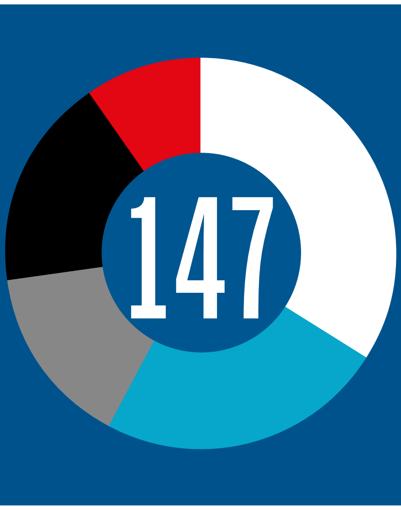
Digital Identity

Proof-of-Identity and Access to Mobile Services*

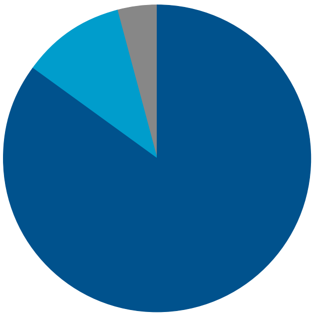
1 billion people make up the identity gap who lack formal proof-of-identity, predominantly in developing countries in Sub-Saharan Africa and Asia



147 countries require proof-of-identity for mobile SIM registration

- **50** in Africa
- **35** in Asia Pacific
- **22** in Europe
- **26** in Latin America
- **14** in the Middle East

Government rules on how mobile operators should handle SIM registration data where proof-of-identity is mandatory



- **85%** capture & store
- **11%** capture & validate
- **4%** capture & share with government

20% of adults cite a lack of proof-of-identity as a key barrier to financial inclusion

11 countries require mobile operators to capture customers' biometric data to meet SIM registration requirements

76% of all SIM cards globally (7.7 billion mobile connections) are prepaid, **92%** of which are in countries where mandatory proof-of-identity is required for SIM registation

The ability to prove that you are who you say you are is critical to accessing basic services such as healthcare, education, employment, financial services and voting

www.gsma.com/access-to-mobile-services

*data from 2017

Access to a government-recognised digital identity will be increasingly crucial as countries are implementing their digital transformation strategies

- For individuals' to fully participate in a digital economy, the ability to digitally identify themselves – online and offline – will be key to accessing life-enhancing services including healthcare, financial services and social protections.

Mobile plays a key role in enabling digital participation yet having a unique mobile subscription in most countries depends on presenting proof-of-identity

- As of January 2018, governments in 147 countries require mobile users to present proof-of-identity when registering for a prepaid SIM card in their own name. GSMA research[1] found that where such policies exist, mobile penetration is often directly proportional to the official identity penetration coverage in a country.

Policy considerations for governments wishing to accelerate digital transformation while enabling access to mobile services

- **Establish accessible and inclusive digital identification systems:** Ensure that all citizens and residents have access to government-recognised identification. This is particularly crucial for vulnerable groups such as those living in very remote locations, women and girls, and forcibly displaced persons[2] who may lack a proof-of-identity and face a higher risk of social, digital and financial exclusion.

- **Maintain robust and query-able identification databases:** The robustness of a government-recognised identification credential and the ability of mobile operators to query and validate that credential against a government-maintained database could significantly improve the effectiveness of a SIM registration policy (where mandated) while mitigating the risks of digital and financial exclusion.

- **Ensuring industry participation when designing digital identity ecosystems:** Engaging early on and/or partnering with mobile operators and other key stakeholders from the wider identification ecosystem, can help drive consensus on technical standards, broaden the reach of the ecosystem and accelerate digital transformation.

- **Drive demand, adoption and usage of innovative and interoperable digital identity solutions** (e.g. through developing and encourage the use of eGovernment portals and offering incentives to targeted beneficiaries for accessing digital social protection services).

- **Create effective privacy and data protection frameworks to build trust in digital identity ecosystems:** Trust is key for incentivising people to register for a mobile subscription and accessing digital services in their own name (particularly where this is mandatory). Countries embarking on their digital transformation journeys with inadequate privacy and data protection frameworks are more likely to face calls for stronger regulatory measures and policies that promote transparency on how personal data are used, and tools for consumers to make simple and meaningful choices about their privacy.

Roles mobile operators can play in digital identity ecosystems

- Support enrolment to (digital) identity systems, leveraging retail presence and agent network.

- Assist with the digitalisation of legacy physical ID-systems.

- Strengthen Know-Your-Customer (KYC) processes and/or offer Digital ID-linked Authentication services.

- Create functional digital identities for their customers, e.g. based on their transaction and top-up history.

[1] www.gsma.com/access-to-mobile-services
[2] www.gsma.com/mobile-services-for-the-forcibly-displaced