DIGITAL IDENTITY LANDSCAPE: SURVEY

Compiled by: S. Lefophane, S. Ntshangase and S. Mthethwa

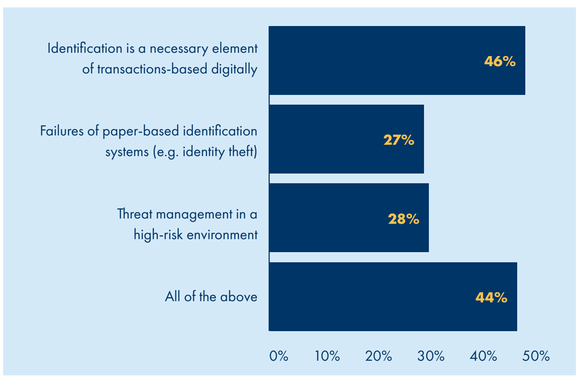
SUMMARY

The digital identity questionnaire was completed by 306 respondents from a total of 16 sectors. The largest sector was information technology, professional, scientific and technical (41.9%). All other sectors contributed 7% or less of the input. The respondents reflected a mixture of private organisations, government departments and other public institutions. The Gauteng province was predominantly represented in the responses, with almost half (49%) of the respondents, followed by the Western Cape, at 19%, as the second most represented province. All other provinces, except KwaZulu-Natal at 11%, were represented by 6% or less. A third of the organisations employed 30 to 100 staff, with just under a third (28%) reported having 101 to 999 employees. Organisations with 2 000 plus employees made up 17% of the total.

DATA ANALYSIS AND INSIGHTS

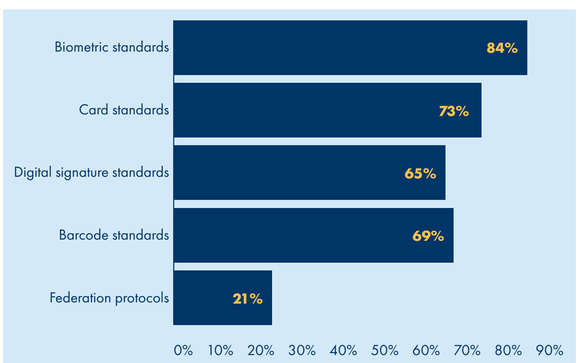
1) WHY IS DIGITAL IDENTITY IMPORTANT?

South Africa has seen an increase in the deployment and use of digital technologies and the continuous improvements of the national identification and registration system. Digital Identity (ID) systems refer to methods of identifying people, both online and offline, using other existing models of identification and authentication. Digital ID comprises identifiers, attributes and credentials that are electronically recorded and stored. These attributes and credentials are capable of accurately and uniquely identifying a person. The process of setting up a digital ID system starts with establishing registration standards, requirements for enrolment and mechanisms for validation of the captured information. The result is the issuance of electronic identity documents containing unique numbers and features. The processes involved in managing the system are considered to ensure accurate and up-to-date records for the digital ID.

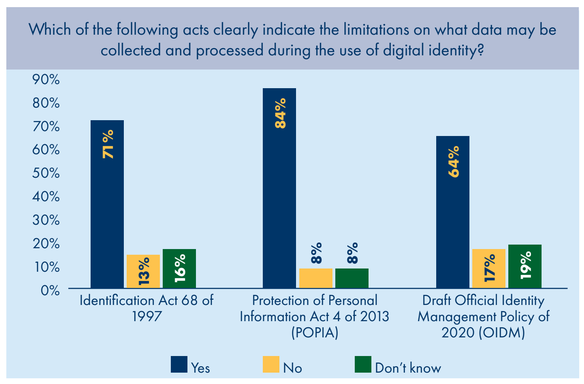


2) LEGISLATIONS AND STANDARDS WIDELY USED IN SOUTH AFRICA INFLUENCING THE ADOPTION OF DIGITAL IDENTITY SERVICES?

Most respondents (80%) believed that there were international standards and frameworks for identification systems available for the South African context, although 20% disagreed. Knowledge of a South African standard or framework was significantly associated with participating in an awareness workshop or with the respondents coming from an organisation that required specialised digital identification training in-house. The biometric standards were the most mentioned as widely available (84%), with two-thirds or more respondents citing card standards, digital signature standards and barcode standards.

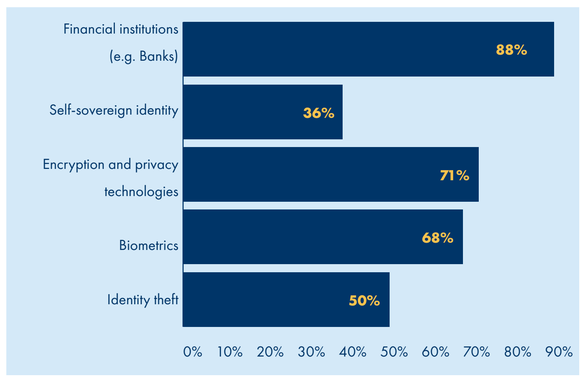


Most respondents (84%) believed that the Protection of Personal Information Act of 2013 most clearly indicated limitations on what data could be collected during the use of digital identity, with less (71%) agreeing with the same for the Identification Act, 1997 (Act 68 of 1997) and were least likely (64%) to mention that the Draft Official Identity Management Policy of 2020 limited data that could be collected.



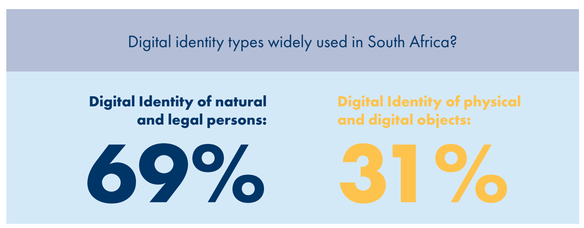
3) DIGITAL IDENTITY DRIVERS WITHIN THE SOUTH AFRICAN MARKET

Financial institutions (88.0%) were considered the most important driver of the South African digital identity market. Over two-thirds mentioned both encryption and privacy technologies (71%) and biometrics (68%) as drivers, while half reported identity theft. Only a third (36%) mentioned self-sovereign identity.



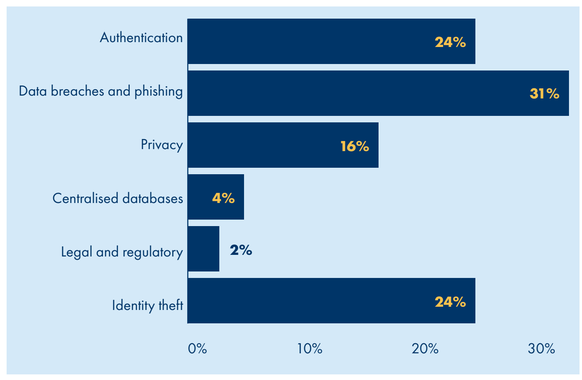
4) DIGITAL IDENTITY SERVICE TYPES WIDELY USED IN THE SOUTH AFRICAN MARKET

The most widely used digital identity type in South Africa was believed to be the identity of legal and natural persons (69%), with a third (31%) agreeing that it was the digital identity of physical and digital objects.

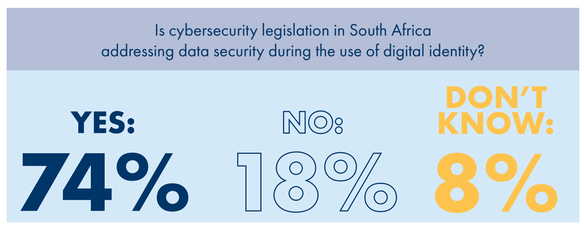


5) SECURITY RISKS FOR DIGITAL IDENTITY SERVICES

A third (31%) of the respondents rated data breaches and phishing attacks as the highest security risk to digital identity, with similar proportions (24%) reporting that it was authentication and identity theft. Privacy was rated at 16%, and the lowest of all threats mentioned was centralised databases (4%) and legal and regulatory compliance (2%).

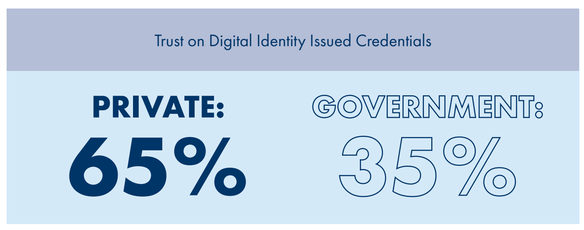


Around three-quarters (74%) felt that cybersecurity legislation in South Africa was addressing data security during the use of digital identity.

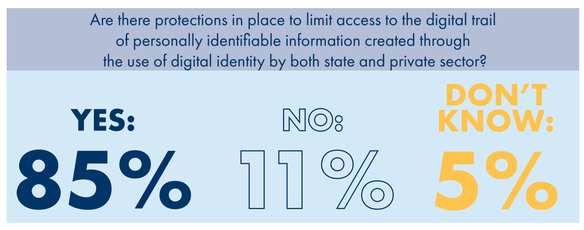


6) TRUST IN DIGITAL IDENTITY SERVICES

Respondents were more likely to trust the private sector (65%) compared to only a third (35%) in the public sector as related to digital identity credentials issues.

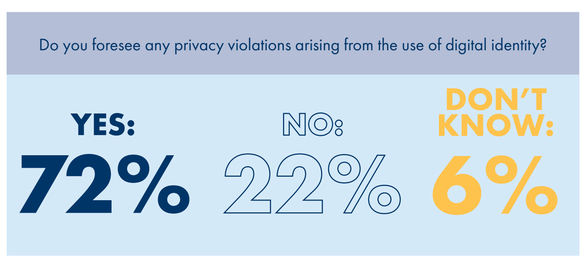


Most respondents (85%) believed there were protections in place to limit access to the digital trail of personally identifiable information created through the use of digital identity by both the private and state sectors.



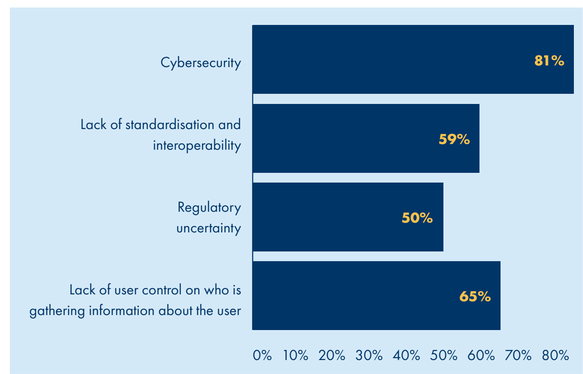
7) PRIVACY VIOLATIONS ARISING FROM THE USE OF DIGITAL IDENTITY SERVICES

Three-quarters of respondents foresaw privacy violations arising from the use of digital identity, while a quarter disagreed (22%), indicating different opinions on the risk of privacy.

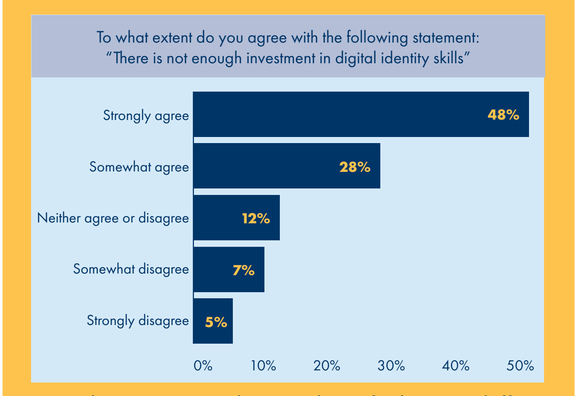


8) CHALLENGES IMPACTING THE ADOPTION OF DIGITAL IDENTITY SERVICES IN SOUTH AFRICA

The greatest challenge to the adoption of digital identity was seen as cybersecurity (81%), with lower ratings for lack of user control on who is gathering information on the user (65%) and lack of standardisation and interoperability (59%). Regulatory uncertainty (50%) was considered the lowest challenge.



IN CONCLUSION



- There is a moderate digital identity skills gap in South Africa;
- Organisations need to invest in skills development, offer competitive packages and foster a diverse and inclusive work environment;
- The Certified Information System Security Professional (CISSP) qualification was the most (76%) sought-after certificate, with a quarter (24%) reporting the NIST Cyber Security Framework;
- Identity and access management technical skill was valued the highest (81%) and architecture design technical skills were valued lowest at 51%;
- A range of future skill requirements were put forward by respondents, the highest being artificial intelligence and machine learning (74%), followed by digital identity for devices and applications (64%); and
- A lower proportion (70%) felt there were adequate mechanisms to address exclusion from digital identity systems.

science & innovation
Department:
Science and Innovation
REPUBLIC OF SOUTH AFRICA

For more information, visit **www.csir.co.za**

CSIR
Touching lives through innovation