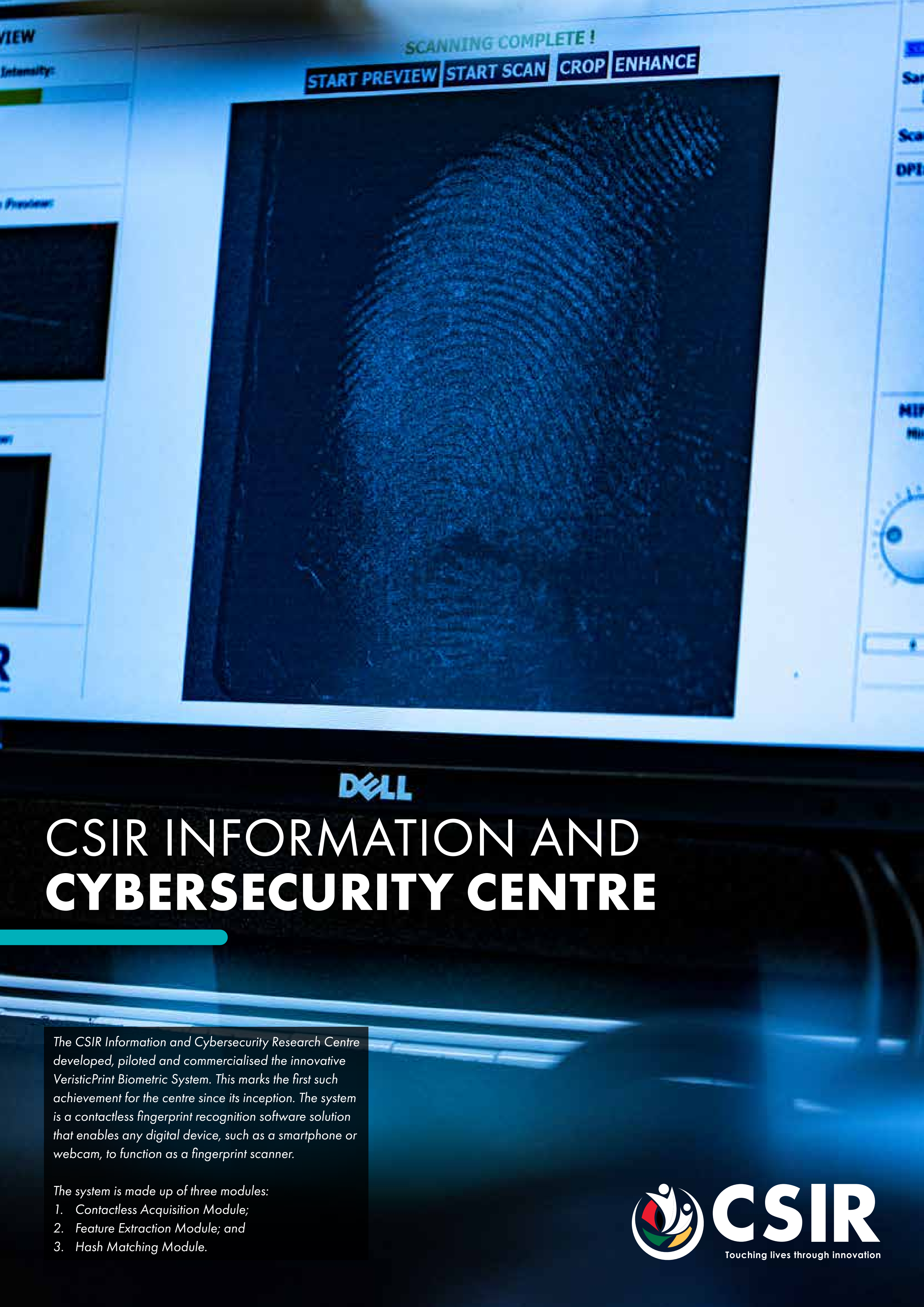


CSIR INFORMATION AND **CYBERSECURITY CENTRE**

The CSIR Information and Cybersecurity Research Centre developed, piloted and commercialised the innovative VeristicPrint Biometric System. This marks the first such achievement for the centre since its inception. The system is a contactless fingerprint recognition software solution that enables any digital device, such as a smartphone or webcam, to function as a fingerprint scanner.

The system is made up of three modules:

1. *Contactless Acquisition Module;*
2. *Feature Extraction Module; and*
3. *Hash Matching Module.*

CSIR
Touching lives through innovation

ABOUT THE CSIR INFORMATION AND CYBER SECURITY RESEARCH CENTRE

Established in 2019, the CSIR Information and Cyber Security Research Centre is a consolidation of all CSIR research and development (R&D) capabilities in cybersecurity, information security and identity authentication. These capabilities were developed over decades of working for the Department of Defence and, over the last ten years, for government departments and agencies, such as the Department of Communications and Digital Technologies, state-owned enterprises and private sector players.

The centre aims to support industry, contribute to an efficient, secure and capable state and grow cybersecurity capacity and capabilities in the country. It also develops systems and solutions that are relevant to the local context and makes them available for commercialisation, which is in line with CSIR's strategic focus on industrialisation.

The CSIR has a recognised track record locally and abroad, based on its work with and support for numerous stakeholders and institutions. Since the nineties, as cyberspace became everyone's playground, several technologies were brought to local users. These include antivirus software and an early warning detection system for small businesses encompassing both software and hardware components. A major achievement was a CSIR-developed encryption solution (encoder/decoder) that led to the creation of the pay-TV giant M-Net.

Innovation is homegrown. Initiated by the CSIR and collaborators in the public and private sectors, test and evaluation platforms and cybersecurity educational and training packages have been prototyped, and some have been implemented in operational environments.

With significant experience in R&D, product innovation and capability development, the CSIR is well positioned to lead the building of a robust, agile and formidable national cybersecurity capability and capacity, as well as to foster innovation for a thriving future industry.

The centre's focus areas are:

- Securing ICT systems;
- Combating cybercrime;
- Cyberwarfare;
- Identity management;
- Awareness and human capital development
- Governance, risk and compliance, and
- Embedded security.

www.csir.co.za

FOREWORD

Local is best: Why home-grown technologies and capabilities are needed to advance South Africa's cybersecurity technology sovereignty

In an era where digital transformation is exponentially accelerating, cybersecurity has become a dominant concern worldwide. As the digital landscape evolves, so do the threats that target critical infrastructure, sensitive data, personal information and national security. Against this backdrop it is of paramount importance for nations to focus on the development of home-grown cybersecurity technologies and capabilities to gain – and retain - strategic advantage. The CSIR's Information and Cybersecurity Centre, through the support and partnerships with state entities such as the South African Department of Science and innovation (DSI), is investing in the development and nurturing the nations' local cybersecurity capabilities. Centre Manager, Dr Jabu Mtsweni and his team have crystalised the levers and target interventions to drive this mission.

SOVEREIGNTY AND NATIONAL SECURITY

Relying on foreign technologies can expose a country to significant vulnerabilities as these can have backdoors or hidden vulnerabilities that adversaries can exploit. By developing home-grown technologies, countries can maintain absolute control over their critical systems and data. Thus, ensuring that security measures align with national interests and are free from external interests.

CUSTOMISATION AND ADAPTABILITY

Every nation has unique cybersecurity needs based on its specific threat landscape, regulatory environment and infrastructure. Home-grown technologies allow for greater customisation and adaptability to meet these specific local requirements.

ECONOMIC BENEFITS AND JOB CREATION

Investing in the development of home-grown cybersecurity technologies and capabilities has significant benefits in terms of fostering the growth of local technology industry, creating jobs, and stimulating innovation.

A critical element is building a skilled national workforce capable of developing advance cybersecurity solutions – now and in the future.

Not only supplying to local need, development of technologies for the export market opens new economic opportunities and global acclaim and competitiveness.

PROMOTING INNOVATION AND RESEARCH

Localising technology development drives innovation and research. Thus, encouraging academic institutions, research councils, public and private industries to invest in the development of advanced cybersecurity technologies and capabilities, pushing through to new levels of ingenuity.

WHAT ROLE DOES THE CENTRE PLAY IN THESE OBJECTIVES?

The CSIR's Information and Cyber Security Centre, through the support provided by the Department of Science and Innovation, has embarked on R&D themes that resonate with these goals and focus capability development in areas such as authentication, detection and analysis, and governance and legal compliance. These focal points include:

1. **Enabling integrated and secure identity authentication:** the development of integrated identity as a service capability for the public sector.
2. **ZeroTrust authentication:** building foundational capability to enable continuous and efficient authentication, validation, and authorisation of users and devices across trusted and untrusted networks.
3. **Threat landscape and situational awareness:** development of low-cost capabilities to enable contextual threat landscape and situational awareness using data security analytics supported by Artificial Intelligence/Machine Learning and other emerging technologies.
4. **Low-cost early warning threat detection:** development of low-cost algorithms, hardware, and software for early warning cyber threat detection.
5. **Formalising threat intelligence sharing** development of web-based threat intelligence sharing tools to enable the sharing of indicators of compromise.
6. **Toolkits for enhancing compliance to regulatory requirements:** enhancing the protection of personal information composed of diverse instruments and templates, and tools for promoting information and cybersecurity compliance to legal and regulatory requirements across different jurisdictions.

Successes in developing home-grown cybersecurity technologies is driven by collaboration and innovation. The CSIR works closely with academic institutions, industry partners, and government agencies to leverage diverse expertise and resources. This collaborative approach leads to a better understanding of emerging threats, and continuously evolution and improvement of responding solutions. Not least of which is the investment made in training and developing cybersecurity professionals, ensuring a sustainable pipeline of talent for the republic for the future.

All this in the interest of a safe cyber-SA.

By Dr Jabu Mtsweni
Dr Jabu Mtsweni, Head of the CSIR Information and Cyber Security Centre, CSIR Chief Researcher, NRF-Rated Researcher (C2), Certified Cybersecurity Manager, Research Fellow at the Stellenbosch University, Technical Leader of the National Policy Data Observatory; Member of the International Telecommunication Standards body (Study Group 7: cyber security. Recently honoured as one of top 50 Cybersecurity Professionals in South Africa, amongst his accomplishments.

YOUR IDENTITY IS **ON THE LINE**

In an age when lives and businesses are run in cyberspace, efficient identity management has become paramount. The CSIR's Secure Identity Systems research group is at the forefront of interventions to ensure and protect national identity-driven information security systems and infrastructure.

Many studies estimate that Africa will be the most populous continent by the end of this century. Presently, Africa ranks as the second most populous continent after Asia, with an approximate population of 1.5 billion people, projected to reach 4.2 billion people by the year 2100.

Given the substantial population growth, Africa is in need of infrastructure, organisations and systems to facilitate the development of its economies and upliftment of its people. One of the key capabilities crucial to the development of the African continent is identity management.

The CSIR dedicates itself to the national imperatives of building a capable state, ensuring the safety of citizens and communities, and contributing to the development of reliable and robust social and economic infrastructure. The primary focus of the Secure Identity Systems group is tackling technological challenges and delivering research, development and innovation interventions for identity authentication mechanisms that underpin service delivery, prevent crime and support personal and national security.

With identity-driven systems dominating the way people operate, robust authentication technologies are needed to safeguard online activity, protect identities and prevent fraud and theft. Protection on one side of the coin and effective detection on the other: Strong identity management capabilities allow authorities to track criminals more efficiently, reducing unauthorised immigration and its associated security threats.

CASE STUDY: ACCESS TO SOCIAL GRANTS

South Africa integrates social services and financial inclusion to enhance the lives of its citizens. People with a secure and verifiable identity can access financial services such as bank accounts and credit, thus contributing to the economy. However, some challenges in the social services sector require expert intervention.

Identity management is a cornerstone of service delivery. Using the Republic of South Africa as an example, social services and financial inclusion are integrated to enhance the lives of its citizens. People with a secure and verifiable identity can access financial services such as bank accounts and credit, thus contributing to the economy. However, some challenges in the social services sector require expert intervention.

For instance, grant payment systems rely on fingerprints to link each client to a unique identity. The fingerprints of new grant applicants are compared against those of existing clients. A grant application is only processed after determining that the applicant's prints do not match those of any other client in the system.

This is in response to past identity-based social grant fraud, where one person succeeded in applying for more than one social grant using different identities, and multiple people applied for child support grants for the same child using different identities. However, challenges arise in comparing fingerprints, particularly with children, as existing fingerprint scanners have difficulty capturing good-quality fingerprints, especially those of newborns and infants. The prevalence of fraudulent payouts will only be solved with technology capable of capturing infant biometric characteristics.

WHY *"IDENTITY FROM THE CRADLE TO THE GRAVE"* IS OUR MANTRA

The CSIR develops biometric-based technologies that can be deployed to a myriad of applications, including access control, registration of individuals for the provision of services and improvement of the identification of children or minors. The group has created multimodal biometrics systems and multifactor authentication platforms to counter cyberattacks on identity systems.

In addition to working with individuals, they also focus on livestock identification and traceability systems.

The organisation has also developed technology to read the biometric measurements of cadavers by detecting subdermal minutia. Currently in use at selected government morgues, the technology assists in dealing with a backlog of unclaimed deceased individuals.

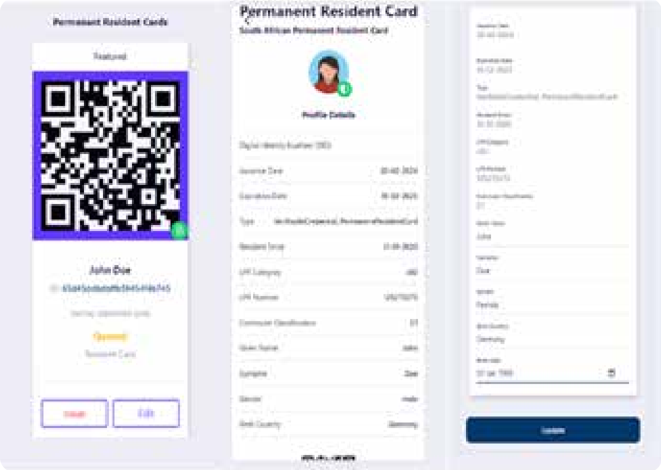
Furthermore, with the rapid digitisation of consumers' lives and enterprise records, along with the associated risk of breaches, the CSIR is developing decentralised digital identity systems that can be used across enterprises. This would limit data exposure to cyberattacks and give users control over their data.

The CSIR aims to assist African countries by strengthening research, development and innovation in identity management. Researchers are developing an identity management capability that aims to support a capable state through the implementation of robust authentication technologies for security and crime prevention. With effective identity management, the state can verify the identities of persons, thereby minimising unauthorised immigration and potential security threats. Furthermore, a strong identity management system makes it harder for criminals to steal identities and commit fraud, protecting citizens from financial loss and identity theft. In the context of digitalisation of identity management, the CSIR possesses emerging capabilities, such as:

Decentralised digital identity

The rise of the internet and the fourth industrial revolution has led to a new era of "digital identities" which enables ease of digital identification, authentication, verification and authorisation. Digital identity is the unique and detailed digital representation of a subject in the form of attributes and credentials for digital services. In today's digital and interconnected world, the ability to issue, use and verify users' identity attributes online is crucial.

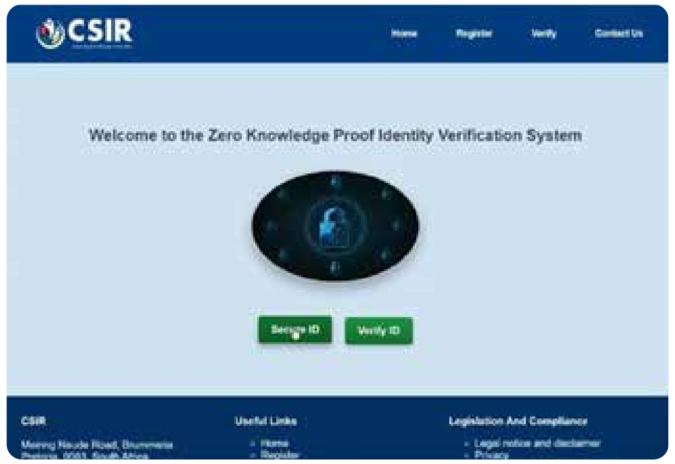
As service delivery becomes increasingly digital, dependent on digital identities, individuals, governments, businesses and other organisations must trust the correctness and integrity of the information or identity shared with them. Governments and public and private sector organisations worldwide are working towards employing digital identities for service delivery and developing frameworks to promote trusted environments online or when using digital identities (to promote cross-border usage).



Zero-knowledge proofs

The CSIR is developing an identity theft prevention technology that allows individuals to prove their identity without revealing sensitive information, such as their identity number, based on zero-knowledge proofs (ZKP). ZKP are a set of methods that allow one party (the 'prover') to convince another party (the 'verifier') that a statement is true, without revealing any information beyond the statement's truthfulness, using cryptography. The developed proof of concept is aimed at curbing identity fraud around key credentials.

For the proof of concept, a user is required to enter their full names and identity number to register. This information is processed, and proofs are generated and stored for later verification. Proofs, in the form of a PDF token, are sent via email for demonstration purposes. This token does not display sensitive information but will be used later to verify the individual's identity.


Welcome to the Zero Knowledge Proof Identity Verification System
CSIR
Home
Register
Verify
Contact Us
Secure ID
Verify ID
CSIR
Meiring Naude Road, Brummeria
Pretoria, 0083, South Africa
Useful Links
Home
Register
Legislation And Compliance
Legal notice and disclaimer
Privacy

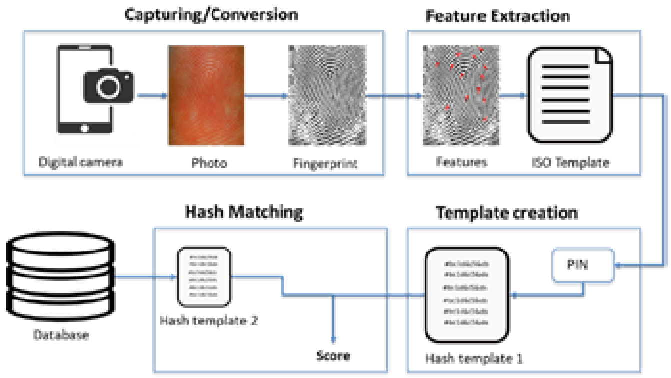
Hardware agnostic biometrics - VeristicPrint

The World Association of Telecoms Operators usually ranks African countries by the ability to connect their citizens to the mobile internet and compares them to the rest of the world. The association uses factors such as infrastructure, prices of mobile devices and packages, the degree of predisposition of non-connected citizens to learn new skills or cultures or political environments, as well as content to rank countries. The African continent has been shown to have potent potential on these factors. This means that a mobile device will be very critical to the socioeconomic life of Africans.

The CSIR has developed VeristicPrint (VP), a technology which aims to unlock service delivery on the African continent by employing contactless biometrics to authenticate individuals so that they can access a service. This innovative solution has implemented fingerprint biometrics on mobile devices, which are ubiquitous in Africa. The technology can be used by small, medium and micro enterprises (SMMEs) and large corporations for mobile, on-the-fly verification of identity so that services can be provided with less fraud, waste or non-compliance to KYC processes. This is possible because the technology eliminates any hardware needs, such as fingerprint scanners and replaces them with a mobile device to verify or identify people.

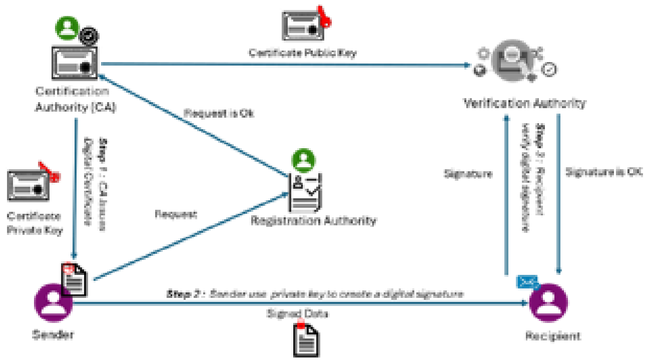
This very act also makes VP one of the most important ingredients to the forthcoming digital identity. This is because biometrics are a critical credential in digital identity and VP already puts fingerprints on mobile phones for seamless integration with service provision. One of the key tenets of digital identity is self-sovereignty over identity credentials.

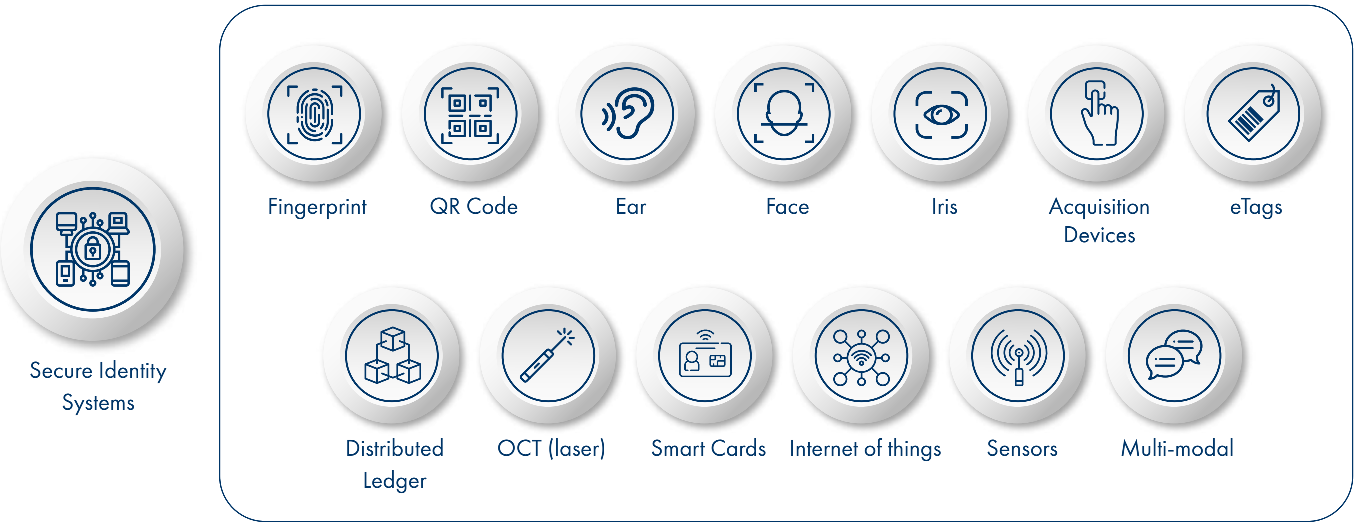
VeristicPrint is composed of a module to convert a picture captured by a mobile device into a fingerprint image, a module to extract features to be used for matching, and a module that matches features only after they have been hashed; thus, fingerprint images are not stored.

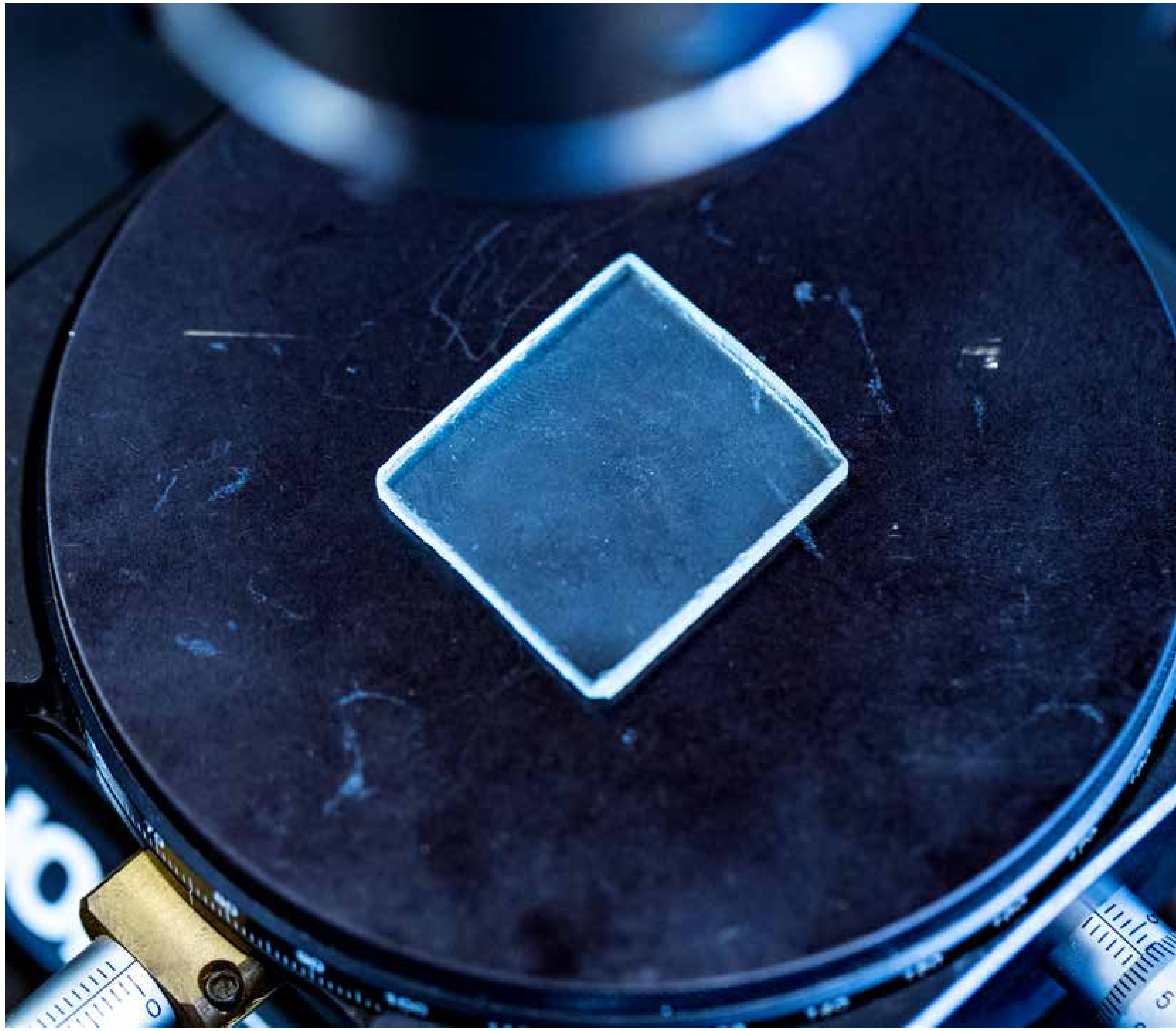


Public key infrastructure

The CSIR has conducted a landscape study in the Republic of South Africa, which revealed that the South African government has established a public key infrastructure aimed at augmenting the security of electronic communications and transactions. This infrastructure presently supports a range of applications, including secure email, digital signatures and encryption, which are critical for maintaining the integrity and confidentiality of data.


Certificate Public Key
Certification Authority (CA)
Verification Authority
Request is Ok
Step 1 : CA issues Digital Certificate
Certificate Private Key
Request
Registration Authority
Signature
Step 3 : Recipient verify digital signature
Signature is OK
Step 2 : Sender use private key to create a digital signature
Signed Data
Sender
Recipient





SELECTED RESEARCHERS

ICSC RESEARCHERS PROFILES

Researcher Profile:

Dr NNP Mkuzangwe

Dr Nenekazi holds a PhD in electrical and electronic engineering from the University of Johannesburg and an MSc in mathematical statistics from Rhodes University. She obtained her first degree in 2001. She has taught mathematical statistics/statistics to science, commerce and health science students at Nelson Mandela University. Nenekazi joined the CSIR in August 2013 under a PhD Studentship Programme and was permanently employed as a network and data security researcher in January 2018. In July 2020, Nenekazi joined the CSIR's Data Security and Analytics research group.

Research Interests: Predictive modelling, intrusion detection, data security/privacy

Masters Students:

4. Currently mentoring Hombakazi Ngenjane. Digital Forensics Supported by Machine Learning for the Detection of Online Sexual Predatory Chats.

She has mentored university students in applying statistics-based machine learning techniques to analyse real-life data to inform decision-making in a project called "Data Science for Impact and Decision Enablement," sponsored by the Department of Science and Innovation. She has reviewed an international journal article in the field of intrusion detection.

Researcher Profile:

Dr Moses Dlamini

Dr Moses Dlamini is a senior researcher with a focus on information security, cybersecurity, cloud computing security, security of the internet of things, securing artificial intelligence and machine learning classification models, security of operational technology and industrial control systems, securing industry 4.0, digital deception, context-aware and behavioural authentication, privileged access management, identity and access management, conflict-aware access control, digital forensics and chaos-based cryptography.

Dlamini publishes his research work both in both national and international forums. He is also a reviewer of several information security and privacy journals and conferences. He is passionate about technology that serves the needs of society and industry.

He holds a PhD in computer science (2020), an MSc in computer science (2010) and a BSc Hons. in computer science (2007), all from the University of Pretoria. He also obtained a BSc in computer science and mathematics from the University of Swaziland (2002)

Research Interests: Information and cyber security analytics, detection and prevention of adversarial artificial intelligence and machine learning attacks, design of future-proof and zero-trust cybersecurity architectures, detection of digital deception and fourth industrial revolution security. Cybersecurity governance, cybersecurity culture, security awareness, training and education.

Researcher Profile:

Sipho Ngobeni

Sipho Ngobeni is a senior researcher and plays a leading role in assisting industry and government in developing and implementing cybersecurity governance instruments (strategies, policies, processes, procedures, frameworks and standards), cybersecurity assessments, security configuration reviews, threat modelling and operationalising computer security incident response teams. He has authored and co-authored numerous peer-reviewed papers.

Ngobeni holds an MSc in computer science from the University of Pretoria (2016), a BSc Hons. in computer science from the University of Zululand (2007) and a BSc in computer science from the University of Zululand (2006).

Research Interests: Cybersecurity governance, cybersecurity assessments and audits, data privacy and protection, digital forensics and security operations.

Researcher profile:

Rethabile Khutlang

Rethabile Khutlang's interests are biological image analysis, exemplar and latent fingerprint acquisition and 3D image analysis using optical coherence tomography. Khutlang has a master's degree in biomedical engineering from the University of Cape Town. His experience at the CSIR includes working as a biological and biometrics engineer. Khutlang leads teams working on embedded tokens, data analytics platforms, fingerprint analysis software development kits and a biometrics suite platform. He also leads a team using OCT to address fingerprint spoofing, usage of fingerprints inside skin and lifting fingerprints none destructively from crime scenes.

Research interests: Image processing, machine learning, biometrics and data analysis

Researcher profile:

Dr Namosha Veerasamy

Dr Namosha Veerasamy is a senior cybersecurity researcher with a demonstrated history of working in the research industry. She is skilled in management, networking, security, cyber awareness, and cyber defence.

Her qualifications include a BSc in it computer science, a BSc Hons. in computer science (Honours), an MSc in computer science (with distinction) and a PhD in Computer Science. She is also a Certified Information System Security Professional (CISSP) and a Certified Information Security Manager (CISM).

Research interests: Financial technology threats, cybersecurity policy, cybersecurity skills assessment, cybersecurity awareness creation and the knowledge of cyber threats.

Researcher profile:

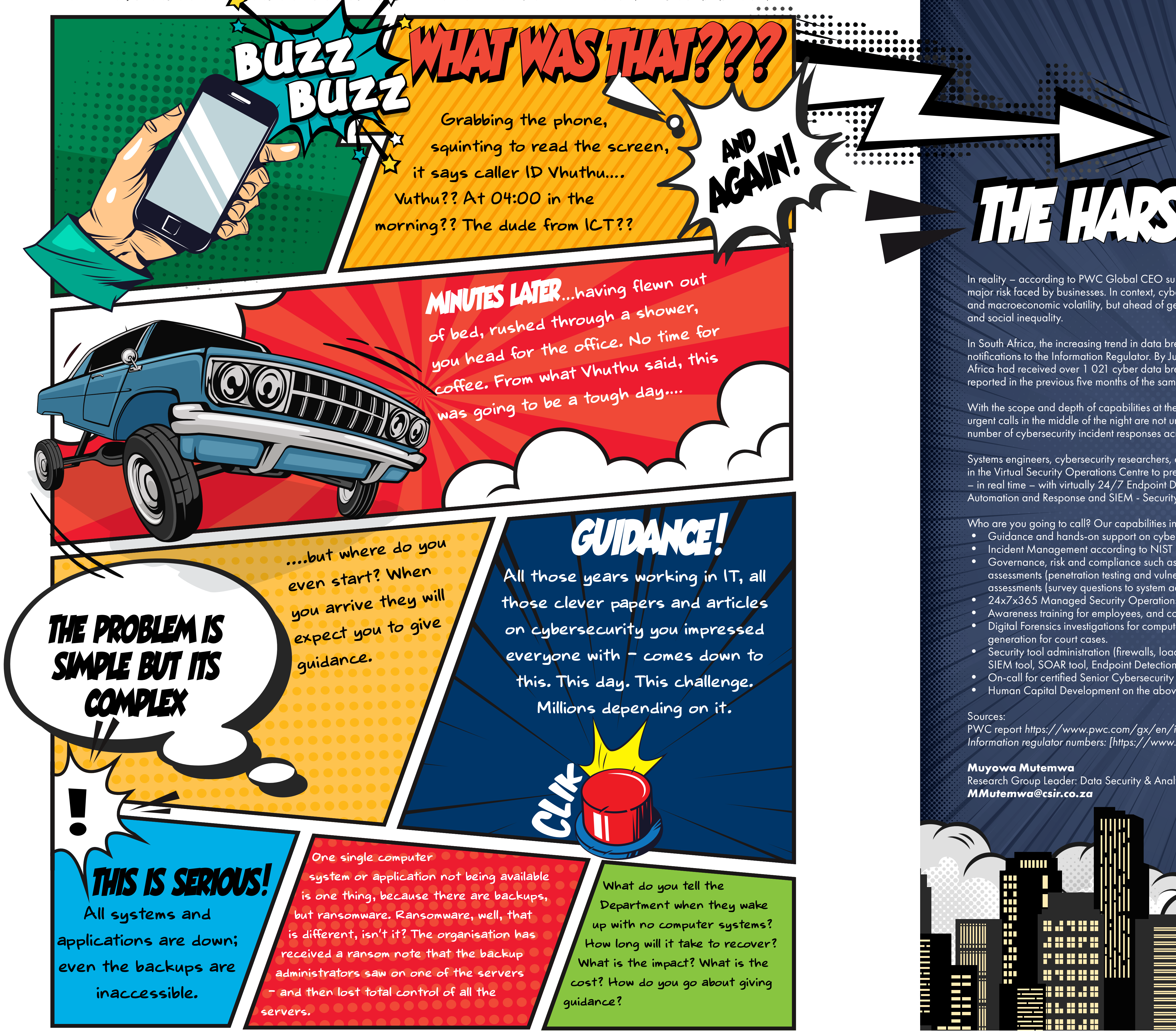
Dr Andre Mcdonald

Dr Andre McDonald is an experienced technology specialist with a demonstrated history of working in the research industry—a strong professional skilled in dynamical systems, chaos theory, signal processing, information theory and cybersecurity.

He holds a BEng in Computer Engineering, a BEng Hons. and a MEng in electronic engineering.

Research interests: Dynamical systems, chaos theory, signal processing, information theory and cybersecurity.

DO YOU HAVE WHAT IT TAKES TO BE A CYBER WARRIOR?


BUZZ BUZZ
WHAT WAS THAT???
Grabbing the phone, squinting to read the screen, it says caller ID Vhuthu.... Vuthu?? At 04:00 in the morning?? The dude from ICT??
AND AGAIN!
MINUTES LATER...having flewn out of bed, rushed through a shower, you head for the office. No time for coffee. From what Vhuthu said, this was going to be a tough day....
THE PROBLEM IS SIMPLE BUT ITS COMPLEX
....but where do you even start? When you arrive they will expect you to give guidance.
GUIDANCE!
All those years working in IT, all those clever papers and articles on cybersecurity you impressed everyone with – comes down to this. This day. This challenge. Millions depending on it.
CLIK
!
THIS IS SERIOUS!
All systems and applications are down; even the backups are inaccessible.
One single computer system or application not being available is one thing, because there are backups, but ransomware. Ransomware, well, that is different, isn't it? The organisation has received a ransom note that the backup administrators saw on one of the servers – and then lost total control of all the servers.
What do you tell the Department when they wake up with no computer systems? How long will it take to recover? What is the impact? What is the cost? How do you go about giving guidance?

THE HARSH REALITY

In reality – according to PWC Global CEO survey report of 2024 – cyber risks are the third major risk faced by businesses. In context, cyber risks to organisations are only behind inflation and macroeconomic volatility, but ahead of geopolitical conflict, climate change, health risks, and social inequality.

In South Africa, the increasing trend in data breaches is also observed through breach notifications to the Information Regulator. By June 2023, the Information Regulator in South Africa had received over 1 021 cyber data breach notifications - double the number that was reported in the previous five months of the same year

With the scope and depth of capabilities at the CSIR Information and Cyber Security Centre, urgent calls in the middle of the night are not unusual as they are called upon to assist with a number of cybersecurity incident responses across South Africa every year.

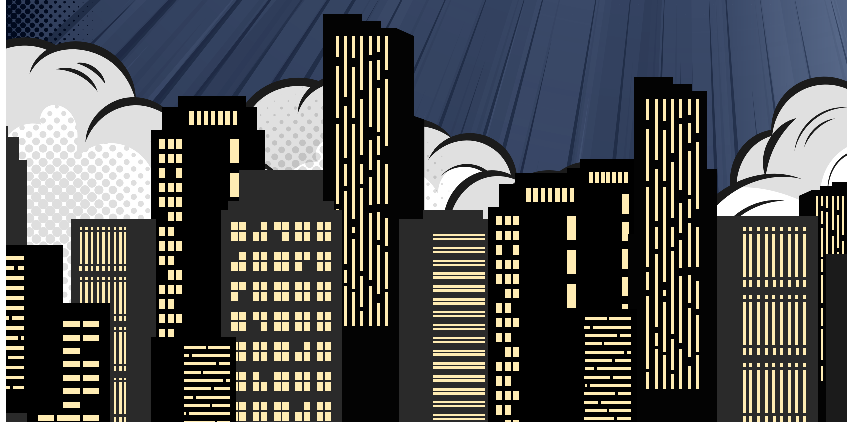
Systems engineers, cybersecurity researchers, analysts and cybersecurity engineers operate in the Virtual Security Operations Centre to prevent or manage critical cybersecurity threats – in real time – with virtually 24/7 Endpoint Detection and Response, Security Orchestration, Automation and Response and SIEM - Security Information and Event Management.

Who are you going to call? Our capabilities include:

- Guidance and hands-on support on cybersecurity incident response.
- Incident Management according to NIST SP 800-61.
- Governance, risk and compliance such as policies, procedures, quantitative risk assessments (penetration testing and vulnerability assessment) and qualitative risk assessments (survey questions to system administrators).
- 24x7x365 Managed Security Operations Centre according to NIST SP 800-137.
- Awareness training for employees, and contractors.
- Digital Forensics investigations for computers, servers, mobile phone, emails, and report generation for court cases.
- Security tool administration (firewalls, load balancers, internet proxy, email gateway, SIEM tool, SOAR tool, Endpoint Detection & Response, and so on).
- On-call for certified Senior Cybersecurity Professionals.
- Human Capital Development on the above services.

Sources:
PWC report *https://www.pwc.com/gx/en/issues/c-suite-insights/ceo-survey.html*
Information regulator numbers: [https://www.itweb.co.za/content/j5alrMQAJOQMpYQk].

Muyowa Mutemwa
Research Group Leader: Data Security & Analytics
MMutemwa@csir.co.za



CONTACTS

DR JABU MTSWENI

Head of the Information and Cyber Security Centre
JMtsweni@csir.co.za
+27 12 841 4394

SIPHO NGOBENI

Research Group Leader: Governance, Privacy and Trust
SNgobeni@csir.co.za
+27 12 841 5018

BILLY PETZER

Research Group Leader: Cybersecurity Systems
BPetzer@csir.co.za
012 841 7313

RETHABILE KHUTLANG

Research Group Leader: Secure Identity Systems
rkhutlang@csir.co.za
012 841 2257

MUYOWA MUTEMWA

Research Group Leader: Data Security and Analytics
mmutemwa@csir.co.za
012 842 7326

CSIR
Touching lives through innovation