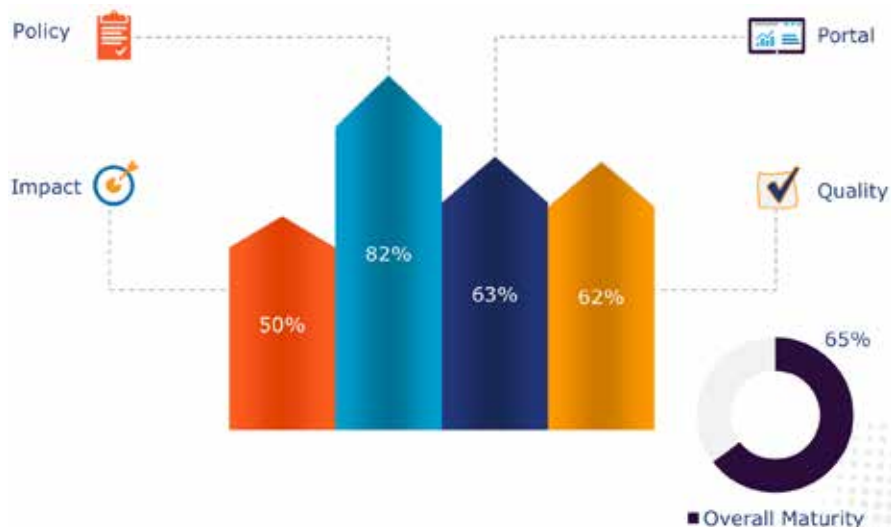
Open data maturity scores by policy, impact, portal and quality, EU 28 2018

European countries that already have a solid foundation in place, in both terms of policy and portal.

The overall results across Europe emphasize the heterogeneity in the speed of transformation and the priorities that countries have set along the road. With an overall maturity level of 82 percent across the EU28 on the policy dimension, Europe has reached maturity in terms of its policy foundation. Countries are now setting new focuses. The less advanced open data countries choose to take the natural next step and invest in the modernization of their national portals as main gateways to open data available throughout the country. The more open data mature countries now shift to boosting the quality of data publication. The top performing ones are now prioritizing the impact derived from open data and undertake activities to monitor and capture this impact. The 2018 results reflect this observation.

With a maturity level of 63 percent on the portal dimension, the EU28 average captures both the advanced level of maturity achieved by one third of Europe's national portals and the 'room for improvement' observed in the other two thirds. In terms of open data quality, a similar observation holds true. With an overall level of maturity of 62 percent on the quality dimension, Europe is only advancing at a sluggish pace. Only seven of Europe's 10 top performers showcased very good results of 75 percent and above on this dimension as well as a clear focus on improving the quality of published data and metadata. Concerning the fourth element – open data impact, the results in 2018 are modest. The

overall maturity of 50 percent on the impact dimension provides evidence of the very slow pace at which the EU Member States are moving, with only three of Europe's top performers recording a maturity level of 75 percent and above on this dimension. This underlines the need for more strategic action to help increase the awareness around the pivotal role that demonstrating impact has. The modest result also emphasizes the urgency to develop a strategic approach to monitor and measure the impact derived by the use of open data.

Speed and focus

The heterogeneity in terms of the speed and focus that European countries show in their transformation is also reflected by this year's maturity clustering. In 2018, only five European countries qualified as 'trend-setters'. Ireland, Spain, France and Italy provided solid evidence of their sustained open data efforts, with scores of 80 percent and above. Cyprus has frog-leaped its transformation in 2018 and has now reached an overall maturity score of 79,6 percent. This great progress ensured Cyprus a place amongst the top five European best performers.

The decrease in scores of many of last year's 'trend-setters' also led to a larger group of 'fast-trackers' in 2018, with now 16 countries pertaining to this group. In general, only limited progress can be observed at Member State level, with the majority of Europe scoring around the same levels as in 2017. Only a few countries recorded signifi-

cant drops in scores. This can be attributed to the fact that open data was deprioritized on the political agenda at national level, as well as the faster speed at which other countries have pushed progress in 2018.

This year's assessment strengthened the position of those countries that remained consistent in their efforts to drive transformation through open data.

Progress monitoring

With its content, the open data landscaping report achieved both its benchmarking and benchlearning purpose. In terms of its benchmarking purpose – enabling monitoring of progress, the 2018 report sets the baseline against which progress across Europe will be measured. This progress gains in relevance when weighed against the broader goals set by the European Commission in the data field. In terms of the research's benchlearning objective – enabling learning from each other, the report provided a series of good practices sourced from the observation of the European countries' open data initiatives.

Strategic awareness

The report underlines the necessity for a better transfer of knowledge and expertise from Europe's more advanced countries to the less open data-savvy ones. While keeping the different maturity levels and country focus areas in mind, the 2018 results highlight an overall urgency to ensure publication of high-quality data to help boost reuse, as well as a compelling need to increase the strategic awareness on the impact generated by open data. With data quality representing a pivotal element to enable reuse and impact, more effort is needed in this regard at national level. The relatively modest scores on the impact dimension highlight the progress that still needs to be done. At the same time, the results emphasize the complexity of the goal, particularly in terms of defining the 'what' and the 'how' of measuring impact. This will be Europe's main challenge in the years to come.

by EU Portal Team
European Commission

Increasing access to data while retaining trust

New research explores issues and solutions experienced by organizations which share or publish data, or who have expert knowledge of data sharing practices in specific industries. What are the challenges? Are current models up to it?

Today, organizations face many challenges when sharing data, whether they are using current information models or introducing new ones. Sectors of particular importance and interest include Fintech, extractives, transport, healthcare and environmental. Research by ODI found these five sectors varied considerably in the degree to which data was shared and in the willingness to share more. For example, the healthcare sector is people-focused with significant privacy concerns about highly-personal data. Conversely, the transport industry has many demonstrated success stories and a general recognition of the value of opening data. Despite differences, the sectors shared some similar challenges suggesting the possibility to learn from emerging models.

Data control and access

The need to resolve issues of data control and access among multiple competing stakeholders was seen as a barrier to sharing. In the automotive industry, it is not clear who should control data generated by modern automobiles. Access to the data could be claimed by drivers, passengers, car owners, car manufacturers, software or hardware providers, or the wider transport network. Similarly in the extractives industry, there are differing views on who controls or has access to data about deposits and reserves — the government, the extraction company, the public, or international bodies. The issue becomes further complicated when data includes a personal component. What data should an individual control or own?

Resolving these issues may require an unaccustomed degree of collaboration and sharing among otherwise competing parties and a shift of organizational or industry culture may be required before any technical solution can be effective. Slow progress in meaningful sharing of healthcare data is an example of halting progress. Similarly, the transport sector may need higher degrees of cooperation and data sharing to join separate networks and enable increased transport usage and industry growth.

Managing data as part of the infrastructure will require resolving multiple overlapping data rights each with their own motivations and challenges.

Trust

Research found there are significant identified problems on the PSD2 regulation when it comes to trust, because of the way the payment services regulation and payment service directive was written.

Trust in data quality is dependent, in part, on the credibility of its source. This is particularly important in extractives where trust is low throughout the sector. Both extractive companies and some governments are assumed to be acting in their own interests rather than the public interest. Companies are not trusted to released unbiased data and data released by governments who aren't see to be generally credible will not be trusted. However, this varies by sector. In the autonomous vehicles sector, data from local authorities may be seen as more trustworthy than data from a private company.

One way Transport for London (TfL) gained consumer trust for the Oyster card system was by solving customer problems quickly and issuing refunds instantly where needed, thus increasing customer willingness to allow TfL access to individual journey and payment data.

Public trust can be damaged by data breaches, so successful sharing models must include robust data security technology and governance. Part of the research indicated opinion that the technical standards for regulated parties in the payment services directive (PSD2) were currently too weak, making a data breach more likely.

Consumers will also lose trust where they feel they have been misled. The UK's National Health Service (NHS) experience with care.data showed the consequences of failing to earn the trust of stakeholders by rushing to share data without robust data governance processes in place. The Caldicott enquiry that followed highlighted the importance of rigorous data governance policies in establishing trust. While this example is from the healthcare sector, it could apply to other sectors dealing with highly sensitive data.

Transparency

People own the resources, they should know about what their governments do so that they can hold both companies and their governments accountable. Transparency is often opposed by those who feel they or their organization will be seen negatively if data is released. This issue crosses sectors, from government resource departments unused to detailed public scrutiny, to NHS GPs concerned about the use of league tables. Within any environment however, there will be natural allies of data sharing. Revenue authorities may be more interested in opening details of extractive activities than the departments working more closely with extractive companies. When discussions about healthcare data sharing have included both patients and GPs, GPs have been more willing to share data when they directly see patient support.

Business cases

Research and surveys by ODI found that traditional business models are being destroyed and new ones created at the same time – which is is not straightforward or easy. Many organizations lack knowledge of business models that would support greater degrees of data sharing. It was felt that in the rapidly-evolving transport sector there are not enough successful examples to overcome the reservations of risk-averse managers. In the historically secretive extractive industry, organizations typically only see downsides of sharing data that they have always viewed as commercially sensitive. When extractive organizations do share data, the terms of the sharing agreement are rarely made public so the industry lacks good examples to learn from. Furthermore, examples can take time to develop whereas the downsides of data shar-

ing, e.g. resources required, are usually more immediately apparent.

Personal data

Many organizations and sectors struggle with how to make effective legal use of personally-identifiable data. The lack of test cases of GDPR has led to organizations being very cautious. People who have historically dealt with confidential data may be reluctant to share that data even when there is a clear legal basis. One interviewee remarked that data protection is often used as an excuse not to share data.

Anonymization in particular is both a technical and a cultural issue. Data publishers and decision makers may not understand the anonymization spectrum or feel sufficiently informed to design or make decisions about data aggregation or anonymization processes. Responses from the environment and healthcare sectors raised this issue, but it could affect any sector which deals with personal data.

New impetus

Effective data sharing requires the motivation and willingness to do so as well as the technical and management skills to implement it effectively. Changing market conditions will be one impetus for data sharing. Examples from ATMs and mobile phone networks in the past have shown how organizations shared data in order to make these systems work for customers and grow the market. Legislation and government policy that requires or enables data sharing will also have an effect, though some feel that legislation works too slowly to take advantage of technical innovation.

Successful examples of data sharing can demonstrate benefits to market players and influence sharing throughout the sector. However if details of data sharing agreements are themselves not made public, their impact will be muted. Hence a trend for extractive companies to publish contract terms could be an important step to greater openness in that sector. Long-term stakeholder engagement to enable culture change was seen by healthcare sector interviewees as essential to increased data sharing in healthcare. Lessons learned in this sector could prove useful to other sectors. Discussions with GPs and patients about data

Extractives may share some data publicly to pre-empt increased regulation

sharing and with clinicians and researchers about data collection, management, and use were suggested. Accountability and data governance needs to be developed together with stakeholders to ensure it works for all.

Data sharing models

The UK Environment Agency now considers data sharing whenever a new dataset is created. They use a checklist to help managers determine which data can be shared with an open license and which needs a more restrictive license. Oil companies sometimes share data about their resources in order to attract or reassure investors. Both transport companies (such as Uber) and extractive companies may share some data publicly or with regulators in hopes of pre-empting increased regulation. The Open Banking regulatory framework allows existing financial institutions and new organizations to share financial data for the benefit of consumers. The NHS does not have centralized data governance, it allows individual trusts to make independent agreements.

New models are being suggested and tried within the transport and autonomous vehicles sector. If market players do not cooperate, a model of competing ecosystems led by a few major players may develop. The importance of high quality training data for autonomous vehicles shows the potential for public bodies to license CCTV and other relevant data to industry entrants.

Synthetic data sets of edge cases used for training autonomous vehicles are a candidate for sharing amongst developers as it is likely to increase car safety, leading to the market acceptance.

by Open Data Institute

Digital Economy Conference organized by Wise Media in Abu Dhabi

DEC Summit, a uniquely influential thought-leadership symposium, created by a forward-thinking community is moving forward with a series of initiatives aimed at anticipating, assessing and addressing the evolution of the Digital Economy. A milestone event for the Arab digital economy was hosted at the Emirates Palace to promote digital transformation for peace, progress and sustainable development

The Digital Economy Conference was organized by Wise Media on 16 to 17 December 2018 at the Emirates Palace, Abu Dhabi, under the patronage of the UAE Government and with the support of the Council of Arab Economic Unity of the League of Arab States.

The event opened its doors as the eighth Sustainability Summit initiative endorsed by the European Commission, with the participation of the Director General International Cooperation & Development. DEC 2018 was supported by the League of Arab States, CAEU and by AFDE as hosting government sponsor.

A world-class speaker line up

Designed as a summit on how to foster the regional alignment of digital transformation agendas to drive societal development, DEC 2018 saw high profile speakers and delegations representing the United Nations, World Bank, OECD, League of Arab States, CAEU, AFDE, European Commission, NATO, prime academic institutions and governments convene in Abu Dhabi from around the world to contribute to a vibrant exchange on how to best address the needs of the digital society at a regional level to promote peace, progress and sustainable development.

Launch of a new strategy

The Arab Digital Economy Strategy reviewed by a committee of 65 experts from around the world was presented by AFDE to government delegations attending from the 22 member states of the Arab League, in the presence of H.H. Sheikh Saif bin Zayed Al Nahyan, Deputy Prime Minister and Minister of Interior of the UAE.

Keynote addresses by the Secretary General of the League of Arab States, the Secretary General of the Council of Arab Economic Unity, the Chairman of the Arab Federation for Digital Economy and the

DEC 2018 saw high profile speakers and delegations from all major international organizations, governments, NGOs and other prime institutions convene in Abu Dhabi

Call to action in the era of AI

As a highlight of the event program of DEC 2018, a series of conference sessions were furthermore designed respond to Wise Media's ongoing initiative on digital transformation in the era of AI: 'A new Agenda for Education and Labor', 'Healthcare Leveraging Disruptive Technologies' and 'Finance in the Digital Economy' saw policy makers and luminaries from academia discuss opportunities and challenges faced by the digital society in key sectors of the global economy in light of the advent of Artificial Intelligence and the Internet of Things (IoT).

Bilateral and multilateral exchanges

DEC 2018's two-day conference program was completed with high-profile networking activities. A comprehensive agenda of bilateral meetings and multilateral discussions took place, paving the road to intensive activities to follow-on to the introductions made in Abu Dhabi. As of December 15, exclusive activities were organized for select guests, including the gala dinner 'Sharing a Vision and a Strategy', the private reception dinner 'Connecting Continents', as well as private visits to the Grand Mosque. High-profile government representatives were introduced to H.H. Sheikh Mohamed Bin Zayed during a ceremony organized for ministers attending the first Arab Digital Economy Conference.
www.decsummit.com

President of Cairo University illustrated a regional plan of cooperation that was discussed with government representatives and experts throughout the two-day conference.

Select members of the Expert Group activated to review the Arab Digital Economy Strategy prior to its launch were invited as guest speakers to comment on the initiative and contribute to the ongoing discussions.

The Arab Digital Economy Strategy was launched at DEC 2018 by AFDE addressing government delegations attending from the 22 member states of the Arab League

Empowering eGovernment with mobile ID

There is a growing complexity in eGovernment ecosystems due to connectivity, mobile productivity and interoperability, but are traditional credentials, such as passwords and smart cards, keeping up? Is mobile the answer to this challenge?

Just as the proliferation of mobile devices, the Internet of Things and other elements of increasing connectivity have impacted our everyday lives, these trends are rapidly changing the landscape for government agencies. More agencies than ever before leverage advanced eGovernment applications to deliver citizen services. Government workers are at the forefront of the mobile workforce growth, with around 90 percent of government employees using at least one mobile device for their daily work.

Collaboration among agencies and between states is increasing interoperability of eGovernment systems and networks. All of these elements of growing connectivity have the potential to significantly increase productivity, streamline operations and enhance service levels to citizens and stakeholders. But these benefits are only one side of the story. The added complexity of the new eGovernment environment also creates many new challenges, as government agencies search for effective ways to secure and control access to the rapidly growing number and variety of gateways to their ecosystems.

Cybercrime threat

It seems hardly a week goes by without reading of another major data breach or cyber attack in the headlines. The numbers do not lie: four years ago cybercrime and data breaches reached an all-time high — an estimated one in four Americans received a breach notice over a 12 month period — and this growth has continued. Government agencies are attractive targets for cyber-criminals, as they tend to hold particularly sensitive (read: valuable) information.. Not only are breaches becoming more frequent — they are becoming more costly.

One side of the problem is the growing complexity of cyber attacks, aided by increased computing power and advanced algorithms. Sixty percent of U.S. state CISOs reported a notable increase in the sophistication of the cyber threats they face. The other side of the problem? The so-called 'human-factor' challenges that are amplified by the connected workforce. Human errors - from weak passwords to workarounds - account for almost half of all government breaches.

Today, we are all tethered to our mobile devices. So it follows naturally that we want to use the mobile device of our choosing in our work lives. Many government agencies are embracing a BYOD environment as part of the overall productivity boosting goals of empowering the mobile workforce. Along with using their own devices, mobile workers are also used to finding a specialized app for everything, and they take the same approach to their mobile productivity on the job. A survey found that 80 percent of U.S. workers admit to using non-approved applications in their jobs, creating an entire 'Shadow IT' world of unsanctioned app use and data exchange that blurs the lines of a government agency's digital ecosystem.

Whether accessing sanctioned or unsanctioned applications, many government employees fail to maintain strong security controls on their devices. A recent study found that 41 percent of government employees admitted to regularly practicing 'potentially harmful behaviors'. These included: 25 percent fail to use passwords to secure their mobile devices; 33 percent admit to using passwords that are easy to guess; 31 percent regularly use public WiFi networks; 52 percent fail to use multi-factor authentication or data encryption.

Evolving regulations

As they maintain particularly sensitive information, government agencies have always

been subject to strict data security regulations. But the increased risk - and increasingly successful attacks - in the government world are leading to more demanding standards, tougher regulations and harsher sanctions and fines for non-compliance. From the new NIST Cybersecurity Framework 1.0 to IRS 1075 regulations, to new requirements from CMS and the Office of Child Support Enforcement, agencies in every field are facing tougher standards that require more complex and comprehensive data security solutions.

While all agencies feel the growing pressure of security threats, there is not matching growth in funding for these projects. In fact, more than half of state governments have a security budget that accounts for less than five percent of total state spending. The challenge, then, is finding a security solution that enables government organizations to do more with less.

Identity at the core

Identity is the core element of all of these trends shaping the connected government ecosystem. Government employees access eGovernment systems and mobile applications with identity credentials - and cybercriminals gain unauthorized access through hacking, stealing or otherwise subverting these identity credentials. To position themselves for success in this new landscape, government agencies need to focus on making trusted identity the core of their security strategy. With the ability to quickly and effectively authenticate the identity of both the user and the device, an agency can fend off sophisticated threats while empowering the streamlined productivity and enhanced service levels of a fully connected, anytime-anywhere workforce.

Passwords secure access to 99 percent of all digital resources. But 'secure' is not exactly the right word. Given enough time, sophisticated cybercriminals can hack even the strongest of user-generated passwords - because passwords fall victim to two key human-factor flaws: people and passwords are predictable. Every year, security experts publish lists of the most common passwords, demonstrating a troubling truth: the majority of user-generated passwords fall on a list of just 100 or so. Even when users try to be clever and complex, they are unknowingly predictable. Half of all passwords follow one of 13 common (hackable) patterns.

According to statistical research, the average U.S. worker uses 19 different usernames and passwords to access the digital resources in their jobs. We prize innovative approaches to overcoming obstacles and increasing productivity in the workplace. So it is no surprise that, given the task of juggling 19 different identities - and the expectation of regular password refreshes - government employees find creative ways to work around these cumbersome security requirements.

Sophisticated cybercrime threatens even the strongest passwords. The password flaws above are susceptible to 'brute force' cyberattacks - directly guessing or cracking the plain-text password. But today's advanced hacking techniques can find side doors for gaining access. Techniques such as rainbow tables enable hackers to 'pass the hash' - cracking the underlying encryption of a password system. This method is faster than brute force hacking, and even long, complex and truly random passwords are still susceptible, since the hackers no longer need to crack the plain-text password.

Complex systems

Hard tokens and stronger controls impede productivity. Faced with weak passwords and frequent work-arounds, many government agencies fall victim to assuming that stronger, more complex access controls equal better security. This means implementing password complexity requirements, mandating frequent password refreshes, and adding hard tokens — such as smart cards or OTPs — to authentication protocol. In practice, this adds up to even more cumbersome workflows and end-user burdens that hamper productivity. A survey of government workers found 69 percent agreed that security protocol reduced their productivity by slowing workflows.

Rather than looking to add complexity to authentication protocol, government agencies must look for ways to simplify. In looking for an identity solution for empowering a workforce tethered to and driven by their mobile devices, the simple answer is built into the challenge. Modern mobile devices have powerful built-in security capabilities that can assist in establishing a trusted identity for each unique user and secure access to the entire digital ecosystem. Just as importantly, users already carry their mobile devices with them at all times and already love their convenience and usability.

Mobile identity security

A mobile identity solution provides a much more secure authentication platform than traditional credentials like usernames and passwords or hard tokens, enhancing digital

Cybercriminals gain unauthorized access through subverting identity credentials

Proliferation of mobile and other connectivity devices are changing the IT landscape

- block jail broken phones: restrict the ability for users to jailbreak their phones bypassing manufacturer security;
- mobile device authentication: ensure you know and authorize each unique device connecting to you network and only allow authorized users in;
- mobile device management: provide the ability to provision security policies and remotely manage devices to mitigate risk;
- use secure work partitions: Mobile Device Management (MDM) platforms are helpful to segregate "work" and "personal" data on the device;
- signed/vetted applications: legitimate applications downloaded onto a mobile device will have been signed and vetted before they are loaded onto your system. So long as they are from an official store - such as the Apple App Store - they have gone through a rigorous process to enhance their security and stability.

security by leveraging the inherent security capabilities of today's mobile devices:
- device location and attributes: GPS lets you identify the location of the individual authenticating for access and flag unexpected or suspicious locations for further investigation. GPS also helps locate lost or stolen mobile devices;
- application sandbox: Applications on mobile platforms run separately from the core operating systems. Hackers cannot gain unauthorized access to the entire mobile device (and the mobile identity) via a single compromised app. This also prevents malware located on one app from corrupting other apps;
- cryptography: Mobile devices include native encryption to secure data and protect sensitive information as it moves throughout a digital ecosystem;
- biometrics: Many mobile devices feature easy-to-use biometrics capabilities such as fingerprint or facial scanning.

These capabilities enable enhanced, multi-factor identity authentication that establishes the true physical presence of the individual authenticating for access. Because the user friendly biometric reader is built into the mobile device, they drive greater compliance and fewer high-risk 'work-arounds'. Trusted Execution Environment or Secure Element: Many mobile devices feature a tamper-resistant micro-controller capable of securely hosting applications and crypto-

graphic data. These elements are like small firewalls within a mobile device, enabling secure transaction processing.

While the mobile device provides a trusted platform for identities and transactions, there are a number of best practices that should always be considered when designing mobile applications:
- force PIN/biometric access: for devices that support it, require the use of the most secure access restrictions possible on the device;
- find-my-phone apps: most mobile platforms have apps and services to help track down lost or stolen phones;

Productivity-boosting

Embedding trusted identity within an already-popular device puts a convenient identity authentication solution at your users' fingertips, eliminating the need to manage myriad complex passwords and tote additional credentials or tokens along with them.

Users authenticate faster and move through workflows more efficiently, boosting productivity and helping to enhance citizen service levels. And with mobile productivity becoming essential to efficient operations

There are best practices to be considered when designing a mobile application

Traditional access control card systems are being replaced by mobile authentication

and services, trusted mobile identity creates a seamless experience as mobile workers move from authenticating to accessing mobile apps to carrying out their daily work functions, anytime and anywhere, via their mobile devices.

Though most IT administrators know the security and customer-usability flaws of traditional identity authentication methods, budget constraints keep many from examining alternatives. Ripping out a government agency's entire authentication architecture would be a costly, time-consuming affair - and could impact interoperability between agencies and states.

Instead, mobile identity provides a solution that is easily implemented within the existing authentication architecture of most government agencies. Advanced mobile identity solutions enable the mobile credential to replace username/password authentication, serve as a hard token, and even provide biometrics-based proof-of-presence - all within the same front-end log-in framework and back-end authentication architecture that an agency is currently using for application and network access. And because most users already carry compatible mobile devices, the deployment of a mobile identity solution is fast and cost-effective, with minimal downtime.

Enhanced eGovernment

To provide a better understanding of the full power and potential of a mobile identity solution, here is a look at real-world ways in which mobile identity enhances security and empowers productive eGovernment: VPN authentication, transaction signing, transaction verification and mobile derived credentials

Signing into a VPN can be a frustrating task. Government employees generally must manage a complex password and an additional hardware token. With mobile push authentication, a mobile push notification is automatically sent to the verified, secure mobile device. The user simply simply clicks 'OK' to confirm the authenticity of the VPN session - no password required and no searching for a single-purpose token lost at the bottom of their work bag.

Many government processes and workflows require formal, signed approvals to move to the next step, close the transaction or validate the information. Traditional digital signing is complex to deploy and often has poor user experience that slows workflows. A mobile identity platform can leverage the built-in biometrics capabilities of a mobile device to allow fast, easy and secure digital signing. A push notification alerts the user that a digital signature is required, and the user simply scans a fingerprint or puts in their password to enable a cryptographic signature of the data.

Whether it is an inspector submitting a report, a law enforcement officer obtaining a warrant, or an employee submitting a requisition, the ability to conveniently and securely sign a document, verifying both

identity and authenticity, can speed operations, provide better customer service and dramatically boost productivity.

Transaction verification

When transferring government funds between agencies, making payment to citizens or even accessing sensitive data, how can you be sure your system isn't infected with malware ready to intercept the transaction? Online transactions bring an even greater risk of cyber attack and other fraud that can bring high costs and exposes sensitive citizen data. Hackers use sophisticated malware to 'ride' on authenticated user sessions - and these vulnerabilities most often go undetected until it is too late. With a mobile identity platform, users can receive push notifications with key transaction details. Users quickly and easily verify transactions 'out of band' and can immediately identify suspicious activity to defeat account takeovers before they are executed on the server side.

With eGovernment ecosystems growing more complex thanks to increased connectivity, mobile productivity and interoperability initiatives, traditional credentials - passwords, tokens and access cards - simply cannot keep up. Government agencies need a better solution to protect their ecosystems while empowering the productivity benefits of the connected workforce.

Today, the anytime-anywhere connectivity of the smartphone makes it the center of our personal professional lives - and make it a natural, user-friendly and cost-effective answer to this identity challenge. Leveraging the built-in security capabilities of the mobile device - from push notifications and advanced encryption to biometrics - government agencies can effectively establish user and device identity, mitigate the risk of cyber attacks, and protect sensitive data and citizen information. At the same time, mobile identity gives government employees streamlined authentication workflows that simplify their work lives, boosting productivity, increasing operational efficiency and enhancing the level of service delivered to the citizens you serve.

by Mike Byrnes
Entrust Datacard

An identification portfolio covering a complete range of ICs for smart cards, tags, labels and readers

NXP's offering ranges from low-cost smart label ICs for high-volume supply chain management applications through to their next generation 32-bit smart-computing platform for powerful multi-application smart cards. The identification portfolio covers a complete range of ICs for smart cards, tags, labels and readers, featuring many coprocessor, security, memory and interface options.

NXP also offer a comprehensive range of contact and contactless reader ICs for various identifica-

tion applications. NXP RFID technology is utilized in a wide range of applications, including animal identification, public transport, logistics and supply chain management — all supported by their product families Hitag, Mifare, ICode and UCode — covering all RFID frequencies. Its numerous possibilities, plus the fact that there are over 2 billion NXP RFID-based cards, tickets, tags and labels issued and over 7.5 million contactless readers installed worldwide, make it suitable for use in an incredibly wide array of design scenarios.

NXP creates semiconductors, system solutions and software that deliver better sensory experiences in mobile phones, personal media players, TVs, set-top boxes, identification applications, cars and a wide range of other electronic devices. Investment in research and development at NXP is high with some 7,500 engineers working at 26 R&D centers located in 14 countries, they hold over 25,000 patents.

Mikronweg 1
8101 Gratkorn
Austria

Tel.+43 3124 299 324
Fax+43 3124 299 330

www.nxp.com

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 150 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 dual interface banking and e-ID documents, the company brings value to its customers by pre-certifying the performance of cards using its technology and guaranteeing card functionality in the field.
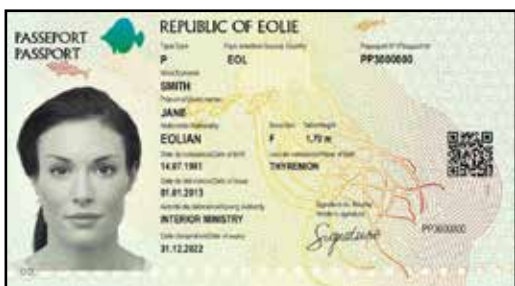
85 avenue de la Plaine
ZI de Rousset-Peynier
13790 Rousset — France

Tel. +33 442538830
Fax +33 442538448

www.s-p-s.com
contact@s-p-s.com

ABnote
www.abnote.com

MF -C, RFID, NFC -C (MG, CM, SM, CL, FP), M (SL), TAG (RF<HF>)

2200 Fletcher Avenue, 07024 Fort Lee, NJ, Usa

Tel. 1/201/592/3400   Fax 1/201/224/2762

Access IS Limited
www.access-is.com

MF -C, RFID – R (OCR, RF, CL, BC), DC – R (OCR, RF, CL, BC), BC -R (RF, CL, POS)

18 Suttons Business Park, Reading, Berkshire, RG6 1AZ, United Kingdom

Tel. 44/7748/770 632   Fax 44/118/926/7281

ActivIdentity (HID)
www.actividentity.com

MF, SH -C -C (SM), R(HH), T (HH), SW

6623 Dumbarton Circle, 94555 Fremont, CA, Usa

Tel. 1/510/5740100   Fax 1/510/5740101

AEG Identifikationssysteme GmbH
www.aegid.de

MF, SI -C, RFID -C (MG, CM, SM, CL, OPT), M (L, SL, TTR, I) TAG (RF<LF, HF, UHF>), IC, A, P (POS) R (HH, FX, RF, I), RF, EP, GP

Hörvelsinger Weg 47, 89081 Ulm, Germany

Tel. 49/7/3114/00880   Fax 49/7/3114/0088/9000

Alp Vision
www.alpvision.com

SH, SI – C, DC – SW, M (MK, VF)

Rue du clos 12, 1800 Vevey, Switzerland

Tel. 41/21 948/6464

Arjo Systems
www.arjo-systems.com

SH, SI – B, C -C(CL,CM,SM), DC, EP, GP, H, NFC, R, RFID, T(VT)

32 rue Jacques Ibert, 92300, Levallois-Perret, France

Tel. +33 (0)181938850

ARM Ltd
www.arm.com

MF -C -IC

110 Fulbourn Road, CB1-9 NJ Cambridge, UK

Tel. 44/1223/400400   Fax 44/1223/400410

ASK
www.ask-rfid.com

MF -C, RFID -C (CL), M (SL), TAG (RF<HF, UHF>), P (HH), R (HH)

2260 route des Crêtes, BP337, 06906 Sophia-Antipolis, France

Tel. 33/4/97214000   Fax 33/4/92389321

Atlantic Zeiser
www.atlanticzeiser.com

MF, SI, SH -C, RFID -M (L, SL), C (MG, CM, SM, CL, FP), TAG (MK, RF<HF,UHF>), P (I), R (RF), SW, EP, GP, MC, MV

Bogenstraße 6-8, 78576 Emmingen, Germany

Tel. 49/7465/2910   Fax 49/7465/291166

Atmel
www.atmel.com

MF -RFID -IC (CL, RF<LF, HF, UHF, MW>)

2325 Orchard Parkway, 95131 San Jose, CA, Usa

Tel. 1/408/4410311   Fax 1/408/4364200

Atos Worldline
www.atosworldline.be

MF -C -T(POS, HH)

1442 Chaussée de Haecht, 1130 Bruxelles, Belgium

Tel. 32/2/727/6111   Fax 32/2/727/6767

Austria Card
www.austriacard.at

MF, SH -C -C (MG, CM, SM, CL), M (L, H), A, SW, EP, GP

Lamezanstrasse 4-8 , 1230 Vienna , Austria

Tel. 43/1/610650   Fax 43/1/61065701

Axcess International, Inc
www.axcessinc.com

MF, SI -RFID, C -TAG (RF), R, SW

3208 Commander Drive, 75006 Carrollton, TX, Usa

Tel. 1/972/4076080   Fax 1/972/4079085

Bell ID BV
www.bellid.com

SH -C -SW

Stationsplein 45 - Unit A6.002, 3013 AKRotterdam, The Netherlands

Tel. 31/10/885/1010   Fax 31/10/885/1011

BioLink Solutions
www.biolinksolutions.com

MF, SI -B, C -C (FP), S, SW

PO Box 404, _/_ IPS, 511 Avenue of the Americas, PMB 572, 10011 New York, NY, Usa

Tel. 44/808/189/1360

BGI
www.bginge.com

MF-C, RFID-C (CM, CP, MG)

ZAC de la Goulgatiere, 4 rue Paul Langevin, 35220 Chateaubourg, France

Tel. 33/2/99008997   Fax 33/2/99008998

Blumer Maschinenbau AG
www.blumerag.com

MF -C -MC

Libernstrasse 22, 8112 Otelfingen, Switzerland

Tel. 41/1/8476565   Fax 41/1/8476566

Company	Products/Services		Tel	Fax
Böwe Cardtec GmbH www.boewe-cardtec.com	MF ‑C ‑MC, SW Balhorner Feld 28 , 33106 Paderborn, Germany		Tel. 49/5251/180860	Fax 49/5251/1808699
Bundesdruckerei GmbH www.bundesdruckerei.de	MF, SI, D, SH ‑C, B ‑C (SM, CL, FP), P, R (HH, FX), T (FP, FP, FF, VF), SW, EP, GP Oranienstrasse 91, 10969 Berlin, Germany		Tel. 49/30/25980	Fax 49/30/25982205
CardLogix Corp. www.cardlogix.com	MF, SH ‑C ‑C (MG, CM, S, CL), P (I), T (POS), SW 16 Hughes, Suite 100, 92618 Irvine, CA, U.S.A.		Tel. 1/949/380/1312	Fax 1/949/380/1428
CodeCiphers www.codeciphers.com	MF, SH ‑B, C ‑C (CL) B, IC Rua Bogaert 107 Villa Vernehla, 04298-020 Sao Paulo, Brazil		Tel. 55/11/2175/1106	Fax 55/11/2175/1171
Cogent Systems, 3M www.cogentsystems.com	MF ‑B, C, RFID, BC ‑C (MG, CM, SM, CL, OPT, FP), TAG (RF <HF>) R (HH, FX), S (FX POS, I) T (HH, FX, RF, I, BC, FP, IF, FF), SW, EP 639 N. Rosemead Blvd., 91107 Pasadena, CA, Usa		Tel. 1/626/325/9600	Fax 1/626/325/9700
Comercial Arqué www.arque.com	VAR ‑C, RFID, BC ‑C (MG, CL), TAG (RF<HF, UHF>), A, P (I, TTR) Carretera del Mig. No 54, L'Hospitalet de Llobregat, 8907 Barcelona, Spain		Tel. 34/932635100	Fax 34/933372690
Confidex Ltd. www.confidex.com	MF ‑RFID, NFC ‑TAG (RF<HF, UHF>, I), M (SL), C (CL) Haarlankatu 1B, 33230 Tampere, Finland		Tel. 358/10/4244 100	Fax 358/10/4244 110
Cryptomathic Ltd www.cryptomathic.com	SH, SI ‑C ‑SW 327 Cambridge Science Park, Milton Road, CB4 0WG Cambridge, UK		Tel. 44/1223/225350	Fax 44/1223/225351
Dartagnan BV www.dartagnan.eu	SI, SH ‑C, B, RFID ‑C (SM, CL), R (RF), T (RF, FP, IF, FF, VF), SW Triport 3, Westelijke Randweg 51, 1118 CRLuchthaven Schiphol, The Netherlands		Tel. 31/20/405/4149	Fax 31/20/405/4171
Databac Group www.databac.com	MF, SH, SI, VAR, D ‑C, RFID, B ‑C (MG, CM, SM, CL, OPT, FP), M (L, SL, TTR, H, I), TAG (RF<HF>), P (TTR), R (HH, FX, RF), S (HH, POS), T (HH, RF, BC, FP, IF, VF), VR, SW, EP, GP Number One, The Ashway Centre, Elm Crescent, KT2 6HH Kingston, Surrey, UK		Tel. 44/208/546/9826	Fax 44/208/547126
Datastrip Ltd www.datastrip.com	MF ‑B, BC ‑R (HH), T (FP) 7 Thame Park Business Centre, Wenman Road, OX9 3XA Thame, Oxfordshire, UK		Tel. 44/1844/215668	Fax 44/1844/215669
De La Rue Identity Systems www.delarue.com	MF, SI ‑C ‑C (CM, CL, SM, FP), SW De La Rue House, Jays Close, RG22 4BS Basingstoke, UK		Tel. 44/1256/605000	Fax 44/1256/605004
Deister Electronic www.deister.com	MF ‑C, RFID ‑C (CL), TAG (RF<LF, HF, UHF>), R (HH, FX, RF, I), T (RF) Hermann-Bahlsen-Str. 11, 30890 Barsinghausen, Germany		Tel. 49/5105/516111	Fax 49/5105/516217

Dermalog Identification System GmbH	MF,SH,SI,VAR,D‑B,C,RFID,BC‑C(CM,SM,CL,OPT,FP),TAG(RF<HF>),A,R(HH,FX,RF,I),S(HH,FX,POS,I),T(HH,RF,BC,FP),SW
www.dermalog.com	Mittelweg 120, 20148 Hamburg, Germany Tel. 49/40/4132270 Fax 49/40/41322789

Digital Identification Solutions AG	MF, SH, SI ‑C, B ‑C (CM, CL, SM, MG, OPT, FP), M (TTR, H, I), P (CP, I, TTR), EP, GP, SW, MC
www.digital-identification.com	Teckstrasse 52, 73734 Esslingen, Germany Tel. 49/711/3416890 Fax 49/711/341689550

Diletta Maschinentechnik GmbH	MF ‑C, RFID ‑C (CL), P (I), GP, EP, MC
www.diletta.com	Industriestrasse 25-27, 64569 Nauheim, Germany Tel. +49/6152/1804 - 0 Fax +49/6152/1804‑22

DILETTA ID-SYSTEMS

For more than five decades DILETTA has been engaged in producing 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.

Elatec GmbH	MF ‑C, RFID ‑C (CM, SM, CL), M (L, SL, I), TAG (RF<LF, HF, UHF, MW>), R (HH, FX, RF, I), SW
www.elatec-rfid.com	Max-Planck-Str. 16, 82223 Eichenau, Germany Tel. 49/8141/534980 Fax 49/8141/5349829

Elsag Datamat	MF, SH, SI ‑C, B, RFID, DC ‑C (CM, SM, CL), TAG (RF<HF, UHF>), P (I), R (HH, FX, RF, I), S (POS, I, OCR), T (FP, FF), SW, GP, EP
www.elsagdatamat.com	Via Puccini, 2, 16154 Genova, Italy Tel. 39/010/6582215 Fax 39/010/6512329

Elyctis	MF, SH ‑ C, RFID ‑ R (RF, HH, FX, CL, OCR), SW
www.elyctis.fr	240 rue François Gernelle, 84120 Pertuis – France Tel. +33 6 27 71 37 68

EMJ Data Systems Ltd	D‑BC,DC,C,RFID,B‑C(MG,CM,SM,FP),M(L,TTR,H),A,P(CP,I,TTR),R(HH,FX,I),S(HH,FX,POS,I),T(HH,FX,RF,I,BT,BC,FP,VT)
www.emj.ca	7067 Wellington Road. 124, RR6, N1H 6J3 Guelph, ON, Canada Tel. 1/800/265/7212 Fax 1/877/801/6300

Entrust Datacard	MF ‑C, B ‑C (CM, SM, CL, FP), EP
www.entrustdatacard.com	1187 Park Place, Shakopee, MN 55379, USA Tel. 1/952/933 1223 Fax 44/1489/555601

Evolis	MF ‑C, RFID ‑C (MG, CM, SM, CL), M (TTR, H), TAG (RF <LF, HF, UHF, MW>), P (CP, I, TTR, POS), T (POS), SW, EP, GP
www.evolis.com	14 avenue de la Fontaine , 49070 Beaucouze, France Tel. 33/2/41367606 Fax 33/2/41367612

Exceet Group	MF ‑C, RFID ‑C (CM, CL, SM), R (HH), TAG (RF <LF, HF, UHF, MW>)
www.exceet.ch	Marktplatz 4, CH-9004 St. Gallen, Switzerland Tel. 41/4179848/56

Fargo Electronics Inc	MF ‑C ‑P (CP, I, TTR), C (MG, CM, SM, CL)
www.fargo.com	6533, Flying Cloud Drive, 55344 Eden Prairie, MN, Usa Tel. 1/952/9419470 Fax 1/952/9417836

Fastcards	MF, SH ‑C, BC, RFID, B ‑C (MG, CM, SM, CL)
www.fastcards.com.au	PO Box 3888, 4101 South Brisbane, Qld, Australia Tel. 61/7/38444623 Fax 61/7/38464591

Feig Electronic GmbH	MF ‑RFID, NFC ‑R (HH, FX, RF, I)
www.feig.de	Lange Strasse 4, 35781 Weilburg, Germany Tel. 49/6471/31090 Fax 49/6471/310999

Fingerprint Cards AB	MF ‑B ‑IC, T (FP), C (FP), SW
www.fingerprints.com	P O Box 2412 (Kungsportsplatsen 2), 403 16 Gothenburg, Sweden Tel. 46/31/607820 Fax 46/31/137385

Foba Laser Marking + Engraving (Alltech)	MF ‑C, DC ‑MC, TAG (MK), MV
www.fobalaser.com	An der Trave 27-31, 23923 Selmsdorf, Germany Tel. 49/38823/550 Fax 49/38823/55222

| **Fortress GB Limited** | SI -RFID, C -C (SM, CL, FP), TAG (RF<HF>), T (HH, FX, RF, HG, POS), SW | | |
| www.fortressgb.com | South Block, Tavinstock Square, Tavinstock House, WC1H 9LG London, UK | Tel. 44/20/7874/7595 | Fax 44/7874/7599 |

| **Gemalto** | MF -C -C (CM, SM, CL), EP, GP, T (HH, POS), R (FX, HH), SW | | |
| www.gemalto.com/govt | 6, rue de la Verrerie, 92127 Meudon Cedex, France | Tel. 33/1/5501/50 00 | |

| **GET Group** | SI - C - P (CL, CM, VF) | | |
| www.getgroup.com | 230 Third Avenue, Waltham, MA 02451 – USA | Tel. +1 781 890-6700 | Fax +1 781 890-6320 |

| **Ghirlanda SpA** | MF, SI -C -C (MG, SM), SW, GP, EP | | |
| www.ghirlanda.it | via Galileo Ferraris, 80/90, 20010 Marcallo con Casone, MI, Italy | Tel. 39/02/972331 | Fax 39/02/9761657 |

| **Giesecke & Devrient GmbH** | MF, SI -C, B, NFC, RFID -C (SM, CL, FP), M (H), IC, P (CP, I), R (FX), T (FX, BC, FP, FF), EP, GP | | |
| www.gi-de.com | Prinzregentenstrasse 159, 81677 Munich, Germany | Tel. 49/89/41190 | Fax 49/89/41191535 |

| **HID Global** | MF -C, RFID -C (MG, CM, SM, CL, OPT), M (TTR, H, I), TAG (RF,LF,UNF HF), IC, P (CP, I, TTR, POS). R (HH, FX, RF, I), SW, EP | | |
| www.hidglobal.com | 15370 Barranca Pkwy, 92618 Irvine, CA, Usa | Tel. 1/949/732/2000 | Fax 1/949/732/2120 |

| **Hirsch Electronics Corp.** | MF -B,C,RFID -C (MG,CM,SM,CL,OPT,FP),TAG (RF<LF,HF,MW>),R (HH,FX,RF,I),T (HH,FX,RF,I,BC,FP,IF,VT,VF),SW,EP,GP | | |
| www.hirschelectronics.com | 1900-B Carnegie Ave., 92705 Santa Ana, CA, Usa | Tel. 1/949/250/8888 | Fax 1/949/250/7372 |

| **HJP Consulting** | SH, SI -C, RFID -SW | | |
| www.hjp-consulting.com | Hauptstraße 35, 33178 Borchen, Germany | Tel. 49/5251/417760 | Fax 49/5251/4177666 |

| **Honeywell Access Systems** | MF, SH -RFID, B -C (MG, CM, SM, CL, FP), M (TTR, H), P (TTR), R (HH, RF), S (HH) | | |
| www.honeywellaccess.com | 2700 Blankenbaker Pkwy, Suite 150, 40291 Louisville, KY, Usa | Tel. 1/800/6753364 | Fax 1/502/2975770 |

| **IAI Industrial Systems** | MF - C - EP | | |
| www.iai.nl | De Run 5406, 5504 DE Veldhoven – The Netherlands | Tel. 31/40/2542445 | Fax 31/40/2545635 |

| **Identitas** | D -C, B -C (CM, SM, OPT), T (FP), GP, EP | | |
| www.identitas.it | Via Tiburtina 912, 00156 Rome, Italy | Tel. 39/06/4072199 | Fax 39/06/4086199 |

| **Identive Group** | MF -RFID -TAG(RF<HF, UHF>), M (SL), D – RFID, NFC – IC, TAG (RF<LF, HF>) | | |
| www.identive-transponders.com | Mu_hlweg 2c, 82054 Sauerlach, Germany | Tel. 49/8104/6495100 | Fax 49/8104/6495110 |

| **Idesco Oy** | MF -RFID, C -C (SM, CL), TAG (RF<LF, HF>), R (RF), T (RF) | | |
| www.idesco.fi | Teknologiantie 9, 90570 Oulu, Finland | Tel. 358/20/74384175 | Fax 358/20/7434176 |

IDTeck
www.idteck.com

MF, D ‑C, B, RFID ‑C (CM, SM, CL), TAG (RF<LF, HF, UHF>), T (RF, FP, FF, VF), SW

5F, Ace Techno Tower B/D 684-1, Deungchon-Dong, Gangsuh-Gu, 157-030 Seoul, Korea Tel. 82/2/26590055 Fax 82/2/6590086

iDTronic
www.idtronic-group.com

MF ‑C, RFID ‑C (CL), M (SL), TAG (RF<LF, HF, UHF>), R (HH, FX, RF, I), T (RF)

Donnersbergweg 1, 67059 Ludwigshafen am Rhein, Germany Tel. 49/621/66900940 Fax 49/621/66900949

Imprimerie Nationale Groupe
www.imprimerienationale.fr

MF, SI, ‑ C, B ‑ C, EP, R, SW

104 avenue du Président Kennedy, 75016 Paris Tel. 33 01 4058300 Fax 33 01 40583085

ImageWare Systems, Inc.
www.iwsinc.com

MF, SH ‑B, C ‑T (FP, HG, IF, FF), VR, SW

10883 Thornmint Rd , 92127 San Diego, CA, Usa Tel. 1/858/673/8600 Fax 1/858/673/1770

Industrial Innovation Group
www.industrialinnovationgroup.com

MF, SH – C, B, NFC, RFID – C(MG, CM, SM, CL, FP), M(L, H), TAG(RF), P(I), SW, EP, GP, MC

Building Z-2, Executive suite 85, SAIF Zone, Sharjah a/p, P.O. Box 9015, Sharjah, UAE Tel. 00971 6557 0725 Fax 00971 6557 4810

Infineon Technologies AG
www. infineon.com

MF –RFID, C ‑IC

Am Campeon 1 – 15, 85579 Neubiberg, Germany Tel. 0800/4001

Infineon is a world leader in semiconductors. Combining entrepreneurial success with responsible action, at Infineon we make the world easier, safer and greener. Infineon designs, develops, manufactures and markets semiconductors and system solutions. The focus is on automotive & industrial electronics, RF applications, mobile devices and hardware-based security. We are playing a key role in shaping a better future — with microelectronics that link the digital and the real world. Our semiconductors enable smart mobility, efficient energy management and the secure capture and transfer of data.

Ingenico
www.ingenico.com

SH, SI ‑C, B ‑T (HH, FX, RF, CL, BC, FP, POS), SW, VT

192 avenue Charles de Gaulle, 92200 Neuilly, France Tel. 33/1/46258200 Fax 33/1/47725695

Innova Card
www.innova-card.com

MF ‑C ‑IC, SW

ZI Athélia IV - Le Forum, Bât. A, Quartier Roumagoua, 13600 La Ciotat , France Tel. 33/4/42981480 Fax 33/4/42083319

Intelcav
www.intelcav.com

MF ‑C ‑C (MG, CM, SM, CL, OPT, FP, H)

Rua Hungria 514, 50 andar Jardim Paulistano, SP 01455-000 São Paulo, Brazil Tel. 55/11/2169/0750 Fax 55/11/2169/0769

Interflex Datensysteme GmbH & Co. KG
www.interflex.de

MF, SI ‑B, C ‑T (RF, FP), SW

P.O. Box 81 03 60, 70520 Stuttgart, Germany Tel. 49/711/13220 Fax 49/711/1322/111

International Bar Code
www.interbar.com

MF ‑C, BC ‑C (CL), R (RF), S (FX, I)

160 Oak Street, 06033 Glastonbury, CT, Usa Tel. 1/860/6599660 Fax 1/860/6573860

International Biometric Group
www.biometricgroup.com

SI ‑B, C ‑SW

One Battery Park Plaza, 10004 New York, NY, Usa Tel. 1/212/8099491 Fax 1/212/8096197

International Security Tech.
www.ist-china.com

MF ‑C, BC, B ‑C (MG, CM, SM, CL, OPT, FP)

No. 99 Meicun Road, 518049 Shenzhen , Guangdong , P. R.China Tel. 86/755/83124964 Fax 86/755/83315467

Iris Corporation Berhad
www.iris.com.my

MF, SI, SH, D, VAR ‑C, B ‑C (CM, SM, CL, CMA), B (FF), P (CP), R (HH, FX, RF, I), T (IF, HH, FX, I, FP, L, MK, OCR), SW, EP

Iris Smart Technology Complex, Technology Park Malaysia, 57000 Bukit Jalil, Kuala Lumpur, Malaysia Tel. 603/89960788 Fax 603/89960441

Ixla srl
www.ixla.it

MF ‑C ‑MC, SW, GP, EP

Via Ponte Chiusella 28, 10090 Romano Canavese, Italy Tel. 39/0125/719286 Fax 39/0125/718455

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.

Keynectis

www.keynectis.com

SH - C - SW (SM, CM, CL, VF)

11-13 rue René Jacques - 92131 Issy-les-Moulineaux Cedex, France

Tel. +33 1 55 64 22 00   Fax +33 1 55 64 22 01

Keyware

www.keyware.com

MF, SH, SI -C -C (MG, CM, SM, CL, FP), T (RF, POS), SW, EP

Ikaros Business Park, Ikaroslaan 24, 1930 Zaventem, Belgium

Tel. 32/2/3462523   Fax 32/2/3471688

Kronos Systems Ltd

www.kronos.com/uk

MF -B, C -T (FP)

Kronos House, Carey Road, RG40 2NP Wokingham, UK

Tel. 44/118/9789784   Fax 44/118/9782214

Kugler Womako

www.kugler-womako.com

MF - C - MC, C (CMA)

Schlosserstraße 15, 72622 Nürtingen, Germany

Tel. +49 7022 70020   Fax +49 7022 33444

Labau Technology Corporation

www.labau.com.tw

MF -BC, C -R (HH, FX), P (CP, TTR), S (FX), T (POS)

3F-3, No 125, Ln 235, Bau Chiau Road, 231 Taipei, Taiwan

Tel. 886/2/89191371   Fax 886/2/89191771

Linxens

www.linxens.com

MF - C, RFID, NFC - TAG (RF <LF,HF, UHF>), A, M(SL), C (CL)

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.

Logicode PTE Ltd

www.logicode.com.sg

D -BC, C, RFID -S (HH, FX), R (RF), P, T (RF, BT, BC)

10 Ubi Crescent #05-28, 408564 Ubi Techpark (Lobby B), Singapore

Tel. 65/64588/337   Fax 65/64588/553

Magna Carta Chipcard Solutions

www.magna-carta.com

MF -C -C (MG, CM, SM, CL), T, SW

Naritaweg 126, 1043 CAAmsterdam, Holland

Tel. 31/20/582/20/50   Fax 31/20/582/20/51

Magtek

www.magtek.com

MF -C -S (POS), T (POS)

20725 South Annalee Avenue, 90746 Carson, CA, Usa

Tel. 1/800/421/5208

Cards

Masktech GmbH
www.masktech.de
sales@masktech.de

SH -C, B, RFID -IC, SW

Nordostpark 45, 90411 Nuremberg, Germany   Tel. 49/911/955149-0   Fax 49/911/955149-7

MaskTech is the leading independent provider of high security multi-application operating systems (OS) and customized Flash/ROM masked products for electronic travel documents and ID applications. Our embedded solution (MTCOS) protects e-documents in more than 65 countries worldwide. MTCOS is a fully open standard (ISO/IEC) compliant, Common Criteria EAL5+ certified operating system which includes a large variety of ID applications e.g. ICAO/BSI ePassport, national e-ID, -sign, -health, -driving license and PKI. It supports the RFID, dual interface or contact interface.

Matica System S.r.l.
www.maticasystem.com

MF -C -C (MG, CM, SM, CL, FP), M (TTR, I), P (I, TTR), EP, GP, MC, MV

Via G. Rossa 4/6, 20037 Paderno Dugnano (MI), Italy   Tel. 39/02/92272501   Fax 39/02/91084372

Maurer Electronics GmbH
www.maurer-electronics.de

MF -C -MC

Hanauer Strasse 1, 80992 Munich, Germany   Tel. 49/89/139268630   Fax 49/89/1392680

Melzer maschinenbau GmbH
www.melzergmbh.com
sales@melzergmbh.com

MF -C, RFID -MC, C (MG, CM, SM, CL), M (L, SL), TAG (MK, RF<LF, HF, UHF, MW>)

Ruhrstr 51-55, 58332 Schwelm, Germany   Tel. 49/2336/9292/80   Fax 49/2336/9292/85

MELZER offers fully automatic production lines for: e-Passport, ID Cards, Driving Licenses, Resident Permit Cards, e-Visa Stickers; Smart Cards, Dual Interface Cards; Smart Labels/Tickets; RFID Luggage Tags. Customized solutions, the modular machine system and the lean production approach ensure and maintain unsurpassed yield rates, flexibility and profitability. All machinery solutions offer fully automated industrial production processes.

Microsoft Corporation
www.microsoft.com

SH -C, B, RFID, DC -SW

One Microsoft Way, 98052-6399 Redmond, WA, Usa   Tel. 1/800/642/7676   Fax 1/425/936/7329

Morpho
www.morpho.com

MF, SI -C, B -C (CM, SM, CL, FP), R (RF), T (RF, FP, IF, FF), SW, EP, GP

Le Ponant de Paris 27, rue Leblanc, F-75512 Paris Cedex 15, France   Tel. 33/1/5811/2500   Fax 33/1/4070/2550

Mühlbauer Group
www.muehlbauer.de

MF, SH, SI -RFID, C -C, M (SL), TAG (MK, RF), P (CP, I, TTR), T (FX, RF, I, BT, FP, IF, FF, VF), SW, EP, GP, MC, MV

Josef-Muehlbauer-Platz 1, 93426 Roding, Germany   Tel. 49/9461/9520   Fax 49/9461/9521101

Multicard AG
www.multicard.com

MF -C -C (MG, CM, SM, CL), T (FP, FF, VF)

Widenholzstrasse 1, 8304 Wallisellen, Switzerland   Tel. 41/44/8779000   Fax 41/44/8310003

Nadra
www.nadra.gov.pk

VAR, SI, SH -C, B, RFID, DC -SW, EP, GP

State Bank of Pakistan Building, Shahrah-e-Jamhuriat, G-5/2, 44000 Islamabad, Pakistan   Tel. 92/51/9205568   Fax 92/51/9202939

Nagra ID
www.nagraid.com

MF -C, RFID -C (MG, CM, SM, CL), M (L, TTR, H, I), TAG (RF<LF, HF, UHF>), EP, GP

Crêt du Locle 10, 2301La Chaux-de-Fonds, Switzerland   Tel. 41/32/9240404   Fax 41/32/9240400

NBS Technologies Limited
www.nbstech.com

MF -C -C (MG, CM, SM, CL) M (TTR, H), P (CP, I, TTR), SW, EP, GP

B1 Moorfield Point, Slyfield Industrial Park, GU1 1RU Guildford, Surrey , UK   Tel. 44/1483/563200   Fax 44/1483/511189

NEC Solutions (America) Inc
www.necam.com/ids/law

SI -B -T (FP), SW

10850 Gold Center Drive, Suite 200, 95670 Rancho Cordova, CA, Usa   Tel. 1/800/777/2347   Fax 1/916/4637041

Nexus
www.vps.de

SH, SI -C, B, NFC, RFID -SW, EP, GP

Carl-Zeiss-Strasse 2, 76275 Ettlingen, Germany   Tel. 49/7243/54880   Fax 49/7243/548811

Nfive Software
www.nfive.com

SH -C, BC, RFID, B -SW

Edificio OneWorld, Urb Belo Horizonte Lt20, 2655-241 Ericeira, Portugal

Tel. 351/261/860450

Fax 351/261/865/647

Oberthur Technologies
www.oberthurcs.com

MF, SI -C -C (MG, SM, CL), SW, EP, GP

50, quai Michelet, 92300 Levallois-Perret, France

Tel. 33/1/ 5546/7200

Fax 33/1/ 5546/7201

Omnia Technologies
www.omniatags.com

MF -RFID, C -TAG (RF<LF, HF, UHF>)

Plot No. 68, Sector - 5, IMT Manesar, 122050 Gurgaon, Haryana, India

Tel. 91/124/4366411

Fax 91/1244366410

Orell Füssli
www.ofs.ch

MF -C -C (CL,CM), EP

Dietzingerstrasse 3, CH 8036 Zurich, Switzerland

Tel. 41/44/466/7711

Fax 41/44/466/7901

Otto Künnecke GmbH
www.kuennecke.com

MF, SI -C -C (MG, SM), GP, EP, MC

Zeppelinstrasse 10, 37603 Holzminden, Niedersachsen, Germany

Tel. 49/5531/9300545

Fax 49/5531/9300903

PAV Card GmbH
www.pavcard.de

MF -C, RFID -C (MG, CM, SM, CL), EP, GP, TAG (RF<HF>), M

Hamburger Strasse 6, 22952 Luetjensee, Germany

Tel. 49/4154/7990

Fax 49/4154/799151

Prooftag
www.prooftag.com

MF -C -C (OPT), M (L), TAG (MK)

350, Av d'Italie, 82000 Montauban, France

Tel. 33/5/63211050

Fax 33/5/63211058

---

ruhlamat GmbH
www.ruhlamat.com

MF - C, RFID - A, C(CL), EP (MK), GP, MC

Sonnenacker 2, 99819 Marksuhl, Germany

Tel. 49/369259290

Fax 49/36925929111

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.

RF IDeas Inc
www.rfideas.com

MF -RFID, NFC -C (MG, CM,SM, CL), TAG (RF<LF, HF>), R (RF)

4020 Winnetka Ave, 60008 Rolling Meadows, IL, Usa

Tel. 1/847/8701723

Fax 1/847/4831129

Safe ID Solutions AG
www.safe-id.de

MF, SI -C, RFID -C (CL), GP, EP, SW, MC

Ottobrunner Str. 43, 82008 Unterhaching, Germany

Tel. 49/89/4521260

Fax 49/89/452126126

SafeNet, Inc.
www.safenet-inc.com

MF -C -C (SM), SW

4690 Millennium Drive, 21017 Belcamp, MD, U.S.A.

Tel. 1/410/931/7500

Fax 1/410/931/7524

ROLE IN THE VALUE CHAIN		PRODUCT CATEGORIES		PRODUCT SPECIFICATIONS			
D	= Distributor	A	= Antenna	BT	= Batch	IF	= Iris Feature
MF	= Manufacturer	C	= Cards	BC	= Barcode	L	= Labels
SH	= Software House	EP	= Electronic Personalization	CL	= Contactless	LF	= Low Frequency
SI	= System Integrator	GP	= Graphic Personalization	CM	= Contact Memory	MG	= Magnetic
VAR	= Value Added Reseller	IC	= Integrated Circuits	CMA	= Card Materials	MK	= Marking
		M	= Media	CP	= Compact	MW	= Microwave
TECHNOLOGIES		MC	= Machinery	DNA	= DNA	OCR	= Optical Char. Recognition
B	= Biometrics	MV	= Machine Vision	EAS	= Electronic Art. Surveillance	OPT	= Optical
BC	= Barcode	P	= Printers	FF	= Facial Feature	POS	= Point of Sale
C	= Cards	R	= Readers	FP	= Fingerprint	RF	= Radio Frequency
DC	= Data Collection	S	= Scanners	FX	= Fixed	SL	= Smart Labels
NFC	= Near Field Comm.	SW	= Software	H	= Holograms	SM	= Smart
RFID	= Radio Frequency	T	= Terminals	HF	= High Frequency	TTR	= Thermal Transfer Ribbon
	Identification Device	TAG	= Tags	HG	= Hand Geometry	UHF	= Ultra High Frequency
RTLS	= Real Time Loc. System	VR	= Voice Recognition	HH	= Handheld	VF	= Verifier
				I	= Industrial	VT	= Vehicle Terminal

LEGENDA

Schreiner LogiData
www.schreiner-logidata.com

MF -C, RFID, BC -C (SM, CL), M(L, SL, I), TAG (RF<HF, UHF>)

Bruckmannring 22, 85764 Oberschleissheim, Germany

Tel. 49/89/31584/4140   Fax 49/89/31584/4109

SCM Microsystems (Identiv)
www.scmmicro.com

MF -RFID, NFC -R (HH, FX, RF), T (HH, FX, RF)

Oskar-Messter-Straße 13, 85737 Ismaning, Germany

Tel. 49/89/9595/5000   Fax 49/89/9595/5555

SecureTech Consultancy
www.securetech-consultancy.com

SH, SI, VAR - C (CL, CM, SM), EP, T (FF, OCR, TTR)

827, Street No. 85, I-8/4, Islamabad-44000, Pakistan

Tel. +92 51 111 111 782   Fax +92 51 4436480

Selex Elsag
www.selexelsag.com

MF, SH, SI -C, B, RFID, DC -C (CM, SM, CL), TAG (RF<HF, UHF>), P (I), R (HH, FX, RF, I), S (POS, I, OCR), T (FP, FF), SW, GP, EP

Via Puccini, 2, 16154 Genova, Italy

Tel. 39/010/65821   Fax 39/010/6512898

SICPA Security Solutions
www.sicpa.com

MF, SH - C - P, SW, TAG (L, MK)

Av de Florissant 41, 1008 Prilly – Switzerland

Tel. +41 21 627 61 55   Fax +41 21 627 57 27

At the core of SICPA's security expertise are high-performance security inks that protect the majority of the world's banknotes, security documents and value documents from counterfeiting and fraud. SICPA's Government Security Solutions Division enables Governments to protect tax revenues and deliver associated policy objectives by providing unique and secure authentication and traceability solutions. SICPATRACE® combines material based security with state-of-the-art information technology which enables our partner Governments to secure revenue and protect consumers. SICPA is a pioneer in this field and has successfully implemented and operated nationwide track and trace solutions for Governments worldwide.

Sitroncis
www.sitronics.com

MF -C -C (SM), IC

39/5 3-ya Tverskaya-Yamskaya St. Building I, 125047 Moscow, Russia

Tel. 7/495/2250030   Fax 7/495/2250036

Skidata AG
www.skidata.com

MF, D, SI -C, RFID -C (SM, CL, OPT, MG), M (L, TTR), TAG (RF<LF, HF>), P (CP, TTR), R (HH, FX, RF), S (HH, FX, POS), SW, T (HH, FX, BC, POS, VT)

Unterbergstrasse 40, 5083 Grödig - Salzburg, Austria

Tel. 43/6246/8880   Fax 43/6246/8887

Smartware
www.smartware.fr

MF -C, RFID -EP, GP, R (RF)

11, Avenue des Andes, Le Carthagène, Z.A. de Courtaboeuf, 91940 Les Ulis, France

Tel. 33/1/6486/2525   Fax 33/1/6486/2526

SPS - Smart Packaging Solutions
www.s-p-s.com

MF - C - A, C (CMA, CL, HF), IC, DATAPAGE

85 avenue de la Plaine, ZI de Rousset-Peynier, 13790 Rousset – France

Tel. +33 4 42 53 88 30   Fax +33 4 42 53 84 48

Spartanics
www.spartanics.com

MF -C, RFID -C (MG, CM, SM), M (L), P (I)

3605 Edison Place, 60008 Rolling Meadows, IL, Usa

Tel. 1/847/3945700   Fax 1/847/3940409

STMicroelectronics
www.st.com

MF -C, RFID, B -C (CM, SM, CL, FP), M (SL), TAG (RF<HF, UHF>), IC

39, Chemin du Champ des Filles CP 21, 1228 Plan-Les-Ouates, Geneva 15, Switzerland

Tel. 41/22/9292929   Fax 41/22/929/2900

Studio Card Ltd.
www.rfid.bg

SI, VAR, D -C, RFID -C (CL, SM), M, TAG (RF<LF, HF>), R (RF), T (RF)

36, Dragan Tsankov Blvd., Interpred World Trade Centre, Office B 324, 1040 Sofia, Bulgaria

Tel. 359/886/718545   Fax 359/2/9693330

Symbolic S.p.A.
www.symbolic.it

D -C -C (SM)

Viale Mentana 29, 43121 Parma, Italy

Tel. 39/0521/708811   Fax 39/0521/776190

Szzt Electronics Group
www.szzt.com

MF -C, DC -C (MG, SM), R, P, T (HH, BC, POS), SW, EP, GP

5/F, West Coast Bldg, Nan You Rd, 518054 Nan Shan Dist., Shenzhen, Guangdong, China

Tel. 86/755/26490094   Fax 86/755/26490099

Texas Instruments RFID Systems
www.ti-rfid.com

MF -RFID, C -C (CL), M (SL), TAG (RF<LF, HF, UHF>), IC, A, R (HH, FX, RF), T (RF), SW

6550 Chase Oaks Blvd, 75023 Plano, TX, Usa

Tel. 1/800/962/7343   Fax 1/214/567/7343

Thales	MF, SI -B, NFC -IC, A, T(FX, FP, IF, FF), SW, EP		
www.thalesgroup.com	20-22 rue Grange Dame Rose, 78141 Velizi, France	Tel. 33/1/73320000	

Trüb AG	MF, SI -C, B, NFC -C (MG, CM, SM, CL, FP), M (H), TAG (RF<LF, HF>), IC, A, P (TTR), SW, EP, GP, MC		
www.trueb.ch	Hintere Bahnhofstrasse 12, 5001 Aarau, Switzerland	Tel. 41/62/8320000	Fax 41/62/8320100

Ultra Electronics Card Systems	MF -C, BC -M (TTR, H), P (CP, TTR)		
www.magicard.com	Hampshire Road, DT4 9XD Weymouth, Dorset, UK	Tel. 44/1305/784738	Fax 44/1305/777118

Unisys	SI, SH, VAR -C, B -C (MG,SM,OPT,FP), T (HH, FX, RF, BT, BC, FP, IF, FF, VF), VR, SW, EP, GP		
www.unisys.com/biometrics	801 Lakeview Drive, 19422 Blue Bell, PA, Usa	Tel. 1/215/986/4011	

Vasco Data Security International	MF -C -R (HH), SW		
www.vasco.com	Koningin Astridlaan 164, 1780 Wemmel, Belgium	Tel. 32/2/6099700	Fax 32/2/6099709

VeriFone, Inc.	MF -C -T (HH, POS), P, SW		
www.verifone.com	2099 Gateway Place, Suite 600, 95110 San Jose, CA, Usa	Tel. 1/408/232/7800	Fax 1/408/232/7811

Verisign	SI -C, DC, RFID -C, SW		
www.verisign.com	487 E. Middlefield Road, 94043 Mountain View, Usa	Tel. 1/650/4263535	

Vision-Box	MF -C, B -C, R (FX, FF, FP, VF), T		
www.vision-box.com	Rua Casal do Canas n.2, Zona Industrial de Alfragide, 2790-204 Carnaxide, Portugal	Tel. 351/21/154/3900	Fax 351/21/154/3901

Vlatacom d.o.o.	MF, SI, SH -C, B, DC -R(HH, FX,RF<HF>), S(OCR), T (HH, BC, FP, FF, RF, VF), SW, EP, GP		
www.vlatacom.com	5 Milutina Milankovica, 11070 Belgrade, Serbia	Tel. 381/11/377/1100	Fax 381/11/377/1199

Wick Hill Group plc	D -B, C -C (SM, CL, FP), SW, EP		
www.wickhill.com	River Court, GU21 5RP Woking, UK	Tel. 44/1483/227600	Fax 44/1483/227700

Wincor Nixdorf International GmbH	MF, SH, SI -RFID, C -T (HH, FX, RF, BC, POS, VF), R (HH, FX, POS), SW, P (CP)		
www.wincor-nixdorf.com	Heinz-Nixdorf-Ring 1, 33106 Paderborn, Germany	Tel. 49/5251/69330	Fax 49/5251/6936767

WiseKey	MF, SH - C, DC - T (VF), SW		
www.wisekey.com	World Trade Center II, 29, Route de Pré-Bois, P.O. Box 853, CH-1215 Genève 15, Switzerland	Tel. +41 22 594 30 00	

ZeitControl cardsystems	MF -C, RFID -M (SL), TAG (RF<LF, HF>), A, R (HH,FX,RF,I), T (HH,FX,RF,I), EP, MC		
www.zeitcontrol.de	Siedlerweg 39, 32429 Minden, Germany	Tel. 49/571/505220	Fax 49/571/5052299

Guiding citizens through the digital public sector maze

While data privacy, choice and consent are still key issues that go towards public trust and confidence, how can digital service delivery channels become pivotal for citizens who need to interact with service providers and government departments?

Today, government departments and large public organizations across the world are focusing on the pursuit of a vision of a future where automation, data analytics and machine learning improve the citizen and customer experience.

Mukul Agrawal is Chief Citizen Experience Officer with the Australian Government's Department of Human Services and a member of a global expert group which is helping review the Arab Digital Economy strategy.

In this exclusive interview, he discusses how digital transformation and automation can bring relief to both citizens and Department of Human Services (DHS) frontline staff through AI-based 'digital assistants' to help guide people through the maze of policies and rules that exists in a government department like the DHS.

What is your role in introducing digital technology, which can enhance the interface for citizen applications?

Today with ever developing technologies and continuous policy changes in government, there is a need to shape how we respond to the challenges they pose and design systems more proactively for the future.

My role is to assist the government in this move to provide better experiences incorporating digital technology in order to help citizens and improve service delivery.

How has technology been used to design an interface for citizens to use when requesting or looking for information?

We are continuously looking at ways to help citizens achieve their outcomes in faster and more efficient ways.

To this end we have deployed many technologies such as artificial intelligence, self-help tool visual systems whether it is to guide citizens to reach their answers or achieve self-service outcomes, if we believe it is easier for them to do it on their own.

We also use the tools to assist our front-line staff who deliver face-to-face interaction with the public as well as on the phone. This

means they can have tools to resolve issues and access better information to serve citizens.

What are some of the highs and lows and indeed obstacles you face when introducing state-of-the art technologies such artificial intelligence?

The biggest learning here is to really understand the problems that need to be solved when applying new technology. For example the role of artificial intelligence needs to be assessed. Is it to help staff answer questions and help resolve queries more efficiently or is it purely to help guide self-service through the best channel accessible to citizens?

Until clarity is reached on this issue, technologies may just be deployed for the sake of introducing something new. If this is the case, it does not achieve the necessary or expected outcomes and even result in increased time or greater complexity for both citizens and frontline staff, who may not understand how to use the technology or why it is relevant to their day-to-day activities.

Another third issue is to implement effective change management, which means ensuring visual literacy not only for customers but also staff, who cannot be expected to adapt to the new technology without proper consideration. Some systems are of course

sometime intuitive but others require support, education and training to achieve the best result.

So which of these comfort zones are more important to address in terms of obstacles and potential resistance – that of the end-user or of staff?

Both are of equal importance. Each one has complex areas with its own history, different objectives and desired outcomes. In the case of staff, they have years of experience in dealing with customers and have habits they have formed in doing their jobs in the best way they can. So in order to break those habits, there needs to be an understanding of their motivation and ways of working so technology can be introduced to enhance this through digital assistants and not lose the benefits already built up over time.

For example, the skills that staff develop working in human services call centers and shopfronts, along with attributes like empathy, compassion, discretion and fairness which they possess, is a kind of intellectual property that must not be lost.

Similarly, customers have preferences whether it is through certain channels of service or how they like to be acknowledged. Data plays a key role here as well whether surrounding issues of privacy or how data is used to good effect.

As a resukt of complexity, some systems require support, education and training to achieve the best result for frontline staff

**Mukul Agrawal,
Department of Human Services,
Federal Government of Australia**

What type of services are being delivered via the platform that has been implemented using the AI layer? Is it designed to embrace national ID or payments or transport services, for example?

It is primarily designed to embrace any type of service request so that the first time someone accesses our website they can navigate intuitively to the section or information they require faster and more easily. As the project started two years ago it is still ongoing in terms of development and it is not yet fully automated as an end-to-end service.

There has been a high hit and resolution rate regarding how citizens are using the technology through virtual assistants and self-service chats that pop up to help them in their request.

What is your involvement as a member of the expert group reviewing the Arab Digital Economy strategy for streamlining policy-making across the region of the 22 Arab states?

My role in the group is to give a perspective on how a strategy such as this is developed from a context perspective - in my case this is Australia – and how to achieve a breakdown through considered thought to reach a roadmap that provides tangible results. It is critical to start as early as possible when developing a new strategy for the digital economy so that all governments, individual department s and agencies are on board and can work together for a clear strategy.

by Victor March

Smart villages: stimulating economies in tech-starved regions

Projects aimed at bringing new levels of digital capability to remote unconnected regions of the world are no longer a pipe dream. Today, even remote villages that have zero digital connection, no internet and outdated telecommunications are able to leapfrog heavy infrastructure to bring their community full connectivity and boost their economy

As societies embrace new digital technologies in the era of what is being called the fourth industrial revolution, the developing world, in particular, is seeing transformational change in the way societies form around work and industry. There is a blurring between the physical world, the digital world and the biological world, which is accelerating. In this interview Dr. Greg Curtin, founder and CEO of CivicConnect, talks about his vision for digital governance with particular reference to smart villages in Africa focusing on education, labor and digital trade routes.

Why is the fourth industrial revolution an enabler for service-based verticals such as education and labor?

What we are seeing here is not simply a jump ahead in terms of efficiency and productivity which were the main hallmarks of previous industrial revolutions. There is a fundamental change in the way people work and communicate. A statistic from the World Economic Forum that ties into education and work, is that sixty-five percent of the children today that are entering primary school, will be working in jobs that do not exist today. That shows how fast this fourth industrial revolution is moving and really how transformational it is.

In what is now being called the gig economy is the fact that any group of people, anywhere on the planet, can come together and offer a service that can generate value and receive value for it.

How is this being manifested in key enabling technologies and connectivity in smart cities?

Usually we think about smart cities as already urbanized modernized cities taking yet another step into the modern future by connecting what they already have. But the bigger value and the greater opportunity is in emerging countries and markets, which have been starved of technology and economic stimulus because technology and infrastructures were heavy and incredibly expensive.

So now we have transformative technologies that tend to be lighter and can be put in place very quickly. This means there is an opportunity in emerging markets such as in smart villages, where infrastructure can be laid in an almost leapfrog effect. In areas where there where is no heavy physical infrastructure, we can now drop in a smart package.

Can you illustrate this concept in practice – such as the project you have been involved with in developing countries?

As an example, we are working with a group of companies within the smart cities consortium along with Inmarsat, a satellite company with a large presence in Africa. The Government of Niger have a program called Niger 2.0 with the aim of bringing the entire country to a new level of digital capability. However, there are 15,000 remote villages spread throughout the country that have absolutely zero connectivity, no internet, very little telecommunications and some mobile penetration - reflecting the culture and the life of the majority of Niger's population.

So in terms of this smart villages concept, we have carried out a pilot in the village of Fachi to show that these new technologies can be used to bring connectivity to one of the most remote communities.

Solar energy is used to generate power for Internet connectivity

Inmarsat and the smart cities consortium dropped in satellite-based Internet connection utilizing solar power, in order to show what can be done for a very remote village at a low cost to provide connectivity for the village to use.

The fascinating thing that came out of this one pilot was that the minute that village was connected, the villagers and the community found ways to use it before any training was provided. Through the mobile connection, they found a way within two weeks of that pilot beginning, to purchase a refrigerator unit for the village to use at a communal level.

How does this impact in the wider sense of learning and growth?

This sort of organic understanding of the power of digital technology without any history of it whatsoever, shows what can be done to generate economic activity with regard to societal change in education and healthcare. It shows that without any sort of stimulus other than providing the connectivity, this particular society is also starting to use the Internet for going online for information about agricultural products thereby helping to grow the local economy.

Inmarsat has brought a satellite based Internet connectivity to the village of Fachi in Niger, as part of a pilot project to increase people's digital capability

How does this impact on village life and the traditional way of doing things?

As part of this smart village initiative for Niger, the plan is to create an architected smart village network. In essence it will be a digital platform that builds towards the future so as to disrupt the villages in a positive way.

It is not about changing what the villages are doing. The idea is not not to bring the city to them or have them move into the city or form new societies, but to continue living a life that they choose as long as they want to. They will continue to do the things that have historically and culturally made them who they are, but will be able to enter a digital economy that shares and derives value for their village.

What is the future of this project in terms of potential expansion in Niger and beyond?

The whole idea is to use this to create the actual digital platform for a digital economy, so that 15,000 villages will be connected either all to each other or via a hub-and-spoke system. This remains to be seen, as it needs to be somewhat organic in terms of how they are organized. But at some level, all those villages will be part of a true digital economic platform, where they can buy and sel and where they can communicate with each other.

Enhancing this in another area, Niger has been chosen by the World Bank for one of its digital ID pilot projects as well. In fact, there are five or six countries involved in the western Africa region, so Niger is also looking to combine with those players to be

Meet Greg Curtin

Gregory G. Curtin, founder and CEO of CivicConnect, pioneered the use of technology and data to transform the public sector, and is now regarded as a revolutionary technology entrepreneur. Dr. Curtin is accredited for his work as a Senior Fellow at the World Economic Forum (WEF) and serves as a Charter Member of WEF's Global Agenda Council on the Future of Government. During his 10-year tenure with the United Nations Global E-Government Survey and Report, Dr. Curtin served as the principle investigator and one of its senior contributors.

part of a digital identification program. This will allow for every person to have a legal identity via a digital platform.

This also means attaching directly to a true digital platform for e-commerce, health and education to allow those villages and villagers to thrive online in a world where they previously had no technology nor connectivity.

Would you say this is also now completely transforming traditional trade routes ?

This is a major transformation as these are villages that are days away from each other and from urban areas in terms of traveling time. Now people do not necessarily need to walk or ride or drive to other areas in order to trade or acccess services. They can do it online in real time.

So connectivity is effectively creating digital trade routes for locally produced artisanal products, agricultural produce and livestock. This will have a huge impact in a country that is vast in terms of the different types of geography and the types of prpducts traded between the regions. From a technology point of view, it is interesting to look at this at the country level and be able to push technology faster and farther in these emerging market settings because they do not necessarily have the legacy infrastructure, technology and baggage to deal with.

Predicting the future of biometrics in payments

Biometrics has become the buzzword within the payments industry in recent years, so is the influx of pilot schemes confirmation that the biometric revolution is now a pressing reality? New research says it is

Following a number of successful trials using fingerprint sensor technology within smart cards across multiple markets, (including Bulgaria, the US, Mexico, Cyprus, Japan, the Middle East and South Africa) the biometric smart card is reaching its inflection point. Key players within the banking industry, including Visa and Mastercard, are already heavily invested in this new payment technology and anticipate that biometrics will play a key role in the revolution of the payments industry. With mass market rollout on the horizon, there are five key predictions for the biometric payment industry in 2019.

The first half of 2017 reported 937,518 cases of financial fraud, resulting in losses of an astonishing £366.4 million, a clear demonstration that the PIN is no longer fit for purpose. Recent research from IDEX Biometrics supports this claim and found that

29 percent of consumers surveyed felt concerned about the use of PINs to keep their money secure, and as many as 70 percent believed that contactless payment cards left them exposed to theft and fraud. As consumer concerns continue to grow around the security of payments, so too does the need for a personalized, secure and convenient payment solution.

2019: the year of dual interface

Enter the biometric dual interface payment card. It is expected that 2019 will see biometric fingerprint sensors integrated into cards with both a micro-processor and contactless interface, removing the need for PINs. This will provide consumers with the reassurance that their money is safe as any transactions will require their fingerprint to

authenticate it. 2019 will be the year of the dual interface where biometric authentication will be available for both contact and contactless payments!

These advances in technology and those within the payments market have meant that the concept of biometric authenticated payments is no longer a novelty. In fact, according to forecasts by Goode Intelligence, nearly 579 million biometric payment cards will be used globally by 2023. The integration of the biometric sensors in the payment card will be one of the next-generation transformative innovations to breathe new life into the payment industry next year and assist in the fight against payment fraud.

For mass market deployment of biometric smart payment cards to be possible in 2019, banking infrastructures must look at the implementation of biometric technology

and ensure that this method of enrolment is accessible and convenient to all. The elderly or those with physical health limitations may struggle leaving the house to enroll within bank branches and even those who work a 9-5 day can often find making it to the bank within opening hours a challenge.

Remote enrolment

The latest advancements in remote enrolment of biometric payment cards will mean that enrolment for biometric payment cards can take place in the comfort of your own home. Card users will be able to enroll straight onto the card by simply placing their finger on the sensor (with the aid of a small device that comes with the card) to upload their print to the card's highly secure EMV chip. There is no need for an external computer, smartphone or internet connection. Once loaded, the fingerprint never leaves the card, thus eliminating multiple attack points.

Bridging the financial inclusion gap

In 2019, advances in biometric fingerprint authentication will be a vital ingredient when bridging the gap to financial inclusion. Currently, 1.7 billion adults remain unbanked across the globe today, according to statistics. This is for many reasons, from immigration issues, to illiteracy as well as mental health. Those living with dementia are also at risk of losing their financial independence as their short-term memories decline. A fingerprint sensor on the card can take the place of a PIN or even signature, meaning sufferers are able to stay financially independent for longer.

Currently those who lack access to financial services are missing out on the many benefits financial inclusion has to offer. Fingerprint authentication will remove the barriers that face those with literacy challenges, or face difficulty with memory, as card payments will no longer be about what you know, or what you can remember, but who you are.

Biometric authentication will be a simple, secure and convenient solution eradicating the need for passwords and PINs as a form of authentication. For this to work as a solution to financial inclusion, banking infrastructures and card manufacturers must work together to reach a price point that enables this technology to be available to all.

New adoption

While biometric authentication technology is already being used with smartphones and passport identification in the UK, 2019 and beyond will see endless possibilities for the use of biometric smart cards into payments and beyond. We can even expect to see biometrics branch into the Government issued identification and IoT enabled devices arenas.

In fact, a whole host of public services is set to benefit from this secure means of authentication. The use of biometric smart cards within the UK's National Health Service (NHS), for example, could see access to sensitive patient records limited only to the patient themselves. Biometric social benefits cards could control how the money is spent and that it is spent by the right person. According to IDEX research, 38 percent of consumers surveyed would like to see biometric methods of authentication introduced to wider government identification including driving licenses, National Insurance numbers and even passports.

In 2019, authentication will get even smarter, and further technological advances such as multi-modal or multi-factor authentication will further enhance security within the payments landscape. This refers to technology that combines a variety of different types of biometrics in order to add an additional layer of security, including persistent authentication. For example, instead of having one single authentication, smartphones could continuously scan features to ensure the correct person is using the device.

Whilst the biometric dual interface smart payment card is set to hit the mass market next year — this is just the beginning. The payment card of tomorrow will go beyond just transactions. Biometric smart cards will serve multiple purposes — a payment card, a form of ID for restricted goods and even a loyalty card!

The early days of biometrics where it was felt to be invasive and a privacy concern are long gone. In fact, according to recent research, 56 percent of consumers surveyed state they would trust the use of their fingerprint to authenticate payments more than the traditional PIN. Further to this, 52 percent would feel more confident if their fingerprint biometric data was stored on their payment card, rather than a bank's central database.

Consumers are ready for the use of biometric fingerprint methods of authentication for card payments and 66 percent expect their roll out to authenticate in-store transactions in 2019. IDEX predicts that by 2019 biometric smart payment card adoption will go into many millions.

by Stan Swearingen,
IDEX Biometrics

Biometric authentication will eradicate the need for passwords and PINs

Dermalog

Improving secure identification worldwide by innovative biometrics

DERMALOG

Mittelweg 120
20148 Hamburg
Germany

Tel. +49 40 4132270
Fax +49 40 41322789

www.dermalog.com
info@dermalog.com

DERMALOG Identification Systems GmbH with head offices in Hamburg is Germany's pioneer for biometry and the largest German manufacturer of biometric devices and systems. The company provides biometric identification solutions including high-performance Automated Fingerprint Identification Systems (AFIS) and Automated Biometric Identification Systems (ABIS) as well as the latest generation of fingerprint and document scanners. DERMALOG's product range is complemented by biometric border control solutions, biometric identity cards and passports as well as biometric voting systems.

DERMALOG's technology is currently used in more than 220 large-scale installations around the globe. This includes one of the world's largest biometric installations set up in Nigeria. The branches of 23 banks and the Central Bank of Nigeria have been equipped with DERMALOG's ABIS. Bank customers are uniquely identified by fingerprints and face patterns, which effectively prevents fraud with false identities. The

Nigerian banks have already successfully registered more than 35 million customers.

DERMALOG's innovative solutions also provide outstanding services such as project management, installation, and customization as well as maintenance and support of the delivered products. These and additional services form the basis for a long-term and trustful cooperation that connects DERMALOG with numerous customers.

Human Recognition Systems

Biometric technology that enables critical safe

secure environments to operate effectively

HUMAN RECOGNITION SYSTEMS

2000 Enterprise Way,
Liverpool
L13 1FB
UK

Tel. +44 151 2542888

www.hrsid.com

In 15 years, Human Recognition Systems has pioneered and driven the adoption of automated identification technology around the world, from smoothing passenger journeys in the largest airports to keeping Construction workers safe across thousands of sites and protecting major events like the 2012 Olympic Games. We continue to challenge the status quo and have built the team to make a difference.

Today, the company develops a series of industrial software and hardware systems, enabled through biometric technology, that help construction companies, airports, oil & gas facilities and other 'critical safe secure' environments operate effectively. Innovation is actively encouraged within Human Recognition Systems, approaching any situation or problem with an open and imaginative mind ensures clients that they receive a solution that best fits their requirements. Everything is approached with energy, enthusiasm and drive.

Human Recognition Systems takes pride in fulfilling potential and maximising the growth of the business as a trusted provider who deliver intelligent and bespoke solutions that are valued by their clients.

Safran Identity ⚬ Security (Morpho)

A broad range of biometric solutions and multimodal recognition for multiple business sectors

Safran Identity & Security, formerly known as Morpho, is a global leader in security and identity solutions, deploying solutions in more than 100 countries. We employ more than 8,700 people in 57 countries and generated revenues of nearly €1.9 billion in 2015. Backed by more than 40 years of experience in biometrics, the company develops innovative technologies for a wide range of markets and applications for people, governments and business. The company's solutions manage identities, secure payments and transactions and safeguard privacy,

for an increasingly digital and connected world. Safran also contributes to supporting law enforcement and protecting borders, for safer and easier everyday lives.

Safran Identity & Security's broad range of biometric solutions calls on technologies such as fingerprint recognition, multimodal recognition combining fingerprints and vein patterns, facial recognition and iris recognition. It reflects our unrivaled experience in biometrics, built up over the years by providing solutions for many different sectors.

Safran Identity & Security offers different biometric solutions and components, including portable terminals, sensors, software, mobile applications and automated control gates. Virtually all of these products are designed to collect, stock and process (by comparing data) biometric information, and produce a result or authorize an action.

Vision⚬Box

Advanced biometric-based solutions in border control, identity management and surveillance

Vision-Box is a leading provider of Automated Border Control and electronic identity solutionsusing ICAO-compliant standards.

Since the deployment of the first worldwide eGate to use biometric facial recognition, we have been blazing a path of success, offering advanced biometric-based solutions in Border Control, Identity Management and Surveillanceto Governments, Border Control Authorities, Airports or all Organizations needing to improve their security processes.

The company provides end-to-end Passenger Experience and Electronic Identity Management solutions that use ICAO and NIST-compliant standards, with over 1,000 operational Automated Border Control & Passenger Experience solutions in more than 50 airports across the globe and 3,000 Identity Management solutions worldwide.

Vision-Box partners with the most prestigious organizations worldwide, delivering dependable border control, identity management and security solutions for the most critical security scenarios, such as complex integrated border management deployments for air, land and sea borders, and for challenging innovation contexts, like citizen biographic and biometric enrollment in remote places, and self-service identity document delivery.

3M www.3m.com/security	**MF -RFID -C (CL), M (L)** Center Bldg 225-4N-14, 55144-1000 St Paul, MN, Usa	Tel. 1/800/3280067	Fax 1/800/2235563
Accu-Time Systems Inc www.accu-time.com	**MF -B, DC -T (FX, FP)** 420 Somers Road, 06029 Ellington, CT, Usa	Tel. 1/860/870/5000	Fax 1/860/872/1511
Advanco SA www.advanco.be	**SI -BC, B -M (L, TTR), P (CP, I), S (HH, FX), T (RF, BT, FF)** Rue de la Fusée 66, B-1130 Brussels, Belgium	Tel. 32/2/7268800	Fax 32/2/7264039
Allegion www.securitytechnologies.ingersollrand.com	**MF -C, B -C (CL), T (HG), R (RF)** 11819 North Pennsylvania Street, 46032 Carmel, IN, Usa	Tel. 1/317/8103700	Fax 1/317/8103989
Aoptix Technologies www.aoptix.com	**MF -B -SW, SI -B - R (I), T, SW (I, OPT)** 675 Campbell Technology Parkway, CA 95008 Campbell, Usa	Tel. 1/408/558/3300	Fax 1/408/558/3301
ARH Inc. www.arhungary.hu	**MF -B, RFID, DC, BC -BC, R (HH, FX, RF, I), S (HH, FX, POS, I, OCR), SW (S)** 41 Alkotas St., HU-1123 Budapest, Hungary	Tel. 36/12019650	Fax 36/12019651
Arjo Systems www.arjo-systems.com	**SH, SI - B, C -C(CL,CM,SM), DC, EP, GP, H, NFC, R, RFID, T(VT)** 32 rue Jacques Ibert, 92300, Levallois-Perret, France	Tel. +33 (0)181938850	
AuthenTec www.authentec.com	**MF -B -T (FP)** 709 South Harbor City Blvd. , 32901 Melbourne, FL, Usa	Tel. 1/321/308/1300	
Aware www.aware.com	**SW -B -SW (FF, I)** 40 Middlesex Turnpike, MA 01730 Bedford, Usa	Tel. 1/781/276/4000	Fax 1/781/276/4001
Bio-key International, Inc. www.bio-key.com	**SH -B -SW** 3349 Highway 138, Building D Suite A, 07719 Wall, NJ, Usa	Tel. 1/732/359/1100	
BioLink Solutions www.biolinksolutions.com	**MF, SI -B, C -C (FP), S, SW** 511 Avenue of the Americas, PMB 572, 10011 New York, NY, Usa	Tel. 44/808/189/1360	
Biometrika Srl www.biometrika.it	**MF -B -C (FP, CL, CM, SM), T (FP), S (FX), SW** Monte Santo, 21, 47122 Forli, FC, Italy	Tel. 39/0543/370680	Fax 39/0543/456198
Biometry.com AG www.biometry.com	**MF, SH -B -T (FF), VR, SW** Chilcherlistrasse 1, 6055 Alpnach OW , SWitzerland	Tel. 41/41/6703272	Fax 41/41/6703276
Biomorf www.biomorf.co.id	**MF, SH - B - S (FP, I, FF, FX, HH, HG, OPT, OCR), SW** Menara BCA, JL.MH.Thamrin 1, Jakarta 10310 – Indonesia	Tel. +6221 2358 4793	Fax +6221 2358 4794
Bundesdruckerei GmbH www.bundesdruckerei.de	**MF, SI, D, SH -C, B -C (SM, CL, FP), P, R (HH, FX), T (FP, FP, FF, VF), SW, EP, GP** Oranienstrasse 91, 10969 Berlin, Germany	Tel. 49/30/25980	Fax 49/30/25982205

CodeCiphers

MF, SH -B, C -C (CL) B, IC

www.codeciphers.com

Rua Bogaert 107 Villa Vernehla, 04298-020 Sao Paulo, Brazil

Tel. 55/11/2175/1106   Fax 55/11/2175/1171

Cogent Systems, 3M

MF -B, C, RFID, BC -C (MG, CM, SM, CL, OPT, FP), TAG (RF <HF>) R (HH, FX), S (FX POS, I) T (HH, FX, RF, I, BC, FP, IF, FF), SW, EP

www.cogentsystems.com

639 N. Rosemead Blvd., 91107 Pasadena, CA, Usa

Tel. 1/626/325/9600   Fax 1/626/325/9700

Cognitec Systems GmbH

MF, SH -B -T (FF), SW

www.cognitec.com

Grossenhainer Str. 101, Tower B, 01127 Dresden, Germany

Tel. 49/351/862/920   Fax 49/351/862/9210

Cognitec develops market-leading face recognition technologies and applications for enterprise and government customers around the world. Various independent evaluation tests have proven the premier performance of our FaceVACS® software. Cognitec's portfolio includes products for facial image database search, recorded video investigation, real-time video screening and people analytics, border control, ICAO compliant photo capturing and facial image quality assessment.

Crossmatch

MF -B -R (HH, FX), S (HH, FX), T (HH, FX, FP, IF, FF, VF), SW

www.crossmatch.com

3950 RCA Boulevard, Suite 5001, Palm Beach Gardens, FL 33410, USA

Tel. 1/561/622/1650   Fax 1/561/622/9938

Daon

SH -B -SW

www.daon.com

11951 Freedom Drive - Suite 1400, 20190 Reston, VA, Usa

Tel. 1/703/984/4000   Fax 1/703/984/4099

Dartagnan BV

SI, SH -C, B, RFID -C (SM, CL), R (RF), T (RF, FP, IF, FF, VF), SW

www.dartagnan.eu

Triport 3, Westelijke Randweg 51, 1118 CR Luchthaven Schiphol, The Netherlands

Tel. 31/20/405/4149   Fax 31/20/405/4171

Datastrip Ltd

MF -B, BC -R (HH), T (FP)

www.datastrip.com

7 Thame Park Business Centre, Wenman RoaD, OX9 3XA Thame, OxfordSHire, UK

Tel. 44/1844/215668   Fax 44/1844/215669

Dermalog Identification System GmbH

MF,SH,SI,VAR,D -B,C,RFID,BC -C(CM,SM,CL,OPT,FP),TAG(RF<HF>),A,R(HH,FX,RF,I),S(HH,FX,POS,I),T(HH,RF,BC,FP),SW

www.dermalog.com

Mittelweg 120, 20148 Hamburg, Germany

Tel. 49/40/4132270   Fax 49/40/41322789

DigitalPersona

MF, SW -B -R(FX, FR, HH), SW

www.digitalpersona.com

720 Bay RoaD, CA 94063 Redwood City, USA

Tel. 1/650/474/4000   Fax 1/650/298/8313

Ekey Biometric Systems

MF, SH -B, RFID -S (FX, POS, I), T (FP, RF, I, POS), SW

www.ekey.net

Lunzerstrasse 89, 4030 Linz, Austria

Tel. 43/732/890500 2000   Fax 43/732/890500 2002

B iometrics

Entrust Datacard
www.entrustdatacard.com

MF -C, B -C (CM, SM, CL, FP), EP

Forum 3, Solent Business Park, PO15 7FH Whiteley, Fareham, UK — Tel. 44/1489/555600 — Fax 44/1489/555601

Eter Biometric Technologies Srl
www.eter.it

D, VAR, SI -B, RFID -C (MG, CM, SM, CL, OPT, FP), TAG (RF<LF, HF, UHF>), R (RF), T (RF, FP, HG, IF, FF, VT), VR, SW

Via Cartesio 3/1, 42100 Bagno, RE, Italy — Tel. 39/0522/262/500 — Fax 39/0522/624/688

Fingerprint Cards AB
www.fingerprints.com

MF -B -IC, T (FP), C (FP), SW

P O Box 2412 (Kungsportsplatsen 2), 403 16 Gothenburg, Sweden — Tel. 46/31/607820 — Fax 46/31/137385

Fujitsu
www.fujitsu.com

MF, SH -B -R (FX, HH, HG), SW

1-5-2 HigaSHi-SHimbaSHi, 105-7123 Minato-ku Tokyo, Japan — Tel. 81/3/6252/2220

Green Bit SpA
www.greenbit.com

MF -B, -T (FP, HH), SW

Via Rivalta n. 9 , 10095 Grugliasco (TO) , Italy — Tel. 39/011/7703811 — Fax 39/011/7703880

Hirsch Electronics Corp.
www.hirschelectronics.com

MF -B, C, RFID -C (MG, CM, SM, CL, OPT, FP), TAG (RF<LF, HF, MW>), R (HH, FX, RF, I), T (HH, FX, RF, I, BC, FP, IF, VT, VF), SW, EP, GP

1900-B Carnegie Ave., 92705 Santa Ana, CA, Usa — Tel. 1/949/250/8888 — Fax 1/949/250/7372

Hitachi
www.hitachi-eu.com/veinid/

MF, SH -B -T (FP)

Whitebrook Park, Lower Cockham RoaD, MaidenheaD, SL6 8YA Berkshire, UK — Tel. 44/1628/585581 — Fax 44/1628/585440

Honeywell Access Systems
www.honeywellaccess.com

MF, SH -RFID, B -C (MG, CM, SM, CL, FP), M (TTR, H), P (TTR), R (HH, RF), S (HH)

2700 Blankenbaker Pkwy, Suite 150, 40291 Louisville, KY, Usa — Tel. 1/800/6753364 — Fax 1/502/2975770

Human Recognition Systems
www.hrsid.com

SH, SI -B, RFID -R (FX, I, FP, HG, OPT), T (HH, FX, I, BC, FP, HG, IF, FF VF), SW

1st Floor, Building 2000, Vortex Court, Wavertree Technology Park, L13 1FB Liverpool, UK — Tel. 44/151/254/2888 — Fax 44/151/254/2999

IBM United Kingdom Ltd.
www-03.ibm.com/industries/government/

MF, SI, SH -B, RFID -T (FP, FF), SW

New Square, TW14 8HB Bedfont Lakes, Feltham, UK — Tel. 44/7802/461174

Identification Technologies Company (ITEC)
www.itec.snz.ru

D, SI -B, RTLS -TAG (RF, MW), R (RF) T (HG, VT)

18 Vasiljeva St, p/o 65, 456770 Snezhinsk, Cheljabinsk Region, Russia — Tel. 7/35146/21173 — Fax 7/35146/25741

IDesia Ltd.
www.idesia-biometrics.com

MF -B -T (VF), SW

7 Halamish Street - POB 3080, 38900 Caesarea Industrial Park, Israel — Tel. 972/4/6371938 — Fax 972/4/6376088

IDTeck
www.idteck.com

MF, D -C, B, RFID -C (CM, SM, CL), TAG (RF<LF, HF, UHF>), T (RF, FP, FF, VF), SW

5F, Ace Techno Tower B/D 684-1, Deungchon-Dong, Gangsuh-Gu, 157-030 Seoul, Korea — Tel. 82/2/26590055 — Fax 82/2/6590086

ImageWare Systems, Inc.
www.iwsinc.com

MF, SH -B, C -T (FP, HG, IF, FF), VR, SW

10883 Thornmint Rd , 92127 San Diego, CA, Usa — Tel. 1/858/673/8600 — Fax 1/858/673/1770

Industrial Innovation Group
www.industrialinnovationgroup.com

MF, SH – C, B, NFC, RFID – C(MG, CM, SM, CL, FP), M(L, H), TAG(RF), P(I), SW, EP, GP, MC

Building Z-2, Executive suite 85, SAIF Zone, Sharjah a/p, P.O. Box 9015, Sharjah, UAE — Tel. 00971 6557 0725 — Fax 00971 6557 4810

Ingenico

www.ingenico.com

SH, SI -C, B -T (HH, FX, RF, CL, BC, FP, POS), SW, VT

192 avenue Charles de Gaulle, 92200 Neuilly, France

Tel. 33/1/46258200

Fax 33/1/47725695

Inside Secure

www.insidesecure.com

MF -RFID, NFC -C (CL), M (SL, L), IC

41 Parc Club du Golf, 13856 Aix en Provence, France

Tel. 33/4/42396300

Fax 33/4/42396319

Interflex Datensysteme GmbH & Co. KG

www.interflex.de

MF, SI -B, C -T (RF, FP), SW

P.O. Box 81 03 60, 70520 Stuttgart, Germany

Tel. 49/711/13220

Fax 49/711/1322/111

International Biometric Group

www.biometricgroup.com

SI -B, C -SW

One Battery Park Plaza, 10004 New York, NY, Usa

Tel. 1/212/8099491

Fax 1/212/8096197

IRIS Corporation Berhad

www.iris.com.my

MF,SI,B,C,NFC,RFID,C(BC,CL,CM,H,MG,RF),EP,GP,P(CL,CM,MK),R(BC,CL,CM,CP,FP,HH,POS,RF,SM,VF),S(CL),SW,T(BC,CL,CM,FP,HH,POS,RF,SM,VF)

IRIS Smart Technology Complex, Technology Park Malaysia, Bukit Jalil, 57000 Kuala Lumpur, Malaysia   Tel. 603/89960788   Fax 603/89960441

To ensure a fast yet smooth implementation, it is important to select suppliers with extensive experience and proven track record in trusted identification. As the inventor of ePassport and multi-application eID, IRIS is the only supplier with extensive experience in ePassport since 1998 and in multi-application eID since 2001. We have international presence in over 28 countries where we deliver unrivalled service exceeding our customers' expectations. IRIS is committed to innovation and is the proud owner of over 40 patents in trusted identification products.

Julius Ltd.

www.powertouching.com

MF, SI, D -B, RFID -T (FP), SW

Nezavisimost str., 7000 Rousse, Bulgaria

Tel. 359/82/887475

Fax 359/82/809019

Kee Square

www.keesquare.com

SH -B -SW

Via DonaTel. lo 11, 20131 Milano, Italy

Tel. 39/02/36533368

Fax 39/02/36533329

Kronos Systems Ltd

www.kronos.com/uk

MF -B, C -T (FP)

Kronos House, Carey RoaD, RG40 2NP Wokingham, UK

Tel. 44/118/9789784

Fax 44/118/9782214

Legic Identsystems AG

www.legic.com

MF -RFID, NFC -IC (CL, RF <HF>), R (RF), T (RF), EP

Binzackerstrasse 41, CH-8620 Wetzikon, SWitzerland

Tel. 41/44/9336464

Fax 41/44/9336465

LEGENDA

ROLE IN THE VALUE CHAIN		PRODUCT CATEGORIES		PRODUCT SPECIFICATIONS			
D	= Distributor	A	= Antenna	BT	= Batch	IF	= Iris Feature
MF	= Manufacturer	C	= Cards	BC	= Barcode	L	= Labels
SH	= Software House	EP	= Electronic Personalization	CL	= Contactless	LF	= Low Frequency
SI	= System Integrator	GP	= Graphic Personalization	CM	= Contact Memory	MG	= Magnetic
VAR	= Value Added Reseller	IC	= Integrated Circuits	CMA	= Card Materials	MK	= Marking
		M	= Media	CP	= Compact	MW	= Microwave
		MC	= Machinery	DNA	= DNA	OCR	= Optical Char. Recognition
TECHNOLOGIES		MV	= Machine Vision	EAS	= Electronic Art. Surveillance	OPT	= Optical
B	= Biometrics	P	= Printers	FF	= Facial Feature	POS	= Point of Sale
BC	= Barcode	R	= Readers	FP	= Fingerprint	RF	= Radio Frequency
C	= Cards	S	= Scanners	FX	= Fixed	SL	= Smart Labels
DC	= Data Collection	SW	= Software	H	= Holograms	SM	= Smart
NFC	= Near Field Comm.	T	= Terminals	HF	= High Frequency	TTR	= Thermal Transfer Ribbon
RFID	= Radio Frequency Identification Device	TAG	= Tags	HG	= Hand Geometry	UHF	= Ultra High Frequency
		VR	= Voice Recognition	HH	= Handheld	VF	= Verifier
RTLS	= Real Time Loc. System			I	= Industrial	VT	= Vehicle Terminal

Lumidigm
MF -B -T (FP)
www.lumidigm.com
801 University Blvd SE, STE 302, 87106 Albuquerque NM, Usa
Tel. 1/505/2727084
Fax 1/505/2727354

Masktech GmbH
SH -C, B, RFID -IC, SW
www.masktech.com
Fischerstrasse 19, 87435 Kempten, Germany
Tel. 49/831/51210771
Fax 49/831/51210775

MaxID
MF -RFID, B, BC -C (CL, FP, SM), TAG (RF<LF, HF, UHF>), R (HH, RF, I), S (HH, POS, OCR), T (HH, RF, FP, POS, BC)
www.maxidgroup.com
530 Lytton Ave. 2nd Floor, 94301 Palo Alto, Usa
Tel. 1/650/617/3370

Morpho
MF, SI -C, B -C (CM, SM, CL, FP), R (RF), T (RF, FP, IF, FF), SW, EP, GP
www.morpho.com
Le Ponant de Paris 27, rue Leblanc, F-75512 Paris Cedex 15, France
Tel. 33/1/5811/2500
Fax 33/1/4070/2550

Nadra
VAR, SI, SH -C, B, RFID, DC -SW, EP, GP
www.nadra.gov.pk
State Bank of Pakistan Building, SHahrah-e-Jamhuriat, G-5/2, 44000 IslamabaD, Pakistan
Tel. 92/51/9205568
Fax 92/51/9202939

NEC Solutions (America) Inc
SI -B -T (FP), SW
www.necam.com/ids/law
10850 Gold Center Drive, Suite 200, 95670 Rancho Cordova, CA, Usa
Tel. 1/800/777/2347
Fax 1/916/4637041

Nfive Software
SH -C, BC, RFID, B -SW
www.nfive.com
Edificio OneWorlD, Urb Belo Horizonte Lt20, 2655-241 Ericeira, Portugal
Tel. 351/261/860450
Fax 351/261/865/647

Oki Electric Industry Co
MF -B -P (CP), S (I), T (I, IF, FF), SW
www.oki.com
7-12 Toranomon 1-chome, 105-8460Tokyo, Minato-ku, Japan
Tel. 81/3/3501/3835
Fax 81/3/3501/3924

Oracle Corporation
SH -B, RFID -SW
www.oracle.com
500 Oracle Parkway, 94065 Redwood Shores, CA, Usa
Tel. 1/650/506/7000

Precise Biometrics AB
MF -B, C -C (FP), T (FP), SW
www.precisebiometrics.com
Scheelevagen 19C, SE-223 70 Lund, Sweden
Tel. 46/46/311100
Fax 46/46/311101

Privaris, Inc.
MF -B, RFID -T (FP, VF, HH, RF)
www.privaris.com
650 Peter Jefferson Parkway, Suite 330, 22911 Charlottesville, VA, Usa
Tel. 1/434/293/4033
Fax 1/434/293/8212

SecuGen Corporation
MF -B -T (FP)
www.secugen.com
2065 Martin Ave Suite 108, 95050 Santa Clara, CA, Usa
Tel. 1/408/7277787
Fax 1/408/8347762

Smartmatic
MF, SW -B -T (FP, VF, HH, RF), R (FO, HG, FX), S, SW
www.smartmatic.com
105 Piccadilly, 6th Floor, W1J 7NJ London, UK
Tel. 44/20/3402/3613

Thales
MF, SI -B, NFC -IC, A, T(FX, FP, IF, FF), SW, EP
www.thalesgroup.com
20-22 rue Grange Dame Rose, 78141 Velizi, France
Tel. 33/1/73320000

Trix Tecnologia Ltd
MF, SI -C, B -P, S (HH,FX), T (RF, BT, FP)
www.xpto.com.br
rua da Paz, 1957 Ch Sto Antônio, 04713 002 Sao Paulo, SP, Brazil
Tel. 55/11/33652000
Fax 55/11/33652070

Trüb AG	MF, SI -C, B, NFC -C (MG, CM, SM, CL, FP), M (H), TAG (RF<LF, HF>), IC, A, P (TTR), SW, EP, GP, MC		
www.trueb.ch	Hintere Bahnhofstrasse 12, 5001 Aarau, Switzerland	Tel. 41/62/8320000	Fax 41/62/8320100

TST Biometrics GmbH	MF -B -T (FP)		
www.tst-biometrics.com	Moehlstrasse 39, 81675 Munich, Germany	Tel. 49/89/9988550	Fax 49/89/99885511

Unisys	SI, SH, VAR -C, B -C (MG,SM,OPT,FP), T (HH, FX, RF, BT, BC, FP, IF, FF, VF), VR, SW, EP, GP		
www.unisys.com/biometrics	801 Lakeview Drive, 19422 Blue Bell, PA, Usa	Tel. 1/215/986/4011	

Vision-Box	MF -C, B -C, R (FX, FF, FP, VF), T		
www.vision-box.com	Rua Casal do Canas n.2, Zona Industrial de Alfragide, 2790-204 Carnaxide, Portugal	Tel. 351/21/154/3900	Fax 351/21/154/3901

Vitronic Stein Bildverarbeitungssysteme	MF -BC, DC -R (I, OCR), S (I, OCR), MV		
www.vitronic.com	Hasengartenstrasse 14, 65189 Wiesbaden, Germany	Tel. 49/611/71520	Fax 49/611/7152133

Vlatacom d.o.o.	MF, SI, SH -C, B, DC -R(HH, FX,RF<HF>), S(OCR), T (HH, BC, FP, FF, RF, VF), SW, EP, GP		
www.vlatacom.com	5 Milutina Milankovica, 11070 Belgrade, Serbia	Tel. 381/11/377/1100	Fax 381/11/377/1199

Voicevault Inc.	SH -B -SW, VR		
www.voicevault.com	400 Continental Blvd., 6th Floor, 90245 El Segundo, CA, Usa	Tel. 1/310/426/2792	Fax 1/310/426/2001

Voxware	SH -B -VR		
www.voxware.com	168 Franklin Corner Rd., 08648 Lawrenceville, NJ, Usa	Tel. 1/609/514/4100	

Wacom Europe GmbH	MF -B -T (POS, VF), SW		
www.wacom-europe.com	Europark Fichtenhain A9, 47807 Krefeld, Germany	Tel. 49/6966/308200	

WCC Smart Search & Match	MF -B, DC -SW		
www.wcc-group.com	Zonnebaan 19, 3542 EA Utrecht, The Netherlands	Tel. 31/30/7503200	Fax 31/30/7503299

Zetes BV	SI -B, C, BC, DC, RFID, RTLS -C (SM, CL), M (L, SL,TTR, I),TAG (RF<LF, HF, UHF>), A, P (CP, I,TTR), R (HH, FX, RF, I), S (HH, FX, POS, I, OCR),T (HH, FX, RF, I, BT, BC, POS,VT,VF),VR, SW, EP		
www.zetes.nl	Science Park Eindhoven, Ekkersrijt 5202, 5692 EG Son, The Netherlands	Tel. 31/40/8444444	Fax 31/40/8444455

Organizations featured in this issue

ID WORLD BUYER'S GUIDE 2019 – 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 technologies focusing on vertical market segments of advanced biometrics authentication, innovative applications for mobile transactions, logical access, 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