NPS/006/003 – Technical Specification for Operational Locks

1. Purpose

The purpose of this document is to specify the design and technical requirements for the access and operational locking systems to be installed within Northern Powergrid. This is a master key system containing various access levels to buildings and equipment either owned or accessed by Northern Powergrid employees or authorised contractors.

This document supersedes the following documents, all copies of which should be destroyed.

Document Reference	Document Title	Version	Published Date
NPS/006/003	Technical Specification for Operational Locks	1.1	Feb 2019

2. Scope

The scope of this document covers the keys, padlocks and cylinder locks used to prevent unauthorised access to Northern Powergrid operational buildings and items of equipment. This includes mechanical, electromechanical or keyless systems and additional hardware and software to support the system type.

A master / sub-master system is specified providing several levels of access or access groups that align with the competency level of the key holder.

The products described within this specification shall comply with all current versions of the relevant International Standards and British Standard Specifications.

The following appendices form part of this technical specification:

- Appendix 1 - Technical Schedule
- Appendix 2 - Self certification conformance declaration
- Appendix 3 - Addendum to Supplier Requirements
- Appendix 4 - Technical Information Checklist

2.1. Table of Contents

3. Technical Requirements

3.1. Background

The locking of the Northern Powergrid assets will fall within the same master/sub-master systems but cover two main areas – building access locks and operational asset locks.

Access locks are required for both Grid Supply Points (GSP), Bulk Supply Points (BSP), Primary and Distribution substation on both internal and external access gates and doors. There will be a requirement for both padlocks and cylinder locks of various designs and sizes.

Operational asset locks are usually padlocks that allow authorised staff to access and work on the distribution network in accordance with the company's safety procedures. This apparatus is usually situated within a secure building therefore a lower security standard may be required at these positions. There is a requirement for mechanical operational locks only.

Northern Powergrid has in excess of 25,000 operational buildings with a varying number of locks required at each site depending on the size of the facility and number of assets contained within the premises.

3.2. Master Key System

In order to safely access, operate and work on our distribution network safe systems of work are required. To ensure that staff can only access areas that they are trained to do so a master key system is required. This is also the case for operating electrical apparatus of voltages between 240V to 132, 000V. There is a requirement for five levels of access that align with the Northern Powergrid Distributional Safety Rules and Operational Practice Manual. The access levels are detailed in section 3.3 of this specification.

Where electromechanical or keyless systems are in use, user groups shall be created in alignment with the access levels detailed in section 3.3. There will also be the ability to restrict access by geographical regions.

3.3. Access Levels

The system shall have a master/sub-master access restriction and align with the Northern Powergrid Operational Practice Manual. Level 1 being the master level that shall be able to operate all sub-levels within the suite. Each other level shall be restricted from operating at any level above its stated level.

Level 1	Chambers containing exposed HV conductors, HV switchgear operating handles
Level 2	Open Compounds containing exposed HV conductors where access and working clearance can be maintained
Level 3	Chambers and enclosures containing exposed LV conductors, Enclosures with short fence inner compound (1.37m)
Level 3 Dual Access	For areas with exposed LV bus bars - This type is required to facilitate dual access to shared locations by providing a up to 3000 "differs" so that the third party has a key unique to that site only but still allowing Northern Powergrid access at the predetermined level
Level 4	Non-operational areas – workshops, toilets etc., Enclosures with fences in excess of 2.0m – non-operational or with no apparatus enclosed
Level 4 Dual Access	For Non-operational areas - This type is required to facilitate dual access to shared locations by providing up to 3000 differs so that the third party has a key unique to that site only but still allowing Northern Powergrid access at the predetermined level
Level 5	Dual Access positions that require landlords access e.g. metering cupboards and doors
Auxiliary Safety* (Aux S)	Feeder Pillar kiosk or auxiliary application when used as a safety point of isolation

*Note – The auxiliary safety lock is a standalone system that is not covered under the master key system.

3.4. Policy Requirements

The suite of locks and keys shall meet the requirements of the current Northern Powergrid operational guidance and policy documents. This includes the following controlled documents:

- Distribution Safety Rules
- Operational Practice Manual
- MNT/006 – Policy for Site Inspections of Ground Mounted Substations
- IMP/009 – Policy for the Enclosure of Ground Mounted Distribution Substations
- NPS/006/002 – Technical Specification for Distribution Substation Enclosures

3.5. Specifications

The following standards are applicable to the products specified in this document:

Security Requirements

Padlocks – BS EN 12320 Grades 1 to 6 Security

Cylinder Locks – BS EN 1303 Grades 2 Attack Resistance and Key Security Grade 6.

Corrosion Resistance

Padlocks and Cylinder Locks – BS EN 1670 Grade 3 .

Loss Prevention Standards

This standard is for the complete building enclosure so the lock standards will have to match or exceed the LPS requirements.

Additional Standards for Electronic Systems

- BS EN 15684: 2012 Grade 6 mechatronic cylinder requirements and test methods.
- BS EN 60079-0 and EN 60079-11 ATEX zone 2. The ATEX approval indicates that the products can be used in areas which contain any types of gases, vapours, ignitable dust or air.
- BS EN 60529 - IP rating (Ingress Protection Marking) Padlocks should achieve a minimum of IP68 and cylinders IP57
- Battery life 5 years' and use industry standard lithium batteries
- Keys, cylinders and Padlocks should be vibration tested under BS EN 60 068-2-6 55- 200Hz (International Electro Technical Commission)
- Keys, cylinders and Padlocks should be tested under BS EN 60 068-2-27 for shock testing 2J (International Electro Technical Commission)
- Keys, cylinders and Padlocks should pass BS EN 60 068-2-2 Bb/Ab Dry Heat and Cold Thermal Shock testing (International Electro Technical Commission)

3.6. Types of Locks

There are numerous different types of pad locks and cylinder locks required to support the current arrangements on the company's asset and system. Appendix 1 – Schedule of Items, details a description of each type with specific technical requirements. The schedule also details the required security and loss prevention grade as required by the associated standard.

Padlocks

Padlocks are specified by security grade requirement (BS EN 12320 – grade 1 to 6), corrosion resistance (BS EN 1670 – Grade 3). Other limiting factors are detailed in Appendix 1.

The schedule of items also includes a requirement for a standard and high security hasp and staple for fixing to wood and steel doors. They shall be supplied with appropriate fixings and be galvanised to prevent corrosion. General-purpose heavy-duty steel chains shall be hacksaw resistant and covered in a protective PVC sleeve.

*Note – where fitted in conjunction with a door lock cloaking device the dimensions of padlocks is critical and suppliers must demonstrate that the products offered enable them to be used in conjunction with all cloaking devices fitted to NPg high security doors. Current padlock dimensions are shown below.

	Dimension (mm)
Vertical Shackle Clearance	29
Horizontal Shackle Clearance	29.5
Shackle Dia	12.7
Body Thickness	31.8
Body Width	65

Cylinder Locks

Cylinder locks are specified by security requirements (BS EN 1303 - Grades 2 Attack Resistance and Key Security Grade 6), corrosion resistance (BS EN 1670 - Grade 3 profile type (euro, oval etc.), single or double cylinder and cylinder length. The BS EN grade requirements for padlocks and cylinders are detailed within Appendix 1 – Schedule of Requirements.

Rim cylinders shall be universal and have a tang length suitable for doors and gates between 45mm and 65mm deep. Where rim, euro and oval cylinders do not match the width of the existing door or gate a suitable spacer shall be provided.

Keys shall be manufactured of an appropriate material designed to provide a prolonged service life with the design permitting use on cylinder locks fitted with security escutcheons.

3.7. Electromechanical and Keyless Access Systems

Electromechanical and keyless systems are required in order provide several advantages over mechanical cylinders and will be installed where Northern Powergrid policy dictates. Key features of the systems are:

- Provide an access audit trail
- Enable strict control of access locations and periods of time
- The ability to disable or restrict access
- A requirement for the user to have their access requirements validated at planned time intervals
- The ability to revoke access rights in the event of key loss or misuse.
- Provide NPg with a live asset performance register of its electromechanical lock base through its key estate.

3.7.1. Security Requirements

- Electronic locks and keys shall be able to receive software/firmware updates via a number of enciphered methods that utilise mutual authentication to encipher the data package. The enciphering algorithms and key lengths shall meet a level deemed ‘acceptable’ by NIST Special Publication 800-131A Revision 2

- Electronic locks and keys shall have evidence of an approved method of IT health check penetration tested and the cryptographic code independently reviewed
- Electronic locks and keys shall have the ability to roll/replace cryptographic keys. Confirmation of all rolled (previous generation utilised) keys shall be electronically assured to be removed from all electronic memory locations. Key material must be wholly owned and managed by Northern Powergrid
- The cryptographic key estate shall use diverse keysets.
- Electronic locks and keys shall be firmware upgradeable
- Electronic locks and keys shall have sufficient storage capacity to permit all anticipated firmware updates
- Lock and key electronics or firmware shall have the capability to implement new cryptographic algorithms
- Electronic locks and keys shall implement NIST 800-131A approved algorithms and key lengths to a minimum of "Acceptable"
- The electronic component of locks shall not fail by any static or alternating (conducted or radiated) magnetic fields through means of manipulation or induction. All electronic devices shall comply with all current and relevant CE EMC directives
- Electronic locks and keys shall contain sufficient storage to maintain a log of successful and failed access attempts
- Electronic locks shall have the ability to explicitly block specific keys
- Electronic locks shall implement protocols to defeat time-based attacks and that these methods shall be provided by the vendor at time of tender submission and during the course of the contract period.
- The supplier shall provide a full penetration test report on the electronic locks, keys and management platform with details of any remediation action taken. The scope of the PEN test shall be provided at time of tender submission be provided during the conclusion phase of any FAT tests and prior to deployment of the live system to the satisfaction of NPg.
- Communication with the key must be encrypted using algorithms and key lengths that meet a level deemed 'acceptable' by NIST Special Publication 800-131A Revision 2
- Public Key Infrastructure shall be used to protect client/server communication with a physical element providing three factor authentication
- There shall be no requirement for customer side networked servers to store any data when a front-end administration solution is utilised in the complete locking solution
- Data at rest and during transmission shall be protected using AES 128/256-bit encryption
- Electronic systems shall be resilient to electrical restoration scenarios.

3.7.2. IT/Ethernet connected Updaters (ITEU)

- All ITEU shall be available as an internal and external version tested to IP57 and IK9 for regular key validation
- ITEU shall support power by PoE or 12-24vdc 34w IEEE
- ITEUs shall be capable of 802.1x network authentication
- ITEU's shall be proxy aware and use PKI to secure server communications

- ITEU’s shall provide visible indication of low battery in a key and shall fully support offline functionality for resilience during network outages.
- ITEU’s shall not store any data locally and external units shall be of anti-vandal construction to IP65 and be available and tested to IEC 62262 Client ITEU’s
- A client PC connected ITEU shall be used as part of a three-factor authentication to allow the application to read a physical device to authenticate access
- The client ITEU shall also allow for local administration of keys e.g. key hand out/in
- A client ITEU shall act as a networked ITEU when not in use.

3.7.3. Readers

- A key insert reader shall be available for electronic switching of Access Control barriers or automatic gates
- A key insert reader shall act as an extension to an ITEU to allow external updates without exposing a network connection.

3.7.4. Advanced Cylinder Features

- Sequential opening shall be possible with specific cylinder firmware requiring multiple keys for operation.

3.7.5. Memory Structures

- Each key shall record a minimum of 2000 time stamped Audit Trails
- Each key shall record a minimum of 20 foreign audits (collected from other systems)
- Each key shall have capacity for 3500 Authorised locks or groups
- Electronic grouping of locks shall allow for minimum scalability of up to 229,000,000 locks in a single key
- Each key shall be capable of storing up to 50 Time Schedules
- Each lock shall be capable of storing up to 2000-time stamped audits
- Locks shall be capable of carrying a blacklist of up to 3000 keys or key groups
- Memory in locks and keys shall be non-volatile

3.7.6. Software Setup/Security

- Hosted solutions shall have data centres with triple redundant servers geographically separated and accredited to ISO27001
- All information shall be backed up at a separate location and updated a minimum of every 30mins.
- Infrastructure Security: The solution shall provide end-to-end security and privacy.
- Infrastructure Scalability: The infrastructure shall be capable of scaling up as required and extending.
- All sensitive data shall be exported by the vendors software and centralised in the application. The vendors software provider shall be part of the same organisation.
- All business logic for handling security shall be handled centrally in the application.

- Centralised services shall enable automatic renewal of certificates to ensure these never need distributing separately.
- Clients that must be trusted are required to mutually authenticate to CWM using client certificates.
- Remote updates either through updaters or Smartphones should use single use session keys so that the devices cannot decrypt the data.
- Access to software shall require as a minimum of triple authentication and require physical credentials for logging into the system.
- Reporting options shall allow for Basic, Enhanced using reporting tools such as Crystal, Yellowfin, BI etc. or Analytic, to allow the reporting and analysis of system usage anomalies.
- The locking system shall be managed through a web-based software interface.
- The software interface shall be provided as Software as a Service (SaaS) or for installation on the client's own servers.
- Proof will be required that the SaaS (Software as a Service) provider achieves a Monthly Uptime Percentage >99.95%
- Mobile software apps shall be available to allow for remote management of key authorisation and access levels using mobile phone technology available for both iOS and android platforms. Communication between the key and mobile device shall be direct and not require any additional equipment or hardware.
- Web Services shall be available to allow full integration with other security and business management software systems. Any web service interaction with the system should follow the same security protocol as user access and should be throttled automatically to ensure stability of the application.
- It shall be possible to use industry standard business information software to develop bespoke reports and dashboards. The data downloads to achieve this shall be automatic with the frequency set by the end user.
- Final commissioning of all software shall be by the manufactures own directly employed engineers.
- The manufacturer shall be able to provide the required SLA with engineering resources that are based in the United Kingdom.
- All software licences shall be registered to the end user who will take ownership immediately on final handover of the fully commissioned system.
- SaaS Software shall be regularly patched and maintained with a documented SLA and maintenance schedule.
- SaaS Software shall be updated regularly with new features to ensure a constantly evolving solution.

3.7.7. Resilience

- Offline revalidation of keys shall be available allowing for customers to gain validation for keys in the event of network disruption – this should be configurable by the customer
- Bluetooth keys shall be able to be validated in an offline state using Biometric identity or PIN code

3.7.8. Keys

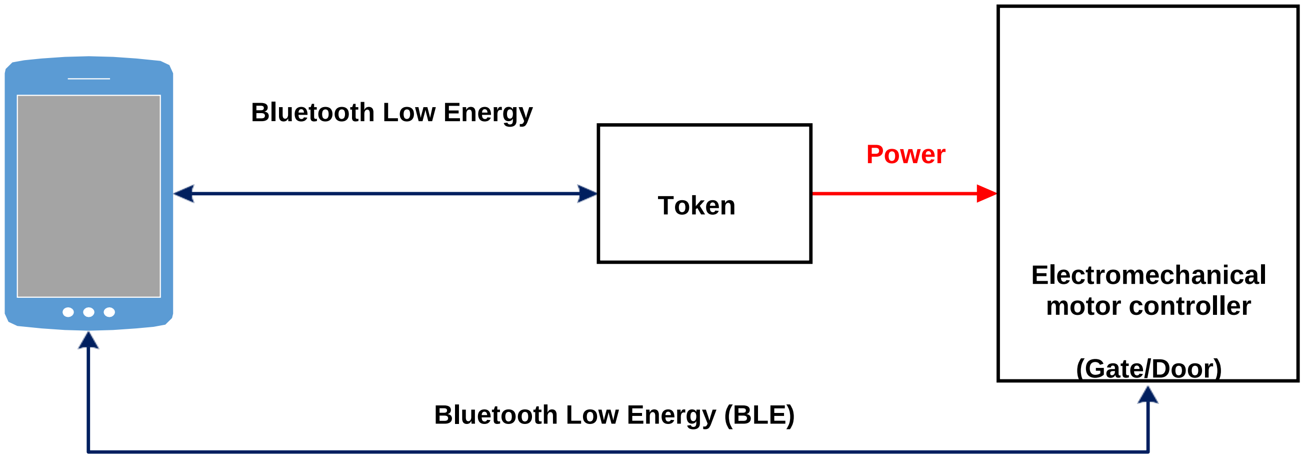
- Keys shall provide visible and audible indications of access granted or denied and all keys shall provide visible and audible indications of low battery
- Keys shall be capable of accepting additional RFID tag insert available for use with other types of access control systems
- Keys shall operate reliably within -20 to +50 degrees Celsius
- Keys shall be capable of keeping accurate time

3.7.9. Bluetooth Keys

- Keys with Bluetooth Low Energy shall be available for remote updating of Access Rights
- Information sent via Bluetooth shall be AES128/256 encrypted and shall not be decrypted by the phone
- Any phone ‘Apps’ shall be freely available from both the Google Play and Apple App stores and shall be maintained and upgraded to support future handsets and phone OS
- The Bluetooth app shall incorporate an identity check of the key holder by means of PIN or Biometric activation of the key
- Online functionality shall be possible whereby the key automatically communicates with the server upon insertion into a lock

3.7.10. Keyless Systems

Mobile Application


Bluetooth Low Energy
Token
Power
Electromechanical motor controller
(Gate/Door)
Bluetooth Low Energy (BLE)

- The phone Application (App) must work with or without an internet connection
- All data to always remain encrypted
- The phone provides “reciprocal multi-level authentication and validation” using data provided by the Token and Central Management System(CMS)
- The App does not have the ability to de-crypt the entire securitysequence
- Neither the App nor the Token can operate without the other securely pairedelements
- The Token provides “multi-level authentication and validation” using the phone’s IMEI

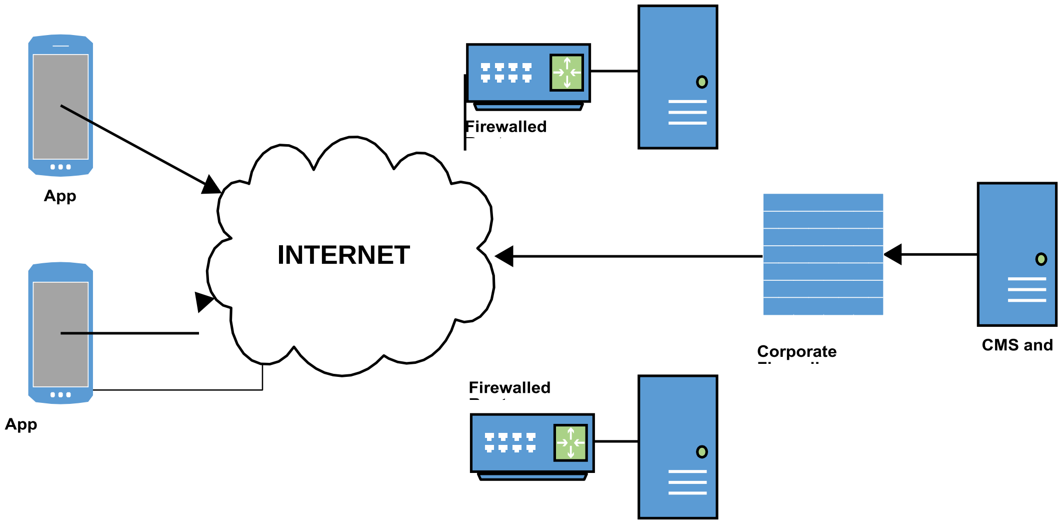
- The Token and phone always operate as a secure pair with nouser intervention
- App updates are always delivered via remote file servers in the background, with no user intervention
- All files are always encrypted via the mechatronic locking device using AES128
- All encrypted data is then encrypted again using Bluetooth Low Energy (BLE) or Transport Layer Security (TLS) algorithms prior to transmission
- BLE and TLS communications are always secured end-to-end and notreleased
- The BLE connection acts as a "tether" between the Token and thePhone
- Any lost/disconnected Tokens are reported directly to the CMS with the location where the tether was lost/disconnected
- Support for additional "biometric, facial recognition security" built-in to application
- Support for secure management of an alarm system(s) viasecure generic interface
- Support for secure management of fire managementsystem(s)
- User interface to equipment control systems and files, with expansion for otheruses
- Unresponsive ("person-down") and/or hazard duty of care protection support
- Back-up 'file servers' facility supporting alternate routing in the event of service interruption, Distributed Denial of Service (DDOS) or maintenance events etc. with the ability to maintain multiple file servers at multiple sites
- Mandatory PIN (alphanumeric) entry is required each time the App is started or brought to the foreground. Note that for security reasons, the randomly generated PIN is set by the CMS and can't be changed by the user (an agreed three strikes rule is applied)
- Secure PIN hash storage has been applied to thesystem
- Barring a user can be accomplished via TWO ways either direct from the CMS WITHOUT field user co-operation or via standard OEM facilities e.g. IOS 'Find My Phone'

Electromechanical Lock Application

- Requires No "hard-wiring" or "alternative power sources" e.g., solar, batteries etc. on the electromechanical locks
- All Token's provide power transfer from their internal battery, which have been optimised to maximise performance e.g., hibernation if not used, to give the maximum life expectancy
- All "field" equipment is maintenance free with performance of each electromechanical lock reported every time it is used; therefore any "potential" issues are identified instantly
- Battery or hard-wired alternatives are supported options if essential/required
- Token transfers power wirelessly to the electromechanical Lock
- Every electromechanical Lock has full redundancy and parallel recovery
- All electromechanical locks never connect to theinternet
- Authentication and Validation both take place at every electromechanical Lock
- The Authorisation and Validation of the App and Token enable these applications to function together in unison to operate the electromechanical Lock(s)

- The electromechanical lock determines authenticity and validation prior to accepting commands
- The App is centrally managed by the CMS, including user profiling including duration for each electromechanical lock (either by individual electromechanical lock or on a collective profile)
- CMS provides "multi-factor authentication" with a "secret relay payload"
- The users PIN provides "multi-factor authentication" through an encrypted "hash"
- Phone PIN provides "multi-factor authentication" through Android or IOS built-in security
- All stored and transmitted data is always multi-encrypted i.e., each "packet" of data contains multiple layers of either AES128 or AES256 encrypted data
- A Full real-time "activity" audit report is produced every time the App is activated or used
- Access rights can be dynamically adapted to safeguard users attending hazardous or closed sites, with user notification via the App
- Dynamic ability to add additional infinite number of additional systems

Remote File Server



Primary

Remote File Server

Secondary

CMS

- Supports multiple CMS administrators and system guardians/management
- Unique, secure CMS access credentials per user
- Unique tiered user rights for each user
- Updates to field user permissions generated by CMS
- Field user permissions delivered to phone securely via encrypted remote file servers
- Full audit trail for each local and remote user
- Centralised 'deep-dive' diagnostic support

- CMS operates entirely within secure corporate firewalled location(s)
- All firewall CMS ports are exclusively outward facing
- CMS securely handles all file transfers from within the corporate firewall(s)
- During initial installation, the CMS generates the second authentication element derived from the phone's IMEI
- During initial installation, the CMS provides the third authentication element with the "secret relay payload"
- The CMS maintains a local fileserver
- There is no direct link from the internet into the CMS
- There is no external access from the internet through the firewall
- All data is always encrypted, whether at rest or during transport
- All communication links are multi-factor secured end-to-end encrypted prior to applying TLS
- Heartbeat connectivity is utilised to oversee/monitor the system
- "Connectivity down" indicators are utilised across all aspects ofthe system
- Live Short Messaging Service (SMS) "Down-time" alert reporting is utilised if the internet is inoperable

Local File Server

- Is an Independent stand/alone application
- Isolates the CMS from direct internet contact
- Securely negotiates the corporate firewall(s)
- All comms uses exclusively outward facing ports

Remote File Servers

- Multiple "live" file servers giving continuity of service
- Dynamically tiered configurations
- Expandable options to additional locations (if required)
- 100% redundancy
- Physically different locations or internet connections (2 minimum)
- Dedicated local firewalls (per file remote server)
- Capable of seamless "real-time" transitioning not matter what file server is being utilised to open an electromechanical lock
- Common secure 'library' support areas for user up-dates
- Access to user folders with unique and secure passwords
- Secure passwords generated automatically by CMS – where all users (at any level) can
- never see the passwords or change them

Physical Requirements

The locking element of the system shall be compatible with replacing locks in LPS1175 SR 2 and SR3 rated security doors and must not reduce the security rating of the overall door system.

3.7.11. Design Development, Pre-Deployment and Production Environment Requirements

The supplier shall include within their scope of works all aspects of work to fully satisfy NPg that their solution has been designed to meet the employers' requirements prior to live deployment (likely to be phased) of the locking solution.

The minimum key steps that would be expected would include, but not be limited to:

- Design and deployment plan and program (development plan)
- Initial scoping survey including physical assessment of lock type requirements
- Initial communications (electronic) survey across all of the NPg estate to ensure full coverage allowing key deployment of their solution
- Consultation with the key team leaders/office/areas in agreeing a pre deployment strategy
- Provide a pre deployment technical build plan with a fully representative NPg estate factory acceptance testing demonstration.
- Allow for all design iterations and consultation because of the design development plan
- Provide a pre-production technical build plan with an indicative live representative of the NPg estate, site acceptance testing phased plan and demonstration, to NPg's acceptance in full.
- Deploy the solution to NPg's acceptance in full.
- Provide a production reference environment for testing firmware upgrades and solution upgrades and changes.
- All works shall be in accordance with NPg's IT and Cyber Security requirements, and the supplier shall full familiarise themselves with the policy in advance of any design works and subsequent revisions.

3.8. Identification of Locks and Keys

Locks should be marked with the customer's identification mark (NPg), British Standard of security rating and the master key access level. They should also have the manufacturer's identification mark and a means of product tractability identifying the year of manufacturer and batch number.

Keys shall be marked with the appropriate access level and a unique key number that can be used to provide an internal audit trail and identify the key holder (i.e. L3 0001). Customer keys with differs at levels 3 and 4 shall be marked with the access level and number of sequential key differs (i.e. L3'd' 0001).

*Note – Keys shall not be marked with the company name Northern Powergrid (NPg)

Keys and locks shall be registered on the immobilisation.com website for security purpose.

3.9. Maintenance

Locks should be virtually maintenance free but if necessary be capable of being carried out without specialist tooling or fluids. There shall be a procedure for releasing frozen lock mechanisms.

3.10. Patent and Copyright Protection

The locking system specified is used to protect strategic operational buildings and equipment belonging to Northern Powergrid. The sites may contain electrical hazards and unauthorised access by the public must be prevented. The key and key profile shall be registered with an international patent protection. Following the expiry of the patent protection period there must be other steps in place that deter unauthorised copying of the keys for an extended period. A secure registered delivery service shall be in place ensuring the security of keys when delivering to the customer.

4. References

The products described within this specification shall comply with the latest versions of the relevant International Standards, British Standard Specifications and all relevant Energy Network Association Technical Specifications (ENATS) current at the time of supply.

4.1. External Documentation

Reference	Title
BE EN 1670	Building hardware – Corrosion resistance – Requirements and test methods
BS EN 12320	Building hardware – Padlocks and padlock fittings – Requirements and test methods
BS EN 1303	Building hardware – Cylinders for locks – Requirements and test methods
BS EN 15684	Building hardware. Mechatronic cylinders. Requirements and test methods
BS EN 60068	Environmental testing - General and guidance
BS EN 60079	Grid Systems for Printed Circuits
BS EN 60529	Degrees of protection provided by enclosures (IP Code)
LPS 1175: Issue 7	Requirements and testing procedures for the LPBC approval and listing of intruder resistant building components, strong points, security enclosures and free-standing barriers

4.2. Internal Documentation

Reference	Title
IMP/009	Policy for the Enclosure of Ground Mounted Distribution Substations
MNT/006	Policy for Site Inspections of Ground Mounted Substations
NPS/006/002	Technical Specification for Distribution Substation Enclosures

4.3. Amendments from Previous Version

Reference	Description
2. Scope	Section expanded to include electromechanical and keyless systems
3.2 Master Key System	Section expanded to include electromechanical and keyless systems
3.5 Specification	Additional standards added for electromechanical and keyless systems
3.6 Types of Locks	Dimensions add for the lock requirements for door lock cloaking devices used within NPg
3.6 Types of Locks	Loss Prevention Standard comparison table removed
3.7 Electromechanical and Keyless Access Systems	New section added
3.10 Patent and Copyright Protection	The requirement for a minimum of 10 remaining patent removed from section
4.1 External Documentation	Reference documents for electromechanical and keyless systems added
5 Definitions	Added
Appendix 1	Electromechanical and keyless items added
Appendix 2 Self Certification Conformance Declaration	Tables for electromechanical and keyless systems added
Appendix 4	The requirement for samples to be provided for assessment added

5. Definitions

Term	Definition
"Differs"	Refers to the number of possible keys for a given lock
Access locks	A suite of locks and keys of any type used to secure the perimeter of all Northern Powergrid substations as well as the HV compounds and buildings within a substation from unauthorised access.
Electromechanical Lock	An electromechanical key lock will provide all the facilities of a mechanical lock but will have some added form of electronic control mechanism, using elements in both the key and the cylinder to give assurance that the correct key is being used.
End-to end privacy	A type of encryption where only the sender and the recipient can decrypt the message.
End-to-end security	The protocols and solutions used to protect the endpoints of a network connection.
FAT test	A process that evaluates equipment during and after the assembly process by verifying that it is built and operating in accordance with design specifications. FAT ensures that the components and controls are working properly according to the functionality of the equipment itself and is usually conducted off site before the final installation.
Keyless locking systems	A wireless system locking which locks and unlock on recipient of secure and end to end encrypted instructions from an authorised device using wireless technology sufficient to ensure that only authorised users are allowed access. The mechanical elements of the lock mechanism being powered by electromagnetic induction and not hard wired or battery powered.
Master key system	A master key system refers a suite of locks and keys which are related in a hierarchy with one key at the top, the Grand Master, which will operate all locks in the suite. Subordinate master keys, sub masters and differs are used within the hierarchy to provide users with keys that will operate locks at chosen levels within the suite based on predementia criteria.
Mechanical Lock	A mechanical key lock is a device used to protect a door or space where the construction and use of the mechanism relies solely on non-electronic components. Operated by the insertion of the correct mechanical key.
Operational locks	A suite of locks and keys of any type used to secure an operational asset to prevent unauthorised or inadvertent operation.
PEN test	An authorized simulated cyberattack on a system, performed to evaluate the security of the system; The test is performed to identify weaknesses, including the potential for unauthorized parties to gain access to the system's features and data, as well it's as strengths, enabling a full risk assessment to be completed.
Safety locks	A dedicated suite of locks and keys used to secure points of isolation, so a safety document can be issued allowing work to carried out on the network, to prevent unauthorised or inadvertent reenergisation

6. Authority for Issue

6.1. CDS Assurance

I sign to confirm that I have completed and checked this document and I am satisfied with its content and submit it for approval and authorisation.

		Date
Liz Beat	Governance Administrator	15/04/2024

6.2. Author

I sign to confirm that I have completed and checked this document and I am satisfied with its content and submit it for approval and authorisation.

Review Period - This document should be reviewed within the following time period.

Standard CDS review of 3 years?	Non-Standard Review Period & Reason	
No	Period: 5 years	Reason: The proposed contract period is five years.
Should this document be displayed on the Northern Powergrid external website?		Yes
		Date
Steven Salkeld	Policy and Standards Engineer	01/11/2023

6.3. Technical Assurance

I sign to confirm that I am satisfied with all aspects of the content and preparation of this document and submit it for approval and authorisation.

		Date
Gareth Pearson	Head of Health, Safety and Training	12/12/2023
Sean Middleton	Security Manger	15/04/2024
Paul Slade	Manager - Is Security Operations	09/01/2024

6.4. Authorisation

Authorisation is granted for publication of this document.

		Date
Paul Black	System Engineering Manager	27/11/2023

Appendix 1 - Schedule of Requirements

Access Level	Type	Standards - Security (Padlocks - BS EN 12320) (Cylinders - BS EN 1303)	Standards - Corrosion (BS EN 1670)	Pad Lock Size (S, M, L)	Cylinder Length	Key Retaining	Electromechanical or Mechanical Option	Typical application
ACCESS LOCKS								
L1	Padlock	3 - Security rating	3	Large	N/A	Yes	Mechanical	Distribution substation chamber doors (hasp and staple) with exposed HV conductors
L1	Padlock	3 - Security rating	3	Large	N/A	Yes	Electromechanical	Distribution substation chamber doors (hasp and staple) with exposed HV conductors
L2	Scandinavian ½ Oval Cylinder with tang	3 - Key Related 1 - Attack Resistance	3	N/A	32.5mm	No	Mechanical	New style LPS rated enclosures
L2	Rim Cylinder	3- Key Related 1 - Attack Resistance	3	N/A	Up to 75mm Door	No	Mechanical	Primary substation compound gate
L2	Rim Cylinder	3- Key Related 1 - Attack Resistance	3	N/A	Up to 75mm Door	No	Electromechanical	Primary substation compound gate
L2	Euro Cylinder	3- Key Related 1 - Attack Resistance	3	N/A	65mm latch with turn	No	Mechanical	Primary substation compound gate
L2	Euro Cylinder	3- Key Related 1 - Attack Resistance	3	N/A	65mm latch with turn	No	Electromechanical	Primary substation compound gate
L2	Oval Cylinder	3- Key Related 1 - Attack Resistance	3	N/A	65mm	No	Mechanical	Primary substation compound gate
L2	Oval Cylinder	3- Key Related 1 - Attack Resistance	3	N/A	65mm	No	Electromechanical	Primary substation compound gate
L2	Padlock	3 - Security rating	3	Large	N/A	Yes	Mechanical	Primary substation compound gate with hasp and staple arrangement

L2	Padlock	3 - Security rating	3	Large	N/A	Yes	Electromechanical	Primary substation compound gate with hasp and staple arrangement
L3	Padlock	3 - Security rating	3	Medium	N/A	Yes	Mechanical	Distribution substation door or gate. Primary substation control room or plant room within secure perimeter. Outdoor network ABSD and regulator installations.
L3	Padlock	3 - Security rating	3	Medium	N/A	Yes	Electromechanical	Distribution substation door or gate. Primary substation control room or plant room within secure perimeter. Outdoor network ABSD and regulator installations.
L3	Padlock	3 - Security rating	3	Small	N/A	Yes	Mechanical	Feeder Pillar kiosk
L3	Rim Cylinder	3 - Key Related 1 - Attack Resistance	3	N/A	Up to 75mm Door	No	Mechanical	Distribution substation door. Primary substation control room or plant room within secure perimeter.
L3	Oval Cylinder	3- Key Related 1 - Attack Resistance	3	N/A	65mm	No	Mechanical	Primary substation control room or plant room within secure perimeter
L3	Oval Cylinder	3- Key Related 1 - Attack Resistance	3	N/A	65mm	No	Electromechanical	Primary substation control room or plant room within secure perimeter
L3	Padlock	3 - Security rating	3	Large	N/A	Yes	Mechanical	Shared access to building with hasp and staple type arrangements. LV risk present. Supplied with 2 customer keys to differ
L3	Euro Cylinder	3- Key Related 1 - Attack Resistance	3	N/A	65mm latch with turn	No	Mechanical	Primary substation control room or plant room within secure perimeter
L3	Euro Cylinder	3- Key Related 1 - Attack Resistance	3	N/A	65mm latch with turn	No	Electromechanical	Primary substation control room or plant room within secure perimeter
L3	Rim Cylinder	3- Key Related 1 - Attack Resistance	3	N/A	Up to 75mm Door	No	Mechanical	Shared access to building with hasp and staple type arrangements. LV risk present. Supplied with 2 customer keys to differ
L3	Padlock	3 - Security rating	3	Medium	N/A	Yes	Mechanical	Distribution substation door or gate with hasp and staple type arrangement (enhanced security)

L3	Padlock	3 - Security rating	3	Medium	N/A	Yes	Electromechanical	Distribution substation door or gate with hasp and staple type arrangement (enhanced security)
L3	Padlock	3 - Security rating	3	Large	N/A	Yes	Mechanical	Distribution substation door or gate with hasp and staple type arrangement (high security)
L3	Padlock	3 - Security rating	3	Large	N/A	Yes	Electromechanical	Distribution substation door or gate with hasp and staple type arrangement (high security)
L3	Scandinavian ½ Oval Cylinder with tang	3 - Key Related 1 - Attack Resistance	3	N/A	32.5mm	No	Mechanical	New style LPS rated enclosures
L4	Padlock	3 - Security rating	3	Large	N/A	Yes	Mechanical	Primary substation - main vehicle or foot gate with hasp and staple arrangement
L4	Padlock	3 - Security rating	3	Large	N/A	Yes	Electromechanical	Primary substation - main vehicle or foot gate with hasp and staple arrangement
L4	Rim Cylinder	3 - Key Related 1 - Attack Resistance	3	N/A	Up to 75mm Door	No	Mechanical	Primary substation non-operational door
L4	Euro Cylinder	3- Key Related 1 - Attack Resistance	3	N/A	65mm	No	Mechanical	Primary substation non-operational door
L4	Oval Cylinder	3- Key Related 1 - Attack Resistance	3	N/A	65mm	No	Mechanical	Primary substation non-operational door
L4	Padlock	3 - Security rating	3	Large	N/A	Yes	Mechanical	Primary substation non-operational door.
L4	Padlock	3 - Security rating	3	Large	N/A	Yes	Mechanical	Shared access to building with hasp and staple type arrangements. Non-operational site. Supplied with 2 customer keys to differ
L4	Scandinavian ½ Oval Cylinder with tang	3 - Key Related 1 - Attack Resistance	3	N/A	32.5mm	No	Mechanical	New style LPS rated enclosures
L5	Padlock	2 - Security rating	3	Small	N/A	Yes	Mechanical	Meter Cupboard with hasp and staple type arrangement. Non-operational site. Supplied with 2 customer keys to differ

L5	Rim Cylinder	3- Key Related 1 - Attack Resistance	3	N/A	Up to 75mm Door	No	Mechanical	Meter Cupboard door. Supplied with 2 customer keys to differ
OPERATIONAL LOCKS								
L1	Padlock	1 - Security rating	3	Small with extended shackle	N/A	No	Mechanical	Distribution switchgear earth switches and transformer tap selectors. Outdoor application only. Primary substation switchgear spouts, earth switches and transformer tap selector.
L1	Padlock	1 - Security rating	3	Small	N/A	No	Mechanical	Distribution switchgear earth switches and transformer tap selectors. Indoor application only.
L1	Padlock	1 - Security rating	3	Medium	N/A	No	Mechanical	Primary and distribution substation switchgear, earth switches and transformer tap selectors. Indoor application only.
L3	Padlock	3 - Security rating	3	Medium	N/A	Yes	Mechanical	Distribution substation door or gate. Primary substation control room or plant room within secure perimeter. Outdoor network ABSD and regulator installations.
OTHER LOCKS AND ACCESSORIES								
N/A	Padlock	1 - Security rating	3	Small		No	Mechanical	Toolbox lock for hasp and staple type arrangement
N/A	Padlock	3 - Security rating	3	Large		No	Mechanical	Storage containers
N/A	Lock Casing Rim Cylinder	Unit is required to provide a high security level of attachment to the door	3	N/A	N/A	N/A	Not Applicable	Rim lock casing
N/A	Lock Casing Euro or Oval Cylinder	Unit is required to provide a high security level of attachment to the door	3	N/A	N/A	N/A	Not Applicable	Euro or oval casing
N/A	Chain	High Security, 1 Meter in length	N/A	N/A	1m Chain	N/A	Not Applicable	Ladder or gate chain

All	Hasp and Staple	Standard Security	N/A	To Facilitate Large Padlock	N/A	N/A	Not Applicable	For Door and Gate Applications
All	Hasp and Staple	High Security	N/A	To Facilitate Large Padlock	N/A	N/A	Not Applicable	For Door and Gate Applications

KEYS

Item	Level	Marking and Key Number
1	Level 1	L1 and Key Number
2	Level 2	L2 and Key Number
3	Level 3	L3 and Key Number
4	Level 4	L4 and Key Number
5	Level 5	L5 and Key Number

Appendix 2 - Self Certification Conformance Declaration

Mechanical Cylinders

Note: One sheet to be completed for each design of lock offered.

Suppliers Part Number		Description
Northern Powergrid Item Number (from schedule above)		

Requirement	Standard	Clause	Grade	PASS / FAIL	Test Certificate Reference	Additional Comments
Corrosion Resistance Grade 3	BS EN 1670	5.2				
Durability Grade 5	BS EN 1303	5.3				
Operation at Extreme Temperatures	BS EN 1303	4.7.2				
Key Strength	BS EN 1303	4.2				
Key Security Grade	BS EN 1303	4.8				
Attack Resistance Grade	BS EN 1303	4.9				

Mechanical Padlocks

Note: One sheet to be completed for each design of lock offered.

Suppliers Part Number		Description
Northern Powergrid Item Number (from schedule above)		

Requirement	Standard	Clause	Grade	PASS / FAIL	Test Certificate Reference	Additional Comments
Corrosion Resistance Grade 3	BS EN 1670	5.2				
Security Requirements	BS EN 12320					

Electromechanical Cylinders

Note: One sheet to be completed for each design of lock offered.

Suppliers Part Number		Description
Northern Powergrid Item Number (from schedule above)		

Requirement	Standard	Clause	Grade	PASS / FAIL	Test Certificate Reference	Additional Comments
Mechatronic cylinder requirements and test methods	EN 15684: 2012		6			
The ATEX approval indicates that the products can be used in areas which contain any types of gases, vapours, ignitable dust or air.	EN 60079-0 and EN 60079-11 ATEX zone 2					
IP rating Padlocks (Ingress Protection Marking)			IP68			
IP rating Cylinders (Ingress Protection Marking)			IP57			
Lithium batteries with a minimum 5 year life						
Keys, cylinders and Padlocks vibration test	EN 60 068-2-6 55		200Hz			
Keys, cylinders and Padlocks shock tested	EN 60 068-2-27		2J			
Dry Heat and Cold Thermal Shock testing	EN 60 068-2-2		Bb/Ab			

Appendix 3 - Addendum to Supplier Requirements

Product Specific Information

The supplier is required to complete the following section (other documents may be referenced or supplementary sheets added).

System Patent Protection	
Additional Measures to Prevent the Copying of Keys	
Cylinder Design and Benefits	
Key Management Procedure	
Maintenance Requirements	
Repair Options	
Frozen Mechanism Procedure	
Routine Manufacturing Testing and Inspection	
Packaging	
Expansion of the System: 1. Additional sizes/Types of padlocks and cylinders that are available with the system offered. 2. Ability to add additional access level(s)	

Appendix 4 - Technical Information Check List

As a minimum the following information shall be provided by the supplier for technical review by Northern Powergrid. Additional information shall be provided if requested.

Failure to provide all the following information may result in the items being deemed as “not technically acceptable”.

Requirement	Provided (Y/N)
Full product descriptions and part number/reference	
Appendix 2 – completed self-certification conformance declaration	
Appendix 3 – complete addendum to supplier requirements	
Complete set of drawings for each item	
Type test evidence	
Manufacturing routine test plan and/or quality plan	
Packaging information	
Instructions/Manuals installation, maintenance and end of life disposal	
Spares availability list	
ISO:9001, ISO:14001, ISO:18001 certificates and Security Standards	
A sample of each design of product offered to be provided for assessment (padlock, cylinder etc.)	