Digital Identity: Realising Smart Cities

About the GSMA

The GSMA represents the interests of mobile operators worldwide, uniting nearly 800 operators with more than 250 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and Internet companies, as well as organisations in adjacent industry sectors. The GSMA also produces industry-leading events such as Mobile World Congress, Mobile World Congress Shanghai, Mobile World Congress Americas and the Mobile 360 Series conferences.

About the GSMA Identity programme

The GSMA Mobile Identity programme is a global initiative established to support mobile operators in understanding and unlocking the potential of electronic and mobile identity. This includes being aware of and prepared for the opportunities and challenges of existing and upcoming legislative and regulatory changes.

Summary

Smart cities will prove the Internet of Things' most visible manifestation. We can already see urban environments becoming increasingly connected, as the practical elements of city life start to come online. The arrival of smart parking, for instance – the ability to seek and allocate parking spaces in advance, keeping unnecessary driving time to a minimum – has brought with it a range of improvements to congestion, pollution, driver convenience and city revenues. Municipal authorities can now also enhance the safety and economic performance of their cities through smart traffic systems, using the data their roads generate to manage vehicle flows in real time. And smart utilities are now poised to become a phenomenal growth area in bringing smart cities to life: the majority of European energy customers and vendors alike are set to enjoy the benefits of remote metering by 2020, which will reduce costs, inaccuracies and time lost for all concerned. As we look further ahead to the mid-century, however, intelligent public services will move beyond the mechanical: two decades from now, increasingly complex and sensitive aspects of our lives will be connected to city infrastructure via IoT.

Early innovations in digital health

Where currently, for instance, we conduct most of our healthcare assessments through in-person appointments, possibilities will arise for remote and automated administration of medical needs. Cities may deploy smart kiosks in public places, for example, via which samples of saliva or blood could be given, on-the-spot analyses made, prescriptions issued and even medicines dispensed. While this may seem far-fetched now, the early signs of such innovations can already be seen. There exist already medical apps to assist in remote diagnoses; as connected wearable and portable devices become more common, accurate data on users' sleeping, eating and exercise habits will be transmissible automatically, to aid in such processes without requiring complex inputs from the individual. The implications for efficiency savings in manpower and overheads – and the wider analytic use to which anonymised data could be put – point to drastic broadening of access to medical care where it can be made an aspect of the city's connected fabric.

New forms of verification to enable enhanced public services

With this proliferation of intelligent public services will naturally come a need for public digital identity solutions, to ensure the security of service users' information. With more and more of our daily lives set to migrate onto connected platforms, two logical certainties arise: that security will become more important than ever, and ensuring it by recall of more and more passwords will become simply unfeasible. The multiplicity of connected public services available will require not only the confidence of those using them, but may also require multiple modes of access, depending on what makes sense for each one – without the inconvenience and unreliability of recalling logins and passwords.

Biometrics then seem sure to play an increasing role in verifying our identities, as we go about our business in the smart cities of two decades hence. We are already familiar with using, say, fingerprint or iris scans; in future, a much wider range of biometric identity solutions is likely to be implemented, as appropriate to context.

Physiological biometrics will come to include recognition of users' DNA, and 3D analysis of the earlobe; research into behavioural biometrics, which presently include analysis of mannerisms such as keystrokes, will soon allow recognition of individuals by their gait. As the intensive research and development in these solutions taking place now begins to bear fruit, public service systems will become increasingly able to determine with certainty that a person is who they claim to be, through increasingly sophisticated and cross-checkable means. And, as the technology becomes cheaper, biometric verification will become available on more and more everyday portable devices such as mobile phones, bringing their potential use cases to a far wider array of services.

With more and more of our daily lives set to migrate onto connected platforms, two logical certainties arise: security will become more important than ever, and ensuring it by recall of more and more passwords will become simply unfeasible.

Improving transport and safety

Emergency services

The importance of digital identity does not, however, stop at the point of individuals accessing services in this way. The smart city of the future will require millions of devices to communicate not only with the people using them, but with each other, in situations of often paramount importance to the safety and wellbeing of the population. These devices must, if they are to operate in concert, be assigned identities of their own, which is what is starting to happen. A connected city facing a major storm, for example, will need its early warning system to send information automatically to emergency services, and set in train pre-approved response sequences to address the danger.

With seamless verification of the warning system's identity, precious time will be saved in closing thoroughfares, evacuating buildings, and dispatching blue-light vehicles. The city's other connected infrastructure such as traffic systems could then also be brought to bear automatically, to chart the best route through the danger period, without waiting for human action to verify individual signals.

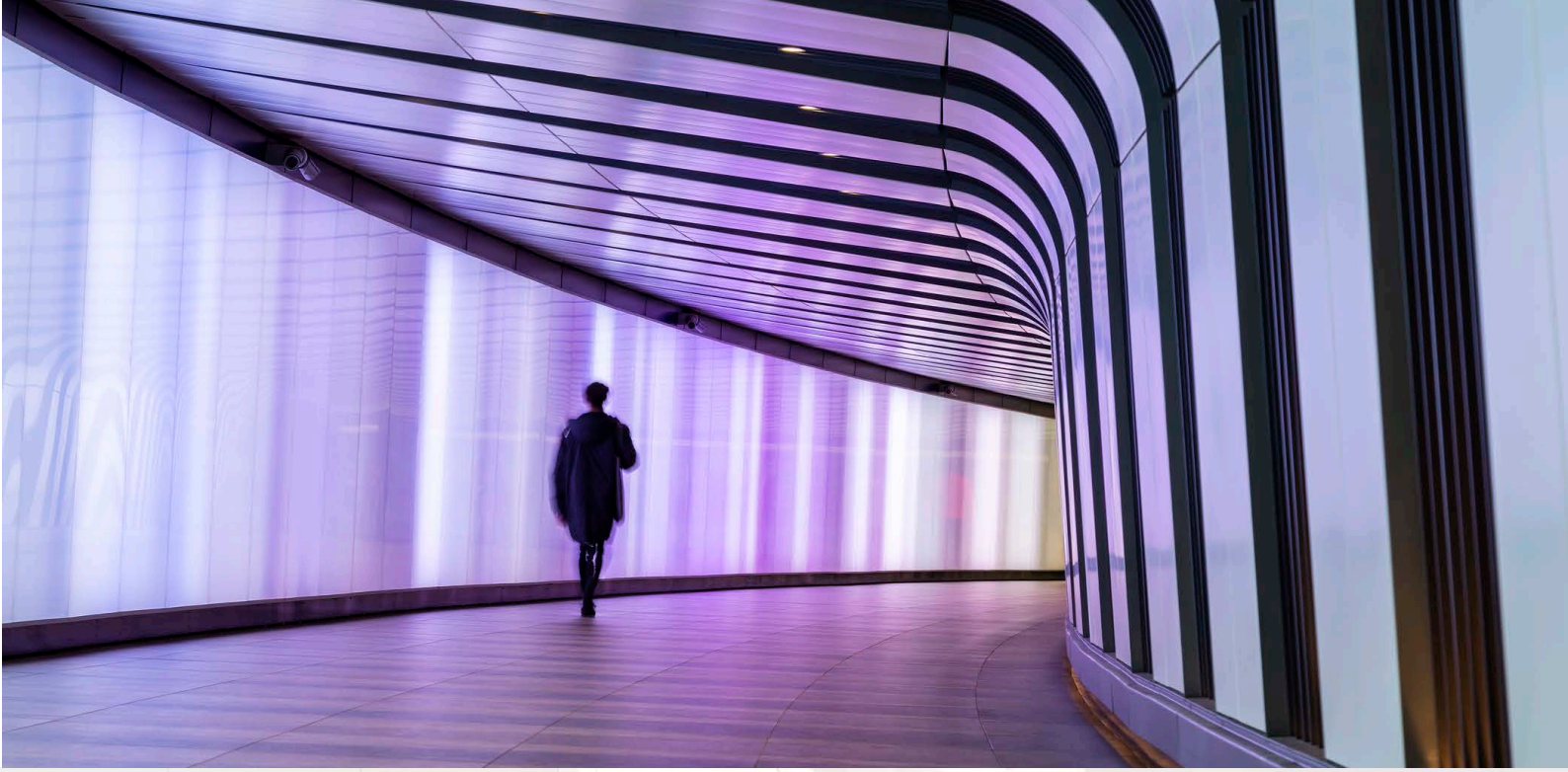
70% of the world's population will live in cities by 2050

Data from the UN indicates that around 70 per cent of the world's population will live in cities by 2050; the bulk of this accelerated urbanisation will occur in the developing world, where the effects of climate change are forecast to be felt disproportionately.[1] Ensuring a seamless chain of identity verification could, in such scenarios, mean the difference between life and death for large numbers of people.

Public transport

Most of the time, however, digital identity will simply be a tool by which we make the daily practicalities of city life more convenient, and their possibilities richer. As we approach the point at which a generation of adults has never known life before the smart phone, institutions and services will be reshaped into an increasingly mobile-only world. Public transport will move towards automated fare collection, most likely via portable devices, in order to eliminate the roughly 15% revenue loss which goes simply on maintaining the present manual systems. If administrators can automatically determine who is on board public vehicles, they can not only charge appropriately but also plan services better; research indicates, for example, that alleviating congestion at peak times by just 5 to 10 per cent could save major cities around $150 million per year.[2]

1. UN World Ubranization Prospects, https://esa.un.org/unpd/wup/
2. The Smart Cities Playbook, https://www.pymnts.com/news/payments-innovation/2016/the-smart-cities-playbook/

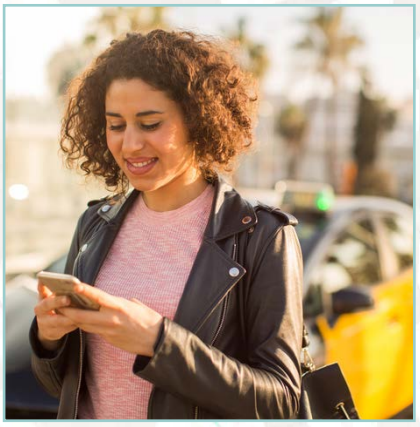


Underpinning blockchain and biometrics with network technology

Blockchain too will cease to be a mysterious thing people may have heard of, but are at a loss to describe; it will become part of the norm of data management in public services. With 3 in 10 medical test results in the United States currently going missing, blockchain's elimination of this possibility presents potential savings of billions of dollars, and thereby many lives.[3]

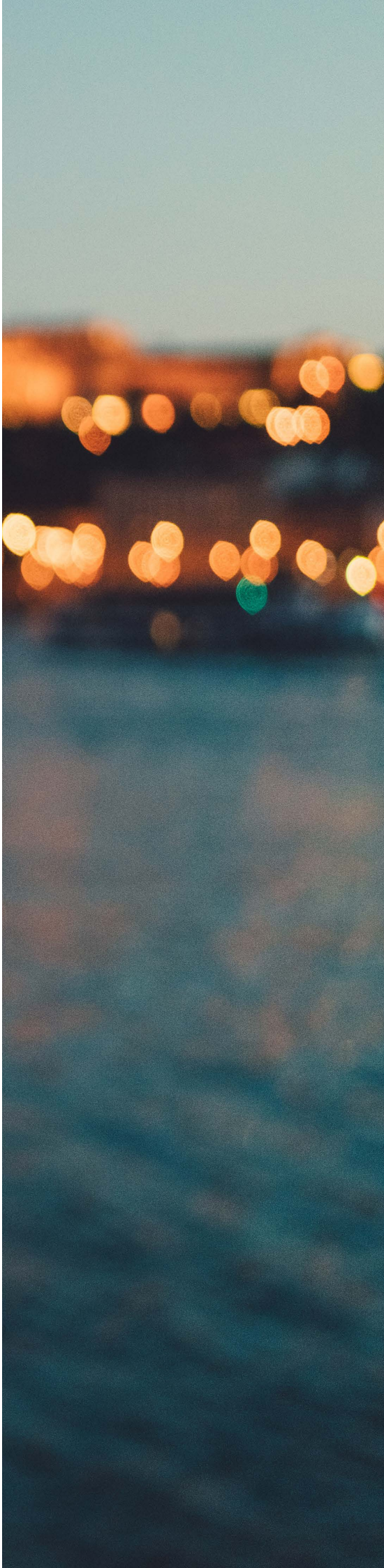
60 countries globally have already made the jump to digital citizenship by engaging in national eID schemes, as they show signs of following in the footsteps of Estonia's remarkable innovations in eGovernment: voting can, where there is confidence in digital identity, be undertaken online as in that country.[4] Sensitive documents such as contracts and licenses, which currently require in-person visits or lengthy wait times, will become dispensable from secure eCabinets; crossing borders too will in time become a far smoother and more automated process, as the identity of each passenger becomes readable remotely as they pass through terminals.

Underpinning both blockchain and biometric identification, however, will be network technology. In recent years, mobile technology has proven more than capable of undergoing fundamental improvements to meet the demands of an increasingly dynamic digital market. For example, low power wide area (LPWA) networks in licensed spectrum are steadily consolidating their position in the IoT's LPWA market, with reliability and security often cited as two of the principal reasons why. Another major network innovation, 5G, is also regularly touted as being central to the smart vision due to its ability to 'slice' networks into vertical-specific functions, which will massively open up commercial opportunities for all manner of services.



Identity is no exception. Emerging technologies that serve the identity market can provide an additional layer of security and ease-of-use by working in tandem with conventional multi-factor authentication mechanisms that integrated into a wallet, app or public ID scheme. What makes mobile network operators a likely partner for companies specialising in biometrics and blockchain is the same reason why new network technologies are sought after; their reliability, security and of course, their near-universality.

3. What You Need to Know About the Future of Healthcare,https://www.forbes.com/sites/annabelacton/2017/07/14/the-future-of-health-its-in-your-hands/#28ccb8e12af2
4. Digital Dividends: Reaping More with eGovernment Services and eID Schemes, https://www.gemalto.com/govt/inspired/digital-dividends



GSMA

Floor 2
Walbrook Building
25 Walbrook
London EC4N 8AF
Tel: +44 (0) 207 356 0600
Fax: +44 (0) 207 356 0601