MicroToken Exchange Data Security Solutions

The MicroEncryption® Process

A Solution for Securing Data-At-Rest

Eclypses MicroEncryption -

MicroToken Exchange

Architecture for Securing Data

Understanding MicroEncryption®

MicroEncryption methodology, developed by Eclypses, is revolutionary in that speed and accessibility are not sacrificed when utilizing this platform architecture.

This is critical when considering the effects of additional latency regarding user's experiences, in and around "the cloud".

While Tokenization has existed since the emergence of the world's first currency systems, it was developed as a means to minimize risk in handling high value financial instruments by replacing them with placeholders.

How It Works

MicroEncryption concepts are now providing a security mechanism for both small and larger scale data protection. It is just one of the applications of MicroToken Exchange®, or “MTE”. Fully deployed, MicroEncryption creates the ability to facilitate end-to-end robust protection, securing data in rest as well as in transit. The premise behind our storage methods is the reality that thus far, bad actors have proven time and time again that they can get into systems. So, with that in mind, MTE ensures that not if, but when they do so, there is nothing of value for them to steal.

The first step in the process is taking a MicroToken™ and implanting it to replace an individualized data element or elements, down to the field level of a record within a database, or a file, of most any type. Within a database, the non-sensitive data fields would remain in place. The concept of protecting only that which requires protection is one of the secrets to maintaining millisecond speeds. Once a piece of data is MicroEncrypted, all that would reside are non-sensitive data field elements along with MicroTokens. These MicroTokens are placeholders, that do not contain any part or piece of the original sensitive data. Typical tokenization methods both use parts of the original data to create the token, as well as at times, expose some of the real data within the token itself.

MTE does NOT. Additionally, the majority of industry type tokens used today utilize the initial six digits, (as Bank Info), along with, or in combination with the last four digits, (card account #), to derive their tokens from. Our MTE MicroTokens are agnostic, and by not using any part or piece of the original data, make it mathematically improbable that they could ever be reverse engineered, even when attempted by quantum computing methods.

With the deployment of MicroEncryption, in the event of a breach though perimeter defenses, including after an encryption scheme is broken, there is NO sensitive data contained within that system to be exploited because it is no longer there. It has been removed.

Data-At-Rest

Provides Data Integrity

Elinimates Mass Data Breaches

eclypses

Comparing MTE To Encryption

Unlike “Bulk” encryption, each data element would be secured and protected as if it were its own database with its own sets of keys and master keys. These keys are never stored in usable fashion, should they ever be exposed. For example, a database with 100,000 records, in which 10 sensitive fields were to be protected, would be secured as if it were 1,000,000 individualized databases. MTE executed in near real-time.

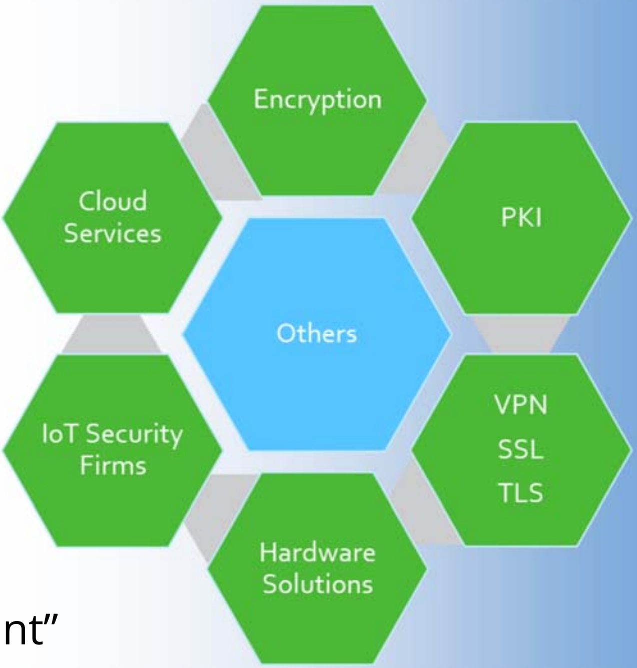
As a MicroToken is implanted to replace original sensitive data elements within the confines of a securely hardened architecture, the individual data elements are removed, relocated, and then encrypted within the new secret location, (The Eclypses Digital Vault).

Additionally, for customized solutions, a programmer’s algorithm of choice can be used. When the data being stored is larger than a single field, (Client specific in customer applications), immediately after encryption occurs. the encrypted piece of data is then broken apart into multiple encrypted pieces or segments. The encrypted segments or individualized micro-pieces of encrypted data are then distributed through an array of varying and randomized hard drives. The sensitive MicroEncrypted data remains fully protected until the very last moment that its use is called upon by an authorized action, and by an authorized user. A multitude of business rules can be integrated for additional layers of protection.

MANAGE RISK
Risk Management
SECURITY
Secure Data From Successful Intrusion
COMPLIANCE RULES GUIDELINES REGULATIONS LAWS
Ensure Confidence And Trust
Security Protection Is Our Highest Priority

eclypses

Database Protection



MTE handles all the “Key Management”
so that others do not have to.

MicroEncryption is agnostic to the type of data protected, as well as type of encryption that has already been applied before being MicroEncrypted. Eclypses systems receive data in most any form and additionally applies its own encryption, while returning the data, when requested, in the same form as it was presented in the first place.

MicroEncrypted data is not only ultra-secure but also readily accessible for real time performance so as to have an unnoticeable impact on the user experience. At the time of need, in database applications, as only sensitive fields are secured and protected individually, they are typically only a few KB in size, making them available to be returned in near real-time. When MicroEncrypted within the same datacenter, we typically see speeds that eliminate any latency concerns. Also, important to note, when that same sensitive data is required for use, only that data that is called upon is decrypted and returned, leaving the balance of the sensitive information fully protected and securely stored. In a typical encryption/ firewall scheme when multiple users are accessing the database, a large portion, if not all of a database sits open in resident memory, exposing it and making it susceptible to attack.

While there is the existence of database encryption schemes, most all are limited to entire rows and columns, not the individual fields. Along with its many layers of protection, our MTE process requires multiple sets of keys to unlock a single piece of data. MTE processes, however, do not store all the keys, and in theory, provides the last key only after several steps have been verified and completed, thus making it mathematically improbable that a piece of data could be

Geo-Disbursement Capabilities

The Eclypses team has also developed a Geo-Disbursement engine, in conjunction with all our services, that both allows and provides the c apability for sensitive data to be stored, in an automated fashion, in the exact location required to comply with various country rules and laws, such as GDPR. While the data is both sent in transit to the appropriate Digital Vault as well as while the data is stored in its final resting place, MTE secures it from start to finish.

In the digital age, tokenization technology was originally intended to prevent the theft of the credit card information while it was being stored. MicroEncryption has created a paradigm shift so that tokenization can now be applied to “Big Data”.

With the advent of MicroEncryption, information remains accessible and usable, while exceeding industry security standards and regulations, thus for the first time, making the possibility of a mass data breach mathematically improbable. And we believe nearly impossible.

To appreciate how this technology evades the ever-lurking threat of exploitation, imagine taking a phone book from a large metropolitan area, first separating each individual first name, last name, street name, address, phone number, and zip code, encrypting each piece, then chopping up those encrypted pieces. Then imagine taking those millions of separate encrypted chunks pieces, shaking them up in a bag, and then giving the bag to somebody to put back together to resemble the original phone book. The person would probably look at you as if you had lost your mind!

Even if somehow, some way, the data could be unencrypted at that point, the challenge would not look much different and the outcome would remain unchanged. The data could not be reassembled into anything meaningful. Essentially, this is what the MicroEncryption technologies do in a cyber setting. Even if the hackers can breach the firewalls, what they find inside are meaningless MicroTokens. One can see how these technologies take the cat and mouse game to a whole new multidimensional level. The platform architecture interacts seamlessly and transparently, streamlining protocols, saving both time and money.

eclypses

Next Generation Data Security

MicroEncryption services are highly scalable, adaptable, and easy to utilize and do not require costly changes to a client's (or client 's partners) business practices or legacy systems.

MicroEncryption is surprisingly easy to implement, whether for businesses or for individuals that have an ongoing need for secure data storage.

MicroEncryption is believed to be the next generation of security and will serve as the catalyst for revolutionizing the storage of sensitive digital information challenges within a cloud environment . Its processes are 100% agnostic with respect to computer architecture and require nothing to install, thus making it friendly and simple to integrate into one's cyber security system. A new security paradigm is required to secure sensitive data in the event of a perimeter defense breach. While penetration testing is still quite the common practice, it does not solve the cyber challenge we face today. It only shines a light upon it.

Twenty-first century information sharing requires trusted, self-sufficient secured data backed by the best technology. This technology must provide full assurance that the information is genuine, unaltered and completely trustworthy and unavailable to internal or external exploitation. This new paradigm must ensure that only the right people get access to the right information at the right time.

Eclypses MicroEncryption capabilities ensure that data at rest and data in transit remain BLACK and unavailable to exploitation even in the event of a traditional network defense breach.

eclypses

Securing Data via MicroToken Exchange

Ensuring that sensitive data remains unavailable to exploitation in the event of an internal or external network breach

Contact Us

Info@Eclypses.com
www.Eclypses.com
+1.719.323.6680