VIRTUALIT™

OnePoint Corp.

La importancia de la encriptación de información para cumplir normas PCI y prevenir fraudes

cyte
We-know-how

OnePoint® Corp.

PORTAFOLIO DE SOLUCIONES

Febrero 2022

GRUPO TECNOLÓGICO ONEPOINT CORP.

- Empresa pionera en Ecuador
- Más de 16 años de experiencia
- Proveedor de soluciones integrales
- Expertos en virtualización y cloud computing

- Más de 18 años de experiencia
- Expertos en gestión de proyectos de TI
- Expertos en RPA
- Especialistas en soluciones tecnológicas basadas en software y aplicaciones

VIRTUALIT®

InnovaSys®

Ofrecemos soluciones tecnológicas con el objetivo de que nuestros clientes sean productivos y eficientes, haciéndolos más competitivos, permitiendo así su crecimiento.

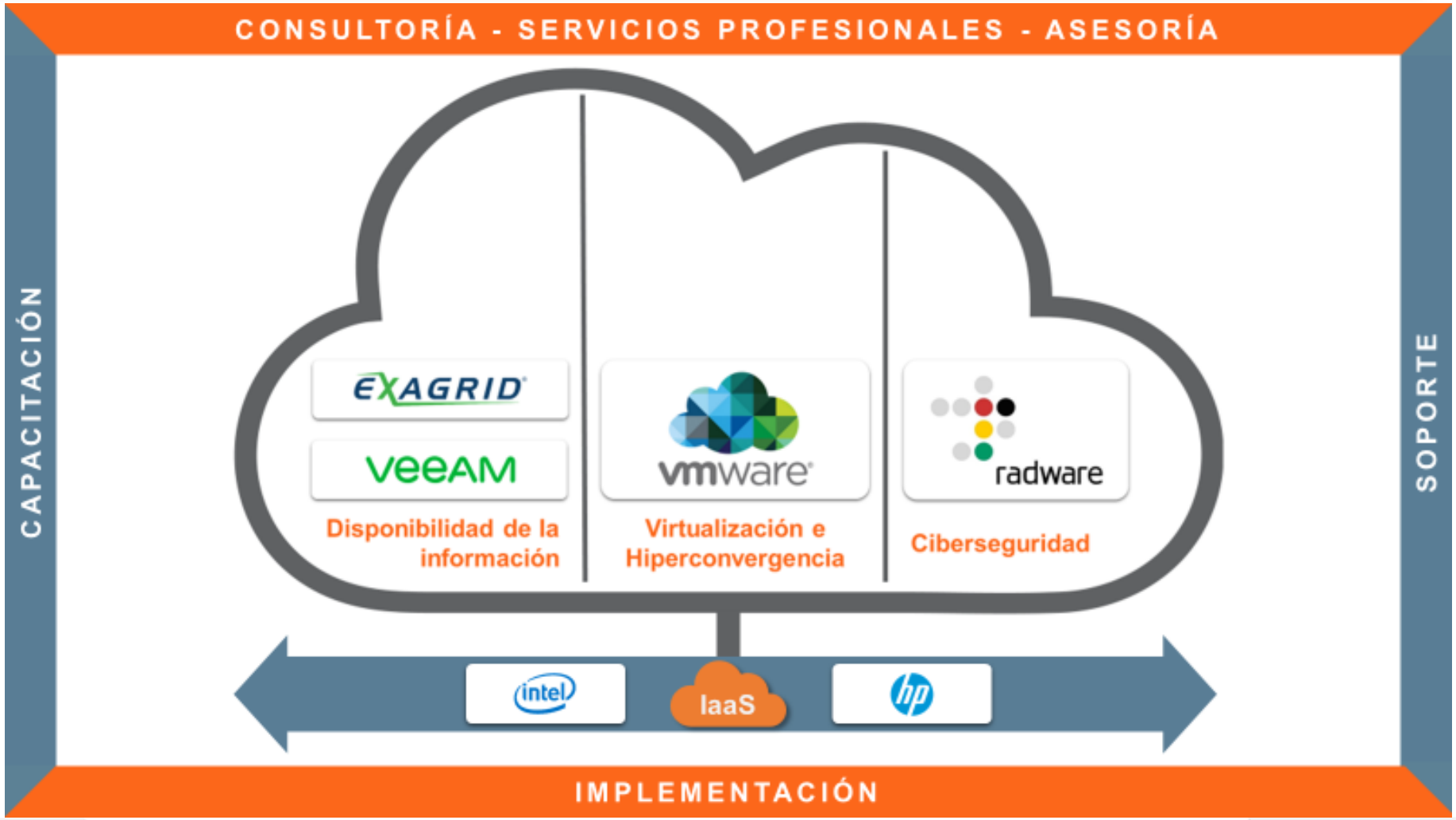
VENTAJAS COMPETITIVAS

OnePoint Corp.

PORTAFOLIO DE SOLUCIONES INNOVASYS

PORTAFOLIO DE SOLUCIONES VIRTUALIT

OnePoint Corp.



NUEVA SOLUCIÓN EN SEGURIDAD DE LA INFORMACIÓN

OnePoint Corp.

cyte
we-know-how®

Fabricante de soluciones de criptografía para la protección de información sensible. Sus soluciones permiten generar espacios de trabajo seguros, eficientes y confiables para salvaguardar la propiedad intelectual de las organizaciones.

ALGUNOS CLIENTES DEL GRUPO TECNOLÓGICO ONEPOINT CORP.

OnePoint Corp.

Produbanco Grupo Promerica

CPN Cooperativa Policía Nacional

BANRED LA RED INTERBANCARIA MÁS GRANDE DEL ECUADOR

IESS INSTITUTO ECUATORIANO DE SEGURIDAD SOCIAL

CELEC EP Corporación Eléctrica del Ecuador

SRi ...le hace bien al país!

ASERTEC ASESORES DE SEGUROS

SEGUROS EQUINOCCIAL TÚ DEDÍCATE A VIVIR

Metrored Centros Médicos

QUIFATEX

Bagó

ORION ENERGY

EP PETROECUADOR

KUBIEC MÁS QUE UN BUEN ACERO

TELCONET

DIRECTV

Cnt

UIDE Powered by Arizona State University

Universidad San Francisco

TOYOTA

VIRTUALIT™

OnePoint Corp.

La importancia de la encriptación de información para cumplir normas PCI y prevenir fraudes

cyte
We-know-how

VIRTUALIT®
OnePoint Corp.

Mgtr. Samuel Sabogal Pardo

Consultor en seguridad de la información

CYTE

cyte we-know-how®

Presentador

Samuel Sabogal Pardo

- Ingeniero de Sistemas y computación de la Universidad Nacional de Colombia.
- Especialista en Seguridad de la Información de la Universidad de Los Andes.
- Becario Fulbright y Master of Science in Information Security de la Carnegie Mellon University, EE.UU. (Top 1 worldwide in the field).
- Tiene más de 15 distintas certificaciones.
- Investigador en Ciberseguridad, EE.UU. (Presentador en RSA Conference, RSA scholar).
- Más de una década en desarrollo software criptográfico, consultorías y hacking profesional en Colombia y EE.UU.
- Profesor de criptografía.

cyte
we-know-how®

La ciberseguridad es esencial

What Are the Top 6 Business Risks in 2022?

- Risk 1: ESG. ...
- Risk 2: Cybersecurity. ...
- Risk 3: Data Privacy. ...
- Risk 4: Rapidly Changing Regulatory Environment. ...
- Risk 5: Economic and Political Instability. ...
- Risk 6: Supply Chain Risks.

Dec 22, 2021

Riesgo top para cualquier analista:

- Forbes
- Diligent
- Visual capitalist
- Weforum
- etc etc etc
- **Post COVID: se agudizó el riesgo de ciberseguridad**

cyte
we-know-how®

Costo de un *data breach*

Según estudio global de IBM Security

- Costo promedio a nivel mundial: **US$3.86 million**
- Costo promedio en América Latina: **US$ 1.82 million**
- Costo de un data breach grande (Equifax): **US$575.0 million**

> *"The total cost of the settlement included $300 million to a fund for victim compensation, $175 million to the states and territories in the agreement, and $100 million to the CFPB in fines."*
>
> *Federal Trade Commission*

cyte
we-know-how®

Adicional a costo monetario…

- Pérdida de confianza de los clientes, pérdida futura en ventas
- Pérdida de partners actuales y futuros

Pérdida de reputación

•Cerrar el negocio

PCI DSS

Consejo de estándares de seguridad: Foro mundial

- Desarrollo y aplicación de normas de seguridad
- Enfocadas a datos de tarjetas
- Pretende reducir riesgos de fraudes
- Fundado en 2006 por VISA, American Express, Discover, Master Card y demás grandes marcas de tarjetas de crédito

cyte
we-know-how®

PCI DSS

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD

Aplica a toda entidad que usa datos de tarjeta para:

- Almacenarlos
- Procesarlos
- Transmitirlos

cyte
we-know-how®

PCI DSS - requerimientos

PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network and Systems	**1.**	Install and maintain a firewall configuration to protect cardholder data
	2.	Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	**3.**	Protect stored cardholder data
	4.	Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	**5.**	Protect all systems against malware and regularly update anti-virus software or programs
	6.	Develop and maintain secure systems and applications
Implement Strong Access Control Measures	**7.**	Restrict access to cardholder data by business need to know
	8.	Identify and authenticate access to system components
	9.	Restrict physical access to cardholder data
Regularly Monitor and Test Networks	**10.**	Track and monitor all access to network resources and cardholder data
	11.	Regularly test security systems and processes
Maintain an Information Security Policy	**12.**	Maintain a policy that addresses information security for all personnel

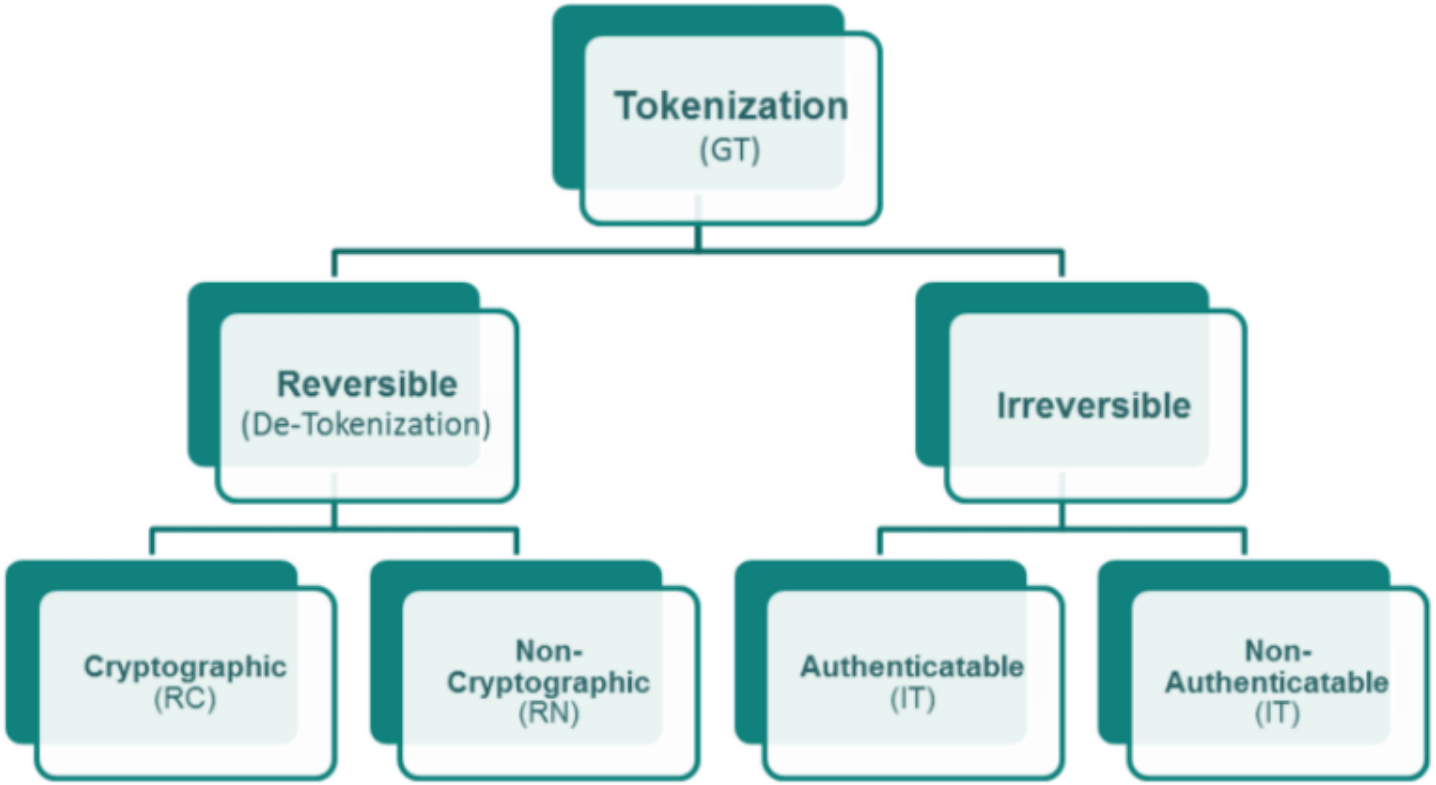
Perspectiva del atacante para brecha de datos

Cientos de ataques

- Una vulnerabilidad puede darse por un error del desarrollador, o de un o un defecto en cualquier pieza de software de terceros.
- Zero day exploits
- Existen herramientas automatizadas de ataques
- Tokenización mitiga una amplia variedad de brechas de datos

cyte
we-know-how®

Tipos de tokenización según “PCI: Tokenization Product Security Guidelines”



cyte
we-know-how®

Diferencia entre tokenización y cifrado tradicional:

Cifrado tradicional:
1234567890 -> ah\x98\xb437@\x87€€#s\-2\xff\dv!\xa8fap”/)18?-

Tokenizado:
1234567890 -> 6154873295

- Se logra criptográficamente con NIST FPE

*Nota: Antiguamente, se hacía con un mapeo entre el cifrado tradicional y un token generado arbitrariamente. Para las necesidades de hoy en día es sumamente ineficiente.

000001	xb437@\x87€
000002	a8fap”/)18?@
000003	\x98\xb437!!-

cyte

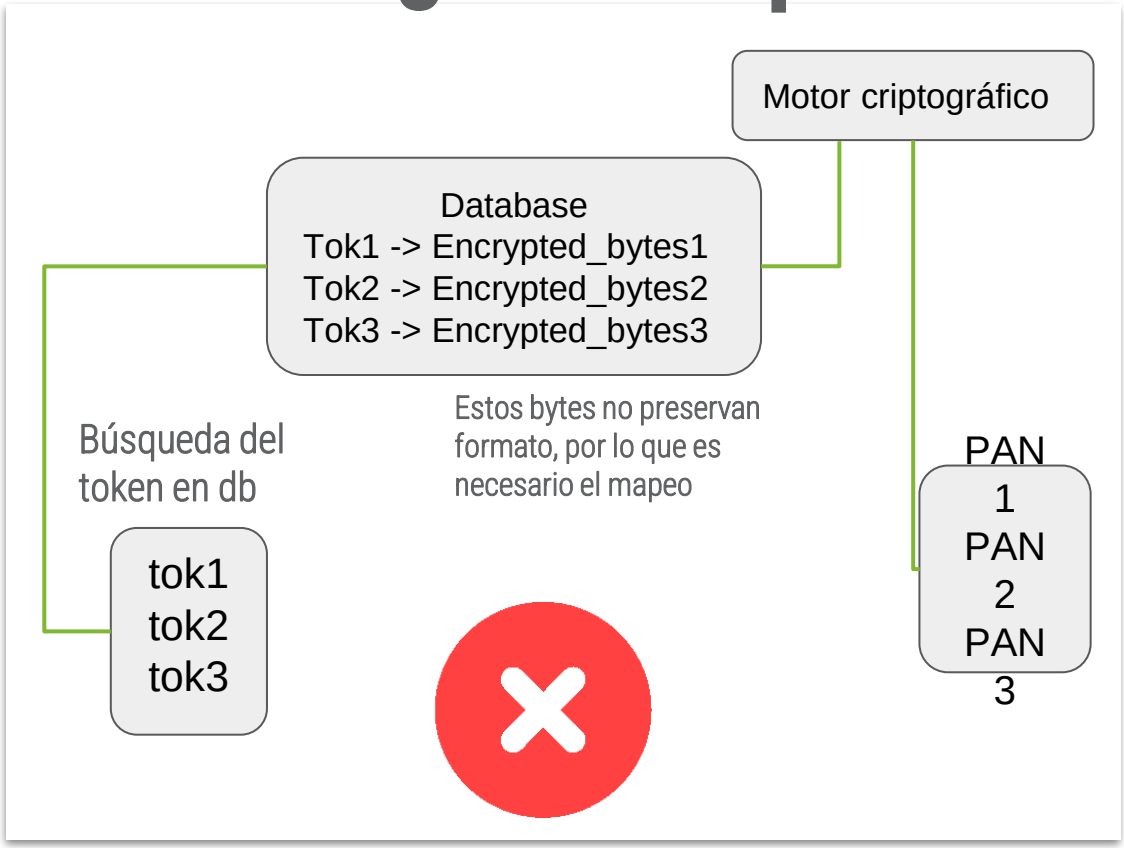
tokenizer

¿Qué es el tokenizador?

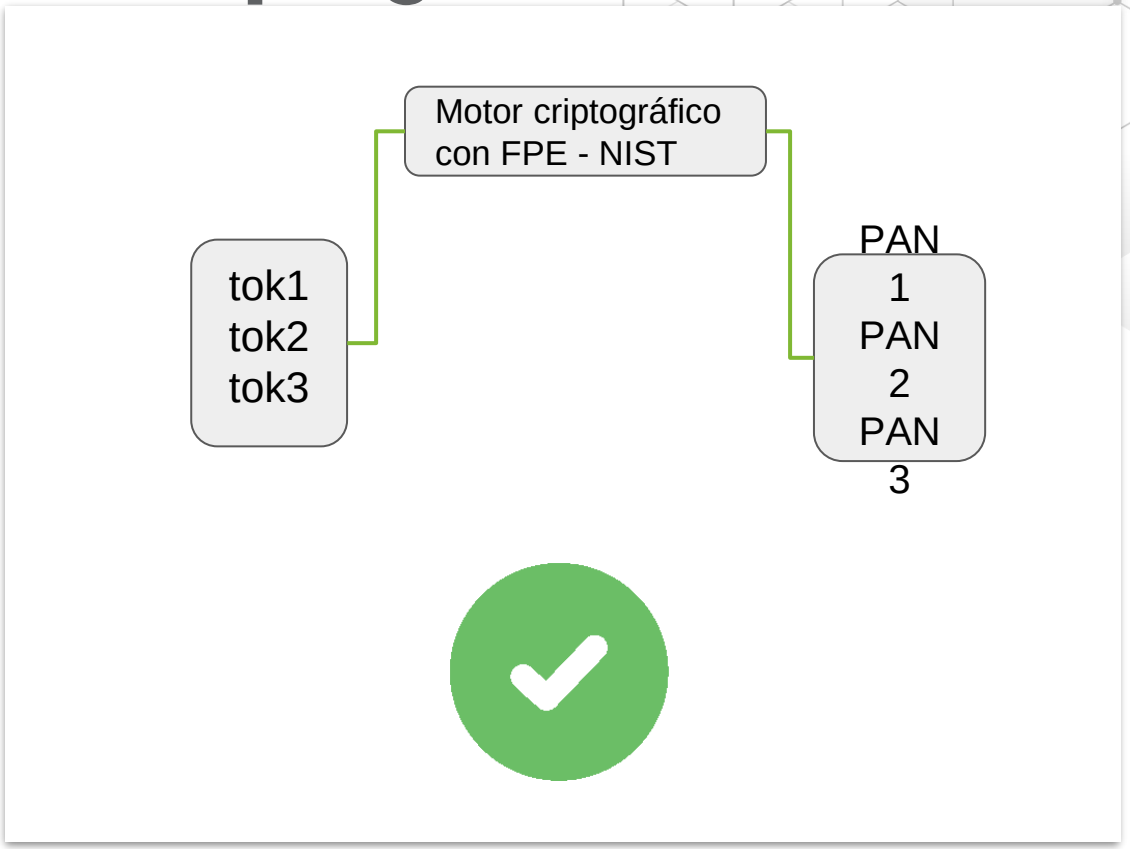
- Motor criptográfico que se integra con cualquier HSM
- Conjunto de interfaces para consumir eficientemente el motor localmente o cloud

cyte

¿Cómo opera el motor criptográfico?



- Costo extra en desempeño por IO de la DB
- Si se añaden procesadores extras, el cuello de botella es el disco
- Es inconveniente tener una base de datos adicional del mismo tamaño del total de los registros.
- Ej: Tengo 16 bytes cifrados, quiero descifrarlos a un resultado de 16 bytes, pero necesito una gran base de datos para hacer esta operación simple.



- No hay costo extra en IO
- Paralelización eficiente
- Si tengo 16 bytes cifrados, no necesito una base de datos
- Vanguardia en criptografía: Aprobado por NIST hace menos de una década

cyte
we-know-how®

El motor se integra a hardware criptográfico (HSM)

- Secure key storage (PCI DSS Requirements 3.5.3 and 3.6.3)
  - Anti-Tampering: auto destruye material criptográfico en caso de ataques

- Key generation (PCI DSS Requirement 3.6.1)
  - "Un generador físico de números aleatorios basado en un fenómeno de físico cuántica que es imposible de predecir." https://www.ibm.com/docs/es/power9?topic=ad-4767-002-cryptographic-coprocessor-fc-ej32-ej33-bsc-ccin-4767

- No es obligatorio utilizar HSM
  - Es recomendado para PCI, aunque es posible utilizar conocimiento compartido
  - Tenemos un módulo para almacenamiento de secretos compartidos

cyte

¿Que se puede tokenizar?

- Datos personales de un usuario
- Valores de un pago de nómina
- Valores de un contrato
- Números de tarjeta
- Direcciones
- Datos confidenciales del negocio específico

Alfabetos configurables. Ej:

```
Calle 127 # 06- 70    ->    0123456789#-abcdefghijklmnñopqrstuvwxyz
```

- **NOTA**: es posible usar el tokenizador para cifrar binarios como imágenes en BLOBS
  - Se aprovechan bondades como administración de llaves, eficiencia de comunicación y APIs del tokenizador

cyte
we-know-how®

Inicio del proceso: Creación de llaves

Creación de llave AES (Advanced Encryption Standard)

- Algoritmo de criptografía simétrica
- Recomendado por NIST
- Se envía únicamente el nombre de la llave
  - La llave nunca la ve un humano
  - Se crea usando el RNG

tokenizer

Tipos de datos tokenizados:
PANs, Direcciones, Historias clínicas… cualquier tipo de dato confidencial.

Tokenización masiva:
Se tokeniza una columna entera de una base de datos en un solo llamado

Tokenización individual:
Se tokeniza un dato que puede estar dentro o fuera de una base de datos

Interfaces:

HTTP

>_

library

Soporte para cualquier HSM

IBM

IBM 4767-002 PCIe Cryptographic Coprocessor (HSM)

THALES

aws Cloud-HSM

cyte

Tiempos de tokenización

- Tiempo: **1.8 millones** de registros aproximadamente **en un minuto**, utilizando 4 procesadores
  - **30 registros por milisegundo**

- En otros esquemas, se han visto tiempos hasta de un segundo por registro.

- Añadir uno o **más procesadores mejora el tiempo significativamente.**

¿Ahora, cómo proteger información en tránsito?

cyte

Realizamos implementaciones “consultivas”

- Una vez se inicia la implementación, se pueden hacer mejoras según se vean oportunidades
  - Desempeño
  - Simplicidad
  - Seguridad
- Equipo altamente calificado
  - Conectado con la academia
  - Décadas en la industria.

cyte

VIRTUALIT®

OnePoint Corp.

GRACIAS

Samuel Sabogal Pardo

info@virtualit.com.ec

cyte we-know-how®

Cosme Renella OE3-95 y Brasil
Quito – Ecuador

Tel (593) 99 731 3447

www.virtualit.com.ec