

TECNOLOGIA DE MONEDERO INTELIGENTE XIGA

1. Monedero electrónico emitido por personas.

1.1 Ficha técnica de Tarjetas

- Cumplimiento de los estándares ISO CR-80 (ISO 7810): Longitud 85,6 mm y anchura 54mm.
- Código QR: Longitud 20 mm y anchura 20 mm
- Vida útil de las tarjetas de PVC: de dos a tres años mínimo.

Hardware utilizado.

- Dispositivo para leer etiquetas con código QR Symbol Modelo DS3578.
- Dispositivo Apple iPod con sistema operativo iOS 11 para la lectura y validación de códigos QR

Software utilizado.

- Sistema operativo Window Server 2012
- Sistema ERP (administración).
 - Entorno de desarrollo: Framework .Net 2.0
 - Lenguaje: C#
- Ws Timex Centralizado (Punto de Venta).
 - Entorno: Framework .Net 4.2
 - Lenguaje: C#
- App del Despachador (iPod)
 - Plataforma: Framework .Net 4.2
 - Lenguaje: C#
 - Xamarin Nativo 11.8

1.2 Ficha Técnica de la APP del Cliente

- Software utilizado:
 - Sistema operativo Windows
 - Lenguaje: C#
 - Plataforma: Xamarin Forms versión 11.8
- Hardware utilizado iOS:
 - Modelo: iPhone 5 en adelante
 - Versión de Sistema Operativo: iOS 9.1 en adelante
 - Arquitectura: 64 bits
- Hardware utilizado Android:
 - Modelo: Varios
 - Versión de Sistema Operativo: Android 6.0
 - Arquitectura: 32 y 64 bits

1.3 Ficha técnica del Holograma con código QR

- Tamaño del holograma: Longitud 50 mm y anchura 25 mm.
- Tamaño del código QR: Longitud 10 mm y anchura 15 mm.

Hardware utilizado.

- Dispositivo para leer etiquetas con código QR Symbol Modelo DS3578.
- Dispositivo Apple iPod con sistema operativo iOS 11 para la lectura y validación de códigos QR

Software utilizado.

- Sistema operativo Window Server 2012
- Sistema ERP (administración).
 - Entorno de desarrollo: Framework .Net 2.0
 - Lenguaje: C#
- Ws Timex Centralizado (Punto de Venta).
 - Entorno: Framework .Net 4.2
 - Lenguaje: C#
- App del Despachador (iPod)
 - Plataforma: Framework .Net 4.2
 - Lenguaje: C#
 - Xamarin Nativo 11.8

NOMBRE DE CLIENTE (1)

IDENTIFICACION TARJETA (2)

XIGA MONEDERO INTELIGENTE

Atención a clientes
800 026 9442

Monedero Electrónico XIGA, S.A. de C.V.



XXXX-XXX|XXX (3)

Identificador	Especificación
(1)	22 caracteres alfanuméricos
(2)	25 caracteres alfanuméricos
(3)	12 caracteres numéricos
QR	Encriptado de información

La imagen muestra extracto del código fuente del módulo del monedero encargado de encriptar los datos del Holograma QR, donde se observa el uso del algoritmo 3DES con llaves MD5.

```
//Generar QR encriptado
#region Encrypt
try
{
    byte[] keyArray;

    byte[] Arreglo_a_Cifrar = UTF8Encoding.UTF8.GetBytes(tarjeta1);

    //Se utilizan las clases de encriptación MD5

    System.Security.Cryptography.MD5CryptoServiceProvider hashmd5 = new System.Security.Cryptography.MD5CryptoServiceProvider();

    keyArray = hashmd5.ComputeHash(UTF8Encoding.UTF8.GetBytes(key));

    hashmd5.Clear();

    //Algoritmo TripleDES
    System.Security.Cryptography.TripleDESCryptoServiceProvider tdes = new System.Security.Cryptography.TripleDESCryptoServiceProvider();

    tdes.Key = keyArray;
    tdes.Mode = System.Security.Cryptography.CipherMode.ECB;
    tdes.Padding = System.Security.Cryptography.PaddingMode.PKCS7;

    System.Security.Cryptography.ICryptoTransform cTransform = tdes.CreateEncryptor();

    byte[] ArrayResultado = cTransform.TransformFinalBlock(Arreglo_a_Cifrar, 0, Arreglo_a_Cifrar.Length);

    tdes.Clear();

    //se regresa el resultado en forma de una cadena
    tarjeta1 = Convert.ToBase64String(ArrayResultado, 0, ArrayResultado.Length);

    tarjeta1 = "XIGA:" + tarjeta1;
}
```

Ejemplo en BD de la lectura-escaneo que se registra a partir de Holograma QR y su contenido.

The screenshot displays the SQL Server Enterprise Manager interface. On the left, the 'Databases' tree shows the 'logXIGA' database. The main pane shows a table with columns: endpoint, station, reference, request, and response. The table contains five rows of transaction data. A 'Value' pane on the right shows the hex value 'XIGA:1d4f3a813b3ec9gRuh1B7G42D81WUC4GPvDYaRShaxL4='. A calendar overlay for February 2024 is visible in the bottom right corner, with the 4th of February highlighted.

endpoint	station	reference	request	response
http://10.255.248.42/wsMonedero/api/AuthSale/	3.461	XIGA:1d4f3a813b3ec9gRuh1B7G42D81WUC4GPvDYaRShaxL4=	["KM":1,"DispenserProtocol":"BENNET","isAppRequest":false,"StationNumber":3461,"CardNumber":"00015-0033","ClientNumber":	["res":1,"firmaMonoCromatica":"Qk1GawAAAA
http://10.255.248.42/wsMonedero/api/AuthSale/	3.461	XIGA:1d4f3a813b3ec9gRuh1B7G42D81WUC4GPvDYaRShaxL4=	["idTransaction":null,"StationNumber":3461,"Reference":"XIGA:1d4f3a813b3ec9gRuh1B7G42D81WUC4GPvDYaRShaxL4=	["KM":1,"DispenserProtocol":"BENNET","isAppRequest":false,"StationNumber":3461,"CardNumber":"00015-0033","ClientNumber":
http://10.255.248.42/wsMonedero/api/AuthSale/	3.461	XIGA:1d4f3a813b3ec9gRuh1B7G42D81WUC4GPvDYaRShaxL4=	["KM":1,"DispenserProtocol":"BENNET","isAppRequest":false,"StationNumber":3461,"CardNumber":"00015-0033","ClientNumber":	["KM":1,"DispenserProtocol":"BENNET","isAppRequest":false,"StationNumber":
http://10.255.248.42/wsMonedero/api/AuthSale/	2.665	0001000010001500204514		

1.4 Almacenamiento

Los datos relativos al monedero, se almacenan de manera indefinida en una base de Datos Microsoft SQL Server 2012 R2 x64, sobre un sistema operativo Microsoft Windows Server Server 2012 R2 x64, en un espacio de almacenamiento HPE MSA 2060 hibrido con 40 TB de espacio, donde los datos de los clientes permanecen inhabilitados al causar la baja, a menos que decidan ejercer sus derechos ARCO para solicitar la eliminación definitiva.

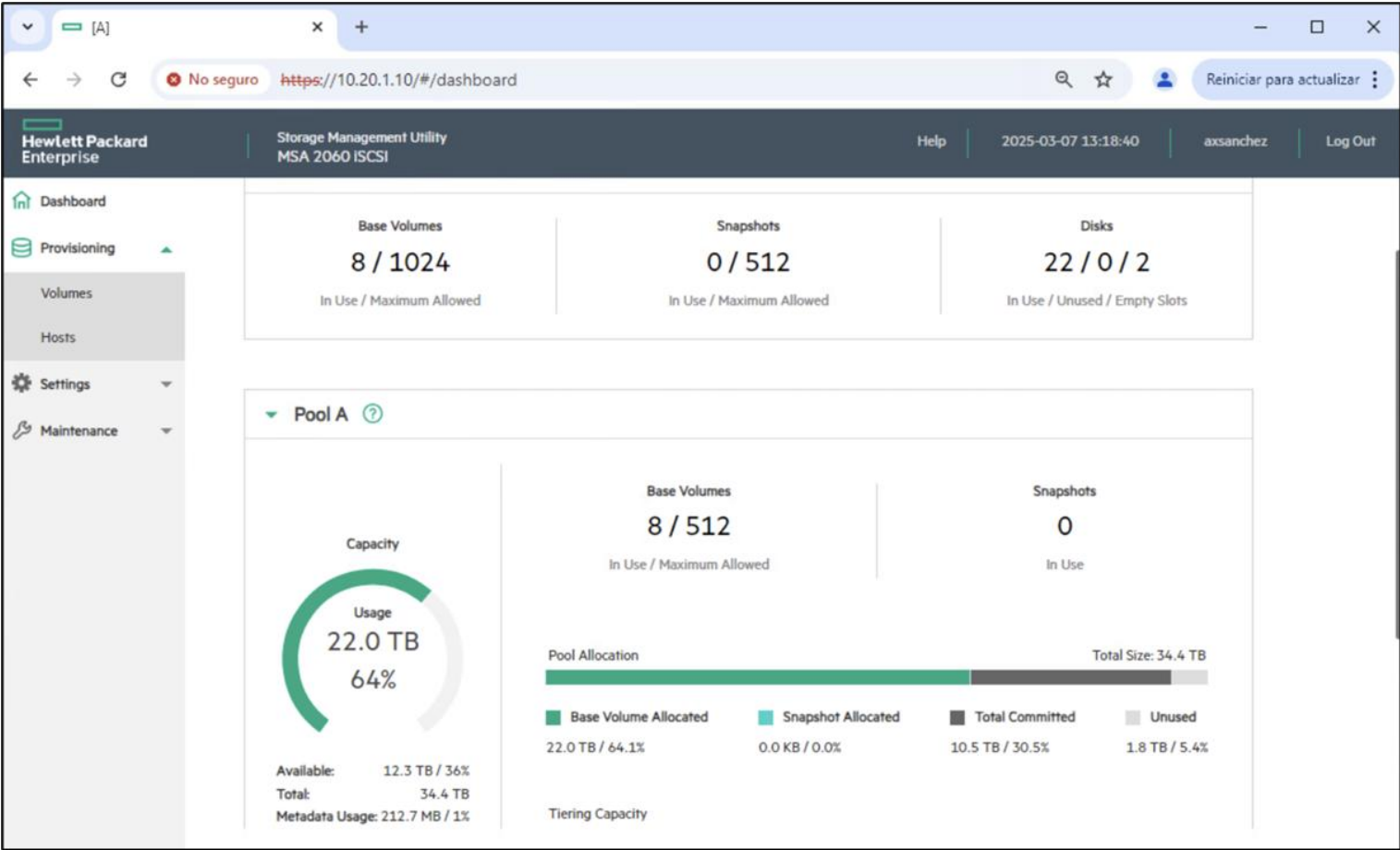


Diagrama Arquitectura Xiga

