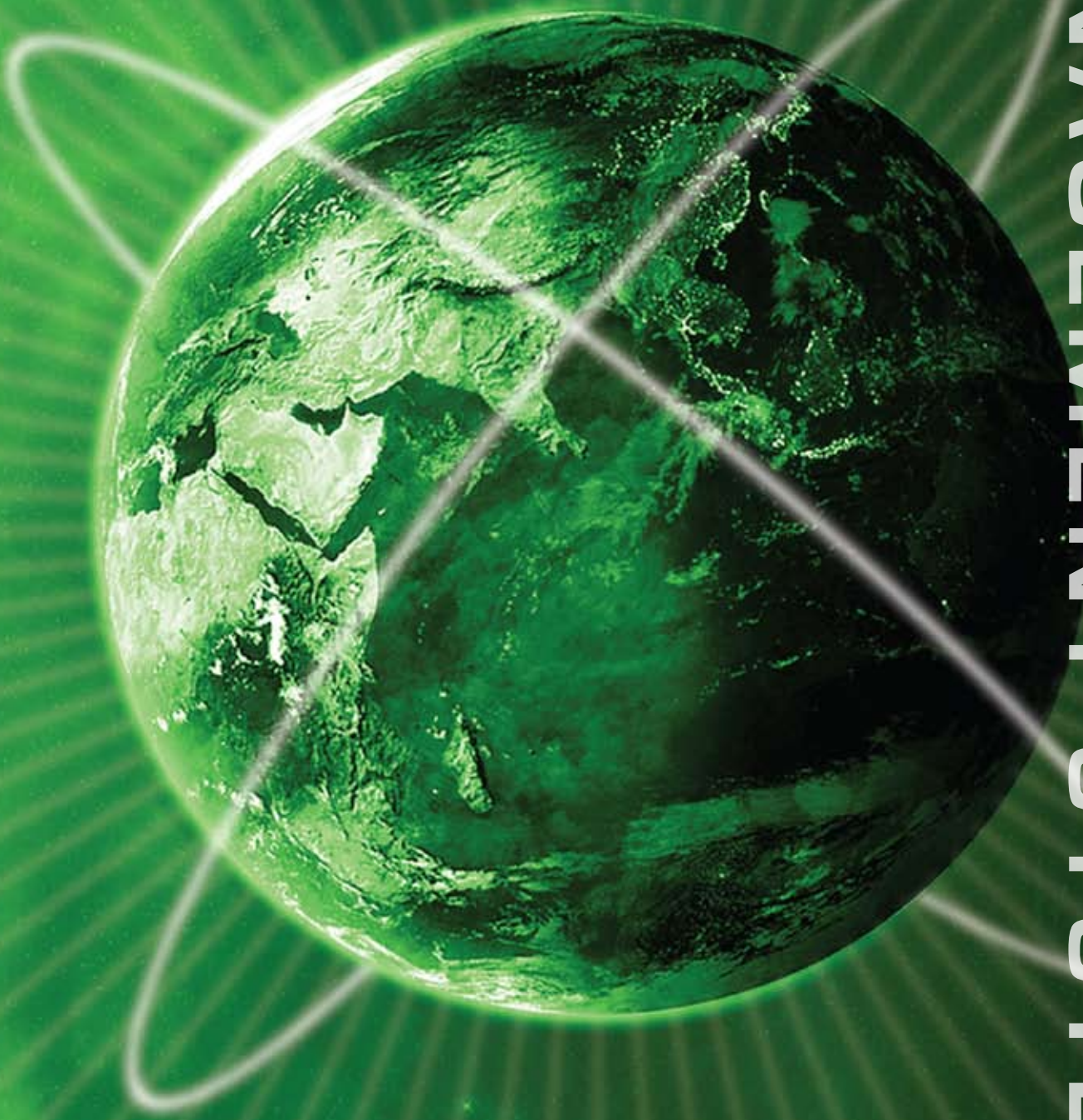


GRIDLOCK ACCESS MANAGEMENT SYSTEM



D F A
OPEN ACCESS NETWORK



The Gridlock Access Management system is a powerful and unique centralised network security management system that enables a centralised site to secure and access manage remote sites and distributed equipment locations.

The Gridlock system provides geographical views of the customer's access points and distributed equipment locations. The system utilises technologies such as GPS, GPRS, RFID and geographical tools such as Google Earth.

The design of the system is such that it is generic in application and can therefore be customised or adapted to a retrofit solution for existing infrastructure like manholes, handhole and cabinets, or a particular environment or application.

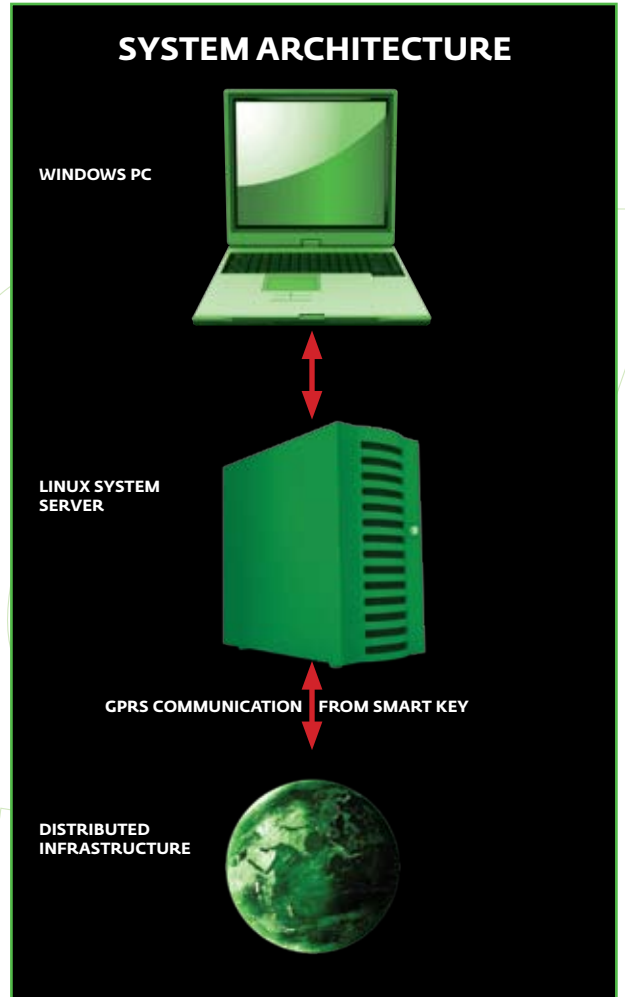
The total system boasts an extremely high level of security as a barrier against unauthorised access, ensuring that only authorised maintenance personnel have access to the telecommunications network.

SYSTEM COMPONENTS:

The system comprises of four basic elements:

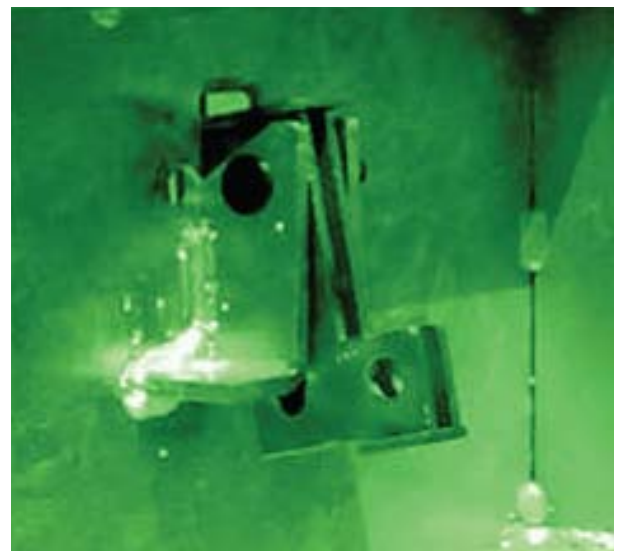
1. Centralised Management Platform

All access requests are processed from this platform. The platform uses Linux based server with a Windows Internet browser application for user access. The keys are pre-loaded with authorisations on an individual node basis. Parameters such as key and lock serial numbers, latch serial number and time intervals, are all utilised in the authorisation and authentication process to grant access to an individual user. The system is therefore centralised, but user access to it can be from any location required, with specific user profile limitations of the features available to end-users. The system also supports a referenced GIS data application to pinpoint security transgressions.



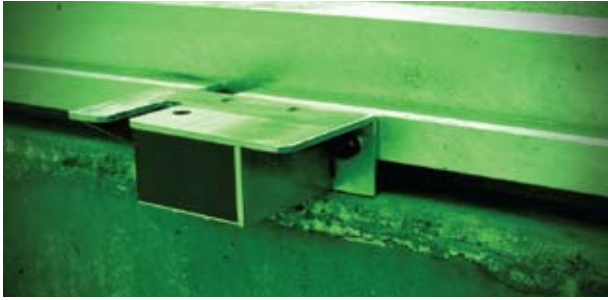
2. Locking Latch

The locking latch is used to lock the lid/door by engaging into a locking device.



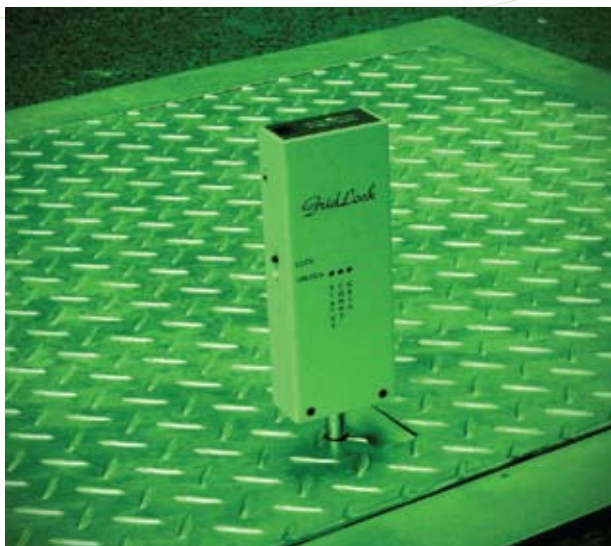
3. Locking Device

The locking device is an encapsulated powerless unit which is fitted to the frame of the lid\door. This locking device is waterproof, contains no active energy source and is designed as a maintenance free unit. It is chemical resistant to a wide range of chemicals, being manufactured from polyethylene and has no electrical contacts exposed anywhere on the unit. The lock is energised from the key and all communication to the lock is by way of an inductive process.



4. Active Key

This unit energises the lock from an internal power source that is rechargeable. The key manages all communication with the lock and detection of RFID technology to authenticate and operate the system. It manages the communication back to the management platform with a GPRS communications channel and records all events per access incident and sends this log file back to the platform once a transaction has been completed. Keys are tamper proof and are automatically disabled if tampered with, or if the required procedure is not followed. The key engages with the lock through a keyhole and protrudes down into a guided keyhole on the locking device. The lock is therefore out of harms way and cannot be damaged in a harsh environment.



ENVIRONMENTAL CONSIDERATIONS

The end user equipment is designed to operate in harsh environments. No batteries are utilised in remote equipment due to maintenance and reliability considerations and all power is drawn from the active key. The units are all self contained and maintenance free for a design period of 40 years. The mechanisms are dust and grit proof, as well as water resistant. They can accommodate outside temperature variations from -20 degrees to +70 degrees Celsius. The lock units are accommodated in a block of polyethylene for isolation against rapid temperature variations, as well as vibration. The units are also chemically resistant to hazardous substances which may have found their way into manhole chambers. All metal parts are manufactured from either high grade polished stainless steel, or 3CR12 lower grade on mounting brackets, as a cost consideration. The units are self-lubricating with a design and tested capability to meet thousands of reliable operations.

COMMUNICATION AND AUTHORISATION PROCEDURE

The system utilises the GPRS network to load remote keys requesting access. The specific access requirement must first be logged on the system by an authorised user, prior to this access request from a specific key. The key only requests transactions against its own serial number, it therefore has no input or influence against the location or time interval. If outstanding authorisations are available on the system, then these are downloaded to the key and a visual indication on the key indicates to the user that the request for access has been reliably transferred, prior to the person driving to the remote location. The access transaction is then between the key and the remote lock, and a combination of serialisation, sequence numbers and RF ID technology are utilised to authenticate the user with the encrypted data transferred to the key.

PRE-AUTHORISATION
Planned work or scheduled maintenance



Log request with monitoring centre on specific node access requirement

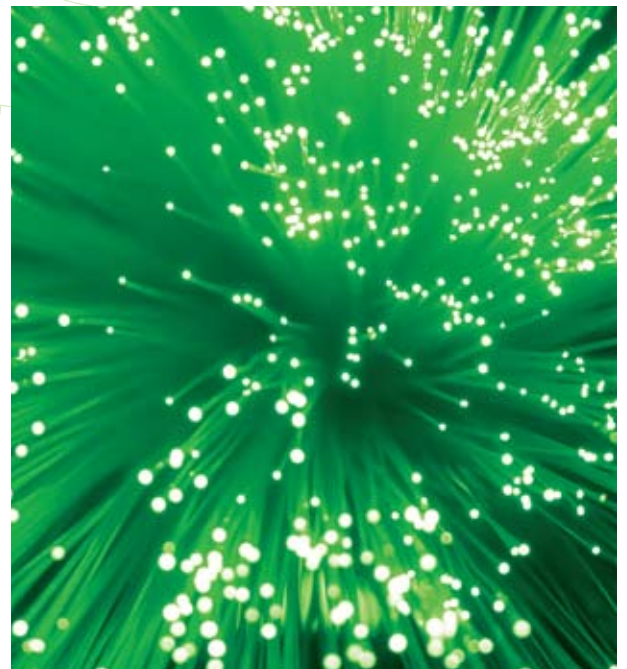
Pre-authorise network nodes for work period and specific access key

System downloads authorisation to the specific key

Specific parameters include:
Specific key code, list of network nodes and period of validity of access request.

After locking of the particular chamber / site / cabinet, the entire log file of events in the key related to this transaction is transferred to the central platform including positive confirmation of the successful locking of the chamber. This data is archived for reporting as a comprehensive audit trail of all events. This action is also monitored by the application and if a transaction is not closed within the predetermined time limit, the key is contacted and the access request deactivated if expired. Keys can also be blocked and will require the reactivation of PUK codes from a central location, to enforce work access procedures.

The solution is fully scalable and there is no physical limitation on the size of the network or number of units that can be deployed. The locks have also been integrated into outdoor equipment cabinets and remote sites and the entire access management of personnel is thus possible from a single platform. This system also provides valuable reports so as to monitor staff movements within the network and effectively manage the workforce.



D F A
OPEN ACCESS NETWORK

55 Regency Drive, Route 21 Corporate Park, Nellmapius Drive, Irene, Gauteng South Africa
Tel. +27 12 345 7540 Fax. +27 86 659 9958 Customer Care. 0800 628 662 Web. dfafrica.co.za