



Power-Grid Security

Protecting National Infrastructures Against Tampering and Espionage

As top officials debate concerns about growing vulnerabilities of national power-grids and advanced metering infrastructure (AMI), MerlinCryption delivers encryption protection for energy providers and end-users.

While firewall is important, it still leaves the smart-grid at risk. Cloners can defraud IP addresses and other protocol methods to force a system shutdown and infiltration. MerlinCryption's security process not only denies access, but also ensures data integrity with encryption, while alerting operators of foul play.

MerlinCryption accommodates minimal CPU requirements with the 200KB Embedded Encryption Platform, the 55KB Low Overhead Platform, and a 22KB encryption engine.

The MerlinCryption cryptosystem's patented random data generator outputs keys and passwords, which are 'generated-destroyed-recreated' on demand, making key/password transfer between end points unnecessary. The communication and storage of encryption keys and passwords are not needed. Costly PKI and risky CAs are eliminated.

Energy providers, industrial-control system manufacturers, and grid operators benefit from the embedded platform's stochastic randomization attributes. The ability to customize MerlinCryption's dynamic components within individual utility companies, reinforces and strengthens security, while decreasing vulnerability of tampering and espionage across the overall smart grid network.

ADVANCED TECHNOLOGY

SOFTWARE & HARDWARE SOLUTIONS

- Embedded Encryption Platform SDK
- Low Overhead Embedded Encryption Platform SDK
- Four-Factor Encrypted Authentication
- Patented Random Data Generator
- Encrypted Storage Media: USB, SSD,

MARKET APPLICATIONS

- **Verticals:** Military • Healthcare • Financial • Law
- **Horizontal:** Cloud • VoIP • eCommerce
- **Infrastructure:** Storage • Virtualization • Communications • Network Management
- **Embedded Connectivity & Device:** IoT • M2M
- **Media Storage:** USB • SSD • Other

TECHNOLOGY SPECS & STATS

- Encryption speed more than twice as fast as AES
- Highly efficient minimal overhead code:
 - Platform = 200K
 - Low Overhead Platform = 55K
 - Encryption Engine as small as 22K
- Portable to any CPU
- Encrypted Payloads transmitted by any communications protocol and on any network
- 1 Patent, 1 Patent Pending
- Eliminates PKI, Cert Authorities, Key Depository
- Written C & C++ for Linux, Windows, DOS, & custom
- Approved for export NLR & OFAC compliant
- Provides compliance with HIPAA, HITECH, & other regulatory guidelines

The Smart-World's Smart-Encryption®

Outmaneuver Attack: Dynamic 4-Factor Authentication

The man-in-the-middle strives to intercept messages, change updates, block alerts, or other false data injection between meters and the utility company. In this instance, the attack against the grid is identified through MerlinCryption's dynamic, variable, changeable authentication.

Authentication is typically based on something you know, something you have, and/or something you are. MerlinCryption secures authentication to the next level by incorporating additional methods based on dynamic

"temporary" factors. This unexpected category includes non-linear and environmental factors, which aptly detect risk of compromise.

The indomitable power behind this solution is not only in the *number* of factors available, but also in the ability to customize each client with factors that are unique to their business environment.

Status messages, alarms, and alerts securely, dynamically, and flexibly transmit between operators, security intelligence, and machines in a sub-second response.

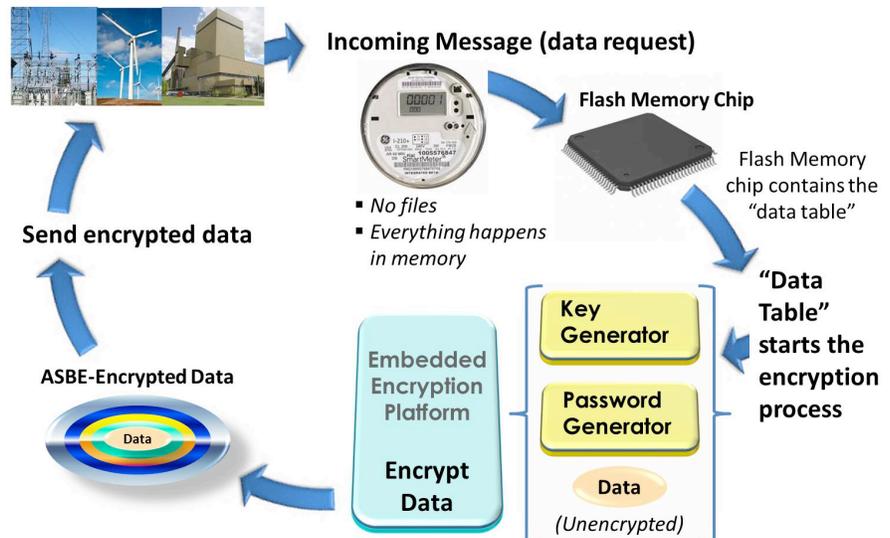
Advanced Innovation: Stay Ahead of the Curve

MerlinCryption uniquely applies stochastic randomization in various aspects of the technology, including the Anti-Statistical Block Encryption (ASBE) algorithm, authentication, key and password generation, and a platform solution.

The patent pending Embedded Encryption Platform utilizes variable key length. Each key scales in size between 2008 bits and 2 GB and enforces scalable passwords up to 64 KB. The ASBE algorithm is not subject to Statistical Analysis or attacks by Cryptanalysis, which secures data, networks, and endpoints across the entire SCADA infrastructure.

Every encrypted transmission between power plants, remote terminal units (RTUs), and meters is different, as the algorithm produces different cyphertext, even when repeating the same plaintext, key, and password input.

*MerlinCryption's
Patent pending embedded
encryption platform SDK is
highly conducive to
integrating into code
modules of other solutions
for a wide variety of use
cases, including Power-Grid
system environments*



Game Changers

- ASBE is more than twice as fast as AES
- Encryption engine as small as 22KB, embedded encrypted platform 200KB, and low overhead platform is 55KB,
- Encrypted Payloads are transmitted by *any* communications protocol and on *any* network
- The encryption software is portable to any CPU
- Two Embedded Encryption Platform SDKs streamline easy implementation
- Written in C and C++ for linux, windows, and can be compiled for other operating systems

THE SMART-WORLD'S SMART-ENCRYPTION®

MerlinCryption develops infrastructure encryption security for embedded, Cloud, VoIP, ecommerce, M2M, IoT, and USB hardware. Breakthrough technology secures dynamic end-to-end encryption for Smart-Grid, SCADA, industrial systems, control, healthcare, financial, and military..

Unprecedented Embedded Encryption Platforms protect data as it is created, viewed, edited, shared, stored, and moved securely across communications channels and in the Cloud.



MerlinCryption Is Changing The Way The World Protects Data

PO Box 150284 | Austin, TX 78716
512-348-SAFE
www.MerlinCryption.com