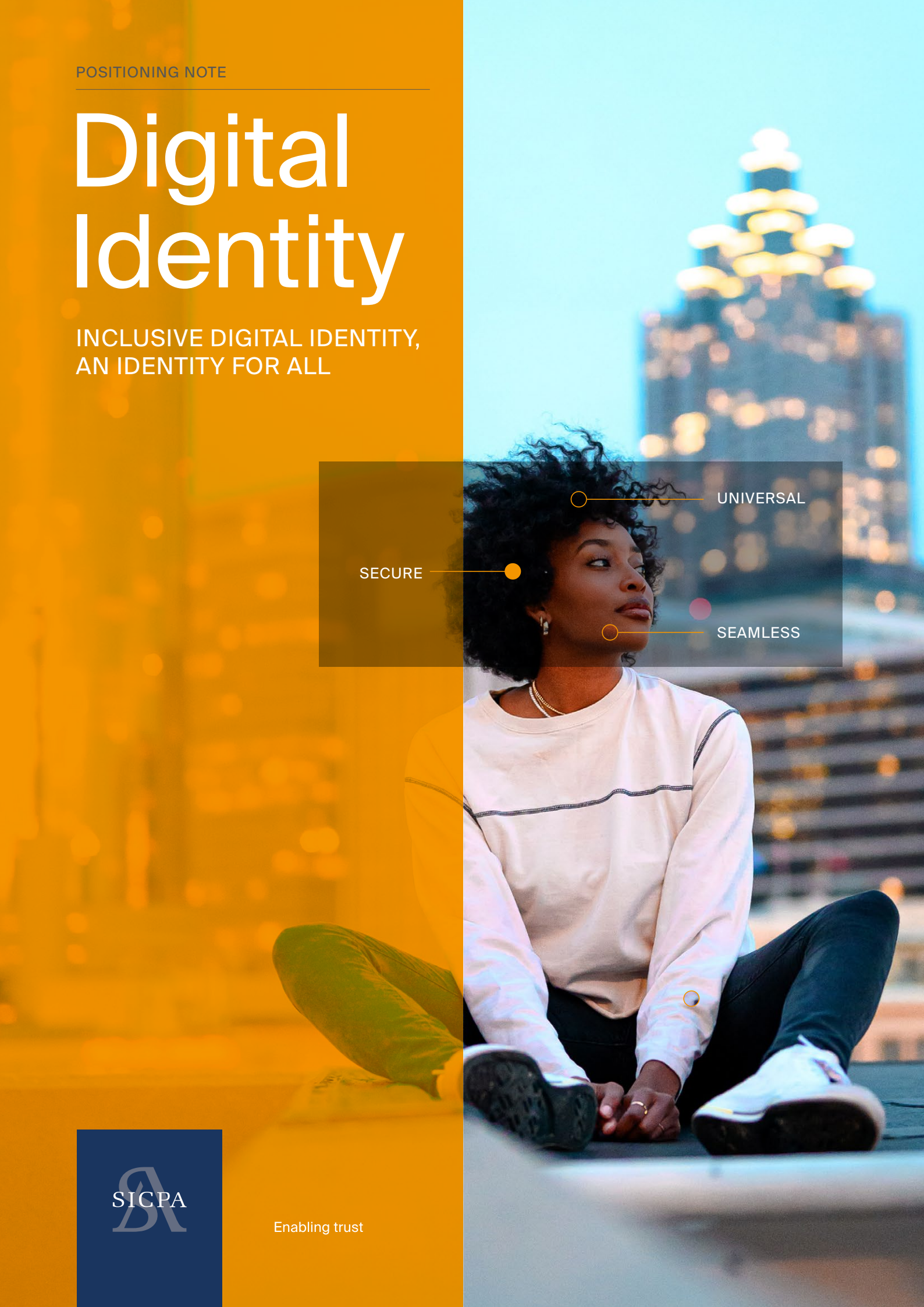
POSITIONING NOTE

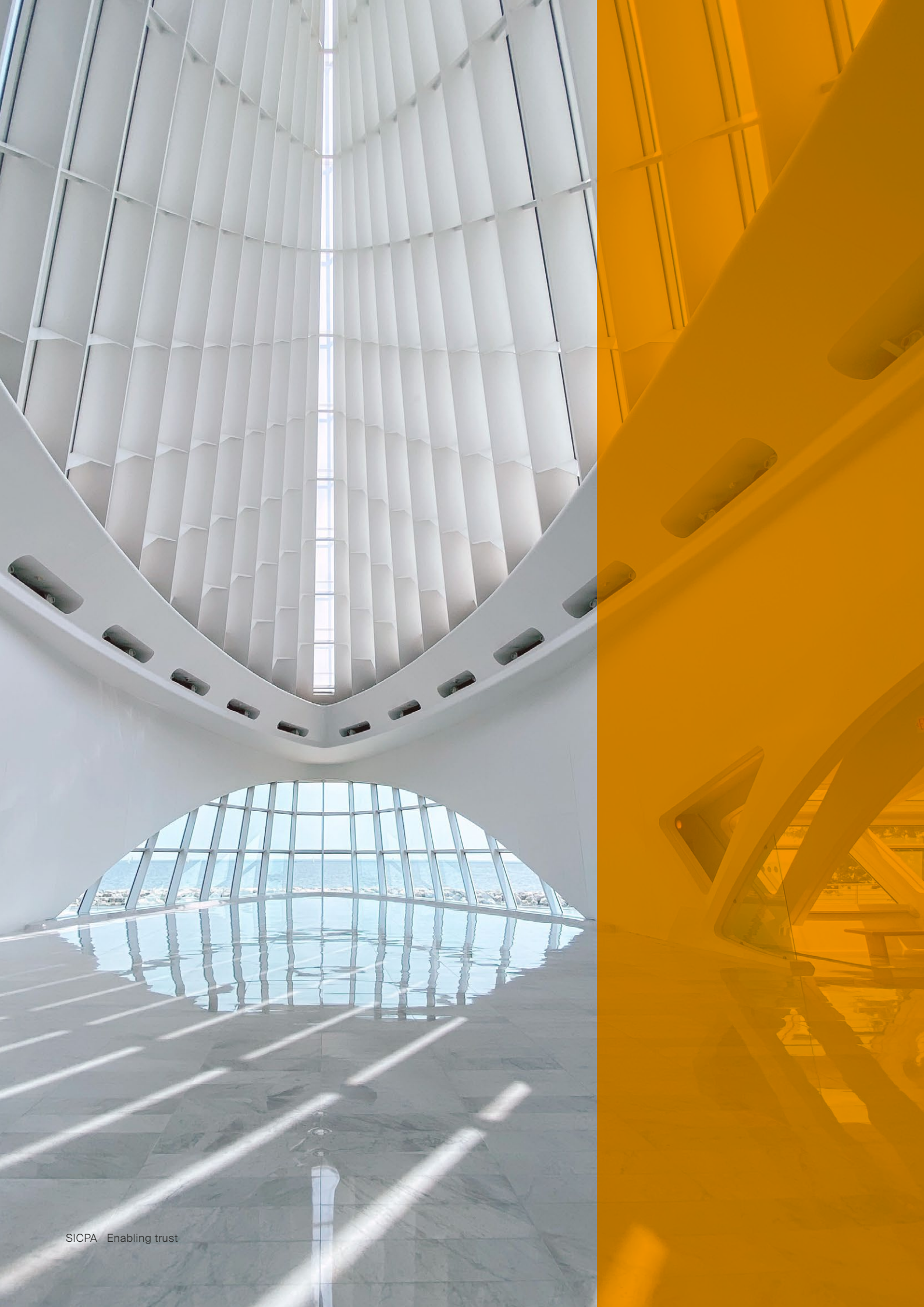
Digital Identity

INCLUSIVE DIGITAL IDENTITY, AN IDENTITY FOR ALL



SICPA

Enabling trust



How can governments foster best-in-class digital identity in the 21st century?

Official identity data and credentials are essential for accessing numerous public and private services in society today. Starting from birth registration, all the way to death certification, daily living in our communities revolves around foundational physical identity documents that enable access to education, health and social benefits, education, finance and commerce over a lifetime. Yet millions of people are excluded from these services due to the lack of formal ID.

The development of digital identity represents a risk of even greater exclusion for those who are already outside society's official systems. The first priority of a digital identity solution is to avoid creating further difficulties for such people, offering them instead a real opportunity for integration, thanks to true accessibility and inclusivity. The move to digital enables governments to make real progress in delivering inclusive identity systems that give access to services for all.

The sovereign functions of governments cover the basic attributes of a state such as managing the currency, external and internal security, justice, and the creation and protection of individuals' identities. Just as in the physical world, every government's digital sovereignty should be guaranteed and exercised over digital identity, digital currency and digital control of institutions and services.

An effective digital identity (ID) system needs to work across borders and different national government agencies, providing a seamless, inclusive experience that safeguards security and privacy. It also must operate with legacy identity structures, assuring full interoperability.

As architect and sponsor of an individual's formal identity, the government's role should focus around three core pillars: governance, the user experience and technology.

1 IDENTITY, A PRIVILEGE FOR MANY, A NEED FOR ALL

An official form of identity is a prerequisite ensuring inclusive participation for everyone in society.

It enables access to health and welfare systems, to education and learning, to social housing and to financial support from government agencies and services. In low and low-middle income economies, a billion people lack any official form of identity[1], such as a residence permit, health record, driving licence or passport. This can impede people's access to services, especially rural residents, those on a low income, women, children, and other vulnerable groups. In upper and upper-middle economies, digital transformation and expanding Internet access create a growing need for digital forms of identity as well.

Name, date of birth, gender and civil status are core elements of an individual's identity, often supplemented by a social security number, health service identification and a tax or pension number. These are – or should be – the foundational credentials held by every person. Additionally, people use multiple contextual credentials in daily life to access email accounts, social media profiles, e-banking accounts, health insurance services, etc. A comprehensive digital identity system serves to collectively capture and authenticate all of these individual credentials in perpetuity.

A far-reaching and fully trusted digital identity system, delivering seamless user experience, paves the way for rapid national and wider international adoption and applicability, facilitating broader access to public and private services. Roll-out of digital identity across society offers the potential to improve the lives of everyone, not only in relation to better access to e-government services, but also for new and improved services related to banking, insurance, health, travel, employment, e-commerce and emerging digital currencies.

Common and unified access to public and private services is an opportunity and intended outcome of a universal and consensual people-first digital identity solution. At the heart of it, fully secured data ensure sustainability, permanence and trust.

Today's reality: Low rates of official ID and scattered access to services

1 billion people lack any form of official ID, according to McKinsey Global Institute.[1]

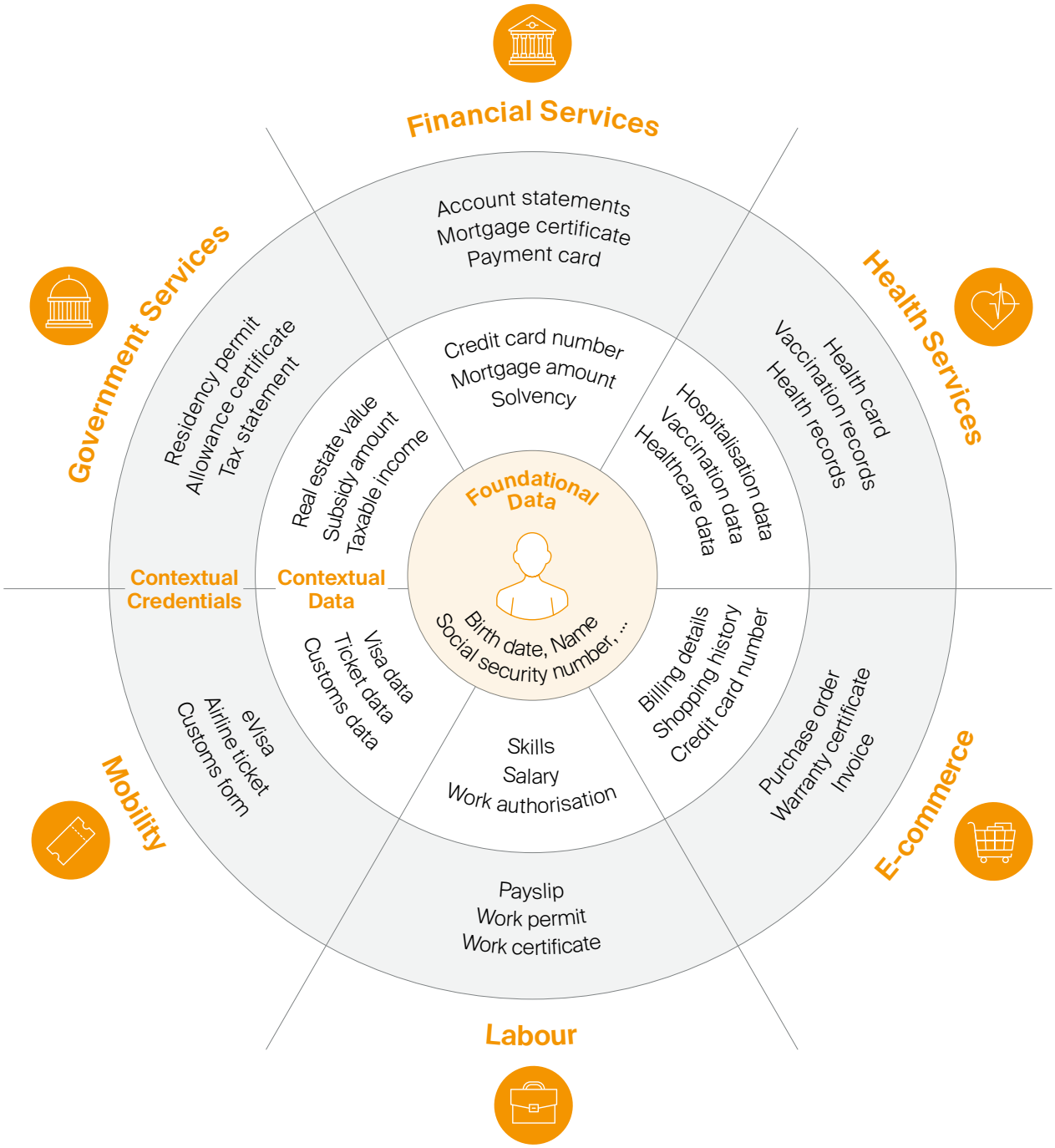
According to UNICEF's 2020 report on birth registration, 1 in 4 children under the age of 5 does not "officially exist".[5]

The World Bank reported **45% of women** over 15 in low-income countries lack an official ID (for men the figure is 30%).[9]

McKinsey Global Institute Report 2019 states that **3.2 billion people** hold an official ID but have no digital sphere.[1]

According to ENISA (European Union Agency for Cybersecurity), reported identity theft **more than doubled** between 2019 and 2020.[3]

The aim of e-government is to provide people with swift, simple, convenient and comprehensive access to public and administrative services.



This schema proposes some examples of foundational data, contextual data and credentials.
For readability reasons, foundational credentials such as passport, national ID card or driver's licence are not included.

AS WELL AS BEING HIGHLY SECURED AND PRIVACY-PROTECTING BY DESIGN, A DIGITAL IDENTITY SOLUTION SHOULD OFFER:

- A seamless one-stop-shop experience for people, supporting fast adoption and endorsement.
- Universal accessibility, supporting nationwide and global use.
- A consent-based approach, putting people's needs, interests and protection at the centre.

2 KEY DIMENSIONS FOR GOVERNMENTS

In order to deliver fast, efficient and inclusive digital identity services, government decision makers should focus on three key dimensions: Governance, User Experience and Technology.

GOVERNANCE

In 2003, just 33 countries offered online transactional services, such as for payment of taxes, fines for motor vehicle violations, postal services etc. using credit, bank or debit cards.[6] By 2016, 148 countries had at least one online transactional service.[4]

Even if the majority of governments have adopted one or more e-governance applications to offer e-services, the systems do not currently embody all the benefits of a fully-fledged digital ID. In most cases, the implemented solution does not enable open, local, national, cross-border and inclusive access for everyone.

Today, people face multiple digital identity encounters that are contextual and related to discrete applications, situations and purposes. Each new application requires a separate sign-up and the provision of different data and identifiers. This has created a sense of "trust by silo" and does not permit transactions across different legitimate and recognised channels.

Large companies, banking consortia and telecom operators are all in the running to become global identity providers. The question of regulation inevitably arises as private companies monetise services notably by using citizen data. Delegating the issuance of identity to commercial entities may ultimately lead to state authorities losing control over governance and the long-term risk of loss of state sovereignty over identity issuance.

There is a compelling case for the issuance of digital identity, and the capture and release of foundational credentials, to remain under the remit of government in order to assure people's privacy and the integrity of personal data. Sovereign authority governance is a cornerstone of sustainable and inclusive identification systems, allowing everyone to have equal access to digital resources and services. More than 4.4 billion people across the world either face exclusion due to the lack of a formal ID or lack of access to digital services.[6] New digital identity solutions therefore provide an opportunity to deliver considerable progress.

Governance – the first priority of digital identity solutions

INCLUSIVITY

Inclusivity places the focus on people. Those previously unable to access public or private services without a formal identity, have an opportunity thanks to digital identity. The core benefit is equal access for everyone regardless of the individual's economic, technological, social or cultural context.

An inclusive solution is compatible with countless applications and situations. It also enables people currently outside the socio-economic or digital sphere to access a range of secured yet convenient public and private services.

For those already integrated in the digital world, digital identity will enable great progress in identity protection and privacy preservation. It will secure online transactions while facilitating usage and overall user experience across multiple systems and organisations.

Security breaches and identity theft are a major challenge in today's cyber communications and in interactions with private or public organisations. Digital identity solutions can serve as a protective shield, safeguarding everyone.

DATA PRIVACY MANAGEMENT

Data privacy management featured in the solution allows a high level of detail for the disclosure of credential data. The holder can select the data fields to be disclosed for each specific purpose. Single data field disclosure has the advantage of allowing holders and issuers the highest possible level of consent. At the same time, it fulfills the objective of data minimisation for organisations wishing to mitigate data management risks and constraints.

GLOBALLY TRUSTED VERIFICATION

Globally trusted verification of credentials paves the way for cross-border applications. Governments and international organisations foresee a double advantage. Existing border control protocols and entry agreements between nations will not be disrupted, but rather reinforced by increasing efficiency and usability.

DATA PORTABILITY

Data portability provides governments and issuers with the immediate advantage of reusing an individual's credentials across several – and potentially unlimited – services, while delivering the highest possible security levels. Portability allows foundational identity information to be safely and seamlessly utilised by public or private stakeholders for the creation of context-specific credentials. This multiplies the number of potential applications and speeds up adoption.

USER EXPERIENCE

Slow global adoption of digital identity[2] results from the lack of governance and coordination at international level. Despite steady effort and resources invested by governments, digital identity, authentication methods and credential management systems have not been globally adopted. Low levels of adoption are largely due to the lack of global standards, poor user experience (for holders and verifiers) and the limited range of applications.

The absence of common standards and interoperability has created a situation where digital identity ecosystems are scattered and silo-based, compelling users to create multiple passwords to access countless applications. The average person juggles around 100 passwords[7], causing an immense strain for anyone trying to remember, manage and access different account services. In a worst case yet common scenario, users keep the same password for several services and applications and save them all in one place. This raises the risk of identity theft and online breaches, causing concerns for personal security.

Digital identity designed for people

EASE OF USE

Ease of use for identity holders and verifiers is of the essence. Fast and simple onboarding, via a login or password-less procedure enables users to swiftly and securely adopt a new credential-based identification solution. For holders and verifiers of a digital identity, the service offers considerable progress in terms of online and offline user experience and identity proofing. It streamlines digital transactions while facilitating usage across multiple systems, organisations and countries. Legal identification documents allow people to access digital applications and services such as for e-government, health, taxes, personal data, and more.

RE-USABILITY

Re-usability of credentials and selected data mean that users and verifiers do not need to go through the same proof of identity process repeatedly. Digital identity and foundational credentials issued by the government can be easily reused and activated in other identity-based contexts and situations, creating a seamless user experience. There is no need for personal data to be entered into the system each time for a new credential or purpose. This eliminates manual errors, aborted inputs and lost time during onboarding. Benefits also include higher trust levels for service providers and a reduction in the cost of KYC (know your customer) procedures. In a future world of sovereign digital identity, identity credentials generated by governments and service providers alike will be based on a certified foundational identity that remains constant. Credentials related to health organisations, private insurance companies, telecommunications companies, notary services, universities, to name a few, will be rooted in foundational credentials issued by the government or government agencies.

CONSENT AND CONTROL

Consent and control are fundamental to meet people's expectations and assure the levels of confidentiality that are currently difficult to achieve. Users should be able to exercise individual control and consent over the personal data processed for the purposes of identification/authentication[8], including the opportunity to selectively provide only the minimum identity attributes required for a particular transaction.

TECHNOLOGY

Technology for digital identity issuance, ownership and verification is evolving rapidly. Decision makers in government are therefore tasked with selecting future-proof technology that will adapt and integrate smoothly with changes over time. They also need to ensure that the solution offers system scalability and sustainability.

Interoperability enables ID systems to systematically exchange data with other services. One of the main challenges is to ensure that data can be exchanged across public and private systems locally and internationally. Ensuring the interoperability of credential systems is a prerequisite for the delivery of seamless user experiences across different platforms, devices and services within a single country as well as across borders. The chosen technology must meet open standard specifications and ensure interoperability in order to meet everyone's needs.

A digital identity solution ensuring extensive and frictionless access to services

COMMON AND OPEN GLOBAL STANDARDS

Common and open global standards are a core feature of the ideal solution making it applicable for credentials across different systems and platforms and compatible with multiple wallets at the same time (similar to the physical biometric passport today). These technical capabilities set the solution apart as an easy-to-integrate and flexible product, with an unlimited range of usability.

OPERATIONAL VIABILITY

Operational viability ensures high performance of the solution in the daily management of existing credentials, online and offline. Digital identity is not a one-off event, but a sequence of sometimes recurrent events corresponding to a life-cycle model. Identity life-cycle allows the management of events from issuance, to additional registration. It includes updates such as name, gender and civil status changes, enabling credentials such as a non-resident entry visa, a residence permit or a driving licence to be blocked or cancelled. Operational effectiveness and efficiency enable swift verification as well as easy and secure credential recovery. The main purpose of digital identity is to be a trusted consent-based service that is user-centric and secure by design. In other words, it is highly reassuring for issuers, verifiers and owners.

Digital identity should:

- **Ensure highest level of governance**
- **Offer efficient operational viability**
- **Guarantee fast integration and adoption**

3 BENEFITS PAVING THE WAY FOR NEW IDENTITY STANDARDS

UNIVERSAL USAGE

Today people use different sets of identifiers and credentials to have access to their personal information. Whether for private health insurance, to authenticate achievements or credits at university, to apply for social welfare or housing, a password and login are the minimum requirements for access.

With a ubiquitous digital identity solution, everyone can use personal identity details and related credentials across a wide variety of different systems and networks in a seamless fashion, depending on the specific context and purpose.

As the solution has an open standard approach by design, it ensures cross-system and cross-organisation usability. Its full compatibility with W3C open standards ensures a natural evolution towards a future global internet of identity.

IDENTITY FOR ALL

Empowering people with convenient access to identification is one of the major promises of the solution. A target of the United Nations Sustainable Development Goals (SDGs) is “to provide legal identity for all, including birth registration” by 2030. Identification, including digital identity is part of the bedrock to enable financial and economic inclusion, social protection, equal access to healthcare and education, gender equality, and more.

An inclusive and trusted digital identity solution reinforces transparency, efficiency and the effectiveness of governance. It will help governments strengthen the fight against fraud, improve welfare support, tax compliance and encourage inclusive and sustainable development.

SEAMLESS EXPERIENCE

Swift and frictionless access to public services improves people’s experience and satisfaction. It also reinforces the long-term credibility of sovereign authorities and helps build trust. The digital identity solution should enable governments to deliver intuitive, convenient, seamless, and swift user experiences when transacting digitally. Depending on the specific level of authentication and verification required for different services, security thresholds will be adapted so that the user experience is more efficient and convenient. Full identity disclosure will not be necessary for every interaction or request, allowing selective disclosure of specific data fields. A best-of-breed digital identity solution provides reliable and easy registration and authentication processes for government agencies and other service providers.

Summary of key benefits:

- Inclusive and sustainable
- Practical, secure and flexible
- Seamless

SICPA AT THE FOREFRONT OF INNOVATION

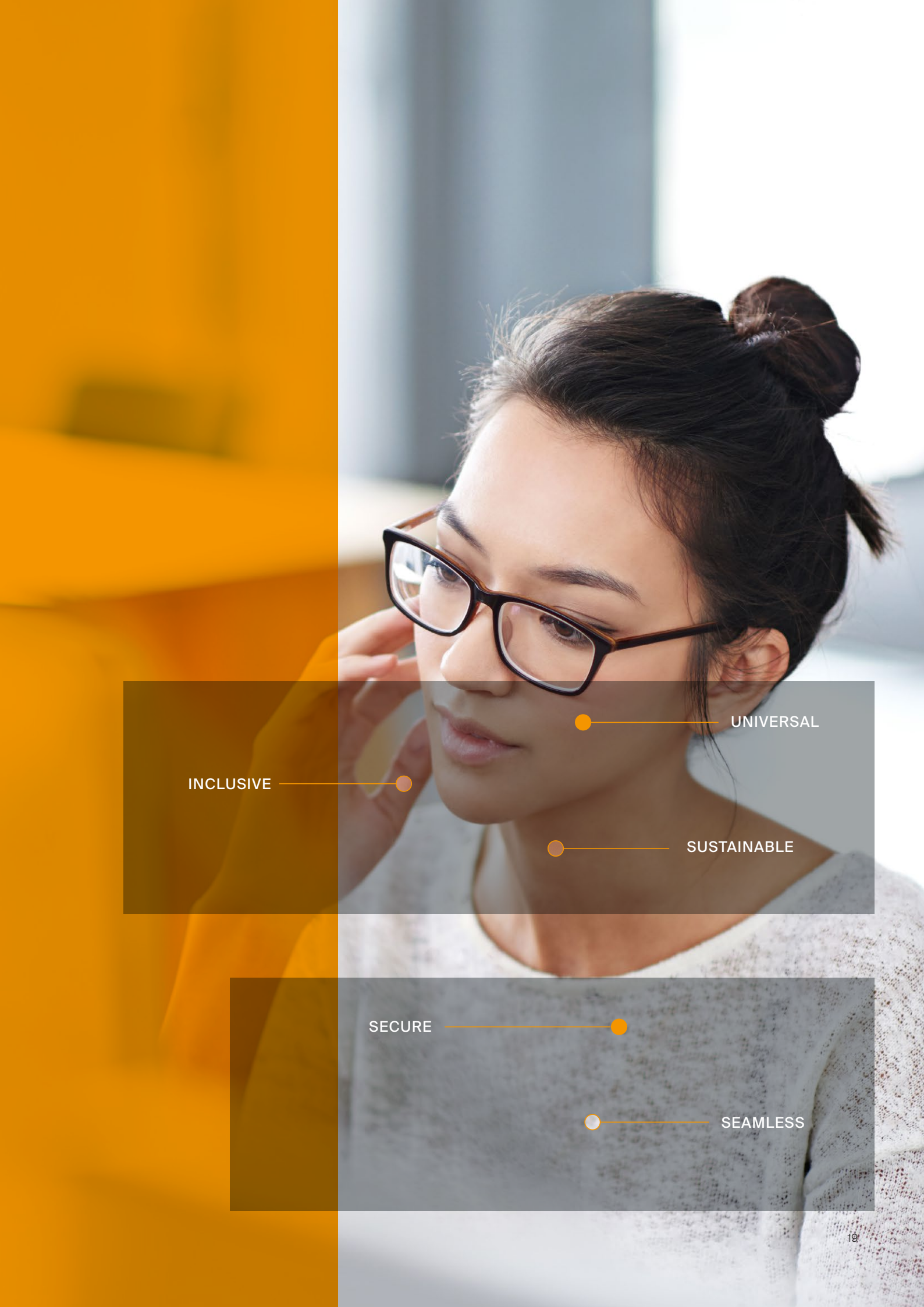
As a trusted technology provider to central banks, governments and the private sector, with decades of innovation experience in physical and user-centric solutions, SICPA is a key stakeholder in inclusive digital ecosystems.

A decentralised digital identity solution, founded on global interoperable and self-sovereign identity standards and allowing seamless accessibility and adoption, is an integral part of SICPA's vision for the 21st century. Interoperable across borders and government domains, the solution supports the trusted digital equivalent to today's physical credentials (residence permits, ID documents, driving licences, visas etc.), while preserving sovereign authority.

SICPA helps governments and public and private entities worldwide deliver fast, simple, convenient and secure access to services, providing lifelong value for everyone in our rapidly-evolving digital society.

SOURCES:

1. **White O. et al (17 April 2019), McKinsey Global Institute Report**
   https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth
2. **Domeyer A. et al (2020), McKinsey & Company**
   https://www.mckinsey.com/industries/public-and-social-sector/our-insights/how-governments-can-deliver-on-the-promise-of-digital-id
3. **ENISA Threat Landscape 2020 – Identity Theft (20 October 2020)**
   https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-identity-theft
4. **United Nations (2016), UN e-government survey**
   https://publicadministration.un.org/egovkb/en-us/reports/un-e-government-survey-2016
5. **UNICEF**
   https://data.unicef.org/topic/child-protection/birth-registration (accessed on 6 September 2021)
6. **The World Bank – Identification for Development ID4D**
   https://id4d.worldbank.org/global-dataset/visualization (accessed 6 September 2021)
7. **Williams S. (21 October 2020)**
   https://securitybrief.co.nz/story/average-person-has-100-passwords-study
8. **The European Commission (January 2018)**
   https://ec.europa.eu/futurium/en/system/files/ged/draft_principles_eid_interoperability_and_guidance_for_online_platforms_1.pdf
9. **Desai V.T. et al (25 April 2018), World Bank Blogs**
   https://blogs.worldbank.org/voices/global-identification-challenge-who-are-1-billion-people-without-proof-identity


UNIVERSAL
INCLUSIVE
SUSTAINABLE
SECURE
SEAMLESS

Avalanche.studio

SICPA SA
Av de Florissant 41
1008 Prilly
Switzerland

Tel +41 21 627 55 55
Fax +41 21 627 57 27
digitalidentity@sicpa.com
www.sicpa.com

WHP 00050 V1 09.21