

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 Windows 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. Dado que el monedero no contiene ningún dato sensible, en este código se observa que del código QR del monedero se obtiene sólo un dato que es el número de identificador del monedero.

```
//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. En la columna "reference" se muestra el resultado de leer el código QR, que equivale al identificador del monedero de manera encriptada.

id	host_endpoint	station	reference	qr_request	qr_response
1	http://10.255.248.42/vs/Monedero/api/AuthSale/	3461	XIGAIdHjg8tMmcgqNuhIBGd2D8WUCAGPwDYdRShawL4=	["KM":1,"DispenseProtocol":"BENNET","isAppRequest":false,"StationNumber":3461,"CardNumber":"00015-0053","ClientNumber":	["idTransaction":null,"StationNumber":3461,"Reference":"XIGAIdHjg8tMmcgqNuhIBGd2D8WUCAGPwDYdRShawL4=
2	http://10.255.248.42/vs/Monedero/api/SaveSale/	3461	XIGAIdHjg8tMmcgqNuhIBGd2D8WUCAGPwDYdRShawL4=	["KM":1,"DispenseProtocol":"BENNET","isAppRequest":false,"StationNumber":3461,"CardNumber":"00015-0053","ClientNumber":	["KM":1,"DispenseProtocol":"BENNET","isAppRequest":false,"StationNumber":3461,"CardNumber":"00015-0053","ClientNumber":
3	http://10.255.248.42/vs/Monedero/api/AuthSale/	3461	XIGAIdHjg8tMmcgqNuhIBGd2D8WUCAGPwDYdRShawL4=	["KM":1,"DispenseProtocol":"BENNET","isAppRequest":false,"StationNumber":3461,"CardNumber":"00015-0053","ClientNumber":	["KM":1,"DispenseProtocol":"BENNET","isAppRequest":false,"StationNumber":3461,"CardNumber":"00015-0053","ClientNumber":
4	http://10.255.248.42/vs/Monedero/api/AuthSale/	3461	XIGAIdHjg8tMmcgqNuhIBGd2D8WUCAGPwDYdRShawL4=	["KM":1,"DispenseProtocol":"BENNET","isAppRequest":false,"StationNumber":3461,"CardNumber":"00015-0053","ClientNumber":	["KM":1,"DispenseProtocol":"BENNET","isAppRequest":false,"StationNumber":3461,"CardNumber":"00015-0053","ClientNumber":
5	http://10.255.248.42/vs/Monedero/api/AuthSale/	2685	000100010001500204514	["KM":1,"DispenseProtocol":"BENNET","isAppRequest":false,"StationNumber":	["KM":1,"DispenseProtocol":"BENNET","isAppRequest":false,"StationNumber":

Value X
XIGA IdHjg8tMmcgqNuhIBGd2D8WUCAGPwDYdRShawL4=

Notifications
No new notifications

Sunday, February 4

February 2024

Su	Mo	Tu	We	Th	Fr	Sa
28	29	30	31	1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	1	2
3	4	5	6	7	8	9

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 híbrido 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.

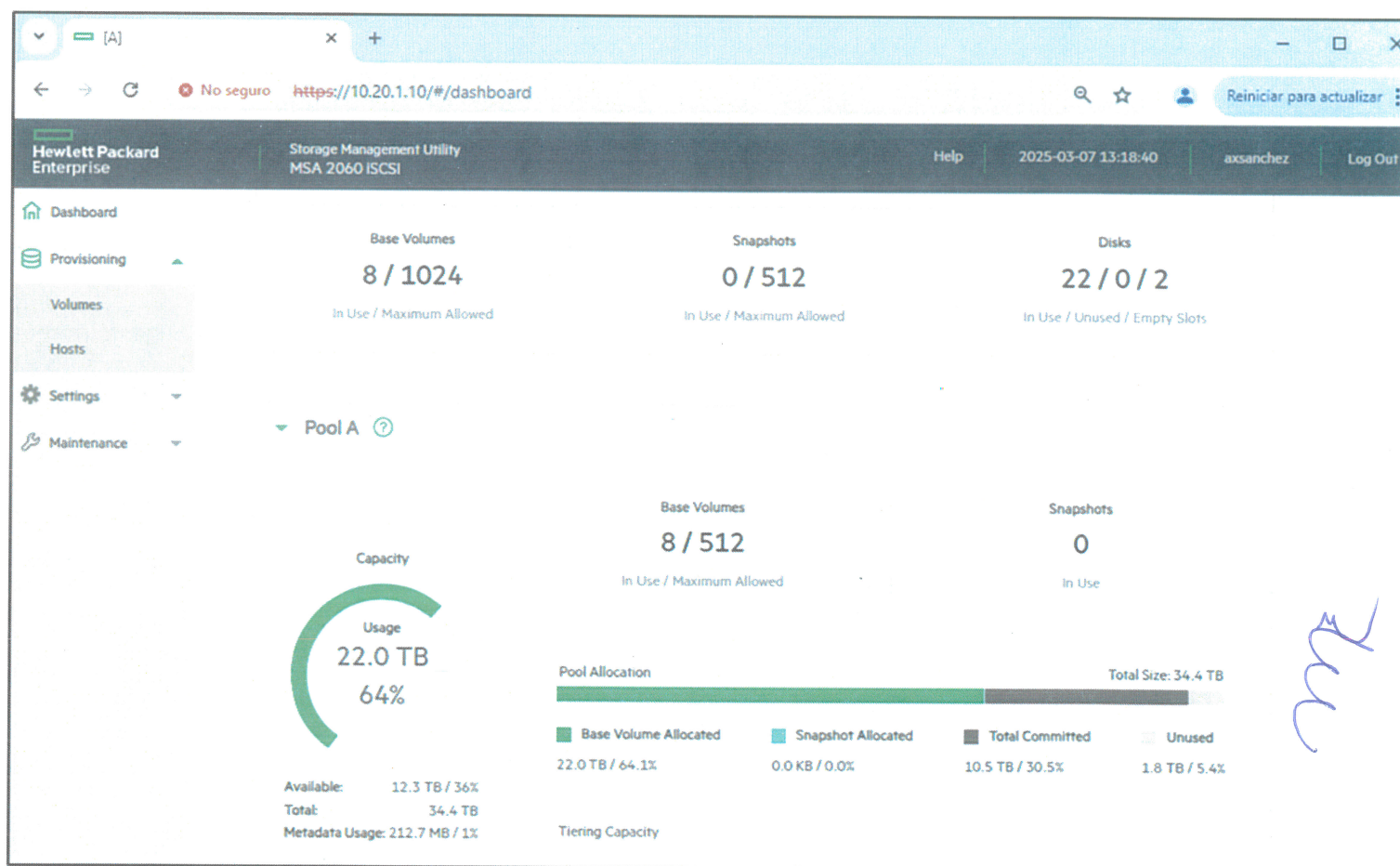


Diagrama Arquitectura Xiga

