ADDAX
add new tech to our business!

KEY MANAGEMENT SYSTEM SECURITY

Nowadays security issues affect all aspects of our life, from communication to work. We have reached a point where we perceive security as a part our daily routine: we cannot imagine our lives without secure authentication to unlock our smart phones, log in to personal computers, unlock the car with a key fob. Yet we are far from realizing the implications of security on our relationship with the utility.

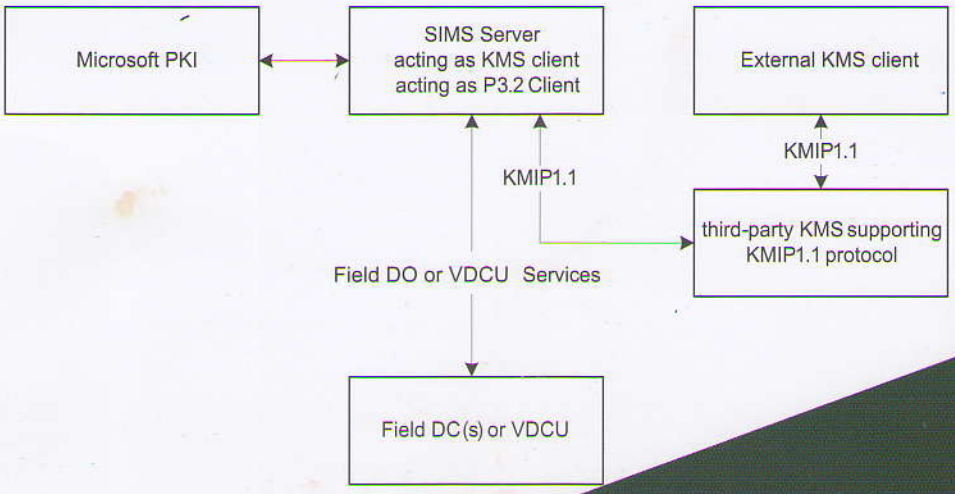
When choosing the appropriate AMI solution Distribution System Operators need to pay attention to security so as to:

·Ensure compliance with current and ever-stricter government regulations.
·Avoid leaks of sensitive information that may impact utility's image and cause lawsuits.
·Protect consumer data related to power consumption
·Assure the continuous availability of the AMI system notwithstanding potential hostile attacks

Many companies seriously think about securing the sensitive information and communication only after there has been some leak instead of proactive approach to secure its critical data.

By choosing a secure-by-design solution, like ADDAX AMI solution, utilities can quickly deploy a secure solution and protect their grid for the decades to come. ADDAX AMI that is connected to a FIPS-140 military-grade Thales eSecurity Key Management System.

SIMS/KMS architecture



www.addgrup.com
+373 22 930 012
info@addgrup.com +373 22 930 015

KEY MANAGEMENT SYSTEM SECURITY

Security

BENEFITS OF ENFORCING IT SECURITY OF ADDAX IMS:

Compliance with data protection regulations

Customer privacy and avoidance of embarrassing leaks

Protection of AMI from cyber attacks and technological risks

Hardware-based Key management Solution provides hardened key storage

Compliant with industry standards

SIMS INTEGRATES WITH:

External third-party KMS *(Key Management System)*, accessible via KMIP *(Key Management Interoperability Protocol)* for managing keys, X.509 certificates and other security sensitive information of field devices.

Microsoft PKI *(Public Key Infrastructure)*, for sending certificate signing requests;

Microsoft Active Directory, for managing SIMS users. Users are assigned to freely defined groups, with a rich set of selectable user rights assigned to each group.

AS RESULT, THE FOLLOWING MANAGING PRINCIPLES ARE USED IN CRYPTOGRAPHIC SERVICE:

Security materials are not stored inside of SIMS. All security materials are stored in external KMS;

End user *(regardless of user rights)* does not have access to security materials from SIMS at all

field-device security is configured by templates. A typical template consists of:

- Relevant information security policy *(i.e., DLMS/COSEM security policy)* settings;
- The list of keys descriptions *(not values!)* or certificates

End user may apply a template to a group of field devices, and monitor the actual progress. For applying a template, SIMS performs a set of tasks.

As usual, the following tasks are performed:

-Requesting new keys/passwords from the KMS;

-Requesting X.509 certificates from the Microsoft PKI;

-Transfer new relevant security materials to meters and data concentrators;

-Registering security material status in the KMS.

Security materials installed during the manufacturing process may be imported to the KMS.

SECURING DEVICES ON MANUFACTURING

STRENGTHENING SECURITY OF FIELD DEVICES

Strengthening security of meter by enabling HLS with authenticated encryption

Strengthening security of DC (enabling HTTPS/X.509)

SECURE COMMUNICATION BETWEEN AMI COMPONENTS:

Secure communication between DC and MDM

Secure communication between different MDM components (inside MDM layer)

Secure communication between SIMS and DC

Secure communication between DC and meters

e-Security keyAuthority® version 4.0

ACHIEVE COMPLIANCE AND AUDIT GOALS

The key manager enforces policies and maintains logs within secure facilities for reporting integrity.

Policy-based controls – Domains and key groups maintain rules for key access and sharing

Asingle point for auditing – A dedicated auditor role simplifies limited system access for reporting activities

Alerting and export – System functions are logged, with the ability to notify through email, SNMP, and syslog, and to securely export audit logs for control attestation

REDUCE COMPLEXITY WITH A UNIFIED APPROACH

The key manager simplifies management by enabling a single global system to maintain. Administrator time and cost is reduced through a unified approach based around best practices.

Single key manager – Application, compliance, and security teams manage centrally from a single console to reduce the need for additional key manager servers

Role-based access controls – Well defined entitlements and separation of duties maintain accountability across applications

Current and legacy protocols – Standards-based and proprietary device interface support provides the flexibility to extend key management to future new applications

CONFIDENTLY MANAGE ENCRYPTION

Key manager reliability for key recovery is a top priority to control data access with confidence.

Encryption deployment is simplified through pre-qualified device integration.

Device certification – Tested and validated solutions based on the KMIP standard accelerate setup and deployment

Extensible – A vendor-neutral approach allows new KMIPcompliant encryption devices to be integrated quickly as new products become available

MEET CONTINUITY AND DATA RETENTION NEEDS

The performance-optimized appliance secures keys long-term using a redundant hardware design to help ensure access

Redundant, FIPS-validated hardware – Hot swappable fans and power supplies, mirrored disks, and tamper-resistance features lower the risk of downtime

Synchronized key replication – Automated failover to a mirrored appliance helps ensure high availability for business continuity

Key backup – Routine backups via NFS to offsite data centers enable quick recovery

* ADD Grup partners with Thales and uses e-Security keyAutority