

# MerlinCryption®

## Leading-Edge Encryption

### *Distinctly Different Key Approach*

Data security in the contemporary business environment is increasingly complex, requiring acute acumen and calculated strategy. With new levels of severe and sophisticated threats penetrating the most fortified systems, a drastic change in security tactics is mandatory.

MerlinCryption meets this demand with an Enterprise Encryption Platform... vastly more powerful encryption, with unpredictable and changing keys, which defeats increasing computer-power and criminal investigative technique.

Utilizing Anti-Statistical Block Encryption (ASBE), the algorithm is not subject to attack models and methods of Cryptanalysis, not based on mathematical technique, and not subject to statistical analysis.

No two encryptions are alike: Each encryption process always results in a different cyphertext with varying length, even when repeating the same plaintext to encrypt, key, and password.

ASBE allows variable length keys that scale between 2008 bits and 2GB, as well as scalable passwords to 64KB.

## Keys and Passwords: Absolute Stealth For Today's Precarious Environment

MerlinCryption overcomes the two major weaknesses in encryption security: 1) short, fixed length, identifiable keys and 2) detectable, predictable key communication.

Common encryptions, such as DES, RSA, and AES, produce simple short key strands, which continually repeat in ciphertext. These fixed-length keys are detectable and they must be sent back and forth between users.

MerlinCryption's variable keys and passwords are sequences of bytes extracted from randomly generated

data files, which can be automated from a data generator or by using the contents of any digital file.

These dynamic keys-in-a-file (CryptoFile®) and passwords-in-a-file are scalable in length, using any portion, or all, of the contents of the file and can be designated in varying locations within the file.

Keys and passwords are user-determined and controlled unpredictable to hackers, versus application-generated and constrained in a way known to hackers.

## TECHNOLOGY HIGHLIGHTS

### PROPRIETARY ALGORITHM

- Not based on mathematical technique
- Not subject to statistical analysis
- No two encryptions are alike, even using the same input

### KEY-IN-A-FILE TECHNIQUE

- Key scales from 2008 bits up to 2 GB
- User-controlled random data key
- Initiated from data generator or digital file
- Key exchange not required

### PASSWORD PROTECTED

- Typed-in PW up to 31 characters, or
- Password-in-a-File 32 - 65,535 bytes

### SIMPLIFIED KEY MANAGEMENT

- Eliminates PKI
- Intrinsic Validation
- No Central Key Depository Needed

*Adapts for enterprise, M2M, and embedded markets. Scales to any business structure.*

## Effective Enterprise Security: Do More With Less

MerlinFusion™ is the core encryption engine in both MerlinCryption Enterprise Encryption Platform and MerlinM2M Encryption Platform. These automated platforms seamlessly generate random data keys, encrypt, scrub memory, and decrypt under the hood, end to end.

The cryptosystem platform's data generator outputs keys and passwords that are 'generated-destroyed-recreated' on demand, eliminating transfer between end points. Each platform incorporates dynamic multi-factor authentication and is run by a scripted controller that 'wraps' the process into a tightly customized and impenetrable sequence of execution.

In an enterprise environment the CryptoFile® approach eliminates Public Key Infrastructure (PKI) and its associated costs, such as Certificates, Registration Authority, and Directory Management. Key protocol not needed. Validation becomes intrinsic. A Central Key Deposit is no longer necessary, as communication and storage of keys and passwords are not needed.

The Enterprise Platform effectively works in tandem with MerlinCryption's stand-alone security programs, based on individual business goals and needs. A simple security blueprint, reinforcing an individual organization's security and operational structure, replaces the complex key lifecycle.

IT has the ability to control all keys or designate key initiation to specific departments and/or individual users.

Management can independently use the encryption process or collaborate with IT departments for automated use.

'Flexible Options' leverages role-based access rights for authorized user ease and accommodates clients, vendors, and end users who have contrasting levels of sophistication or need-to-know status.

In machine-to-machine, embedded, and OEM environments, the MerlinM2M Encryption Platform delivers a small memory footprint in flash memory and files and is portable to any device. Encrypted data-payloads can be sent over *any* transport mechanism, *any* communications protocol, *any* network.



*Research shows that organizations spend between \$47 and \$592<sup>1</sup> for the creation, distribution, and maintenance of each PKI key in use.*

*MerlinCryption Eliminates PKI, Certificates, Registration Authority, Directory Management, Central Key Deposit, External Validation, and Protocol.*

## Encryption Innovation: Partnering in Breakthrough Technology



*Shape-Shifting Encryption:  
Do Now, What You Couldn't Before*

Delivering specialized encryption solutions to companies that need a security component, MerlinCryption helps embedded, M2M, and OEM partners solve challenges and create new opportunities. By bundling breakthrough technology into their solution, partners provide their customers a complete integrated offering with flexible and compliant security.

MerlinCryption business partners benefit from accelerated time to market, reduced development costs, and improved profitability with benchmark encryption security offerings.

MerlinCryption's forward-thinking technology is built for change, easily integrated, adaptable, and scalable. It bundles and assimilates easily into existing ecosystems, strengthening the partner's application as it is... and as it evolves in the future.

## SUPERIOR SECURITY IS IN THE DETAILS

- NSA reviewed, BIS approved for export. OFAC compliant.
- All products check program size to detect tampering and alert if altered.
- All encryption/decryption products scrub memory before exiting
- The log file records all actions taken
- Upon decryption, MerlinCryption performs multiple-stage checking of version, key, and password.
- Automation produces mass-quantity, sub-second file encryption using command line switches with batch mode or shell scripting
- Speed Optimized: Encrypting or decrypting a 1MB file with a 1MB key takes less than 1 second to process on 3.2GHz PC.
- Source code not sold. Only full program execution can be scripted
- HIPAA, HITECH, FDA compliant
- Runs simultaneously with different and multiple applications
- Supports Windows, Linux, DOS, QNX
- User-Centric Security in the Enterprise
  - “Click and Go” GUIs, printable quick guides, and IT handbooks make user self-training an intuitive snap.
  - Online support, help desk, video tutorials, and user forum support ongoing enrichment
  - Decryption-Friendly. Recipients do not need to purchase to decrypt files. Free decrypt-only MerlinReader is downloadable on the website.
- Technology is scalable and adaptable for individual, enterprise, and partners



## MerlinCryption Technology Software

**MerlinFusion™** is both a stand-alone encryption program for IT professionals, and serves as the core of the encryption engine in MerlinCryption’s Enterprise and M2M Platforms.

Fortified with Anti-Statistical Block Encryption (ASBE), the algorithm defeats cryptanalysis, is not based on mathematical technique, and not subject to statistical analysis. The ASBE algorithm always produces different ciphertext results, even when repeating the same data input, same key, and same password. No two encryptions are alike.

Variable, scalable keys and passwords are flexibly created from arbitrary sources rather than deterministic and predictable software-initiated keys.

- CryptoFile embedded key-in-a-file scales in size from 2008 bits to 2GB.
- PasswordFile embedded password-in-a-file to 65,535 bytes in length.

**MerlinFusion Stand-Alone Software for IT Professionals** highlights two program modes to accommodate contrasting levels of access rights and user sophistication.

- EZ Option for busy people and general users with little “need to know” access. An algorithmically chosen mutable key and secret password enables immediate encryption action.
- FLEX Option with user-chosen key and password variables implement fine-tuned role-based security. Allows parameter variables for key and Password input, leveraging measured control and monitoring.

*Every MerlinFusion purchase includes the following independent applications.*

**MerlinGen** random data generator initiates 4 Billion different files ranging in size from 10K to 64K bytes. Each file generated, has over 100 million possible keys or passwords.

**MerlinShred** Five-pass overwrite and delete feature destroys any file.

**MerlinFileView** IT tool views the contents of any file in hexadecimal.

**MerlinReader®** Decrypt-only for non-MerlinCryption file recipients.

**Smart-Encryption Engine for Enterprise and M2M Platforms** is the under-the-hood powerhouse for exponential security, agility, and speed. These automated platforms also include multi-factor authentication, dynamically changing random data generators, and memory scrub and are run by a scripting platform controller.

- Enterprise and M2M partners highly benefit from customization of each encryption engine, which is unique to the individual company’s system and is not interoperable with any other custom engine or standard MerlinFusion software.
- Supports role-based security architecture and access rights management in the enterprise
- Provides machine-to-machine automation for remote machines and all devices.
- No PKI involved.

# The Best of Class Enterprise

## People >Process >Technology >Success

MerlinCryption Enterprise Encryption Platform establishes a complete encryption solution utilizing uncomplicated software mechanisms in tandem with strategic process, designed upon the individual organization's security needs and business structure. This cutting-edge approach successfully positions impenetrable security with affordability and ease.

### START-UP AND DEPLOYMENT

- Rapid integration: Upgrade from a PKI system or launch an original CryptoFile system with uninterrupted security and seamless change management. (No more PKI)
- Efficient implementation and acculturation: *No laborious design phase needed.* MerlinCryption's design-efficient solution assimilates easily to existing security ecosystems, strengthening the organization now, as well as securing its future.
  - The enterprise structure is strategically mapped with desired security paths, aligning organizational scenarios and various authorized user group nuances with airtight security.
  - Relevant mechanisms are determined and scripted to interface with MerlinCryption solution software
  - Once the enterprise security map is established, random data generation for keys and passwords executes in less than a second.
  - Intuitive training supports easy commercialization into the business environment while ease of use expedites favorable adoption by leadership, employees, vendors, clients, and other business partners.

### SCALE OPPORTUNITY

- The MerlinCryption secured enterprise leverages encryption security at a significant scale
  - Increases encryption-enabled application capability with minimal deployment cost
  - Vastly expands keys in use with significant efficiency
- MerlinCryption's astute security-blueprint solution adapts and scales from small businesses, without dedicated IT staffs, to large conglomerates with extensive geographies, business units, and functional areas supporting multiple priorities, objectives and agendas.

<sup>1</sup>[http://www.nyimity.com/Free\\_Privacy\\_Resources/Previews/ReferencePreview.aspx?guid=8539fba5-9d92-4293-b3ea-d10bf4b52cf0](http://www.nyimity.com/Free_Privacy_Resources/Previews/ReferencePreview.aspx?guid=8539fba5-9d92-4293-b3ea-d10bf4b52cf0)

## DATA-IN-USE • DATA-IN-MOTION • DATA-AT-REST • DATA-IN-CHANGE

MERLINFUSION: Business protection with versatility and client solutions

MERLINEZ: Protection for data file storage and transfer... simply

MERLINEYE: On-screen protection for creating, viewing, and modifying data.

MERLIN4CHAT: Instant messaging, email, and broadcast protection

*Custom versions for individual specification and unique solutions*

**MerlinCryption Is Changing The Way The World Protects Data**



512-348-SAFE | [www.MerlinCryption.com](http://www.MerlinCryption.com)

PO Box 341133 | Austin, TX 78734