Mitigating Cybersecurity Threats in Smart Metering Infrastructure Through Standard Security Frameworks

Author & Presenter: K. S Papi – Senior Advisor
Eskom Research, Testing & Development Business Unit

SUMMARY

Smart metering enhances efficiency and control but also creates new cyber risks, evident in recent ransomware incidents and prepaid fraud. Attackers may trigger mass remote disconnections or manipulate prepaid tokens. The DLMS/COSEM[1] standard offers tested safeguards – encryption, authentication, access control and secure updates – that directly mitigate these threats. For South Africa's fragmented distribution sector (a national utility and about 160 municipalities), adopting DLMS/COSEM with a shared PKI would reduce costs, simplify operations and improve resilience. We recommend that the South African Electricity Supply Industry (ESI) considers the adoption of a standardised security framework in line with international best practice to secure present and future deployments of smart metering infrastructure.

KEYWORDS

Smart metering, cyber security, DLMS/COSEM

[1] DLMS/COSEM is an international smart metering standard for data modelling and exchange, published in the IEC 62056 series (including IEC 62056-5-3, 62056-6-1 and IEC 62056-6-2) and maintained by the DLMS User Association.

1 INTRODUCTION

Smart electricity metering is expanding rapidly in South Africa to strengthen revenue collection and grid management [1]. The national distribution network is supplied by Eskom together with numerous municipal distributors, creating a fragmented landscape. Interoperability across this fragmented system is critical: open standards allow different meters and head-end systems to communicate securely, while enabling shared national platforms for key management, PKI certificates and security updates. DLMS/COSEM, an internationally recognised IEC 62056 suite used by meter vendors worldwide, includes a security framework with AES-GCM encryption, ECDSA digital signatures and device authentication tailored to smart metering data exchanges [2]. A common framework would let South African utilities pool resources such as certificate authorities, revocation lists and training across Eskom and municipalities, reducing per-meter security costs and simplifying infrastructure management.

2 CYBERSECURITY THREAT IN SMART METERING

Smart meters' two-way functions introduce new cyber and insider risks [3]. South African utilities have seen real breaches, including ransomware outages affecting hundreds of thousands of customers and insiders exploiting prepaid token systems. Threats range from dishonest consumers and employees to sophisticated actors who could trigger unauthorised disconnections, alter meter settings, or inject false data. Remote disconnect commands and token hijacking are key vulnerabilities. Robust confidentiality, integrity and authentication measures across meters, networks and head-ends are essential to prevent theft, outages and billing errors.

3 BENEFITS OF OPEN STANDARDS

Using open, consensus-driven standards is crucial in South Africa's mixed-distributor context. Open standards provide a vendor-neutral secure data exchange across diverse devices and systems. By contrast, proprietary systems often lock municipalities into a single vendor and complicate inter-agency data sharing. A common standard means that Eskom and all municipal utilities can potentially share a unified security backbone: for example, establishing one national public key infrastructure (PKI) for meter authentication and one certificate authority for meter and head-end systems. This shared infrastructure reduces duplication of effort and cost (fewer separate license fees, one training program, etc.) and allows economies of scale in procurement and updates.

4 DLMS/COSEM - AN OPEN STANDARD

DLMS/COSEM was designed with interoperability in mind. It explicitly defines mechanisms for securing each application association and each message. For instance, DLMS Application Associations use mutually authenticated keys and protect data with AES-GCM encryption and AES-based hashing. These interoperable security services enable meters from different vendors (and even different meter technologies, e.g. electricity and water) to communicate on a common secure model [5]. In practical terms, a DLMS-compliant meter can be swapped between systems (Eskom or municipal) without re-engineering the security. Moreover, DLMS supports layered protection: for example, administrative messages (like firmware updates) can use separate keys or digital signatures (ECDSA) independent of measurement data. This flexibility lets utilities tailor end-to-end security to local needs while still following one agreed framework [4].

Taken together, interoperable DLMS/COSEM standards mean that South African utilities need not each build their own key management or PKI systems. Instead, they can join a single national system to issue meter certificates, revoke lost devices, and coordinate encryption keys. Such coordination improves manageability and is explicitly advocated by international guidelines. For example, NISTIR 7628 (US Smart Grid security guidelines) [5] and IEC smart grid standards [6] highlight the value of centralized credential management for smart metering infrastructure to mitigate rogue-device threats.

Table 1 (below) illustrates how specific DLMS/COSEM features mitigate common AMI attack scenarios. DLMS's layered security is engineered for threats at each point of the system:

Table 1 : DLMS security mapping

Threat	DLMS Security feature
Unauthorized Meter Access / Command Injection	DLMS requires each client–meter association to be secured by authentication and encryption. The DLMS “Security Suite” (e.g. AES-GCM) ensures confidentiality and integrity of every request/response. Any attempt to impersonate a meter or issue commands (e.g. remote switchovers) will fail without possession of the correct keys. The IEC 62056-5-3 standard enforces this by defining separate master keys for different meter functions.
Replay Attacks / Brute Forcing:	DLMS messages include invocation counters and/or nonce fields. Meters track counters so that re-sending an old command is detected and dropped. In addition, DLMS “Communication Port Protection” objects limit the number of bad authentication attempts and time-lock the interface after several failures]. This defeats rapid brute-force tries on meter logins.
False Data Injection	DLMS’s authenticated encryption also protects measurement data. Any modification of payloads in transit is detected at the meter or head-end by checking the AES-GCM tag. Since DLMS typically encapsulates meter readings and time stamps in the protected message, MITM changes are effectively neutralized.
Malicious Firmware Updates	DLMS includes a secure “Image Transfer” object. New firmware is cryptographically signed and then verified in a two-phase load/activate process. A rogue update cannot be accepted because the meter checks its signature before activation.
Logging and Audit	DLMS meters maintain security logs of connections, cipher failures, and abnormal events. These logs (stored in COSEM Generic/Profile objects) allow utilities to detect, for example, repeated authentication failures or unexplained resets, providing forensic visibility.
Physical Tampering / Meter Fraud	Even if an attacker physically captures a meter, DLMS’s reliance on stored keys and challenge-response (rather than static codes) prevents fake token generation. Unlike meter security mechanisms, DLMS caters for the use of symmetric keys and counters in each meter. Manipulating a meter’s credit register would require circumventing its AES engine – a far higher barrier.

In summary, DLMS/COSEM’s security framework directly mitigates the vulnerabilities seen in recent utility incidents, when correctly implemented by meter vendors and operators.

5 REGULATORY INTERGRATION

To realise these benefits, we recommend embedding standards-based security frameworks into South African regulations and standards. NERSA's Distribution Code could explicitly require that deployed smart meters support encryption and authentication.

Internationally, regulators are moving in this direction. The EU Cyber Resilience Act classifies smart meters as critical products requiring certified security [7], complementing the NIS2 Directive which obliges utilities to report incidents and implement risk management [8]. In the US, NISTIR 7628 [9] set comparable standards, requiring robust privacy and security controls for smart meters. South Africa can follow suit by explicitly referencing security standards in electricity metering regulations.

6 CONCLUSION

South Africa's ambitious smart meter rollout must be matched by robust cybersecurity. Established standards like IEC 62056 (DLMS/COSEM) provide a practical defence-in-depth against AMI threats. By adopting interoperable DLMS security features, utilities can cost-effectively share a national PKI and avoid vendor lock-in, while mitigating risks such as unauthorised disconnects, data tampering, and fraudulent tokens. International precedents, including the EU Cyber Resilience Act and US NISTIR 7628 rules, show how policy can drive secure smart meter deployment. Coordinated adoption of standard security frameworks will allow South Africa to reduce smart meter cyber risk while safeguarding the reliability of the national grid in the digital era.

7 REFERENCES

[1] itweb, "www.itweb.co.za," 4 September 2025. [Online]. Available: https://www.itweb.co.za/article/national-treasury-forges-ahead-with-r2bn-smart-meter-rollout/kYbe97Xbg4pqAWpG. [Accessed 9 September 2025].

[2] DLMS User Association, "Security Framework in DLMS/COSEM: Ensuring Data Protection and System Integrity," Zug, 2023.

[3] S. Tweneboah-Koduah, A. K. Tsetse, J. Azasoo and B. Endicott-Popovsky, "Evaluation of cybersecurity threats on smart metering system.," in *In Information technology-new generations: 14th international conference on information technology*, Springer International Publishing., 2017, pp. 199-207.

[4] International Electrotechnical Commission, "IEC 62056-5-3 Electricity metering data exchange - The DLMS/COSEM suite - Part 5-3: DLMS/COSEM application layer," 2023.

[5] The Smart Grid Interoperability Panel–Smart Grid Cybersecurity Committee, "NIST IR 7628 Rev. 1 Guidelines for Smart Grid Cybersecurity," NIST, 2014.

[6] International Electrotechnical Commission, "IEC 62351-9 Power systems management and associated information exchange - Data and communications security - Part 9: Cyber security key management for power system equipment," 2023.

[7] European Parliament, "EU Cyber Resilience Act," 2024.

[8] European Union, "DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL," 2022.

[9] National Institute of Standards and Technology, "NISTIR 7628 Guidelines for Smart Grid Cyber Security (Vols. 1-3)," 2010.