SUSTAINABLE DEVELOPMENT

November 2023

DIGITAL ECONOMIES

Navigating the digital crossroads

ID PEOPLE

A spotlight on Saudi Arabia

HH Mohammed bin Salman: Vision for 2030 on AI

SMART CITIES

Developing interconnected sentient city brains

EGOVERNMENT

Benchmarking Europe's digital public services

ONBOARD TECHNOLOGY

FUTURE MANUFACTURING

Aligning single source processes in electronic assembly

ID WORLD DIRECTORIES

Top 50 Suppliers ePassport technology

Buyers' guide for ePassport and border control

Hadrian Media 15€

IXLA introduces Laser & Inkjet Solution

IXLA
ID LASER SYSTEMS

XPrint

COLOR PRINTING

Color Printing

Color Printing
DoD Printing: High Flexibility Low Costs
Nozzle Resolution: 600npi

LASER MARKING

Laser Marking

All IXLA systems allow the engraving of photos and personal data on the front side of the datapage

- Main portrait picture
- Ghost image
- Indent or Emboss Tactile effect
- Microtext
- Clear Window

CLI / MLI

CLI/ MLI

CHIP ENCODING

Contactess encoding

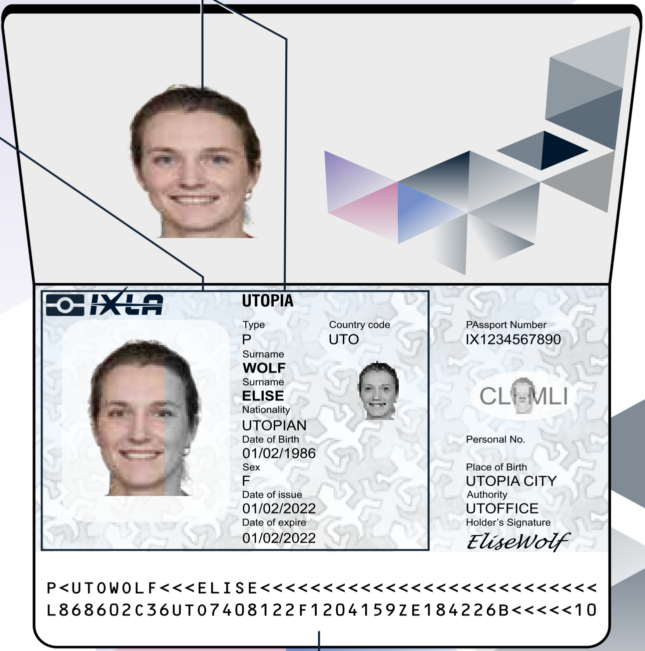
A complete «over IP» HW and SW solution with multitask distributed object oriented operating system.

OCR, XY reg.

MRZ QC

Vision System

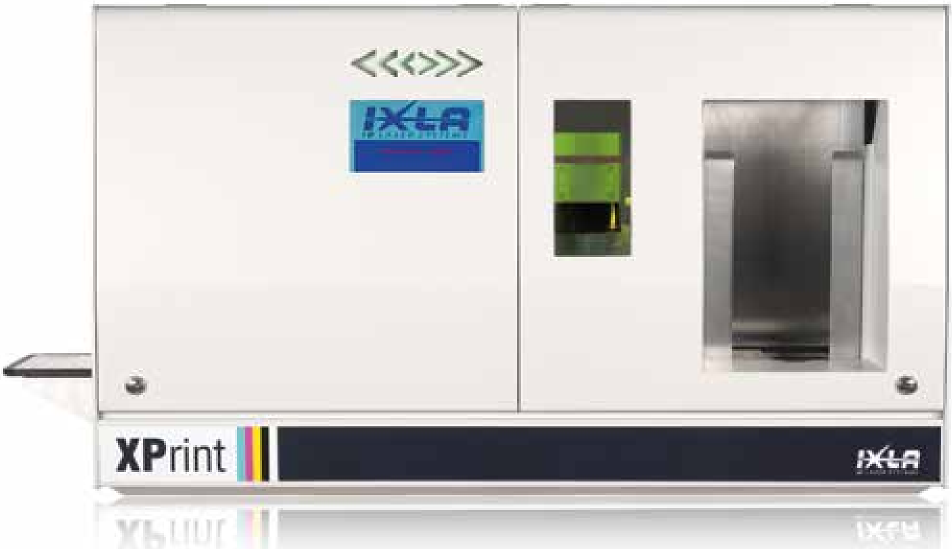
The integrated vision tools allow pre-personalization product inspection, quality control, barcode reading, offset



IXLA
UTOPIA
Type
P
Country code
UTO
PAssport Number
IX1234567890
Surname
WOLF
Surname
ELISE
Nationality
UTOPIAN
Date of Birth
01/02/1986
Sex
F
Date of issue
01/02/2022
Date of expire
01/02/2022
CLI MLI
Personal No.
Place of Birth
UTOPIA CITY
Authority
UTOFFICE
Holder's Signature
EliseWolf

```
P<UTOWOLF<<<ELISE<<<<<<<<<<<<<<<<<<<<<<<<<<<
L868602C36UT07408122F1204159ZE184226B<<<<<10
```

the future of security document personalisation



Desktop Laser and Color e-Passport Printer

Editorial

A decade from now, our retrospective gaze at present perspectives on sustainability will likely be marked by a kaleidoscope of uncertainties.

In our pursuit of the elusive equilibrium necessary for civilization's prosperity, the concept of sustainability has become a complex tapestry woven with concentric circles and moving targets. As we now delve into sustainable development, questions emerge: global warming, resource exploitation, migration, poverty — each a fragment contributing to the intricate puzzle. Amidst this, the digital revolution adds another layer of complexity, challenging our ability to engage in meaningful discourse while fundamental philosophical inquiries linger unanswered.

In the 21st century, the digital landscape, particularly shaped by social media, has transformed human relations, education, politics, and even the nature of warfare. While we bask in the immediacy of digital consensus, we remain oblivious to the far-reaching consequences of our actions. As Homo Digitalis, we wield newfound influence on a global stage, yet the extent of our impact raises ethical dilemmas: how far can we go in our quest for happiness before we have to accept a trade off in terms of justice.

Social media's pervasive influence has liquefied love, inflated the numbers of friendships, and given rise to a digitally empowered society. However, the superficiality and texture of these connections masks a potential void, as our opinions and performances strive for validation on the global stage. The digital era's tendency to follow, like and comment without forethought leaves us disconnected from the consequences of our actions.

Social media's pervasive influence has infiltrated education, with students contending not only with exams but also cyberbullying within their digital school community. In politics, the individual's power to disseminate real or fake information has reshaped the political landscape, from the Arab Spring to the manipulation of democratic elections. The implications of our digital actions often go unchecked, as the thrill of the current emotion overrides consideration of far-reaching or long-term consequences.

The digital revolution has extended beyond influencing political landscapes; it is transforming the nature of conflict itself. Cyberconflict, once confined to factions, is evolving to encompass all digital personas, real, fake, or robotic. The information generated collectively by these personas becomes a powerful force in shaping consensus, motivation, and power dynamics. As we grapple with the aftermath of events like the Cambridge Analytica scandal, the role of artificial intelligence and deliberately disseminated fake news emerges as potent instruments in the unfolding digital warfare of the 21st century.

The journey from Homo Faber to Homo Consumens saw humanity overexploit resources, resulting in dangerous climate change. Today, as Homo Digitalis, we face a new adversary — artificial intelligence. While it empowers us, it also poses a threat that transcends sustainable development concerns, infiltrating the battlefields of both real and digital warfare.

As we navigate this paradox, the onus lies on us to ensure that our digital influence aligns with the principles of justice, contributing to a sustainable future in the age of Homo Digitalis.

Sophie B. de la Giroday

JOIN A COMMUNITY OF THOUGHT LEADERS

> "As the Sustainability Summit Working Groups consolidate more than 20 years of ongoing discussions on how digital transformation is shaping the future of our society, a Sustainable Development Advisory Board, formed in 2020, monitors progress made. The Advisory Board engages decision makers, policy developers and industry leaders from around the world to elevate discussions and look at the latest challenges and goals set internationally."

SUSTAINABILITY SUMMIT

A ROADMAP TOWARDS OUR GLOBAL GOAL

2023

Munich • New York • Zürich • Paris • London

Transportation

Resources

Future Cities

Manufacturing

Infrastructures

ORGANIZED BY:
>>> wise media

ENDORSED BY:

FIND OUT MORE AT:
www.wisemedia.com

Contents

A report on a 'world-first' agreement on artificial intelligence (AI) at a global summit in the United Kingdom to combat the 'catastrophic' risks the technology could present. Views are explored from representatives and companies from 28 countries, who signed the pact, including the US, China and the EU. In a second viewpoint the accelerated social and economic evolution in Saudi Arabia is outlined covering AI and the nation's Vision 2030.

A report on how the global technology landscape is becoming more complex and dynamic as the threat of cybercrime escalates. The belief that one of the main discriminators in both global competition and national and security will be the ability to manage and harness technology. The US National Cybersecurity Strategy is also discussed.

An overview of the digital revolution in eGovernment exploring how security teams are being empowered through the cloud to create more value for an organization and its people. What trends are shaping the market and the key enablers, disruptors and game changers that are underpinning them? The report looks at five key emerging trends. Also in this section, the EU's eGovernment Benchmark is analysed as it sheds light on eGovernment in 35 European countries, referred to as 'Europe' or the 'EU27+and their digital transformation.

ID WORLD

THE SUMMER BUYERS' GUIDE

For the 19th year, our "Top 50 Suppliers of ePassport Technology" features the most active players in the ePassport and eID evolution, who are driving advancements in biometrically enabled, machine-readable identity and travel documents.

Page 31

Top 50 Suppliers ePassport technology

Semiconductor market to grow more than 20 in 2024

IDC has upgraded its Semiconductor Market Outlook by calling a bottom and returning to growth that will accelerate next year with a revenue outlook from $518.8 billion to $526.5 billion in a new forecast. Revenue expectations for 2024 were also raised from $625.9 billion to $632.8 billion as IDC believes the U.S. market will remain resilient from a demand standpoint and China will begin recovering by the second half of 2024 (2H24). IDC sees better semiconductor growth visibility as the long inventory correction subsides in two of the largest market segments: PCs and smartphones. Automotive and industrial elevated inventory levels are expected to return to normal levels in 2H24 as electrification continues to drive semiconductor content over the next decade. Technology and large flagship product introductions will drive more semiconductor content and value across market segments in 2024 through 2026, including the introduction of AI PCs and AI Smartphones next year and a much-needed improvement in memory ASPs and DRAM bit volume. Wafer capacity pricing will remain flat next year as foundry suppliers gradually improve utilization rates and demand returns from their core fabless customers. CapEx is expected to improve by 2H24 as revenue shipments match end demand and regional ChipAct incentives stimulate investment across the supply chain.

EC opens access to EU Supercomputers to speed up AI

The European Commission and the European High-Performance Computing Joint Undertaking (EuroHPC JU) have committed to open and widen access to the EU's supercomputing resources for European AI start-ups, SMEs, and the broader AI community as part of the EU AI Start-Up Initiative. To support the further development and scalability of AI models, access to world-class supercomputers that accelerate AI training and testing is crucial, reducing training time from months or years to a matter of weeks. The statement was made in the context of the fourth AI Alliance Assembly in Madrid, so European AI and high-performance computing (HPC) actors will closely cooperate to drive breakthrough innovation and enhance the competitiveness of the European AI industrial ecosystem.

Amazon passkeys revolutionise password-free

As a step towards redefining user authentication, the introduction of Amazon Passkeys represents a significant leap forward in ensuring both convenience and security for its users, says the company. This innovative approach allows individuals to access their accounts without the need for a traditional password, thereby transforming the login experience on the Amazon website and the iOS Amazon consumer app. Traditional usernames and passwords have long been the cornerstone of online security, however, this method is not without its flaws with passwords being susceptible to theft, hacking, or even human error. Amazon Passkeys work by using biometric data or pin code authentication as a replacement for the conventional password. Biometric identifiers such as fingerprint scans, facial recognition, or unique physical traits allow users to log in seamlessly, eliminating the need to recall complex passwords. They say it reduces the risk of unauthorised access as biometric data is significantly harder to replicate or steal compared to passwords. Amazon states it ensures this sensitive information is used solely for authentication purposes.

IBM acquires Apptio to boost automation

After receiving all required regulatory approvals, IBM has completed its acquisition of Apptio. The deal gives clients the ability to derive additional value through the powerful combination of Apptio and IBM, the companies say. This takeover brings together the industry-leading solutions of Apptio's FinOps offerings, including ApptioOne, Cloudability, and Targetprocess, and IBM's automation portfolio of Turbonomic, AIOps, and Instana to give clients a 'virtual command center' for managing, optimizing, and automating technology spending decisions. With AI and foundation models top of mind for clients and partners, IBM will also augment its watsonx AI and data platform with Apptio's $450 billion in anonymized IT spend data, unlocking new innovation, insight, and value. Under the statement, clients can immediately leverage the early integration between Apptio and IBM through their Cloudability and Turbonomic offerings - as an important first step.

US energy chiefs call to speed up transmission, solar and storage projects

The U.S. Department of Energy (DOE) has submitted a proposal that, if approved, would help speed up certain transmission, solar, and storage projects built on federal land, while clogged interconnection queues are causing headaches in the industry. The proposed changes would affect how the DOE complies with the National Environmental Policy Act (NEPA), adding a 'categorical exclusion' for certain energy storage systems and for upgrading and rebuilding transmission lines and for solar photovoltaic systems. These exclusions would remove the requirement for environmental assessments or environmental impact statements for specific types of projects. The DOE requested a single categorical exclusion for energy storage systems. It says it has not identified sufficient information to conclude that compressed air energy storage, thermal energy storage, or other technologies normally do not present the potential for significant environmental impacts.

Wind and solar to produce 33% of global power by 2030

A report by the Rocky Mountain Institute (RMI), U.S.-based non-profit organisation focused on clean energy, predicts wind and solar projects are on track to account for more than a third of the world's electricity by 2030. This signals that the energy sector can achieve the change needed to meet global climate goals. Sultan al-Jaber, president of the next UN climate summit, COP28, earlier this year called for a tripling of renewable energy generation by 2030 to curb greenhouse gas emissions and help reach goals set under the 2015 Paris climate agreement. Exponential sector growth means wind and solar projects are predicted to generate at least 33 per cent of global electricity, up from around 12 per cent now. This will lead to a fall in fossil fuel-powered generation and cheaper power, the RMI report showed. The RMI carried out the research in partnership with the Bezos Earth Fund, a $10 billion fund created by Amazon owner Jeff Bezos to help fund solutions to climate change. The cost of solar power, which is already the cheapest form of electricity production, will fall as low as $20 (€17.80) per megawatt hour (MWh) from around $40 (€35.70) MWh currently, as more projects are deployed and economies of scale improve, the report said.

Vietnam's airports bring in state-of-the-art biometric security

In a significant move to enhance security and streamline the passenger experience, Vietnam's airports are preparing to implement biometric authentication systems for check-in at all major terminals from November 2023. This innovative step marks a substantial investment in modernising airport operations across the country and underscores Vietnam's commitment to providing a safe and efficient travel environment for both domestic and international passengers. The plan, led by the Vietnam Aviation Authority (VAA), will see biometric authentication technology introduced across all major airports in Vietnam. The scope of the project is expansive, covering key facilities in Hanoi, Ho Chi Minh City, Da Nang, and other major airports across the country. Under this new system, technology will replace traditional methods of authentication, such as paper documents and physical identification checks.

Idemia and HTX partner to boost advanced biometrics in Singapore

A leader in identity technologies, Idemia, and Home Team Science and Technology Agency, of the Ministry of Home Affairs, in Singapore, have signed a master agreement under a Strategic Partnership for Innovation (SPI) to collaborate on research and development in biometrics and forensics technologies. The partnership with HTX will accelerate the development of cutting-edge solutions to ensure the safety and security of Singapore citizens, residents, and visitors. The announcement, say the partners, marks a pivotal next step in the collaboration between the parties and a significant milestone for Singapore's homeland security with technologies and solutions. Under the agreement, Idemia and HTX will jointly be designing and piloting solutions to address present and future challenges in Singapore. The SPI agreement leverages Idemia's presence in Singapore, alongside HTX's scientific and engineering capabilities, to deliver transformative and operationally ready solutions for homeland security.

UAE opens giant solar plant in desert

Abu Dhabi has inaugurated one of the world's largest solar projects ahead of the COP28 climate conference, which will be hosted by the UAE. The two-gigawatt Al Dhafra plant could reduce the city's carbon dioxide emissions by over 2.4 million tonnes a year – equivalent to removing about 470,000 cars from the road. The plant utilises about four million solar panels with bi-facial technology that captures sunlight on both sides for maximum yield, officials said. The project will raise Abu Dhabi's solar power production capacity to 3.2 gigawatts. The site is 35km from Abu Dhabi city and it was built in a single phase, spanning over 20 square km of desert.

National digital ID for Sri Lanka is necessary for prosperity say Chamber

Together with critical stakeholders, the Ceylon Chamber of Commerce recently addressed the need for Sri Lanka to deliver a national digital identity initiative as a key driver for its economy and prosperity. Underpinning digital transformation across public and private sectors, digital ID is now imperative for most modern governments and striven for to serve citizens. Concerned voices calling for fast-track treatment of digital ID include from the Sri Lanka Association for Software Services Company members and the Ceylon Chamber. Moreover, IT providers whose technologies are being embraced and acquired in the private sector are therefore putting pressure on the government over repeated delays to implement a national identity system. Many countries with a digital identity include Pakistan, the Republic of Korea and Singapore, with systems in place to harness existing physical identity infrastructure.

Governments on AI security as tech companies call for clearer approach

Leaders converge to sign a 'world-first' agreement on artificial intelligence (AI) at a global summit in the United Kingdom to combat the 'catastrophic' risks the technology could present. What does the industry think and is AI really one of the biggest threats to humanity, as claimed by Elon Musk?

Following the global AI summit held in the UK earlier in November, representatives and companies from 28 countries, including the US and China, as well as the EU, signed a pact that aims to tackle the risks of so-called frontier AI models.

The UK announced it would invest in an AI supercomputer, while the Tesla and X boss Elon Musk said on the sidelines of the event that AI is "one of the biggest threats to humanity". However, many in the tech community signed an open letter calling for a spectrum of approaches — from open source to open science and for scientists, tech leaders and governments to work together.

The AI agreement is a statement signed all summit attendees, including the US, China, and the EU. It aims to tackle the risks of so-called frontier AI models - the large language models developed by companies such as OpenAI. The UK government called it a world-first agreement between the signatories, which aims to identify the "AI safety risks of shared concern" and build "respective risk-based policies across countries". It warned frontier AI, which is the most sophisticated form of the technology that is being used in generative models such as ChatGPT, has the potential for serious, even catastrophic, harm, either deliberate or unintentional, stemming from the most significant capabilities of these AI models.

However, experts argue the agreement does not go far enough and are calling for a clearer appraoch to policy. Paul Teather, CEO of AI-enabled research firm Amplyfi, said in a news report that bringing major powers together to endorse ethical principles can be viewed as a success, but the undertaking of producing concrete policies and accountability mechanisms must follow swiftly.

"Vague terminology leaves room for misinterpretation while relying solely on voluntary cooperation is insufficient toward sparking globally recognised best practices around AI," he said.

Risk or no risk?

At the summit billionaire tech entrepreneur Elon Musk warned about the risks of AI: "We're not stronger or faster than other creatures, but we are more intelligent. And here we are, for the first time really in human history, with something that's going to be far more intelligent than us," he said. Elon Musk, who co-founded the ChatGPT developer OpenAI and has launched a new venture called xAI, said there should be a "referee" for tech companies but that regulation should be implemented with caution, so regulations do not inhibit the positive side of AI.

Meanwhile, European Commission chief Ursula von der Leyen, warned AI came with risks and opportunities and praised how quantum physics led to nuclear energy but also societal risks such as the atomic bomb. "We are entering a completely different era. We are now at the dawn of an era where machines can act intelligently. My wish for the next five years is that we learn from the past, and act fast!" she said.

Ursula Von der Leyen urged for a system of objective scientific checks and balances,

Elon Musk for once challenging innovation

Ursula Von der Leyen: calling for a system of objective scientific checks and balances

King Charles III: seeing AI as a great leap in the history of human endeavour

Joe Biden: signing AI executive order as US wants to drive tech change

with an independent scientific community, and for AI safety standards that are accepted worldwide. She said the EU's AI Act is in the final stages of the legislative process. She also said the potential of a European AI Office is being discussed which could "deal with the most advanced AI models, with responsibility for oversight" and would cooperate with similar entities around the world.

Also speaking at the summit, US Vice President Kamala Harris said that action was needed now to address "the full spectrum" of AI risks and not just "existential" fears about threats of cyber attacks or the development of bioweapons. She warned against additional threats that also demand action, and that are currently causing harm to many people.

Britain's King Charles III sent in a video speech in which he compared the development of AI to the significance of splitting the atom and harnessing fire. He said AI was "one of the greatest technological leaps in the history of human endeavour" and said it could help "hasten our journey towards net zero and realise a new era of potentially limitless clean green energy". But he warned everyone must work together on combatting its significant risks as welll.

Tech community critics

Meta's president of global affairs Nick Clegg said there was "moral panic" over new technologies, indicating government regulations could face backlash from tech companies. "New technologies always lead to hype," Clegg said. "They often lead to excessive zeal amongst the advocates and excessive pessimism amongst the critics.

Mark Surman, president and executive director of the Mozilla Foundation linked to browser Firefox, also raised concerns that the summit was a world-stage platform for private companies to push their interests. Also Mozilla published an open letter, signed by academics, politicians and employees from private companies, in particular Meta, as well as Nobel Peace Prize Maria Ressa. Mark Surman called for policymakers to invest in a range of approaches - from open source to open science - in the race to AI safety, as open, responsible and transparent approaches "are critical to keep us safe and secure in the AI era."

Representatives and companies from 28 countries, including the US, China, and the EU, signed a pact that aims to tackle the risks of frontier AI models

AI supercomputer

In related news, the United Kingdom announced it will invest £225 million (€257 million) in a new AI supercomputer, called Isambard-AI after the 19th-century British engineer Isambard Brunel. Alongside another recently announced UK supercomputer called Dawn, the government hopes both will achieve breakthroughs in fusion energy, health care and climate modelling.However, there is stiff competition from the US, China and the EU.

However, unlike the EU, the UK has said it does not plan to adopt new legislation to regulate AI but would instead require the existing regulators in the UK to be responsible for AI in their sectors.

China too has been pushing through its own rules governing generative AI. Vice minister of technology Wu Zhaohui said at the summit China would contribute to an international mechanism on AI, broadening participation, and a governance framework based on wide consensus.

Across the pond, in a statement after signing a US AI executive order directing his administration to facilitate the integration of AI-driven educational tools into the nation's education system, President Joe Biden said America would lead the way during this period of technological change

by Victor March

AI fast forward: a spotlight on Saudi Arabia

Central to the nation's hopes for accelerated social and economic evolution, the Kingdom of Saudi Arabia is one of the first countries in the world to explicitly entrench AI in its national development plans: Vision 2030

Saudi Arabia was one of 28 countries to sign Bletchley Declaration to ensure safe use of AI The participants included Abdullah Al-Ghamdi, president of the Saudi Data and Artificial Intelligence Authority, government ministers from a number of countries, and senior representatives of specialist technology and AI institutions. The UK, the US, the EU and China were among those who agreed to work together to ensure that AI technologies are developed and used in a safe and responsible manner.

During the summit it was reported Abdullah Al-Ghamdi held meetings with officials from a number of countries on the sidelines of the event, according to reports. During talks with Jonathan Berry, Viscount Camrose, the British minister for AI and intellectual property, he discussed a number of AI-related topics, and reviewed cooperation between Saudi Arabia and the UK in the field and how it might be enhanced.

In other reports, Abdullah Al-Ghamdi and Gabriela Ramos, UNESCO's assistant director general for social and human sciences, discussed the important role AI can play in promoting the UN's Sustainable Development Goals, along with other issues including UNESCO's recommendations on AI ethics and the Kingdom's work in this area.

In addition, the Saudi delegation said its officials and Alexandra van Huffelen, the Dutch minister for digitalization, discussed how best to deal with AI and its advanced technologies within a framework of international controls that can help guarantee the benefits for the good of humanity. Talks were also held between the Saudi delegation and Singapore's minister of communications and information, Josephine Teo, about ways to enhance cooperation between their countries in the field of advanced technologies within the framework of the Saudi Vision 2030 development and diversification agenda.

Vision 2030, introduced by Saudi Arabia's Prime Minister, Crown Prince Mohammed bin Salman , is aimed at making the kingdom the heart of the Arab and Islamic world, an investment powerhouse, and a hub that connects three continents. It is Saudi Arabia's long-term blueprint for economic diversification and tech-enabled sustainability. The Vision includes AI as well as other advanced high tech as crucial components for future success. This is reflected by the International Center for AI Research and Ethics (ICAIRE) in Riyadh, showing Saudi Arabia's commitment to advancing artificial intelligence on both domestic and global fronts.

Saudi Arabia's Minister of Education, H.E. Yousef Al Benyan, urges for AI in schools

AI in education

In other moves back in Riyadh, Saudi education minister has called for the fear around AI in schools to be abandoned. Saudi Arabia's Minister of Education, H.E. Yousef Al Benyan, has urged the global education community to embrace the potential of artificial intelligence (AI) in schools, emphasizing the importance of equipping teachers with digital knowledge and addressing concerns related to cybersecurity. Speaking at the Global Cybersecurity Forum in Riyadh, he stressed that fear should not hinder the adoption of AI in education, as the benefits far outweigh the risks.

With schools around the world all grappling with how to use AI, Al Benyan told the audience: "We need to recognize that you cannot have an education system above the quality of your teachers. So I think it's very important that the teachers are the foundation for any success in any education system."

Al Benyan, who was CEO of the Saudi chemical manufacturing company SABIC before taking up his role in government, stressed that teachers must be digitally equipped with the knowledge to effectively educate current and future generations. This includes a deep understanding of AI and its applications, as well as cybersecurity measures.

"People are sometimes cautious about using AI," he said in a statement. "But let's remember, any new technology has its own risk. But as of today, I think we have a very strong technology that will allow teachers to enhance their skill set and research using AI in a safe way." The minister drew a parallel between embracing AI in education and making decisions in the corporate world, stating the need to calculate risk.

While emphasizing the importance of seizing the AI opportunity, the minister also called for caution, particularly in addressing the ethical and values-related aspects of AI in education. He cautioned about the implications. "From my conversations with global leaders, the issue is over ethics and values. How can we ethically leverage AI, and how can we create a stronger platform to manage the risk of AI?"

Introducing Saudi Arabia's Vision: PM and Crown Prince Mohammed bin Salman

AI-driven educational tools

The Saudi education minister's comments come on the back of U.S. President Joe Biden signing an executive order directing his administration to facilitate the integration of AI-driven educational tools, including personalized tutoring technology, into the nation's education system.

In a poll, more than two-thirds of parents in the National Parents Union survey of 1,515 respondents see the benefits of AI in schools as outweighing or equal to the drawbacks.

International Center for AI Research and Ethics (ICAIRE) in Riyadh has the status of a Category 2 Unesco Center and underscores Saudi Arabia's commitment to advanced AI

Information security

In other areas of tech developments in the Kingdom, Saudi Arabia's government and private sectors are advancing in cybersecurity, with the leadership strongly emphasizing the importance of electronic information protection, according to an official from the World Economic Forum.

According to reports from the Global Cybersecurity Forum, Akshay Joshi, head of the industry and partnerships at the Center for Cybersecurity at the WEF, highlighted Saudi efforts in cybersecurity and its role in the global landscape. He referenced a well-established national cybersecurity authority as well as leading organizations such as Saudi Aramco, SITE, NEOM and Saudi Telecommunications — all of which are partnering WEF.

Quantum computing

As a WEF partner, Saudi Arabia like the others, also sees opportunities for quantum computing, which the world is essentially waiting for, but that has heightened security-related considerations. As a result of these transformations, cybersecurity is a top concern to the WEF. Therefore, there is no digital transformation without cybersecurity being deep and green. There is also a call for a structural alignment among various industry stakeholders and governments that assesses the ground situation as a business imperative.

by Sophie B. de la Giroday

Leveraging AI for best-in-class biometric algorithms

AI pundits believe the technology is set to be the next generational disruptor. But is this the reality and where does the collection of biometric data for training of neural networks stand in the mix?

Recently, AI-based technologies and products such as OpenAI's ChatGPT and Google's Bard have been hot topics across the media. AI, which has seen exponential development and growth over the last several decades, has recently reached a zenith in terms of hype and ubiquitous use that includes industry, science, medicine, education, and government to name a few. AI is being touted as the next technology that will revolutionize the world and has been compared to the technological innovations initiated with the rapid rise in internet companies during the dotcom boom, the advent of virtual and augmented reality, and the widespread adoption of cryptocurrencies and blockchain. Today, many experts believe that AI is set to be the next generational disruptor with some predicting its effect to be ground-breaking in several applications and fields that may even lead to the redundancy of entire professions.

On a more positive note, AI is an invaluable technology that can be used to great effect to optimize a wide range of activities, which in turn will speed progress, help professionals in their daily work as well as aid researchers like us to develop innovative technologies.

However, AI can also be used with different levels of success, as more than just using some AI approach and standard methods for training may be required to achieve spectacular results.

Today, it is already clear that many technology companies claim that they are using AI in their products, and with Big Tech gearing up for a new AI arms race, more and more players will feel the need to sprinkle AI references into everything they do to appear relevant. Unfortunately, this will quickly lead to the devaluation of belonging to an AI league, blurring of positioning, and confusion in the market.

AI in biometrics

The application of AI for the training of biometric algorithms is not new. The industry started using AI in the early 2000s, when researchers began developing algorithms

Following the success with face recognition, researchers started exploring the use of AI for fingerprint recognition

for face recognition that incorporated ML techniques such as support vector machines (SVMs), allowing computers to learn and recognize faces with increasing accuracy. A decade later, the industry incorporated the use of deep learning-based neural networks for extracting information-rich features from faces. This move towards resource-intensive but accurate algorithms was mainly due to the availability of large-scale training datasets and compute devices such as Graphical Processing Units (GPUs). Following the success with face recognition, researchers started exploring the use of AI for fingerprint recognition – a much more niche domain.

Optimal performance of a biometric algorithm is contingent upon the utilization of specialized domain knowledge for the creation of robust features, bias mitigation using appropriate training strategies, as well as ensuring viability for deployment. Therefore, when analysing any vendor's technology, it is critical to consider technical aspects, such as matching speed and recognition accuracy that have been determined in international tests/evaluations, the size of biometric templates that can affect hardware footprint and total cost of ownership, along with the crucial but often underestimated legal aspect, that is, the collection of biometric data for training of neural networks.

ML techniques such as support vector machines allow computers to learn and recognize faces with increasing accuracy

In addition, it is crucial to ensure that biometric systems are developed and deployed ethically and transparently, with appropriate safeguards in place to protect individuals' data given the ongoing concerns about the potential misuse of AI-based biometric technologies and data, as well as the privacy and security implications of collecting, storing, and analysing large amounts of sensitive personal information.

Data for training

The ability of a neural network to learn and accurately match faces, fingerprints, irises, and other biometrics is made possible through training using large amounts of diverse and representative data for training. The origin of these data has been the subject of much scrutiny and at times controversy. In terms of face recognition, for example, the internet has a plethora of freely available sources of face images – like social networking sites, and other channels. As a result, some companies scrape these face images without any concern as to the legality of the use of the images, and certainly without any official consent from the owners.

In reaction to these practices, several countries are starting to create and implement new legislation to protect citizens' biometric data and rights, and to provide guidelines for these data's fair and legal use. Nevertheless, the fact remains that each company must develop its own ethical policies outlining how they choose to use images responsibly and obtain biometric data for training fairly and legally.

Speed and accuracy

There are three main factors that contribute to the speed and accuracy of biometric technologies.

First, obtaining consent-based biometric data for training is expensive, and there is minimal sharing of these data across industry and academia. The lack of access to these kind of data leads to the creation of unreliable and poor-performing algorithms which can be heavily biased towards certain genders, races, or ethnicities.

Second, the development of a high-performing algorithm that will be used in, for example, an Automatic Biometric Identification System (ABIS), and is capable of matching potentially billions of people with the same high speed and recognition accuracy requires a Research and Development team that has biometric domain knowledge and deep expertise in the design, development, and implementation of such a system. This kind of experience can only be gained through hands on creation of national-scale projects.

Lastly, the development of best biometric algorithms requires constant investment in research, testing, and improvements. There are several independent internationally recognised biometric testing laboratories and institutions, such as NIST (National Institute of Standards and Technology), BixeLab, iBeta, and others, where vendors can test their technologies to ensure quality and understand their position in the market.

Tech5 technologies are highly accurate, robust, and inclusive. The company's IP-protected face, fingerprint, and iris matching algorithms are consistently ranked in the top tier in NIST testing and its research team focuses on unique and novel amalgamation of AI/Machine Learning and specialized domain knowledge from traditional methods. The new fingerprint matching algorithm, submitted is rated as the 2nd fastest and one of the most accurate technologies in the world. This algorithm is based on state-of-the-art AI/machine learning networks infused with fingerprint-specific domain knowledge. This combination allows for higher matching speed and improved accuracy of the technology, which results in a reduced server hardware footprint and a lower total cost of ownership (TCO) for the entity deploying the platform.

T5-AirSnap is a fully contactless biometric capture technology powered by AI

Contactless capture

Furthermore, the development of an algorithm for fast and accurate contactless fingerprint capture that can be performed using a simple camera of a mobile device. The technology allows for accurate biometric acquisition by capturing a fingerprint(s) image(s) with a smartphone's built-in camera, checking and enhancing the quality of the captured image(s), running a liveness check, and then packaging and sending the data for verification or registration, all within seconds. The process ensures that the data is taken from a real person and that the image(s) are of acceptable quality, suitable for use with legacy datasets, and comply with applicable standards and customer requirements. This proprietary and patent-pending contactless fingerprint capture technology, called T5-AirSnap Finger, incorporates Machine Learning and Computer Vision with novel image processing techniques to bridge the gap between contactless and contact-based fingerprint capture and recognition and eliminates the need for purpose-built devices for the capture of fingerprint biometric data

AI-based algorithms will be used increasingly more to enhance the analysis and interpretation of currently used biometric data

These technologies across all 3 biometric modalities – face, fingerprint, and iris – are used in the T5-OmniMatch ABIS matching platform for National ID-scale projects, as well as in every biometric platform within the T5-Digital ID offering, ensuring inclusion across the globe, and are available for certified partners of the company as part of the flagship capture, identification, and verification offerings.

In the coming years, AI is expected to continue to improve the accuracy, speed, and versatility of biometric systems. AI-based algorithms will be used increasingly more to enhance the analysis and interpretation of currently used biometric data as well as improve innovative biometric modalities such as behavioural biometrics, that are not yet widely used.

The AI-based approaches will also help develop new modalities that are not traditional and work in non-ideal conditions. For example, palm recognition works with low-resolution cameras as it does not require stringent capture requirements like traditional fingerprint algorithms. In addition, the rate of algorithm improvements will significantly increase in the areas where traditional algorithms take years compared to AI-based ones taking months. AI will also allow efficiently combining modalities to create robust and high-accuracy algorithms.

by Tech5

Research shows ChatGPT improves response with emotional intelligence

Generative AI tools, such as OpenAI's ChatGPT, have become integral to various aspects of our lives, assisting individuals in reaching personal goals and simplifying professional tasks. However, users often need help to get the desired responses from these AI models. A recent study conducted by Microsoft, William and Mary, and Asian research centres sheds light on a potential solution: leveraging emotional intelligence in prompts. The research explored whether large language models (LLMs) behind generative artificial intelligence tools like ChatGPT can exhibit emotional intelligence. In this context, emotional intelligence refers to the capacity to interpret and manage emotion-infused information, harnessing it for cognitive tasks, from problem-solving to behaviour regulation.

EU launches 4 testbeds for pre-market AI tech

European officials — who reached political agreement on the EU's new Data Act last night — have launched four labs to test AI applications before they're released to the general public. The labs will look at AI and robotics for manufacturing, healthcare, agriculture, and cities. Under the European Commission's Digital Europe Programme, the testing and experimental facilities (or TEFs for short) will investigate the risks and impacts of new AI technologies before they hit the market. Machine learning algorithms, robots, or self-driving cars can thus be tested in simulation and in the physical world by researchers focused on four different areas: manufacturing, healthcare, agriculture and food, as well as cities and communities. pledging €220 million funding for five years.

OECD releases AI Incidents Monitor to address impact

The AI Incidents Monitor, launched by the OECD, seeks to tackle AI challenges through evidence-based policies. Its goal is to offer comprehensive policy analysis and data across various disciplines, shedding light on AI's impacts and fostering discussions to shape informed AI policies. The OECD.AI Observatory released a beta version of the AI Incidents Monitor (AIM). Designed by the OECD.AI Observatory, the OECD AI Incidents Monitor (AIM) is a new tool for assessing the depth of AI-related issues. AIM uses a media monitoring platform that scans 150,000 news sources globally in real time and collects over one million news articles daily to extract data on AI incident occurrences. The initiative is part of the OECD's broader efforts to deepen insights into AI's transformative power and its implications for our economies and societies. The AIM can be particularly useful for evidence-based policymaking, which uses empirical evidence to inform and improve policy decisions. By integrating AI with research methodologies and prioritizing evidence-based policymaking, policymakers can harness the power of data-driven insights to develop adequate policies.

The AI Incidents Monitor combines the OECD and partners' resources to provide data, inform policymakers, and guide towards trustworthy AI. The AIM's focus is on AI incidents or risks posed by AI that have appeared as factual events. Due to the widespread use of AI in diverse sectors, an increase in recorded incidents is expected. To monitor and mitigate these risks, stakeholders require a clear but adaptive definition of AI events. The new tool includes research on incident definition and practices in AI-specific and cross-disciplinary contexts. Additionally, the use of AI will give policymakers the option to simulate various policy strategies to anticipate future impacts and revise plans if necessary. By leveraging the power of AI, policymakers can better make sense of the complexity of an AI-driven world.

Google to boost Malaysia's digital AI economy

The Malaysian government and Google have announced a strategic collaboration aimed at fostering inclusive growth opportunities in Malaysia's rapidly expanding digital economy. The Malaysian government and Google have announced a strategic collaboration aimed at fostering inclusive growth opportunities in Malaysia's rapidly expanding digital economy. The partnership aims to enhance the digital competitiveness of businesses through various initiatives such as responsible AI innovation, skilling programs, investments in digital infrastructure and the adoption of cloud-first policies. Google, through the Go Cloud program will offer learning pathways for upskilling 300,000 Malaysians by 2026. The online courses in these learning paths focus on improving the application of generative AI, data analytics, and cloud-based productivity tools for individuals. This would be an extension of Google's Gemilang program, which has already offered 31,000 Google Career Certificate scholarships to underprivileged individuals to obtain professional certifications in high-demand fields.

New computer chips launched to offset high cost of AI tech

Microsoft announced on Wednesday a duo of custom-designed computing chips, joining other big tech firms that are bringing core technologies in house to offset the high cost of delivering artificial intelligence (AI) services. The tech giant won't be putting its new chips on the market but will instead use them to power the AI capabilities of its subscription software services and Azure cloud computing. Microsoft indicated that it does not plan to sell the chips but will instead use them to power its own subscription software offerings.

Transforming national cyber security in a volatile world

The return of conflict to the continent of Europe – alongside growing threats elsewhere in the world – is seeing a sharpening of national approaches to the global technology landscape

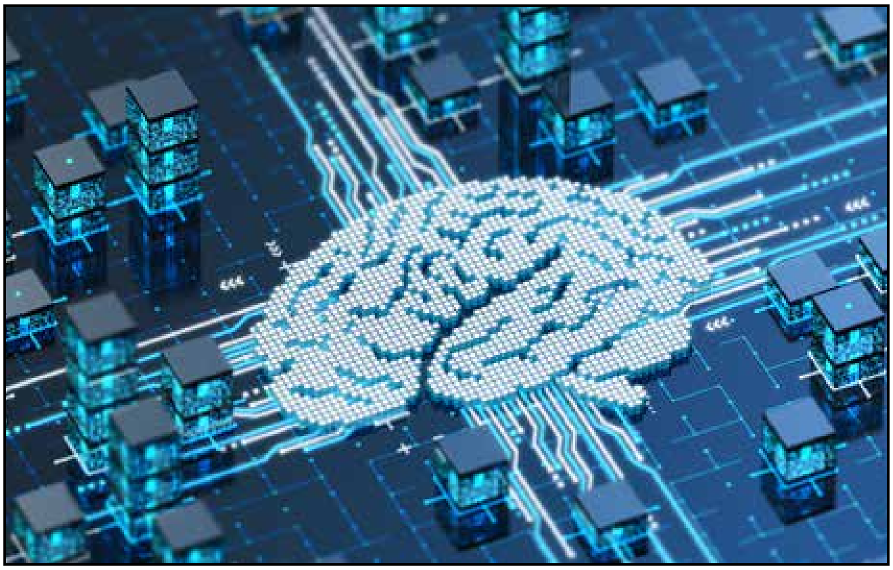
Conflict in Europe and elsewhere is impacting on the security concerns of sovereign nations and the open international order on which stability and prosperity in Europe have depended for over three quarters of a century.

The global technology landscape is more complex and dynamic than ever. The UK Government believes that one of the main discriminators in both global competition and future conflicts will be the ability to manage and harness technology. This underpins the ambition for the UK to be a Science and Technology (S&T) superpower and embrace the important role played within the UK S&T Framework, which sets out the Government's goals and vision for S&T through to 2030.

The pursuit of strategic advantage through S&T in defence, enhances the ability to identify, exploit and secure key emerging scientific and technological developments, push the most relevant technologies into operational capability, and secure a range of national benefits.

Security framework

Investment in advanced research and development (R&D) to create and seize the opportunities presented by new and emerging technologies, to enhance the military capabilities available to the UK and its allies, and to help maintain a strategic advantage.



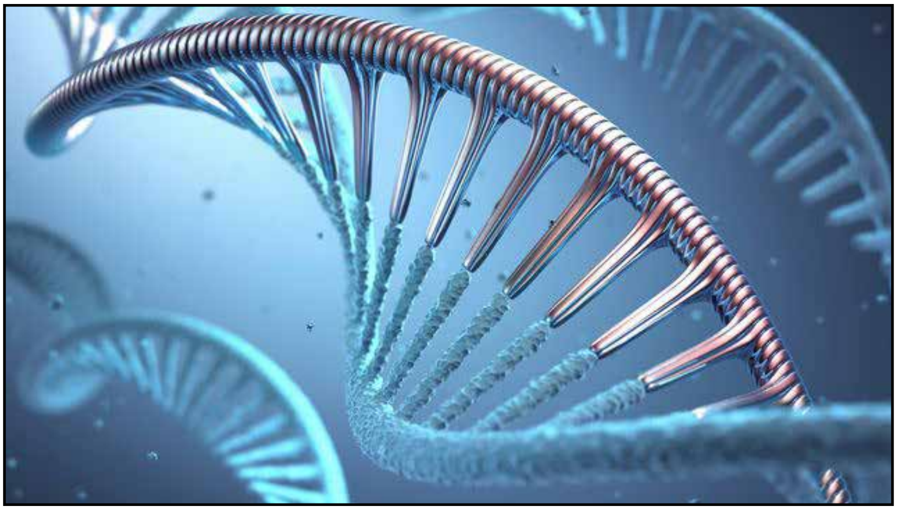
Artificial intelligence is a strategic priority, as set out in the Defence AI Strategy, one of whose key goals is the strengthening of the UK's defence and security AI ecosystem. The department will deliver innovative capabilities to support current operations (primarily in Command & Control and Intelligence) and tools for greater organisational agility like supply chain management. It will increase investment in AI-enabled military capability options, prioritising them in Force Development and 'balance of investment' exercises, and identifying 'quick win' capability enhancements and new AI options in major programmes.

Engineering biology - taking synthetic biology concepts and translating them into real-world solutions presents tremendous opportunities, including applications for future military capabilities. And in future telecommunications, advanced electrical engineering is a priority S&T capability for MOD, with a strong interest in the delivery of effective and secure national digital infrastructure. The Ministry will remain closely engaged with other government and national security departments to support NSTC goals.

Semiconductors are a foundational technology, critical to national prosperity and security. Specific semiconductor technologies are particularly critical to sensing, imaging, weapons, countermeasures, and communications applications. Defence, as a major consumer of semiconductors with market-shaping procurement power, will work closely with the Department for Science, Innovation & Technology (DSIT) to deliver the outcomes set out in the National Semiconductor Strategy.

Artificial Intelligence

AI is fast becoming the 'next big thing' in security. There are a huge number of 'intelligent' tools coming to market, each one promising to solve problems better and faster than traditional approaches. But do intelligent tools actually outperform humans in every case? How can you determine



Synthetic engineering biology translates security concepts into real-world solutions

whether an intelligent tool is right for you? And who would fix your intelligent systems if they were to let you down? This guidance will help you find answers to these, and many other questions.

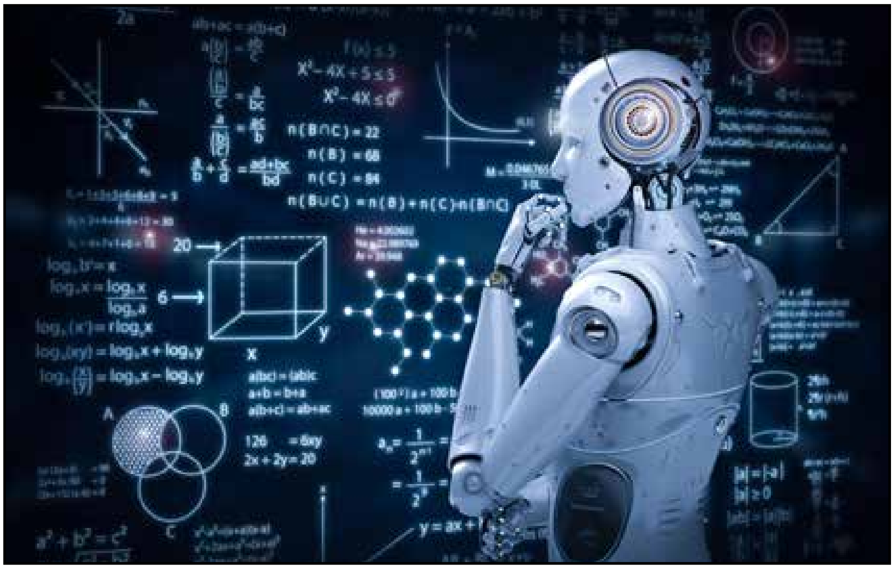
Though the future will likely see AI making significant contributions to many fields, the picture at present is far from clear. Intelligent tools are not without their limitations. Poorly trained AI can have biases and vulnerabilities that we are only just beginning to understand.

Modern AI is usually built using machine learning algorithms. These find complex patterns in data, which can be used to form useful rules. For example, a machine learning algorithm could find similarities in pictures of cats. If you tell it which pictures are of your cat, this can form rules that allows the system to recognise your cat. When you show it a new picture, it will be able to predict whether the new image is your cat or not, based on its learned definition.

A key part of AI is that it takes those patterns and definitions and uses them to automate a decision. AI is good at solving well bounded problems, where the solution, and the method to find it, is completely contained within the data and feedback provided. Here they regularly excel beyond human abilities, for both speed and accuracy.

Another fruitful field for AI has been image recognition and generation, where the problems are to predict which group a new image belongs to, or create a new image of that type. All the information required to classify, or create an image, is contained in the image data provided. AI is less good at solving problems where you need additional context to reach an answer, even if that context would be 'common sense' for a person.

AI takes ML algorithm patterns and definitions and uses them to automate a decision



It may be possible to provide some of this context to an AI in the form of additional data, a model, or feedback from a human, but expanding the bounds of the problem is often expensive and may result in poor performance if expanded too far. At this point, the decision should be passed to a person who is able to use their knowledge of the context to reach a decision.

Cyber security

Situations where context is important are often in the cyber security domain. Accessing a sensitive document might be a suspicious action for one person, but normal behaviour for another. Installing updates is essential for most of your business, but a business risk where it causes compatibility issues with critical software. This is why it is important to find a tool that can work within the context of your business. And why you may need to ensure that a person has the opportunity to step in and apply their knowledge.

The technology underpinning AI is constantly evolving, and we can expect any limitations to be continually tested and redefined. Despite it's rapid pace of change, you need to be aware that there will be some areas where it is too difficult (or expensive) to develop AI capable of solving the problem. To automate cyber security tasks at scale, there is a need for the ability to process data in quantities beyond the capability of any human being.

To do this there is a wide range of tools available, things like AV and firewalls. Until recently, however, these have worked on manually developed rules. Now, the tools are increasingly learning the rules for themselves, using intelligent algorithms to derive these rules directly from our data., in support of DSIT and other departments

by UK Government and the
National Cyber Security Centre

Securing cyberspace across the US

An urgent need to be able to trust that an underlying digital ecosystem is safe, reliable, and secure has seen the launch of a National Cybersecurity Strategy. Will its claim to ensure a strong digital future hold?

Digital technologies today touch nearly every aspect of American life. The National Cybersecurity Strategy is geared to better secure cyberspace and ensure the United States can reap a strong digital future. Cybersecurity is essential to the basic functioning of the economy, the operation of critical infrastructure, the strength of democracy and democratic institutions, the privacy of data and communications and national defense.

The new strategy recognizes that robust collaboration, particularly between the public and private sectors, is essential to securing cyberspace. It also takes on the systemic challenge that too much of the responsibility for cybersecurity has fallen on individual users and small organizations. By working in partnership with industry; civil society; and State, local, Tribal, and territorial governments, the intention is to rebalance the responsibility for cybersecurity to be more effective and more equitable.

The United States has made significant progress toward achieving the President's affirmative vision for a digitally-enabled future, but emerging trends are creating both new opportunities for further advancement and new challenges to overcome. Also, malicious actors threaten progress toward a digital ecosystem that is inclusive, equitable, promotes prosperity, and aligns with our democratic values.

Deepening dependence

The world is entering a new phase of deepening digital dependencies. Driven by emerging technologies and ever more complex and interdependent systems, dramatic shifts in the coming decade will unlock new possibilities for human flourishing and prosperity while also multiplying the systemic risks posed by insecure systems.

Software and systems are growing more complex, providing value to companies and consumers but also increasing our collective insecurity. Too often, there is a layering new functionality and technology onto already intricate and brittle systems at the expense of security and resilience. The widespread introduction of artificial intelligence systems—which can act in ways unexpected to even their own creators—is heightening the complexity and risk associated with many important technological systems.

The Internet continues to connect individuals, businesses, communities, and countries on shared platforms that enable scaled business solutions and international exchange. But this accelerating global interconnectivity also introduces risks. An attack on one organization, sector, or state can rapidly spill over to other sectors and regions, as happened during Russia's 2017 "NotPetya" cyberattack on Ukraine, which spread across Europe, Asia, and the Americas, causing billions of dollars in damage. The potential cost of attacks like this will only grow as interdependencies increase.

Digital technologies increasingly touch the most sensitive aspects of our lives, providing convenience, but also creating new, often unforeseen risks. The COVID-19 pandemic pushed people to live ever more deeply in a digital world. As lives become intertwined with video and audio streaming, wearable devices, and biometric technologies, the quantity and intimacy of personal data collection is growing exponentially. Theft of that data is also growing rapidly, and opening up novel vectors for malicious actors to surveil, manipulate, and blackmail individuals.

Collapsing boundaries

Next-generation interconnectivity is collapsing the boundary between the digital and physical worlds, and exposing essential systems to disruption. Factories, power grids, and water treatment facilities, among other essential infrastructure, are increasingly shedding old analog control systems and rapidly bringing online digital operational technology (OT). Advanced wireless technologies, IoT, and space-based assets—including those enabling positioning, navigation, and timing for civilian and military uses, environmental and weather monitoring, and everyday Internet-based activities from banking to telemedicine—will accelerate this trend, moving many essential systems online and making cyberattacks inherently more destructive and impactful to our daily lives.

Damaging attacks

Malicious cyber activity has evolved from nuisance defacement, to espionage and intellectual property theft, to damaging attacks against critical infrastructure, to ransomware attacks and cyber- enabled influence campaigns designed to undermine public trust. Once available only to a small number of well-resourced countries, offensive hacking tools and services, including foreign commercial spyware, are now widely accessible. These tools and services empower countries that previously lacked the ability to harm U.S. interests in cyberspace and enable a growing threat from organized criminal syndicates.

The cyber operations of criminal syndicates now represent a threat to the national security, public safety, and economic prosperity of the United States and its allies and partners. Ransomware incidents have disrupted critical services and businesses across the country and around the world, from energy pipelines and food companies, to schools and hospitals. Total economic losses from ransomware attacks continue to climb, reaching billions of U.S. dollars annually. Criminal syndicates often operate out of states that do not cooperate with U.S. law enforcement and frequently encourage, harbor, or tolerate such activities. These and other malicious cyber activities continue to threaten Americans across society, including disproportionately affecting those without the resources necessary to protect themselves, recover, or seek recourse.

Deep and enduring collaboration between stakeholders across our digital ecosystem will be the foundation upon which we make it more inherently defensible, resilient, and aligned with U.S. values. This strategy seeks to build and enhance collaboration around five pillars: (1) Defend Critical Infrastructure, (2) Disrupt and Dismantle Threat Actors, (3) Shape Market Forces to Drive Security and Resilience, (4) Invest in a Resilient Future, and (5) Forge International Partnerships to Pursue Shared Goals. Each effort requires unprecedented levels of collaboration across its respective stakeholder communities, including the public sector, private industry, civil society, and international allies and partners.

Critical infrastructure

Defending the systems and assets that constitute our critical infrastructure is vital to our national security, public safety, and economic prosperity. There must be confidence in the availability and resilience of this infrastructure and the essential services it provides. We aim to operationalize an enduring and effective model of collaborative defense that equitably distributes risk and responsibility, and delivers a foundational level of security and resilience for our digital ecosystem. Collaboration to address advanced threats will only be effective if owners and operators of critical infrastructure have cybersecurity protections in place to make it harder for adversaries to disrupt them.

Ransomware incidents have disrupted critical services in the US across all sectors

Finally, the Federal Government can better support the defense of critical infrastructure by making its own systems more defensible and resilient. This Administration is committed to improving Federal cybersecurity through long-term efforts to implement a zero trust architecture strategy and modernize IT and OT infrastructure. In doing so, Federal cybersecurity can be a model for critical infrastructure across the United States for how to successfully build and operate secure and resilient systems.

Regulation

While voluntary approaches to critical infrastructure cybersecurity have produced meaningful improvements, the lack of mandatory requirements has resulted in inadequate and inconsistent outcomes. Today's marketplace insufficiently rewards—and often disadvantages—the owners and operators of critical infrastructure who invest in proactive measures to prevent or mitigate the effects of cyber incidents.

Regulation can level the playing field, enabling healthy competition without sacrificing cybersecurity or operational resilience. Our strategic environment requires modern and nimble regulatory frameworks for cybersecurity tailored for each sector's risk profile, harmonized to reduce duplication, complementary to public-private collaboration, and cognizant of the cost of implementation. New and updated cybersecurity regulations must be calibrated to meet the needs of national security and public safety, in addition to the security and safety of individuals, regulated entities, and their employees, customers, operations, and data.

The Administration has made progress in this area, establishing cybersecurity requirements in key sectors such as oil and natural gas pipelines, aviation, and rail, led by the Transportation Security Administration and water systems, led by the Environmental Protection Agency.

by The White House,
US Federal Government

Analysing Chinese strategy for smart cities: the city brain

Continued evolution of the internet, artificial intelligence and the concept of machine learning, sees smart cities becoming more and more sentient – not least in China with the development of the 'city brain'

Builders of China's surveillance architecture—the Ministry of Public Security and private companies — have been fascinated by the intelligence of interconnected devices in recent years. They began constructing intelligent buildings and later morphed them into smart cities, which they then upgraded into urban environments with a lot of sensors—to include a command centre: the city brain, a concept conceived by Alibaba chief technology officer Wang Jian.

The city brain aggregates and analyses all data through AI-assisted cloud computing and presents it in a visually appealing way for city management staff, who are located in the digital cockpit (a room with large screens). This therefore could finally provide more intelligence to cities. It follows the OODA loop concept created by John Boyd, a U.S. Air Force colonel who developed it to aid with decision-making during combat situations. Now, Huawei cites the OODA loop in its smart city concept and adjusts it to city level decision-making, which consists of the following features:

1. Observe: the system gathers traffic, healthcare, video information;
2. Orient: information is transformed into valuable information;
3. Decide: warning, prediction and prevention alerts are shown;
4. Act: the city brain suggests implementation options.

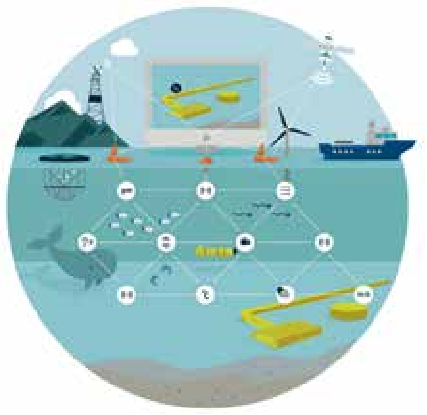
Under this system, feedback is continuously fed into the cycle to shorten the decision-making time and improve the process. The vision for the city brain has been influenced by party leaders, academics and industry. Chinese president, Xi Jinping visited the Hangzhou city brain and noted that it is the key way to make cities smarter by using AI, big data and cloud computing. State-led research institutions are also ardently developing this concept. Liu Feng—dean of Yuanwang Think Tank Digital Brain Research Institute and deputy director and secretary-general of the Urban Brain Special Committee of the Chinese Society of Command and Control—has been one of the key people behind this concept.

Liu Feng lays out a very geopolitical vision for the digital brain predicting it will gradually expand from the city brain, to the provincial brain, national brain, and finally the world digital or a world digital nervous system. In his view, the construction of the world's digital brain will be the third important opportunity to establish the world's technological ecological standards and systems after TCP/IP and the World Wide Web. In other words, the first step for government and industry is to connect various city brains into megalopolis brains, such as in the Guangdong- Hong Kong-Macao Greater Bay Area and the Yangtze River Delta urban agglomerations. The next step would be to have all city brains in China connected.

Expansion

Although the vast majority of urban brains lie in China (500 cities have announced that they are building city brains) the aim is also to expand regionally and globally. Its prime purpose is to raise the efficiency of the traffic management in the Southeast Asian city. The municipal, national, regional and world digital brain are and will be powered by the Beidou geospatial.

Liu Feng, one of the key thought leaders on the city brain, estimates that the world digital brain will be built by 2045. A major challenge to this vision will be to interconnect technological standards present in different world regions. However, national security considerations will likely hamper Chinese city brain deployments in Europe and the United States.



Smart oceans and mountain ranges will likely feature just as importantly in the world digital brain

Not to deploy Chinese city brains is a marker of local agency. But even other countries and municipalities that do acquire city brains have a moderate amount of agency: they do make the conscious decision to buy Chinese gear. One of the primary motivations for Nairobi and Mombasa (both located in Kenya) to acquire Huawei's Safe City technologies was to reduce crime rates in the city; whether this has been achieved is disputed. If local actors are unhappy with certain equipment they can replace the it with the non- Chinese equivalent. Chinese initiatives to push Beidou in Southeast Asia and in the Middle East along the Silk Road are in line with this.

Smart regions

The world digital brain will most probably be made up of thousands of city brains, but it does not stop there. Smart oceans and mountain ranges will likely feature just as importantly in the world digital brain. Data from underwater or mountain peaks will feed into city brains. City authorities will want to know which ships are coming into their port and receive alerts of incoming vehicles that cross mountainous border controls.

However, local agency is curtailed no matter who the supplier is. This is because most countries do not have the ability to secure systems properly. Smart city systems are highly complex, which makes it difficult for importing countries to scrutinise them. City brains—the next evolutionary step of smart cities—are even more complex, potentially incomprehensible, because of their extensive deployment of artificial intelligence. Little appears to be done to increase the auditability of those system. Therefore, it is difficult to know exactly what the system is doing; municipalities might sometimes not be aware where data relating to their city resides or who has access to it. With this lack of transparency, local agency over the confidentiality and integrity of data is hampered.

Local agency over systems acquired is even more important if it pertains to military systems, as those are at the core of national security. Brain-like intelligence is not only being conceptualised in the context of urban environments – the urban brain also has value as a military brain. While the larger strategy of civil-military fusion in China is not yet fully accomplished, due to a historical separation of the defence sector from the private sector, civil-military overlap is visible in the smart city private sector. For example, Digihail creates high resolution digital renderings of cities for Huawei as well as for the military, and has worked on visualisations of aerospace battlefields. To do this, Digihail fuses large-scale geographic information data: it visualises attack surfaces, travel routes, and deployment area of combatants; it creates a virtual display of the 3D battlefield that covers land, air sea, and electronic warfare; and it synchronises information flows from the different branches of the military. Digihail provides a visual decision-making system that integrates key personnel and vehicle monitoring. The company also visualizes space attack and defence operations for the Chinese military.

China's techno-natural utopia in Xióng'an Xinqu, a new smart city development hub in Hebei province is part of the drive to interconnect city brains

City interaction

It will be interesting to see how the various city brains will be interconnected in China and for what purpose. As it currently stands, it appears that the interaction of various city brains ensures that dwellers of one city can take advantage of the same services in a neighbouring city as if it were their own. Interlinking city brains might also allow for cross- regional decision-making of municipal authorities. It might help to better control flows of people or goods.

On a global scale, what would a world digital brain do and what is the value for China of Chinese companies operating city brains abroad? Presently a major benefit may be that it helps with spying. The smarter the exported surveillance infrastructure becomes; the easier spying becomes. In the early 2000s, Chinese as well as international companies exported 'dumb' surveillance equipment. CCTV cameras could record but not analyse images. With time the equipment has become smarter; exported cameras can now potentially identify a Chinese dissident through facial recognition and track their daily commutes.

Overall, the smarter an exported surveillance infrastructure is, the more influence it can wield in other regions, since it could have a privileged but not exclusive capability to control its technology within a given territory.

by LSE Ideas

Safeguarding privacy in smart cities

Privacy considerations in smart cities' development and adoption generally focus on concerns over government surveillance and data security. How can sensitive data really be handled safely and what frameworks need to be in place?

Smart infrastructure and transportation for city operations have the potential to enhance the delivery of government services and tackle a range of societal problems, including managing traffic congestion, reducing carbon emissions, facilitating efficient waste management, improving public health outcomes, constructing affordable housing, and enabling residents to efficiently access government services.

The COVID-19 pandemic also underscored the opportunity for smart cities to improve public health outcomes. For example, New York City launched an app for residents to more easily store and present their vaccine record and COVID-19 testing information. Additionally, Kansas City, Missouri installed air quality sensors in areas of high COVID-19 transmission to help reduce infection rates and improve air quality as part of a grant program with the National Science Foundation, a project that was later expanded to Cleveland, Ohio and Chattanooga, Tennessee. There are smart cities projects around the globe, with 379 fully developed smart cities in 61 countries in 2019. Analysts predict that the smart cities market will top $7 billion by 2023.

A typical smart city initiative might involve internet-connected sensors, mobile apps, public WiFi offerings, high-speed communications networks, utility meters, and cameras. With these operations, smart cities could collect and use a large quantity of data, some of which could be sensitive in nature. Additionally, smart cities technologies might involve processing data with assistance from analytics tools and algorithms. Consequently, commentators have raised privacy concerns that smart cities' potential collection of significant amounts of information about residents, as well as new uses and methods of processing this information, could contribute to government surveillance and cybersecurity risks, among other privacy concerns.

Development concerns

Privacy questions have had an influential role in the development and outcome of prior proposed smart cities initiatives. For example, Alphabet's subsidiary Sidewalk Labs announced plans to build a high-tech neighborhood on 12 acres of Toronto's waterfront in 2017, estimated to reflect at least a $1 billion investment, often called the Toronto Quayside project for the name of the neighborhood. Citizens and privacy advocates raised concerns that the proposed plans could compromise residents' privacy interests.

Cities play an important role in the responsible integration of smart cities technologies to address these privacy concerns and safeguard public trust. There are core privacy considerations raised by smart cities which have been identified – government surveillance and data security and it is important to analyze a set of core principles for smart cities to consider in the development and deployment of smart cities technologies to address privacy concerns. These principles include: (A) human-centric approaches to smart cities design and implementation, (B) transparency for city residents, (C) privacy by design, (D) anonymization and deidenti-

fication, (E) data minimization and purpose specification, (F) trusted data sharing, and (G) cybersecurity resilience.

Data security

Privacy considerations in smart cities development and adoption are raised across academic commentary, public reporting, and past smart cities pilots, and generally focus on concerns over government surveillance and data security.

With respect to government surveillance, some commentators in the US have voiced concerns that the implementation of smart cities technologies runs the risk of chilling First Amendment expression, as residents might be less willing to participate in free speech and public assembly if they perceive they are being recorded by the city. For example, the White House's recent Blueprint for an Artificial Intelligence ("AI") Bill of Rights, the Office of Science and Technology Policy found that individuals and communities "should be free from unchecked surveillance" and technologies like AI should not limit the exercise of civil rights and civil liberties, such as with respect to voting, peaceful assembly, speech, or association. At the same time, however, state and local governments have used technology to facilitate citizens' First Amendment right to vote through the creation of mobile apps that help citizens connect with information about how, where, and when to vote.

Regarding data security risks, privacy advocates and commentators have raised concerns that because smart cities might collect a large quantity of information, some of which may be sensitive in nature, smart cities provide an attractive target for bad actors. For example, city governments have already grappled with the threat of cybersecurity incidents, even outside the smart cities context.

In September 2022, a ransomware attacker gained access to the Los Angeles, California Unified School District, and with it, access to student and teacher data, which led the school district to shut down its computer systems. City governments at large have also been affected, as a ransomware attack on the city of Atlanta caused the city government to shut down its systems in 2018, and a bad actor accessed all of the 156 emergency sirens in Dallas, Texas in 2017.

Nevertheless, there are bright spots suggesting cities can do data security well using smart technologies. Members of Congress have introduced several bills that would, among other things, create literacy for small businesses on cybersecurity best practices and establish voluntary cybersecurity certification programs for IoT devices. Likewise, the National Institute of Standards and Technology (NIST) has issued reports and best practices recommendations related to cybersecurity and IoT devices, including some specific to government operations such as the NIST Security Guidance for First Responder Mobile and Wearable Devices, which helps secure devices worn in emergency response operations. Additionally, partnerships with private actors can help smart cities strengthen cybersecurity resilience. Accordingly, any smart cities framework should be calibrated to consider how to minimize privacy risks while maximizing benefits to citizens and government efficiency.

Command and control centers play a critical role in ensuring public trust with the deployment of surveillance technologies for city government

Public trust

Cities play a critical role in ensuring public trust with the deployment of technologies for city government. This Section explains each of the key privacy principles in turn, and discuss how these principles can help address privacy concerns raised with smart cities. These principles include: (A) human-centric approaches to smart cities design and implementation, (B) transparency for city residents, (C) privacy by design, (D) anonymization and deidentification, (E) data minimization and purpose specification, (F) trusted data sharing, and (G) cybersecurity resilience. These principles are informed by numerous privacy frameworks, such as those proposed by the Organization for Economic Co-operation and Development (OECD), NIST, and the Asian-Pacific Economic Corporation (APEC), as well as existing laws in the European Union and the United States.

Smart cities offer tremendous opportunity to improve how citizens experience and benefit from their city governments. Cities have an important role to play in adopting a privacy framework – such as through the adoption of principles like those described in this paper – to address privacy concerns and foster public trust and confidence in smart cities projects. Privacy in smart cities can be a feature, not a bug, and the principles outlined in this paper can help provide a framework for the responsible adoption of smart cities projects.

by MCity and Covington

International Semiconductor Alliance ISA launched

Tresky GmbH, budatec GmbH, Berliner Nanotest und Design GmbH and Bond Pulse thought in late summer 2023 and thus founded the International Semiconductor Alliance ISA. The intention is to help customers with the selection, project planning and implementation across all processes and to offer this service from a single source. The ISA founding companies combine a high level of technical expertise. Together, they offer the implementation of all sub-processes in packaging technology. Interested companies can obtain all processes in the manufacturing chain from the members of the ISA from a single source, from bonding, soldering and sintering to inspection and quality analysis. In addition, cross-process support and consulting services are offered for an efficient, reliable and reproducible manufacturing process. With Dr. Aaron Hutzler, a well-known process specialist in the industry, the Alliance has an expert with cross-process know-how, which is particularly valuable in the evaluation and assessment of work steps. Based on the end product, the production volume and the specified cost framework, ISA's specialists draw up recommendations for process developments as well as structural and process optimizations. The evaluations ultimately shorten the time-to-market.

Mouser Electronics partners with Siemens for industrial automation

Leading New Product Introduction (NPI) distributor, Mouser Electronics, with a wide selection of semiconductors and electronic components, has announced an agreement with Siemens, in industrial automation. Siemens' operations encompass factory automation and digitalization in the process and manufacturing industries, intelligent infrastructure for buildings and distributed energy systems, rail transport solutions, as well as health technology and digital healthcare services. Mouser will be stocking parts from Siemens in a variety of product categories, including networking devices, human-machine interface (HMI) solutions, circuit protection and power supplies. Mouser now offers Siemens' industrial automation products, such as the Sirius2 contactors, which provide high contact reliability, prolonged endurance and usability in extreme conditions. The contactors feature a modular design and a high performance-to-size ratio, saving valuable control cabinet space.

Renault combines electric cars and software to 'democratize' EVs for Europe

A new independent company, Ampere, has been formed by automaker Renault, which has set out goals for this new combined electric vehicle and software business. Through this the company says it will 'democratize' the market for battery-powered cars in Europe by making them as affordable as gasoline- or diesel-powered models. Combining electric vehicles and software in the new independent company Ampere will mean shorter development times and lower costs as the company faces tough competition from U.S.-based Tesla and Chinese carmakers who are making rapid progress. The company envisions a software-driven car' by 2026 based on an overarching software package that can be used for different electric car models and combines scattered processors in a central architecture that remains constantly connected to computer networks, or the cloud. That will enable over the air software updates and customer retention for servicing the vehicle, the company predicts with a 40% cost reduction in production costs by 2027—28 for the successor models to its Megane E-Tech and Scenic E-Tech.

Jaltek Systems partners with SG Automotive

UK contract electronics manufacturer with AS9100 and ISO 13485 accreditations and over 30 years of experience, Jaltek Systems, has joined with SG Automotive, a Slovenian Electronic Manufacturing Service (EMS) provider known for manufacturing printed circuit board assemblies (PCBA) to support demand from the European and UK markets. With SG Automotive's extensive experience Jaltec says can now cater to customers seeking IATF 16949 certification and a stellar track record in this sector within the EU. Together the companies say they will cover a number of diverse industries including Medical, Defence & Aerospace, Homeland Security, and Clean Energy.

Cadence announces Voltus InsightAI, to address EM-IR violations

A generative AI technology that automatically identifies the root cause of EM-IR drop violations early in the design process and selects and implements the most efficient fixes to improve power, performance, and area (PPA) has been introduced by Cadence Design Systems. Using Voltus InsightAI, customers can fix up to 95% of violations prior to signoff, leading to a 2X productivity improvement in EM-IR closure. Power integrity is a major design challenge at advanced nodes, with designers regularly facing a significant number of EM-IR violations at signoff, making it imperative to address this challenge early in the design phase. One of the major bottlenecks of in-design EM-IR analysis is that it is computationally very expensive due to the size and coupled nature of the power network. The new AI-driven Voltus InsightAI helps to overcome this bottleneck by utilizing new breakthrough machine learning methods for very fast incremental IR analysis. Using Voltus InsightAI, customers can use in-design analysis to enhance on-chip and chiplet power integrity. The technology enables greater engineering efficiency for uncovering issues early and offers key productivity-enhancing feature.

Identco launches wire marking system for labeling

Manufacturer of high-performance labeling solutions for the power equipment, electronics, transportation and general industrial sectors, Identco, has introduced its rugged new automated wire marking system, VortexID, whose stamina and speed raise benchmarks for wire and harness label application. The company highlights its ability to supply labels in customized shapes and sizes for precision-dependent surface mount technology (SMT) manufacturing lines, as well as its recently enhanced series of polyimide masking products. The company's PT Polyimide Discs comprise high-temperature film with silicone adhesive utilized for thermal and electrical insulation. The silicone adhesive's exemplary release properties offer ample protection. The discs are provided on a liner and supplied on a core for automated application settings. VortexID can precisely place up to 20 labels per minute – outpacing other automated units and doubling the output of even the most efficient manual setups – and operate 24/7, a welcome upgrade from the continuous use limitations of many label applicators.

Retired EV batteries to store power for solar farms

A Southern California company B2U Storage, is showing how repurposing EV batteries for stationary storage can extend their usefulness for several years. On a 20-acre parcel outside the Southern California town of New Cuyama, a 1.5-megawatt solar farm uses the sun's rays to slowly charge nearly 600 batteries in nearby cabinets. At night, when energy demand rises, that electricity is sent to the grid to power homes with clean energy. To make renewable energy from intermittent sources like solar and wind available when it is most needed, it is becoming more common to use batteries to store the power as it's generated and transmit it later. The Cuyama facility, uses batteries sending energy to the grid which once powered electric vehicles. The SEPV Cuyama facility is the second hybrid storage facility opened by B2U Storage Solutions. Its first facility, just outside Los Angeles, uses 1,300 retired batteries from Honda Clarity and Nissan Leaf EVs to store 28 megawatt-hours of power, enough to power about 9,500 homes. The facilities are meant to prove the feasibility of giving EV batteries a second life as stationary storage before they are recycled. Doing so could increase the sustainability of the technology's supply chain and reduce the need to mine critical minerals, while providing a cheaper way of building out grid-scale storage.

Koh Young delivers breakthrough operational improvements for Matric Group

A leader in True 3D measurement-based inspection solutions, Koh Young, has demonstrated how Matric Group has leveraged their partnership with Koh Young to be one of the first in the industry to use pre-reflow AOI as a game-changer for line efficiency and improved yield. All while creating a central inspection war room to allow just one person to manage all inline inspection, increasing automation, and control and mitigating talent shortages. Matric Group added pre-reflow AOI to every line and how that immediately improved yield, quality, and efficiency. Together with Koh Young, they managed to reduce the number of technicians managing their inspection processes to one. And learn how they created a long-term partnership where ideas are shared, and new ground-breaking solutions are created.

Emerald EMS acquires Ascentron

A strategic move thqwt sees the purchase of Ascentron by Emerald EMS reinforces Emerald's expansion of its capabilities and geographic presence. Ascentron has a customer base within the Life Sciences and Aerospace sectors. With its FDA registration, Ascentron has established itself as a trusted and reliable partner in the highly regulated healthcare industry. This acquisition not only broadens Emerald's customer base but also adds a wealth of expertise in the specialized fields of Life Sciences and Aerospace. According to the companies, this acquisition perfectly complements Emerald's established network of engineering services and manufacturing facilities, including domestic locations in the US, as well as international facilities in Shenzhen, China, and Penang, Malaysia.

Jabil buys Retronix to advance circular economy initiatives

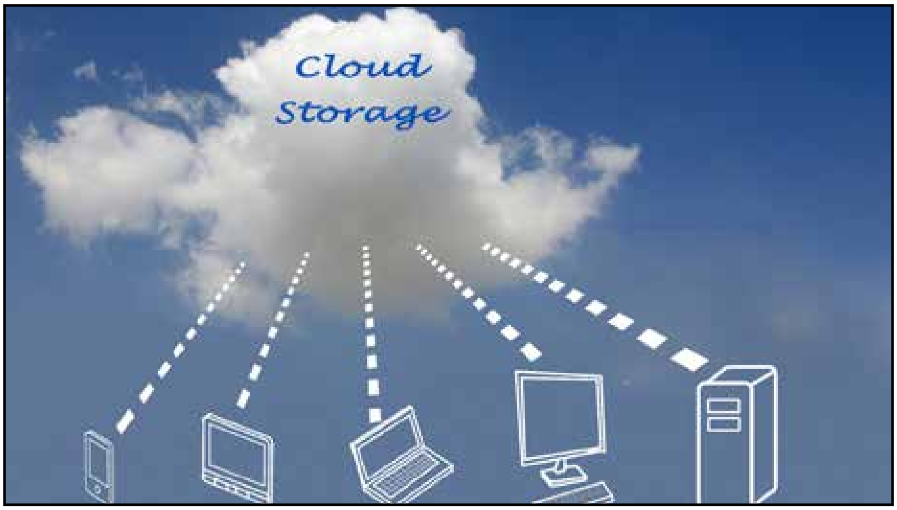
A global leader in design, manufacturing, and supply chain solutions, Jabil, has announced the successful acquisition of Retronix, an innovative provider in the reclamation and refurbishment of electronic components. Retronix sets offers a unique Laser Reballing service, an advanced process delivering multiple advantages for High Reliability applications. This technique eliminates the necessity for a reflow, thus mitigating potential harm to the Ball Grid Array (BGA) components and adjacent regions. By reducing thermal stress, it safeguards the component's integrity and aids in extending its lifespan. Retronix also caters to an array of component preparation services such as component retinning, component recovery, and authenticity verification.

Diving deeply into the next decade of security and digital ID

Security teams are being empowered through the cloud to create more value for an organization and its people. What trends are shaping the market and the key enablers, disruptors and game changers that are underpinning them?

Extraordinary disruptions and challenges organizations worldwide have struggled with for the past several years continue to impact organisations according to an HID report on the security and identity industry for 2023, with five key trends emerging.

Nearly three-quarters (71%) of respondents to the report indicated supply chain issues as a top trend in the security and identity industry for 2023. Similarly, 74% of respondents said supply chain issues negatively impacted them in 2022. When asked if they anticipate supply chain issues will ease in 2023, respondents provided a true split – 50% believe they will ease and 50% believe they will not. From a macro perspective, supply chain disruptions are expected to improve, although labor shortages and high demand will continue to strain global supply chains, including the availability of semiconductors. These integrated circuit chips form the backbone of many security and identity products, including control panels, readers, sensors, detectors, credentials, passports and peripherals.



Sustainability influence

There is growing consensus that governments, organizations and individuals must take more action to address environmental concerns. End users are increasingly demanding that suppliers provide footprint transparency in terms of their operations, product sourcing and research and development practices. So much so that sustainability has taken center stage in business decisions, including purchasing decisions made by end users and supplier decisions made by integrators and installers. Seventy-six percent of survey respondents indicate that sustainability is of increasing importance for their customers, with 62% stating that sustainability is "very important" or "extremely important" to their customers.

Thirdly, hybrid work environments are pushing cloud-based access management further into the mainstream. Digital transformation continues to exert pressure as the global pandemic accelerated the adoption of cloud technologies across many sectors. The convergence of these factors means identity-as-a-service (IDaaS) is quickly becoming the expectation.

In fact, the identity access management (IAM) market is expected to grow at a 22.7% compound annual growth rate to $41.9 billion by the end of 2031.10 As such, SaaS-delivered identities represent huge opportunities in the security industry. Prior to the pandemic, digital transformation and the convergence of physical and logical access caused enterprises to migrate more of their access management capabilities to the cloud. Now, as 81% of respondents to our survey say they are offering a hybrid work model, more companies will deliver identity management "as a service" rather than via on-premises infrastructure in 2023.

Even before the pandemic, digital transformation and the convergence of physical and logical access moved more and more access management capabilities to the cloud. Now, with 81% of survey respondents offering a hybrid work model of in-office and remote work, identity management delivered "as a service" rather than via on-premises infrastructure will expand into 2023. With this adjustment, IT and security teams, particularly in smaller organizations, must consider the underlying governance that accompanies cloud-first mandates, including technology decision-making processes that incorporate engagement with audit, privacy, IT operations and information security. As an example, 67% of respondents state that MFA and passwordless authentication are most important to adapting to hybrid and remote work, with 39% indicating that data strategy, framework and tools are required components to facilitate this new work structure.

Digital ID adoption

The concept of adding authentication to transactions is not new, but is evolving. In the past, identity was tied to something physical, such as a customer presenting a driver's license when paying for goods or services by check. In the modern world, trusted identity is increasingly a digital phenomenon, from passports to student IDs and corporate credentials. This is changing the way security operates. A digital ID is an extension of physical identity and offers a new way to securely verify who we are. Digital IDs include mobile IDs, which are digital IDs stored on and authenticated via mobile devices, including smartphones and wearables.

A combination of factors is driving digital IDs to their tipping point in 2023. According to our 2022 State of Physical Access Control Report, 66% of users have already upgraded to mobile readers or plan to do so, while 41% of respondents say that mobile access would be one of the top features required in a new access control system.

The infrastructure to support digital transactions grew during the past two years alongside the need to offer contactless transactions. In tandem, the adoption of mobile wallet apps that house digital identities on mobile devices also grew. Digital wallets comprised 48.6% of e-commerce transaction value worldwide in 2021, or just over $2.6 trillion.

Hybrid remote work models with ID management delivered as a service are expanding

Digital ID with a range of wearables is an extension of physical identity verification

Digital identities are an extension of physical ones; they offer a new way to securely verify who we are so we can transact safely, work productively and travel freely. Digital IDs include mobile IDs, which are digital IDs stored on and authenticated via mobile devices. The acceleration of digital wallet adoption is expanding to use cases beyond just payments, including employee badges, drivers' licenses, national IDs and passports. To illustrate this adoption curve, 47% of integrators and installers indicate that their customers are using mobile identities for identity verification.

Biometrics

Finally, contactless biometrics are reaching an impressive momentum, according to the report. Modern iris and facial recognition technologies are on the rise as reliable, contactless biometric modalities for both on-premises and remote authentication. While challenges to widespread adoption of biometrics have largely centered on privacy concerns, these perceptions are starting to soften because of these technologies' convenience. Respondents indicating various stages of biometric adoption illustrate this point, with 26% stating they currently use biometrics (contact or contactless) and another 33% stating they plan to test or implement a form of biometrics within the next one to five years. This means new considerations will begin to arise within the value chain, including how to control the environment and ensure privacy as new technologies fuel speed and seamless performance.

There is no doubt that the industry is undergoing a large amount of change. Players must not only identify what is changing, but also take advantage of and evolve with the current trajectory. The unifying themes of the abovementioned trends are the need to adapt faster, deliver exceptional digital plus physical experiences and capitalize on breakthrough innovations in solutions and services.

The digital experience is an enabler in reshaping security, with interconnected devices raising the bar of what can be secured and how. The cloud will power implementations efficiently across physical and logical footprints, elevating the value of data and facilitating servitization to drive specific business outcomes. Big-picture social and economic trends have disrupted business-as-usual, challenging the security industry to rethink the basics down to the concept of identity. The growing expectation is that security, like all other facets of the enterprise, can and will leverage technology to work better and smarter now and into the future.

by HID

Monitoring Europe’s digitalisation of public services

Digital transformation of societies and public services is driven by government policies such as the EU’s Digital Decade policy programme. Will it succeed in leading the way with common targets for 2030 for the EU27+?

Across the EU, eGovernment Benchmark sheds light on eGovernment in 35 European countries, referred to as ‘Europe’ or the ‘EU27+’: the 27 European Union Member States, as well as Iceland , Norway , Switzerland , Montenegro , North Macedonia. A new study evaluates online public services on four dimensions, which consist of 14 underlying indicators, broken down into 48 survey questions. The four dimensions can be described by the following key questions:

User Centricity – to what extent are services provided online? How mobile friendly are they? And what online support and feedback mechanisms are in place? Transparency – are public administrations providing clear, openly communicated information about how their services are delivered? Are they transparent about policy making and digital service design processes, as well as about the way people’s personal data is being processed? Key Enablers – what technological enablers are in place for the delivery of eGovernment services? Cross-Border Services – how easily are citizens from abroad able to access and use the online services? And what online support and feedback mechanisms are in place for cross-border users?

Based on the four dimensions and 48 underlying survey questions, countries receive an overall eGovernment maturity score. This composite score ranges from 0 to 100 points. The European leaders are Malta (96 points) and Estonia (92). Other frontrunners are Luxembourg (89), Iceland (88), Finland (86), the Netherlands (85), Lithuania (85), Denmark (85), Latvia (82) and Norway (80). The EU27+ overall performance averages at 70. Compared to last year, some countries showed remarkable growth.

The User Centricity dimension is still a spearhead, standing at an EU27+ average of 90 points, and can be used as the impetus to improve all other key dimensions.

With an average of 71 points, the key enablers dimension shows promising performance growth, with countries demonstrating information from base registries for more and more services. Cross-Border Services (57) are ready or the next step: creating online services for foreign users can quickly accelerate with more than 30 countries connected to eIDAS and the ongoing improvements on the Your Europe portal. The Transparency of eGovernment (currently at 62 points) can be improved upon by consistent service processes that are clear.

Users at the heart

The eGovernment Benchmark consistently shows that many government services are available online. Still, many citizens do not interact with the government online at all. The question could therefore be: are online services designed with their audience in mind? How seamless is the user journey for citizens and entrepreneurs looking for an online service? Issues include finding the right government website in the user journey. Portal websites combine information from organisations, also known as one-stop-shops. More than nine out of ten services can be found via a government portal (94%).

In addition, fast government websites avoid frustrations for users. The average European government websites take 1.9 seconds before becoming fully interactive, where below 3.8 seconds is considered fast. Yet, government websites are not yet accessible to all users on all devices. Currently, 93% of European government websites are mobile friendly, but web- accessibility remains a challenge, with more than eight out of ten public sector websites (82%) violating one or more Web Content Accessibility Guidelines (WCAG) criteria.

Findings show easy-to-understand government portals make users' lives easier. Users are typically provided with information on how to access government services online. For example, 95% of websites have a frequently asked questions section and 90% of websites have some form of instruction or demonstration on how to obtain the service; 98% of services have information online, but more clarity about service processes is required. Only 46% of websites provide an estimated time for the application process and only 60% of websites explicitly state the delivery timelines of services.

Secure eID

Current benchmark trends show seven out of ten services allow secure authentication with eID while 17% of services still require in-person authentication enabled for eID use, only about half (49%) of services allow single sign-on. Moreover, in almost eight out of ten (77%) of services, users could submit or download required documents online. Also, 84% of government services can be completed fully online1, up from 81% last year. This means that users obtain these services fully digitally.

Europe strives to have all its key public services online in 2030 at the end of this Digital Decade. Currently the Digital Decade indicators Digital public services for citizens and Digital public services for businesses stand at 77 and 84. To rise to the challenge for 2030, Europe needs to bridge three gaps. Bridge the gap between cross-border users and national users. Cross- border users face many hindrances when obtaining services online. Language issues and being unable to authenticate with their own eID are the most common barriers. Secondly, bridge the gap between citizens and entrepreneurs: European entrepreneurs enjoy mature digital services provided by their government with 92% of services for entrepreneurs are online, compared to 80% for citizens.

Thirdly, bridge the gap between local and regional governments and central governments. As it stands, 88% of evaluated central government services are completely online, compared to 76% of evaluated regional government services and 62% of evaluated local government services.

Interoperability is supported by the SingleDigital Gateway and the eIDAS Regulation

Interoperability

Europe's interoperability framework and its new Interoperable Europe Act will play a vital role in this move forwards. Instead of each town or city reinventing the wheel for themselves and creating their own services, they can reuse what is already there. Architectural building blocks, such as eID and eSignature, can be easily adopted on other websites.

Interoperability is further supported by the Single Digital Gateway and the eIDAS Regulation, making cross-border services in the future just as easy as national services. Having all services in standard formats, in multiple languages, accessible with your own eID makes lives easier for citizens and entrepreneurs alike. Services across Europe will be similar, independent of country and service provider. By making the push towards interoperability and implementing the Single Digital Gateway, Europe is Connecting Digital Governments.

by EU Commission

European Council and Parliament agree on eID

With a view to ensuring a trusted and secure digital identity for all Europeans, the Council presidency and European Parliament representatives reached a provisional agreement on a new framework for a European digital identity (eID). The revised regulation constitutes a clear paradigm shift for digital identity in Europe aiming to ensure universal access for people and businesses to secure and trustworthy electronic identification and authentication. Under the new law, member states will offer citizens and businesses digital wallets that will be able to link their national digital identities with proof of other personal attributes (e.g., driving licence, diplomas, bank account). Citizens will be able to prove their identity and share electronic documents from their digital wallets with a click of a button on their mobile phone. The new European digital identity wallets will enable all Europeans to access online services with their national digital identification, which will be recognised throughout Europe, without having to use private identification methods or unnecessarily sharing personal data. User control ensures that only information that needs to be shared will be shared.

HID launches high-volume desktop personalisation system

Identity solutions provider, HID, has introduced the HID Element range of printing, coding, and engraving solutions, designed to transform industrial ID and financial card personalisation and issuance by combining high-volume, superior-quality UV inkjet printing and laser engraving onto a single, robust yet easy-to-manage desktop system. The product solutions deliver optimal card personalization and accommodates projects that require high-resolution UV ink printing, laser engraving or both. It is purpose-built to meet the industrial speed and output requirements of large government ID card programs, financial institutions, enterprise corporations, and service bureaus; addressing the demand for greater print speed, higher resolution, larger card output and better cost-per-card economy.

OIX explains DNA of digital ID for global interoperability

The Open Identity Exchange (OIX) has launched a new paper – Digital ID DNA – Interoperability across Trust Frameworks – that will be crucial to understanding and navigating the different digital ID trust frameworks around the globe, and achieving interoperability. OIX says one of the biggest challenges driving significant debate as digital ID progresses around the world is the ability for trust frameworks with different policy criteria to interoperate. Digital ID must be able to interoperate safely and securely across the different regulatory and technical boundaries that are defined in trust frameworks, usually by a government or for a specific geographical area. The work of the non-profit global organisation, OIX, has been focused on ensuring that digital ID works well for anyone that wants it and that it works seamlessly all over the globe. To achieve this, the OIX carried out unique and extensive analysis of the policies of eight very different digital ID trust frameworks across the globe. The goal was to explore how these frameworks and other parties could express their policy position in a consistent way, so that interoperability of IDs across these ecosystems could be achieved.

Evolis launches game-changing retransfer card printer

A leader in direct-to-card printing, Evolis, has launched its retransfer card printer, Agilia, designed and manufactured at its production site in France. With this new product, Evolis aims to increase its market share by 20% over 4 years. To be credible in a market such as retransfer, Evolis understands that it must offer a product capable of disrupting the market. Agilia integrates key features including high 600 dpi print quality, over the edge, the ability to print on a wide range of card types, and a lifetime warranty on the print head. Evolis sqays it has gone beyond the expected functionality, taking into account the different needs of users: single or double-sided personalization, multiple encoding options, high-definition micro text and QR code printing, 200-card feeder, optimized user experience on Windows and Mac, and more.

Tech5 opens access for remote ID verification providers in Europe

Innovator in the field of biometrics and digital identity management, Tech5, is providing its biometric matching and liveness technologies to remote verification and digital onboarding companies in Europe. The recent Pandemic has created an urgency for the implementation of technologies and certification of service providers for remote identification and verification of people wishing to access public or private online services when they do not have a digital identity recognised by these services. Therefore, in accordance with the latest regulation in France, the French National Cyber Security Agency (ANSSI), supported by the Ministry of the Interior, now evaluates and certifies remote identity verification services to guarantee the security and reliability of these processes. Tech5 provides facial liveness detection software to various certified remote identity verification service providers in Europe.

High Quality Equipment
Made in Germany
by MELZER-Schwelm
MELZER

Top 50 Suppliers

ePassport technology

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

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

LEGEND

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

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

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

SERVICES
SI = System Integrator
VAR = Value Added Reseller

3M Security Systems Division
www.3M.com/security

CARDS, PERS, HW, SI
1545 Carling Ave., Suite 700, Ottawa, Ontario – Canada
Tel. +1 613 720 2070
Fax +1 613 720 2063

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

Access IS
www.access-is.com

CARDS, MF, HW
18 Suttons Business Park, Reading, Berkshire, RG6 1AZ – UK
Tel. +44 7748 770 632
Fax +44 118 926 7281

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

ASK
www.ask-rfid.com
info@ask.fr

INL, CARDS, HW
2260 route des Crêtes, BP337, 06906 Sophia-Antipolis – France
Tel. +33 4 97 21 40 00
Fax +33 4 92 38 93 21

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

Atlantic Zeiser
www.atlanticzeiser.com
thorsten.tritschler@atlanticzeiser.com

CARDS, MF, PERS, APP, SI
Bogenstraße 6-8, 78576 Emmingen – Germany
Tel. +49 7465 291-0
Fax +49 7465 291 166

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

Austria Card
www.austriacard.at
isales@austriacard.at

CARDS, OS, PERS, APP
Lamezanstrasse 4-8, 1230 Vienna – Austria
Tel. +43 1 610 65-0

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

Bundesdruckerei/Veridos
www.bundesdruckerei.de
info@bundesdruckerei.de
info@veridos.com

CARDS, MF, PERS, APP, HW, SI
Oranienstraße 91, 10969 – Berlin
Tel. +49 30 2589984-0
Fax +49 30 2589984 39

A company formed between Bundesdruckerei and G&D, Veridos is the world's leading provider of integrated identity solutions. Governments, organizations, businesses, and regional authorities worldwide trust Veridos' uniquely comprehensive product portfolio. We support our customers with secure and reliable end-to-end identity solutions, expert guidance and future-proof technology.

Cetis
www.cetis.si
info@cetis.si

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

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

Cognitec Systems
www.cognitec.com
info@cognitec.com

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

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

Crossmatch
www.crossmatch.com
sales@crossmatch.com

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

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

LEGEND

COMPONENTS

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

EQUIPMENT

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

IT SYSTEMS

APP	=Software/Applications
HW	=Readers/Hardware

SERVICES

SI	=System Integrator
VAR	=Value Added Reseller

Cryptovision
www.cryptovision.com
info@cryptovision.com

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

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

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

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

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

Dermalog
www.dermalog.de
info@dermolog.de

DERMALOG

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

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

Diletta
www.diletta.com
contact@diletta.com

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

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

Gemalto
www.gemalto.com
info@gemalto.com

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

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

Entrust Datacard
www.entrustdatacard.com

MF, PERS, APP
1187 Park Pl, Shakopee, MN 55379 – USA
Tel. +1 952 933 1223

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

HID Global
www.hidglobal.com

INL, CARDS, MF, PERS, APP, HW, SI
15370 Barranca Pkwy, Irvine, CA 92618 – USA
Tel. +1 949 732 2000
Fax +1 949 732 2120

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

IAI industrial systems
www.iai.nl
info@iai.nl

PERS
De Run 5406, 5504 DE Veldhoven – The Netherlands
Tel. +31 40 254 24 45
Fax +31 40 254 56 35

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

Idemia
www.idemia.com
info@idemia.com

OS, INL, CARDS, PERS, APP, SI
Boulevard Lénine, BP 428 76805 Saint-Etienne-du-Rouvray – France
Tel. + 33 2 35 64 53 46

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

LEGEND

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

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

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

SERVICES	
SI	=System Integrator
VAR	=Value Added Reseller

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

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

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

Industrial Innovation Group
www.industrialinnovationgroup.com

IC, OS, INL, CARDS, PL, MF, PERS, APP, HW, SI, VAR
Taryam bld., Industrial Area 18, Maleha Street, Sharjah PO Box 123428 – UAE
Tel. +971 65 57 07 2

IIG offers advanced authentication and security technology platform offerings including IDs, cards and secure documents. Other solutions range from on-package authentication measures to a new generation system to help governments to track supply chains. Products and technologies include RFID, holograms, biometrics, security printing, software, taggants and track & trace solutions for the government and public sector, as well as manufacturing and retail.

Iris
www.iris.com.my

IC, OS, INL, CARDS, MF, PERS, APP, HW, SI, VAR
Smart Tech. Complex, Tech. Park, Bukit Jalil, 57000 Kuala Lumpur – Malaysia
Tel. +603 89960788
Fax +603 89960441

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

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

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

IXLA has been the first vendor to release a real desktop laser system for e-Passports, compact and effective.
The product range has grown, adding the new XJ laser and inkjet to the laser-only field proven XP's, all with automatic feeder. Thanks to the uncompromised dedication to product quality, constant innovation and competence, IXLA is still the leading brand in desktop solutions for laser personalization of passports and cards, reaching soon the mark of 3,000 delivered units.

Jdsu
www.jdsu.com

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

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

Linxens
www.linxens.com

MF, IC, INL, PERS, APP
6 Rue Marius Aufan, 92300 Levallois Perret – France
Tel. +33 1 41343450
Fax +331 47576492

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

MaskTech
www.masktech.de

OS, PERS, APP
Masktech GmbH, Nordostpark 16, 90411 Nuernberg – Germany
Tel. +49 9119 551490
Fax +49 9119 551497

MASKTECH

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

Melzer Maschinenbau
www.melzergmbh.com
sales@melzergmbh.com

MF, INL, CARDS
Ruhrstr. 51-55, Schwelm, 58332 – Germany
Tel. +49 2336 929280
Fax +49 2336 929285

MELZER®

Melzer is internationally well-known as the leading production equipment supplier for trendsetting ID documents, Smart Cards, DIF Cards, RFID Inlays and e-Covers for Passports. Customized solutions in combination with the unique modular inline production processes ensure highest productivity, flexibility and security at a maximum yield and lowest per unit costs. Numerous governmental institutions rely on reliable solutions created by Melzer. The Melzer product portfolio also includes advanced RFID converting equipment for the production of smart labels/tickets and luggage tags.

Mühlbauer
www.muehlbauer.de
info@muehlbauer.de

MF, PERS, APP, HW, SI
Josef-Mühlbauer-Platz 1, 93426 Roding – Germany
Tel. +49 9461 952 0
Fax +49 9461 952 1101

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

LEGEND

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

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

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

SERVICES	
SI	=System Integrator
VAR	=Value Added Reseller

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

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

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

Nagra ID
www.nagraid.com

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

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

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

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

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

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

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

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

NXP
www.nxp.com

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

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

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

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

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

On Track Innovations
www.otiglobal.com

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

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

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

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

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

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

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

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

LEGEND

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

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

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

SERVICES	
SI	=System Integrator
VAR	=Value Added Reseller

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

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

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

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

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

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

ruhlamat GmbH
www.ruhlamat.com

IC, INL, CARDS, MF, PERS, HW
Sonnenacker 2, 99834 Gerstungen – Germany
Tel. +49 36925 9290
Fax +49 36925 929111

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

Secunet
www.secunet.com

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

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

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

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

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

SPS INL, PL

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

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

IN Groupe with its secure components brands SPS and SURYS provide secure and high added value components for card and travel document manufacturers.

SPS brand is specialized in the design, manufacturing and sale of contactless solutions dedicated to ID cards, e-passport and dual interface banking cards. Developed and manufactured in Rousset, France, with a subsidiary in Singapore, SPS solutions are specialized in contactless and dual-interface products, with a recognized micro packaging expertise. SPS has delivered several million epassport inlays and ecovers to every continent based on its unique ebooster technology. The Teslin based inlay uses an inductive coupling technology, where there is no physical connection between the antenna and the chip, and a copper wire antenna, offering a highly reliable and cost effective solution to passport manufacturers. SPS completes its offer with Polycarbonate data pages, from finished data page to hinge inlay and electronic components. SPS' technology is designed to accept all chip and OS suppliers on the market. Global leader in optical security solutions, French leader on the document security and traceability market and pioneer in optical-digital authentication, SURYS brand offers an innovative range of optical and digital authentication and traceability solutions on the Identity, Vehicles, Fiduciary and secure traceability markets. With multiple references in these fields, SURYS is an internationally recognized brand for its leadership in a highly innovative technological sector in over 130 countries.

SICPA SP, PERS, APP, SI

www.sicpa.com
Av de Florissant 41, 1008 Prilly – Switzerland
Tel +41 21 627 55 55
Fax +41 21 627 57 27

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

LEGEND

COMPONENTS

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

EQUIPMENT

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

IT SYSTEMS

APP	=Software/Applications
HW	=Readers/Hardware

SERVICES

SI	=System Integrator
VAR	=Value Added Reseller

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

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

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

Supercom
www.supercom.com

IC, CARDS, PERS, HW, SI
1 Arie Shenkar Street, Herzliya 4672501 – Israel
Tel. +972 9 889 0880
Fax +972 9 889 08143

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

Suprema
www.supremainc.com

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

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

Thales
www.thalesgroup.com/security

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

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

UL Transaction Security
www.ul-ts.com

CARDS, PERS, APP, HW, SI, VAR
Delta 1A, Building L'Aimant, Ijsseloord 2, 6825 ML Arnhem - The Netherlands
Tel. +31.26.376.4800
Fax +31 26 376 4840

UL Transaction Security is the world's number one knowledge center in secure transaction technology. UL's Transaction Security service line is a result of the consolidation of Collis, RFI Smart and Witham Laboratories. Our international team of expert consultants and product developers work with you to ensure compliance, interoperability and security for your chip-based products and systems.

Unisys
www.unisys.com

OS, PERS, APP, SI
801 Lakeview Drive, Ste 100, Blue Bell, Pennsylvania 19422 – USA
Tel. +1 215-986-4011

Unisys is global biometrics, identity management and smartcard solution integrator. The company provides a holistic approach to people identity that combines technology, management, business process and operational expertise to deliver higher levels of identity assurance. It helps improve border security by establishing systems for positive identification with biometrics for visa/passport issuance, and entry/exit management in a country.

Veridos
www.veridos.com

SP, OS, INL, CARDS, MF, PERS, APP, HW, SI
Truderinger Str. 15, Munich 81677 – Germany
Tel. + 49 3020095 5480

Veridos creates secure and pioneering idnetification solutions for the international market. As a joint venture of Giesecke & Devrient and Bundesdruckerei, Veridos pools the specialst expertise, the many years of experience and the innovative power of the4 two largest German providers fo high security technologies.

Vision-Box
www.vision-box.com

IC, OS, CARDS, PL, PERS, APP, HW, SI
R. Casal do Canas n.2, Zona Ind. de Alfragide, 2790-204 Carnaxide – Portugal
Tel. +351 21 154 9000
Fax +351 21 154 3901

Vision-Box develops, manufactures and deploys mission critical security systems which integrate biometric technologies. The new VBePASS is the latest achievement in Vision-Box's product portfolio, an ICAO compliant live biometric enrolment kiosk which automatically adjusts height and light intensity for ideal capture conditions of face, fingerprints and signature. VBePass systems have been deployed and installed worldwide as a front end for ePassports, national identity cards and visa programs.

Vlatacom Institute
www.vlatacom.com
info@vlatacom.com

VLATACOM

CARDS, PERS, APP, SI
5 Milutina Milankovica, 11070 Belgrade – Serbia
Tel. +381 11 377-11-00
Fax +381 11 377-11-99

Vlatacom Institute provides end-to-end solutions for issuing of highly secure biometrics:e-ID cards, e-Passports, e-Driving Licenses, Officer-ID cards, etc. With more than 20 years of experience in encryption, software engineering, electronics, telecommunications, system design, system integration and maintenance, Vlatacom delivers its solutions for e-Governance and border management to Governments worldwide. High-end security, improved performance and rapid facilitation of citizens/passengers are achieved using encryption and multimodal biometrics that enable the strong authentication of officers, citizens and documents in the system.

LEGEND

COMPONENTS

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

EQUIPMENT

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

IT SYSTEMS

APP	=Software/Applications
HW	=Readers/Hardware

SERVICES

SI	=System Integrator
VAR	=Value Added Reseller

SUSTAINABLE DEVELOPMENT

Publisher
Roberto Dell'Acqua

Editorial Staff
Victor March, Gaia Steden
idpublications@onpublishing.com

John Matthews, Andrew Fielding
sd@hadrianmedia.net

Advertising
Karina May
karina.may@hadrianmedia.net

© 2023 Hadrian AG
Issue: October 2023

Hadrian AG
Baarerstrasse 10
6302 Zug (ZG),
Switzerland, CHE – 264.162.161

SUSTAINABLE DEVELOPMENT
www.sustainabledevelopmentmagazine.com

ID WORLD
www.id-world-magazine.com

global identification
www.global-identification.com

ONBOARD TECHNOLOGY
www.onboard-technology.com

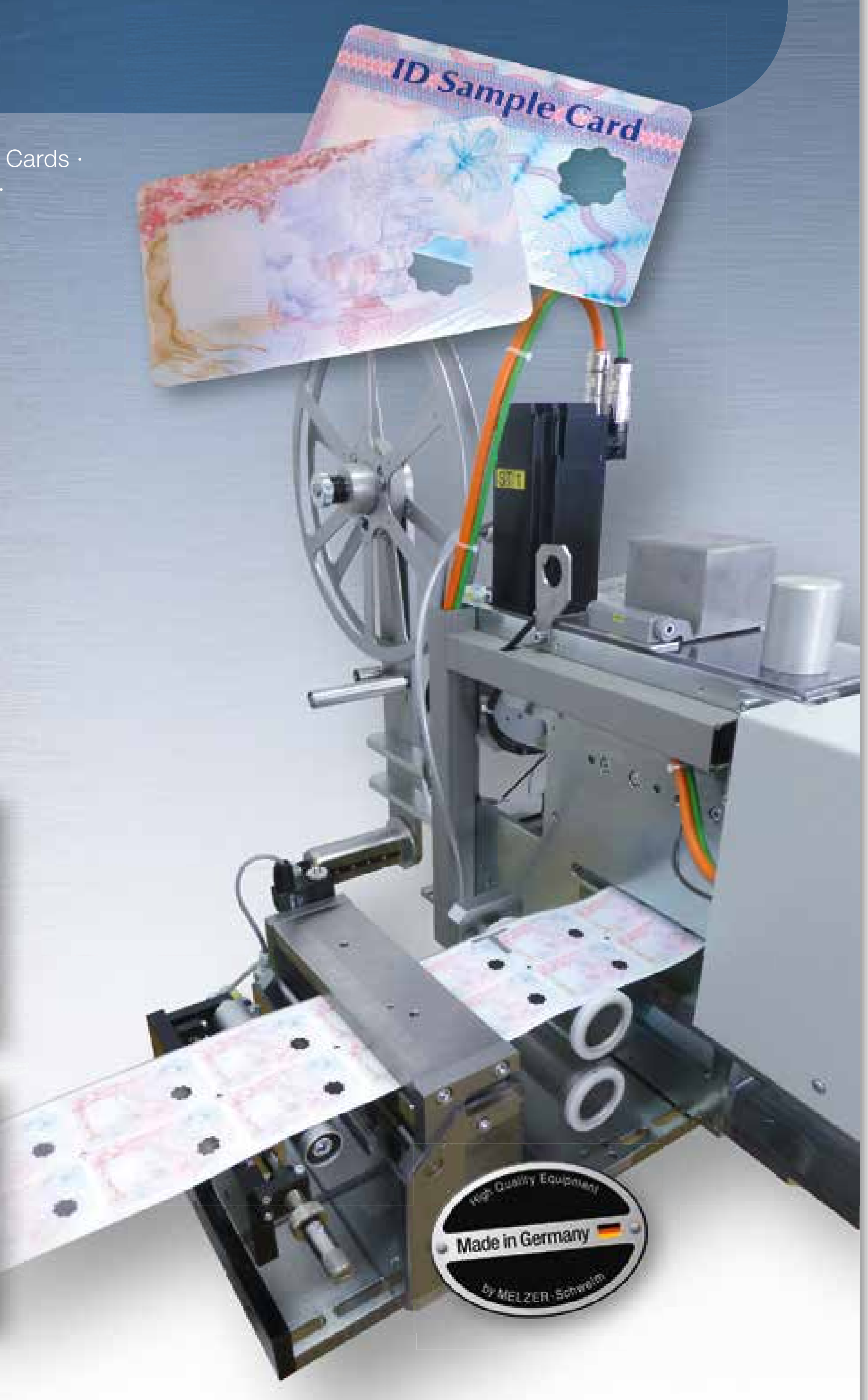
People and organizations featured in this issue

Page	Name	Page	Name	Page	Name
7	Al Dhafra	7	Idemia	15	OECD
6	Amazon	25	Identco	24	Renault
6	Apptio	24	ISA	26	Retronix
24	Cadence	2	Ixla	7	RM Institute
15	ChatGPT	26	Jabil	24	SG Automotive
26	Emerald EMS	24	Jaltec	24	Siemens
6, 28	European Commission	26	Koh Young	7	Sri Lankan Government
48	Gemina	10	KSA Government	4	Sustainability Summit
15	Google	20	LSE Ideas	12	Tech 5
26	HID	22	M-City	16	UK Cyber NCSC
7	HTX	31, 47	Melzer	6	US Energy
6	IBM	15	Microsoft	18	US Government
6	IDC	24	Mouser	7	Vietnam Aviation

Inline Window Application

IPS

Inline Production System for ID Cards · Data Pages · Driving Licenses · Resident Permit Cards



- ▷ Fully automatic punching and inserting
- ▷ For cards and data pages
- ▷ Zero gap technology
- ▷ Full lamination for utmost durability

INNOVATIVE MACHINERY SOLUTIONS SINCE 1956

MELZER®

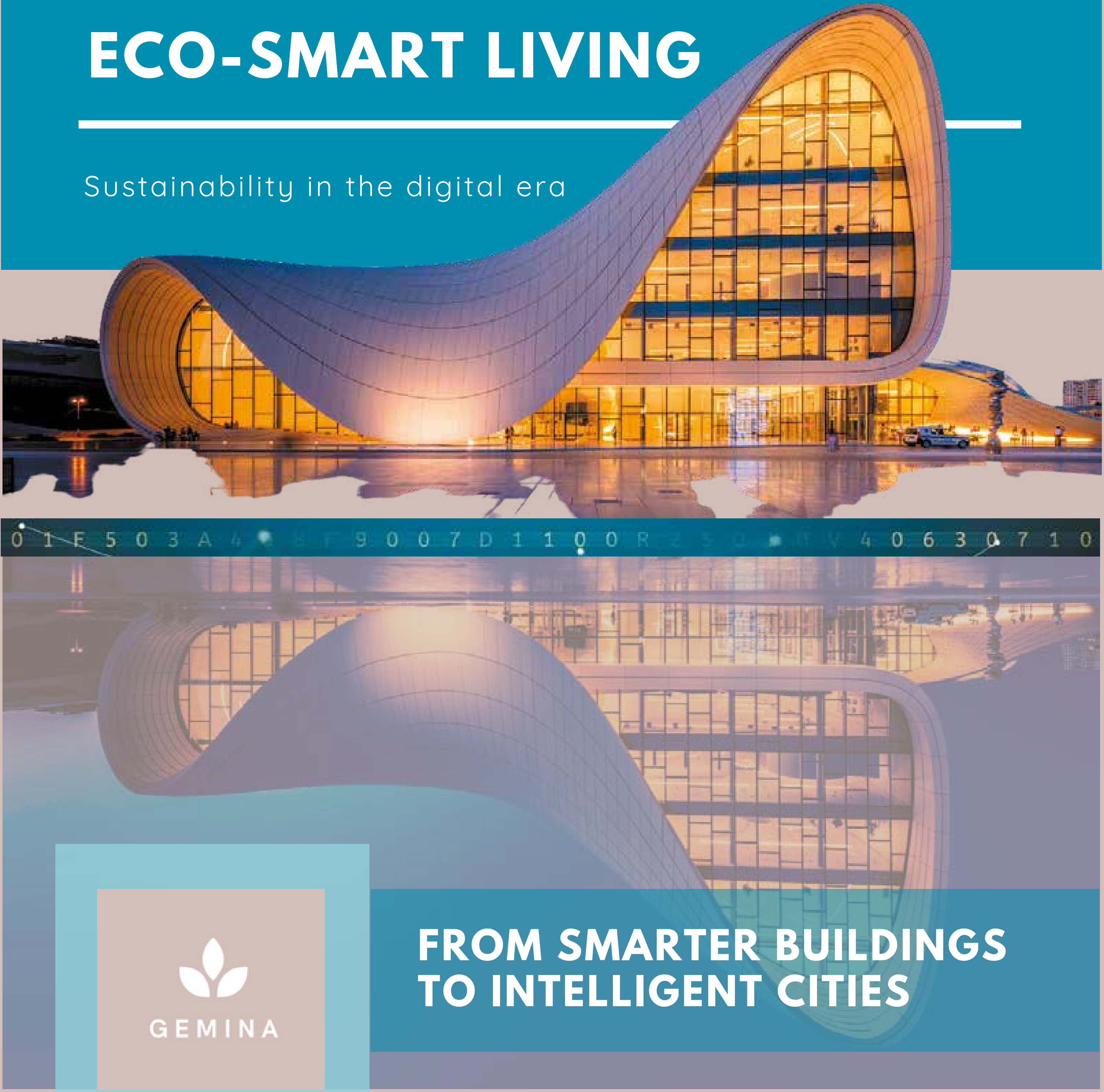
PLEASE VISIT US AT: TRUSTECH, PARIS/FRANCE, 28-30.11.2023, BOOTH NR.D055

www.melzergmbh.com

GEMINA INTERNATIONAL

ECO-SMART LIVING

Sustainability in the digital era



GEMINA

FROM SMARTER BUILDINGS TO INTELLIGENT CITIES

Gemina stands for innovative development and modernization aimed at empowering urban lifestyles, with data and intelligence utilized to reduce the environmental impact. The relentless rise in population and urbanization levels urge communities worldwide to embrace the smart city vision and adopt environment-friendly construction concepts. Today, citizens, businesses and communities can embrace digitization and contain dangerous man-made climate change. Gemina designs and builds to address the main requirements of sustainable urban development, with a focus on all the beneficiaries of future urban living: city dwellers, property owners and the environment.

Gemina: sustainable urban development meets intelligent construction

www.gemina.com