Implementación de Sistema C-Token bajo normativa STS6

Objeto

La actualización de los Sistemas STS por la limitación del tamaño del TID que deberá realizarse a partir del año 2024 y tiene fecha límite de culminación en Noviembre de 2024, lleva a la necesidad de realizar un cambio de los generadores de Token. Este cambio obliga a la realización de un Software que permita la interacción de estos nuevos equipos.

Este nuevo software C-Token, que reemplazará a los Sistemas Nexo o EPS en cualquiera de sus versiones.

El desarrollo fue realizado desde cero, contando con infinidad de aspectos que mejoraran la performance del Sistema con respecto al utilizado en la actualidad y se buscó realizar las mismas interfaces como las usadas hasta ahora, para que nuestros clientes no tuviera que realizar nuevos desarrollos con terceros para interactuar con las mismas.

Se ha cumplido el objetivo de poder ofrecerle a nuestros clientes un sistema que implique un proceso de cambio sencillo, cumpliendo con los nuevos parámetros exigidos, para mejorar la seguridad y velocidad de transacciones.

1. Nuevas Funcionalidades

STS

- Compatibilidad con TSM-500
- STS6 Compliance
- Gestión de TID Rollover: generación de tokens de cambio de fecha base y módulo de monitoreo del proceso
- Time Token: generación de tokens de unidades de tiempo medidores conectados a paneles solares

FACTURACION

- Nuevos tipos de concepto: Tarifa Base, Cargo Fijo Escalonado, Cargo Variable Escalonado, Cargo Combinado Escalonado, Subsidio Cruzado, Cargo Variable con mínimos/máximos y Base no Imponible.
- Asociación de conceptos a Municipios y zonas de Alumbrado Público
- Categorización por Segmentos (N1, N2 y N3)
- Nuevo estado de transacción: "Transacción Errónea"
- Envío de token por SMS/Whatsapp

SEGURIDAD

- HTTPS
- Integración con Windows AD / Azure AD
- Multitenant
- Certificación ISO 27001
- Requerimientos de seguridad

	Concepto	Descripción
1	Autenticación	**Integración con Active Directory o Azure AD para autenticación de usuarios.**
2	Autenticación	**Las contraseñas de cuenta de servicios o conexiones que pueda utilizar la aplicación deben almacenarse utilizando algoritmos diseñados específicamente para proteger contraseñas. Las contraseñas nunca deben transmitirse ni almacenarse en texto plano. Estos algoritmos deben ser no reversibles. Debe tener alto nivel de seguridad por ejemplo (Sha-2)**
3	Autenticación	**Todas las APIs de la aplicación deben contar con autenticación y con niveles de autorización. Aquellas que no posean este requisito deben estar debidamente justificadas**
4	**Autorización**	**Los perfiles de acceso deben permitir establecer los mínimos permisos necesarios para cada grupo de usuarios**
8	**Componentes a autentificar**	**"Todos los componentes de la aplicación se deben autenticar y deben tener el mínimo de privilegios necesarios. Todas comunicaciones entre los componentes de la aplicación, incluidas las API, el middleware y las capas de datos deben estar autentificadas."**
9	**Comunicaciones seguras**	**Todos los protocolos de comunicación que utilice la aplicación deben ser considerados protocolos seguros. En caso de utilizar HTTPS, deben soportar TLS 1.2 o superior**
10	**Definiciones y Documentación**	**La aplicación debe contar con documentación de todos los componentes de la aplicación en términos de las funciones de negocio y de seguridad que proporcionan.**
11	**Expiración de sesiones por inactividad**	**La aplicación debe contar con un tiempo de expiración de la sesión luego de un periodo de inactividad del usuario, a partir del cual el usuario deberá volver a iniciar sesión en la aplicación. Este período debe ser configurable.**
12	**Privilegios de los Componentes**	**La aplicación debe utilizar cuentas de servicios con los mínimos privilegios necesario que requiera la aplicación.**
13	**Registro de actividades**	**"Se deben generar logs de errores, de auditoría, de seguridad y de trazabilidad de operaciones para sus respectivos análisis. La aplicación debe registrar auditoría de eventos de seguridad como login exitoso, login fallido, acceso no autorizado a recurso, asignación de roles y otros. Los eventos que se registren deben contener fecha y hora, así como el usuario, la acción y cualquier información adicional que sea relevante como la IP o equipo. "**
14	**Validación de datos de entrada**	**Debe ejecutarse una validación sobre todas las entradas que lea la aplicación. Siempre se debe realizar la validación antes de procesar los datos de entrada.**

INTERFACE CLIENTE

- Nueva interface web de cliente en reemplazo del actual WinForms (a desarrollar con la confirmación del contrato con plazo de entrega de 6 meses)

AMI

- Integración con SmartAMI para envío de tokens de crédito y validación de saldo.
- Lecturas Mensuales para facturación pospaga *

WEB SERVICE

El software de gestión de medidores prepagos C-Token cuenta con 7 interfaces que permiten:

Integración de los distintos canales de venta.

Exponer un conjunto de servicios web que permiten ejecutar la totalidad de las operaciones sin necesidad de utilizar la consola winforms provista por CSA.

Gestionar el Cuadro Tarifario y las distintas asignaciones mediante Tarifas, Categorías de Cliente, Categorías Impositivas, Categorías de AP, Localidades, etc.

Se permite gestionar los clientes (ABM), vincular/desvincular medidores y realizar asociaciones de conceptos individuales (planes de pago, multas,etc).

Se Obtiene cualquier tipo de token STS, se generan altas individuales o masivas de medidores, se programan los lotes para el proceso TID Rollover y se configuran los servidores de encriptación (HSP).

Permite previsualizar una transacción (sin confirmarla) y emitir la misma por unidades (kWh).

Ante un evento de error conocido, C-Token lo codifica según el origen del error y genera la correspondiente excepción. En cualquier otro caso que no esté tipificado, C-Token genera una excepción del tipo "Unknown Error.