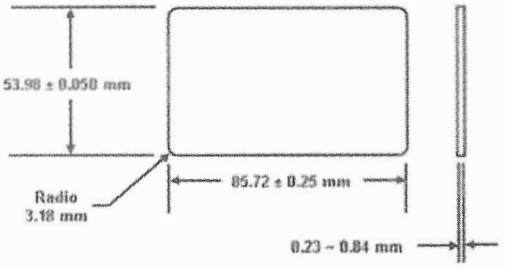
TECNOLOGIA DE MONEDERO INTELIGENTE XIGA

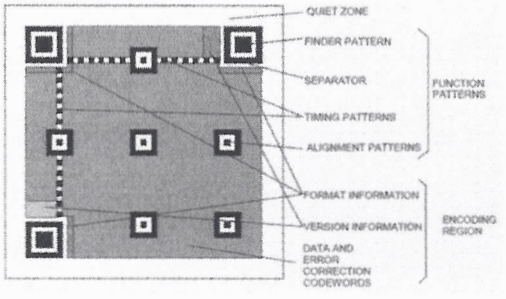
1. Monedero electrónico

1.1 Ficha técnica de Tarjetas

- Cumplimiento de los estándares ISO CR-80 (ISO 7810) para Tarjetas: Longitud 85,6 mm y anchura 54mm.
- Cumplimiento de los estándares ISO *ISO/IEC 18004 para* Código QR: Longitud 20 mm y anchura 20 mm
- Vida útil de las tarjetas de PVC: de dos a tres años mínimo.



Código bidimensional QR (Quick response), en apego a el estándar ISO/IEC 18004



Especificación de Cifrado en código QR

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

Hardware utilizado.

- Dispositivo para leer etiquetas con código Terminal Pax A910, Motorola Moto g70, Ciontek CS50 y Apple iPod Touch 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

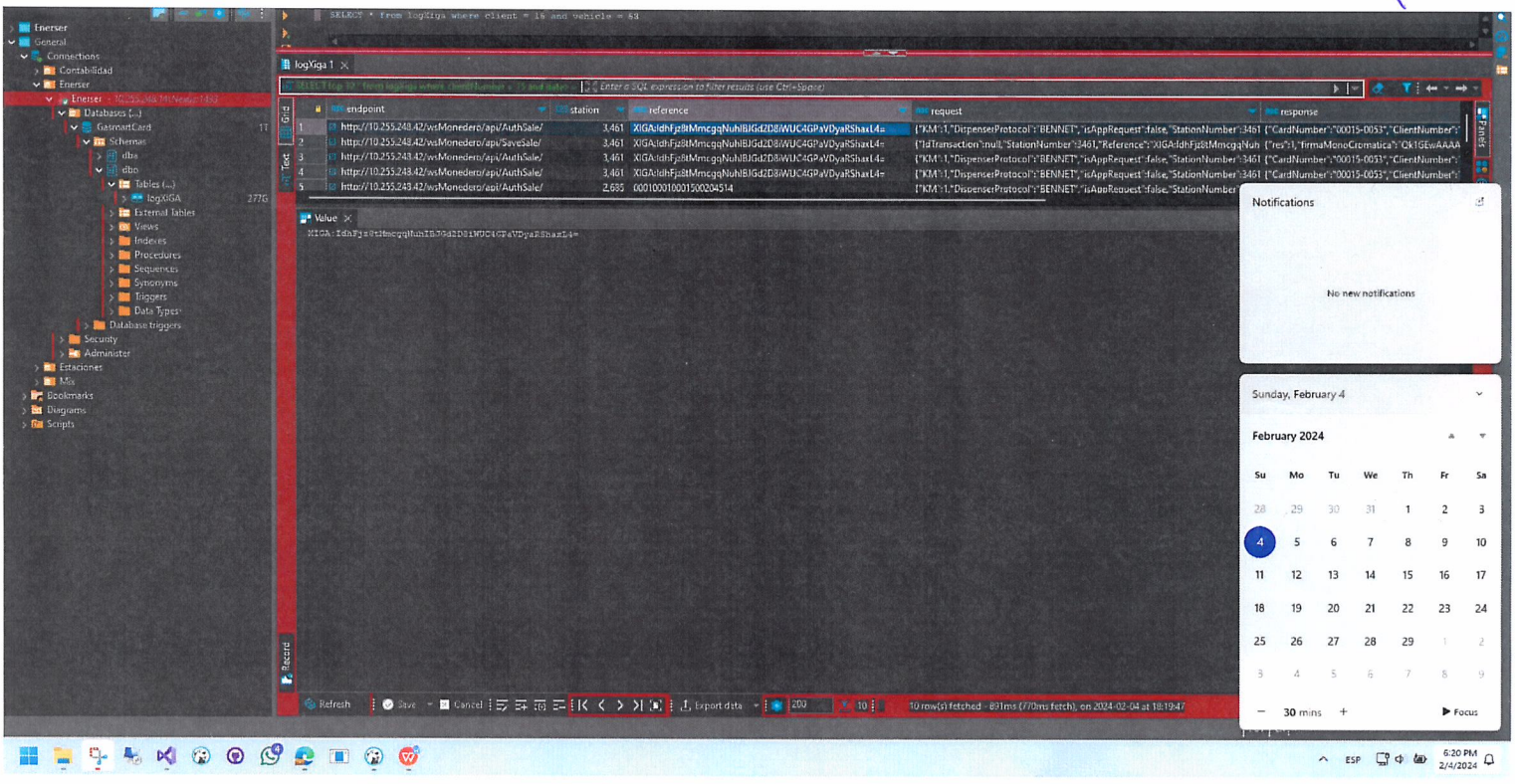
1.2 Ficha Técnica de la APP del Cliente

- 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

La imagen muestra extracto del código fuente del módulo del monedero encargado de encriptar los datos del Tarjeta 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 Tarjeta 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.



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.

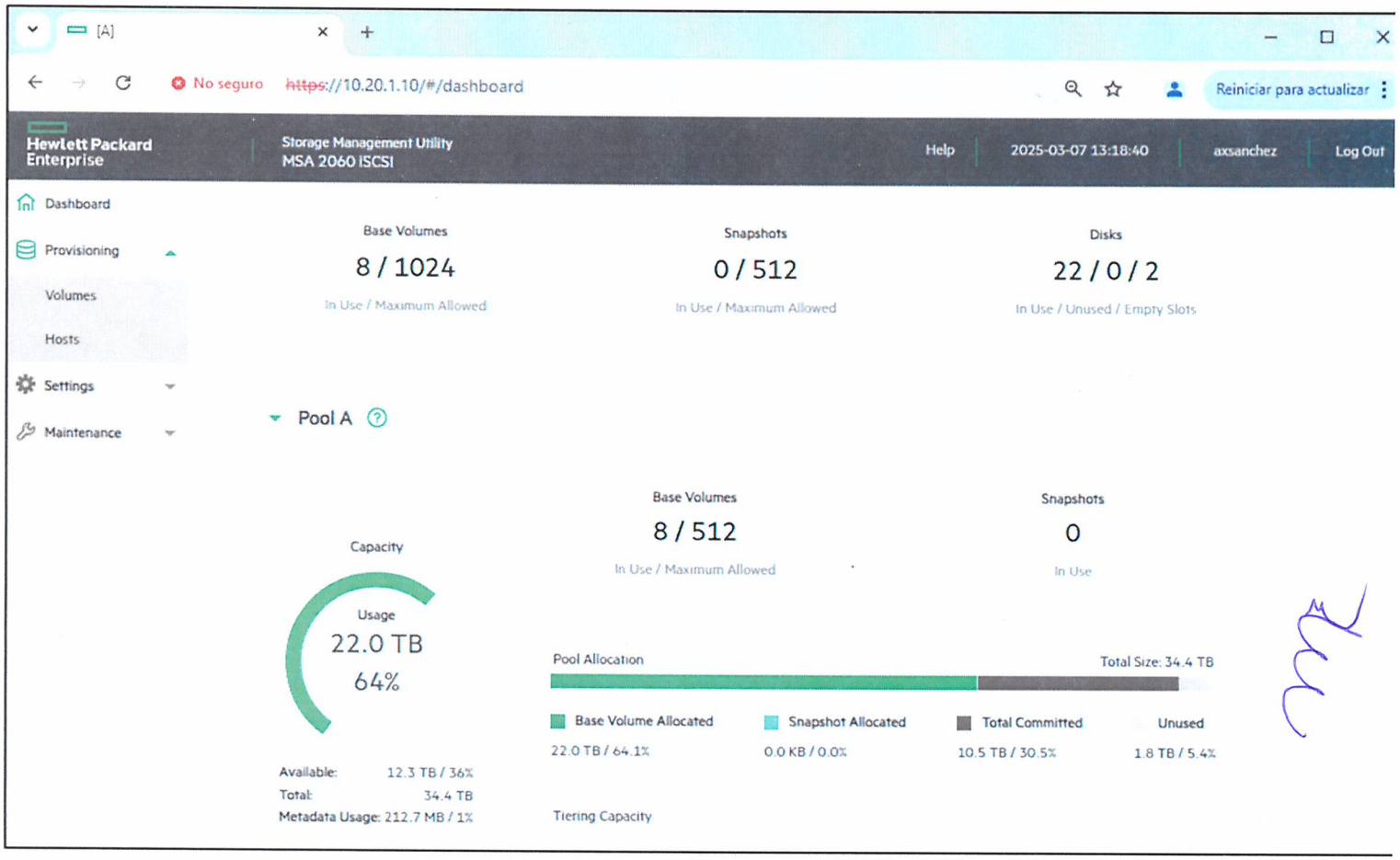


Diagrama Arquitectura Xiga