datacentrix

Cracking the code of identity security with electronic DNA

By Rainer Jeske Consultant at Datacentrix

In the digital age, an individual's identity serves as a cornerstone for engagement with society, governance and digital services. However, with the evolution of technology, identity has also become a double-edged sword – empowering citizens and organisations, but also providing opportunities for cybercriminals to exploit vulnerabilities and wreak havoc.

Thus, you could say that a person's identity has become a critical currency in the digital era. Not only is it used by the individual to gain access to services and by organisations to manage systems and processes, but stolen identities are also being used by criminals to enter through secure gateways, compromise systems and defraud payrolls.

In the face of increasingly intelligent cybercrime syndicates, securing identity has become a matter of national security. Organisations face the complex task of validating and confirming the identities of all staff members against employee records and payroll systems. In distributed environments – where employees may be spread out across country, with some even in rural areas – this presents a significant challenge.

How then does the business manage the vast spread of identities and individuals? How can it keep track of a growing employee headcount with any form of accuracy?

Providing a failsafe with Datacentrix's eDNA

An electronic fraud management solution, like Datacentrix's electronic DNA (eDNA) system, can provide organisations with a barrier to these potential threats. The eDNA architecture ensures that organisations can benefit from positively identified users.

This type of solution provides companies with a single, consistent approach to access and application security, as well as transaction-level accountability across the organisation and its platforms, allowing for the protection of financial systems, personnel and payroll, procurement and other line of business applications.

The Datacentrix eDNA solution follows a nine-step authentication and trusted data management process to ensure that individual identities and data are secured.

> In the digital age, safeguarding identity isn't just a necessity – it's a strategic imperative.

Step one: Secure enrolment

Whether the challenge is to remove ghost workers, reduce fraudulent behaviour or digitally transform organisational security, one of the most important steps to take is ensuring that user enrolment – whether they are full-time employees, contractors, partners, executive directors or suppliers – is secure and accurate. A secure enrolment system should embed the same parameters across every individual and department. This not only ensures accountability across the chain of command and the entire organisation but also plays a significant role in preventing a future crime or attack.

To define positive identity, there are two methodologies that the organisation can use – face-to-face enrolment or self-enrolment. Each of these has benefits and disadvantages and their use case would depend on the size of the organisation, geographical spread, timelines and budgets.

Face-to-face enrolment is the most rigorous method of confirming a person's identity. The person is sitting directly opposite the enrolment officer, their ID card can be verified against them, and the right checks can be executed in person. However, it can be complex and lengthy for both the individual and the organisation, as well as costly should agents need to be deployed across diverse geographic locations.

Self-enrolment allows for the individual to provide the required documentation by following a clearly defined enrolment process. This can be tightly managed by technology solutions, such as biometrics, but self-enrolment is not as secure as face-to-face and can introduce a measure of risk.

Step two: User authentication

Within the secure enrolment process, eDNA embeds authentication with a three-factor approach. This encompasses the use of biometric fingerprinting or facial recognition systems that will only eDNA

The Datacentrix eDNA solution follows a nine-step authentication and trusted data management process

STEP 1 Secure enrolment

STEP 2 User authentication

STEP 3 A gateway to business applications

STEP 4 Define sensitive pages

STEP 5 Establish business rules

STEP 6 Sensitive page transactional security

STEP 7 Business and alert reporting

STEP 8 Forensic reporting services

STEP 9 Tamper-proof data

allow the specific user to gain access, a certified authority key (PKI) that is allocated to the biometrics of that specific user, and the installation of a smartcard that securely carries and matches the key and the biometrics.

This three-factor multi-layered authentication mechanism ensures access and transaction signing security, mitigating the risk of unauthorised system uses.

Step three: A gateway to business applications

In addition to the three-step user-authentication mentioned previously, a fourth factor is used to ensure guaranteed authentication – if the user logs on or transacts, then these three factors are tested for status and validity with the non-repudiated user details and the Public Key structure of the backend system.

Step four: Define sensitive pages

A sensitive page can be defined as any transaction taking place within the customer environment, not limited to the user login, the user enrolment, the employee verification and any logistical and financial customer transactions that constitute real value. All sensitive pages are defined and agreed upon in consultative workshops with the customer.

Step five: Establish business rules

eDNA facilitates the formulation of business rules tailored to track and monitor sensitive transactional data, enabling proactive threat detection and response. The main requirements to be fulfilled in setting up business rules include: a consultative customer workshop to define priority values of the business within the framework, which would most likely include security, governance, performance, renumeration and fraud scenarios; a definition of the customer system requirements; and the creation of sample eDNA report screens.

Step six: Sensitive page transactional security

In all instances, sensitive transactions constitute two pages – the information before the change was entered by the transacting user, and the information after the changes have been completed by the same user. Both pages / sensitive transactions are conducted through an eDNA signing process fortified with cryptographic measures, such as hashing, timestamping and encryption at the source, ensuring data integrity and confidentiality throughout the entire data chain: saving at source, transmission and backend system processes.

Step seven: Business and alert reporting

Harnessing the power of reporting services, eDNA incorporates a robust framework for business intelligence and alerting, enabling organisations to gain actionable insights and promptly respond to anomalous activities.

Step eight: Forensic reporting services

In the event of security incidents, eDNA empowers organisations with forensic reporting capabilities, producing legally admissible evidence to support investigations and judicial proceedings. This could include the three-factor authentication details of the user performing and signing the transaction.

A full non-repudiated validation of the complete authentication process and sealing of the data in the database is used to ensure that there was no tampering. This then creates and stores legally-compliant forensic evidence of transactional data in an ECT Act manner that can be forensically proven to be impartial and tamper-proof evidence that is fully accepted in all legal processing.

Step nine: Tamper-proof data

The final step of the eDNA process entails enforcing the highest standards of security across computing facilities, encompassing physical and logical safeguards, redundancy measures, and secure data storage protocols. By sealing data at its source and leveraging secure network infrastructure, organisations fortify their defences against tampering and data breaches.

In the digital age, safeguarding identity isn't just a necessity – it's a strategic imperative.

Electronic DNA can prove to be a formidable ally in the battle against identity theft, cybercrime, and data breaches. By embracing Datacentrix's eDNA offering, organisations can embark on a journey towards fortified identity security, trusted data transmission, and resilience in the face of evolving cyber threats.

For more information on Datacentrix's eDNA offering, please contact Rainer Jeske by emailing rjeske@datacentrix.co.za