



[Interoperabilidad con las Entidades Financieras de las Administraciones Vascas]

XIV Convocatoria Premios ASLAN

TRANSFORMACIÓN DIGITAL EN LAS ADMINISTRACIONES PÚBLICAS

MiPago WALLET

Resumen	Resumen del caso práctico [MiPago Wallet] para la XIV Convocatoria Premios ASLAN a la [Transformación Digital en las Administraciones Públicas] impulsada por la asociación ASLAN:		
Objetivo	Descripción de la propuesta de la [Sociedad Informática del Gobierno Vasco / Eusko Jaurlaritzaren Informatika Elkarte]		
Destinatarios	XIV Convocatoria Premios ASLAN a la [Transformación Digital en las Administraciones Públicas]		
Contenido	1	Caso Práctico en Innovación	2
	1.1	Resumen	2
	1.2	Por qué se considera que [MiPago Wallet] es un [caso práctico de innovación]	3
	2	Información detallada del Caso Práctico en Innovación	4
	2.1	Antecedentes	5
	2.2	Razones del caso: reto y/o oportunidad estratégica a la que se da respuesta	6
	2.3	Descripción de la innovación introducida y acciones realizadas	6
	2.4	Impacto: resultados obtenidos	8
	2.5	Colaboración con otras organizaciones	9
	2.6	Recursos dedicados	9
		2.6.1. Recursos Técnicos	9
		2.6.2. Recursos Humanos	9
	2.6.3. Recursos Económicos	9	
3	ANEXO: Detalle técnico del proyecto	10	

1 Caso Práctico en Innovación

1.1 Resumen

Razón Social de la Entidad que presenta el caso [Deusto Seidor](#)



[Sociedad Informática del Gobierno Vasco – Eusko Jurlartzaren Informatika Elkartea](#)



Número de empleados 180 aprox

Descripción de la actividad de la entidad [EJIE](#) es la Sociedad Informática del Gobierno Vasco que a través del liderazgo tecnológico facilita la **digitalización de los servicios que el Sector Público Vasco**.

EJIE desarrolla su actividad en el amplio campo de las Tecnologías de la Información y Telecomunicaciones, para lo que cuenta con recursos e infraestructuras, que avalan la prestación de los [Servicios](#) y la oferta de Productos, con las máximas garantías de Calidad, Eficiencia y Seguridad.

- Asistencia Técnica
- Comunicaciones
- Infraestructuras
- Proyectos
- Puesto de Trabajo
- Servicios Corporativos Unificados
- Otros servicios

Denominación del caso práctico MiPago Wallet

Fecha de implementación 2021

Descripción Wallet digital en el móvil que permite realizar de manera segura pagos recurrentes sin necesidad de teclear el número de tarjeta.

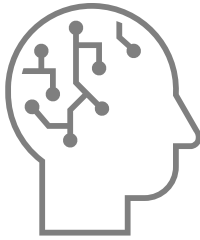
Ámbito Transformación Digital

Datos de Contacto Enrique Rico San Vicente

Dirección C\ Paduleta, 55 1º Ofi. 203
01015 Vitoria-Gasteiz
Araba/Álava
Teléfono/s 945 200 655
email info@deustoseidor.com

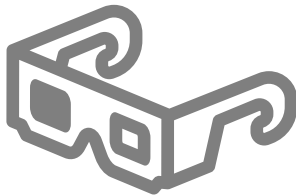
1.2 Por qué se considera que [MiPago Wallet] es un [caso práctico de innovación]

El producto [MiPago Wallet] se considera que es un caso práctico en el ámbito de **innovación** relacionado con la **transformación digital** y el **GovTech** puesto que:



- Se aplica en el ámbito de las [administraciones públicas] una **solución innovadora de pago** (*pago tokenizado*) que hasta ahora prácticamente solo están utilizando grandes tecnológicas como [Google] (*Google Pay*) o [Apple] (*Apple Pay*)

En el estado NO hay ninguna experiencia de aplicación de [pago tokenizado] en el ámbito de las [Administraciones Públicas], pero tampoco son frecuentes las experiencias en *comercios estándar*, más allá del uso de las mencionadas [Google Pay] y [Apple Pay]



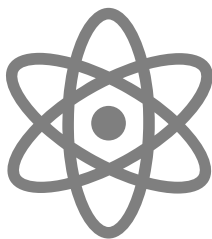
- Se **mejora la experiencia de usuario** puesto que el proceso de pago es mucho más ligero al evitarse el *teclado* en el móvil de la decena de dígitos de una [tarjeta de crédito]: basta con *aceptar* el pago utilizando por ejemplo un factor biométrico como el lector de [huella digital]

... pero [MiPago Wallet] y la experiencia de uso que proporciona NO solo se pueden utilizar para realizar pagos en movilidad sino que también se puede utilizar *-como se verá-* para el pago en la web.



- Se generan **nuevos modelos de relación** con el cliente (*la ciudadanía*) puesto que se “abren” infinitas **nuevas posibilidades de uso** en especial en el caso de los **pagos recurrentes**

- Tarjetas de transporte (*ya se está trabajando con consorcios de transporte para incorporar [MiPago Wallet]*)
- Aparcamiento (OTA)
- Tickets (*se está utilizando [MiPago Wallet] para la compra de tickets en los jantoki de la sede del GV en Lakua y la Academia Vasca de Policía y Emergencias de Arkaute*)



- [MiPago Wallet] permite la introducción del [pago electrónico] en múltiples escenarios de pago en la [Administración Pública] manteniendo todas las ventajas de [MiPago] (*de las que carecen los [TPV virtuales] comerciales*) y que permiten automatizar todo el ciclo de vida de los pagos avanzando hacia una **administración más eficiente**



- [MiPago Wallet] es un medio de pago **seguro** que evita que ninguna de las partes *conozca* el número de tarjeta de crédito / débito, evitando de esta forma el *riesgo* de robo de tarjeta.

A nivel **tecnológico**, [MiPago Wallet] utiliza las últimas tecnologías disponibles en cada área:

Desarrollo de la app móvil [MiPago Wallet] Se ha utilizado [flutter](#) que es un emergente framework de desarrollo de aplicaciones móviles / web impulsado por [Google]

CORE de [MiPago] Basado en [micro-servicios] que se ejecutan en [containers] orquestados en una solución basada en [Kubernetes](#) ([OpenShift](#))
Esta infraestructura *-dado su carácter público-* está albergada en [EJIE] (*empresa pública proveedora de servicios IT para el [Gobierno Vasco]*) pero podría ser albergada en un proveedor en la nube

Servicios de [pago tokenizado] Son proporcionados por [RedSys] a través de un intermediario desarrollado ad-hoc para [MiPago] por parte de [Kutxabank]

Finalmente, se destaca que [MiPago Wallet] (*al igual que todas las soluciones del ecosistema común [MiPago]*) es una solución **sostenible** puesto que constituye un **esfuerzo común** por parte de todas las [Administraciones Vascas] y un conjunto de [Entidades Financieras] que ha ahorrado mucho trabajo y dinero en ya que se ha evitado la existencia de soluciones redundantes.

En particular [MiPago Wallet] es un [wallet digital] que puede ser utilizado en cualquier caso de uso de cualquier [administración pública]: si cada [administración] se construyera su propio [wallet digital], además del gasto redundante en desarrollo y explotación de la solución, la ciudadanía acabaría teniendo múltiples aplicaciones en su móvil cada una para un propósito o una administración en concreto.

TRANSFERIBLE!



La interoperabilidad con las Entidades Financieras ([MiPago](#)) es un caso de éxito paradigmático de la posibilidad de que varias administraciones compartan un sistema tecnológico para dar un mejor servicio a la ciudadanía.

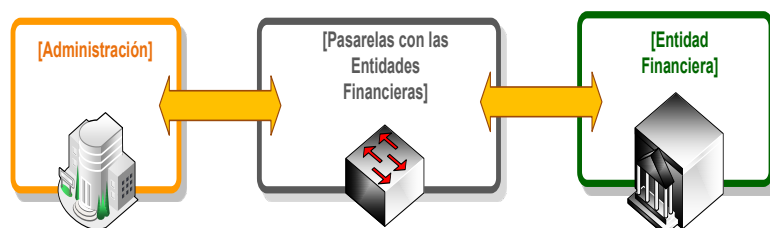
MiPago es utilizado por más de **170** administraciones en Euskadi para proporcionar servicios de pago electrónico y ha sido posible gracias a la colaboración de las administraciones con las Entidades Financieras mas relevantes del Estado Español.

2 Información detallada del Caso Práctico en Innovación

2.1 Antecedentes

El [Sistema de Interoperabilidad con las Entidades Financieras] (**MiPago / NireOrdainketa**) es un conjunto de mecanismos de interoperabilidad (*pasarelas*) entre las [Administraciones Vascas] y las [Entidades Financieras] y que tiene como objetivos generales:

Con las [Entidades Financieras]	Estandarizar formatos de mensajes y mecanismos de interoperabilidad comunes, independientes de la [Entidad Financiera] y la [Administración] usuaria
Con las [Administraciones]	Proporcionar unos servicios comunes sobre operaciones con [Entidades Financieras]
Con la ciudadanía	Proporcionar un interfaz común independiente de la [Administración]



Esta estandarización proporciona fundamentalmente las siguientes ventajas:

- Las [Administraciones] únicamente tienen que integrarse con un sistema: [MiPago] que les proporciona **servicios comunes y únicos independiente de la [Entidad Financiera]**
- Las [Entidades Financieras] solamente tienen que hacer la integración con [MiPago], con lo que se les abre la posibilidad de trabajar con **todas las [Administraciones] vascas** en base a una **única integración**
- Los [Ciudadanos/as] se encuentran con interfaces **comunes**, independientemente de la [Administración] o la [Entidad Financiera], lo que les proporciona **seguridad**

El [Sistema de Interoperabilidad con las Entidades Financieras] viene dando servicio a las Administraciones Vascas desde el año 2000 con una amplia aceptación, siendo algunas de las cifras del servicio:

Administraciones Vascas adheridas al sistema

170: Gobierno Vasco, Diputaciones Forales y Ayuntamientos

Tipos de servicios (tributos, tasas, sanciones, etc) que se pueden pagar

3.489

Entidades Financieras adheridas al sistema

10: KutxaBank, Laboral, Bankoa, BBVA, Santander, Sabadell-Gipuzkoano, Bankia, Popular

Volumen de transacciones de pago en los últimos años

	2018	2019	2020	2021 (hasta junio)
Número de operaciones	588.136	566.924	620.357	355.373
Importe total de operaciones	119.485.769,00	133.482.308,33	202.093.922,13	95.215.570,71

[MiPago] ofrece diversas funcionalidades de interoperabilidad entre [administraciones] y [entidades financieras] como:

- Pago web
- Pago en movilidad
- Pago directo en cuenta
- Consulta del estado de pagos
- Consulta de titularidad de números de cuenta
- etc

Todas estas soluciones se han venido utilizando en las [Administraciones Públicas Vascas] con gran éxito desde el año 2000.

2.2 Razones del caso: reto y/o oportunidad estratégica a la que se da respuesta

Las soluciones de pago introducidas en el punto anterior permiten el pago de cualquier concepto de cualquier [administración pública] tanto en la web como en movilidad, sin embargo, especialmente cuando se trata de **pagos recurrentes** (*pagos que se hacen habitualmente de manera repetitiva como la recarga de una tarjeta de transporte*), la **usabilidad** de estas soluciones de pago *tradicionales* es muy mejorable.

... por esta razón, la mejora de la usabilidad, se pensó que era necesario abordar la construcción de una nueva solución que permitiera el pago seguro pero de forma **sencilla y rápida**, y la solución al problema es el uso del [**pago en base a token de tarjeta de crédito / débito**] que son almacenados en un [wallet] (monedero) virtual:

[MiPago Wallet] simplemente almacena [tokens] que no son mas que sinónimos de una tarjeta de crédito / débito.

Cuando se va a hacer un pago en el móvil o en la web, se *activa* la aplicación [MiPago Wallet] y la persona usuaria únicamente tiene que seleccionar el [token] que va a utilizar (*la tarjeta en definitiva*) y aceptar el pago simplemente mostrando su huella digital o pulsando un botón (*si se trata de un pago de una cantidad muy pequeña*).

... a nivel de **usabilidad** o de **experiencia de usuario**, es muy similar a un **pago contact-less** en **pagos físicos**: simplemente se “*muestra*” el [token] (*la tarjeta*) y se efectúa el pago

El uso de un [wallet] de [tokens] en la [administración pública] es **pionero en el Estado**.

2.3 Descripción de la innovación introducida y acciones realizadas

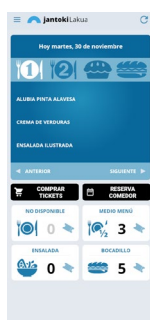
[MiPago Wallet] es una [app móvil] que proporciona una experiencia de pago segura y sobre todo sencilla tanto en el móvil como en la web.

El objetivo de [MiPago Wallet] es que el proceso de pago tenga *fricción* mínima y sea tan rápido como sea posible, evitando para ello el tecleo de una gran cantidad de dígitos: *pagar debe ser tan sencillo como “apretar un botón”*

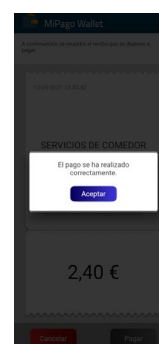
La experiencia de usuario se describe a continuación:

Pago desde una aplicación móvil Caso de uso real: [jantoki de Lakua] (sede central del [Gobierno Vasco]) donde se ha **eliminado completamente el uso del efectivo**: las personas utilizan una [app móvil] donde pueden almacenar [tickets de comida] que presentan al personal del [jantoki] cuando van a comer

Para *comprar* estos [tickets] de comida, la persona usuaria simplemente *rellena* un carrito de compra en la [app]



En el momento de realizar el pago, la [app jantoki Lakua] ofrece el pago a través de [MiPago Wallet]; si la persona usuaria elige esta opción, simplemente se *activa* la app y se pide confirmación a la persona usuaria



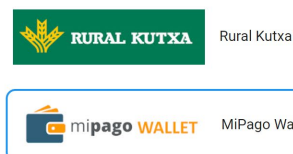
Pago desde una aplicación web

Desde una [aplicación web] (desde el PC de casa o la oficina), también es posible utilizar [MiPago Wallet] para hacer un pago:

La persona usuaria interactúa con una [aplicación web] por ejemplo para apuntarse a una convocatoria de empleo público o pagar una tasa o sanción

The screenshot shows a web interface for making a payment. At the top, there is a navigation bar with four tabs: 'REALIZAR PAGO', 'SOLICITAR JUSTIFICANTE', 'CONTACTO', and 'ACERCA DE'. Below this is a progress indicator with five steps: 1. Selección de CPR (checked), 2. Introducción de datos (current step), 3. Listado de Pagos, 4. Selección Entidad Financiera, and 5. Realización del Pago. A blue banner below the progress indicator says: 'Introduzca los datos que se solicitan. Encontrará estos datos en la parte inferior del impreso de pago.' Below this is a form with two main sections. The first section is 'Carta de Pago' and contains a 'Código Procedimiento de Recaudación (CPR)' field with the value '9050794'. The second section is for payment details and includes fields for 'Emisor', 'Referencia', 'Identificación-Fecha límite Pago', and 'Importe €'. At the bottom of the form are two buttons: '< ATRÁS' and 'SIGUIENTE >'.

En el momento de realizar el pago, [MiPago web] ofrece la posibilidad de utilizar [MiPago Wallet]:



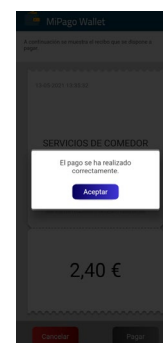
... si la persona usuaria elige esta opción, se le solicita el número de móvil :

The screenshot shows the 'MiPago Wallet' mobile interface. At the top, there is a blue header with the text 'MiPago Wallet' and a close button (X). Below the header, there is a text prompt: 'Introduzca el número de teléfono en el que tiene instalada la aplicación'. Below this is a text input field labeled 'Número de teléfono' and a blue button labeled 'Continuar'.

[MiPago] envía una *señal* al móvil del usuario y se *activa* la [app MiPago Wallet]



y se pide confirmación a la persona usuaria, para realizar el pago:



En las siguientes urls se pueden encontrar unos videos del funcionamiento descrito:

- Enrolamiento <https://www.dropbox.com/s/dup5sqtb8fq8ng8/V%C3%ADdeo%2016-3-21%2010%2050%2002.mp4?dl=0>
- Escenario Web <https://www.dropbox.com/s/frl605ol9pxm4f/V%C3%ADdeo%2016-3-21%2010%2010%2011.mp4?dl=0>
- Escenario APP <https://www.dropbox.com/s/t80r84gq49phqto/V%C3%ADdeo%2016-3-21%208%2058%2028.mp4?dl=0>

2.4 Impacto: resultados obtenidos

Los resultados obtenidos con el producto [MiPago Wallet] se resumen en el siguiente cuadro de ventajas:

Ventajas	Para el usuario/a	<ul style="list-style-type: none">Es ideal para pagos recurrentes (<i>tickets del comedor, carga de tarjetas de transporte, pago de aparcamiento, etc</i>) puesto que solo requiere autorizar la transacción (<i>con la huella dactilar, pulsando un botón o con un password</i>)
	Para la administración	<ul style="list-style-type: none">NO maneja datos de tarjetas (<i>mayor seguridad</i>)Se mantiene la trazabilidad de la [liquidación]Las aplicaciones de las [administraciones] pueden utilizar este nuevo sistema de pago sin necesidad de hacer cambios
	Para la entidad que proporciona el [TPV Virtual] (RedSys)	Se ofrece un servicio válido para cualquier administración y cualquier [Entidad Financiera]
	Para las [Entidades Financieras]	Las [Entidades Financieras] que utilizan los servicios de [RedSys] en principio NO tienen que hacer ningún desarrollo

... y la ventaja más importante es que **se trata de un servicio muy innovador** en el ámbito de las [Administraciones Públicas]

El servicio lleva en uso unos pocos meses así que aún es pronto para extraer datos sobre su uso pero **muchas [administraciones públicas] están empezando a ofrecer el servicio para sus pagos** así que se espera una **adopción exponencial**, especialmente en el momento en que se incorporen casos de uso como los relacionados con el transporte.

El objetivo a corto plazo es que [MiPago Wallet] sea el **wallet común** de todas las administraciones vascas.

2.5 Colaboración con otras organizaciones

El proyecto [MiPago Wallet] ha sido impulsado por la [Dirección de Atención a la Ciudadanía y Servicios Digitales](#), sin embargo, el proyecto ha supuesto un considerable esfuerzo compartido por diferentes entidades:

Entidad participante	Rol / función en el proyecto
Dirección de Atención a la Ciudadanía y Servicios Digitales	<ul style="list-style-type: none"> Sponsor del proyecto Definición funcional
Dirección de Tecnologías de la Información y la Comunicación EJIE - Eusko Jaurlaritzaren Informatika Elkartea / Sociedad Informática del Gobierno Vasco	<ul style="list-style-type: none"> Diseño tecnológico Infraestructura técnica Construcción de [MiPago Wallet]
Kutxabank	<ul style="list-style-type: none"> Proporcionar servicios de intermediación con [RedSys] para pagos de las [Administraciones]
RedSys : Consorcio tecnológico de las [Entidades Financieras]	<ul style="list-style-type: none"> Proporcionar los servicios de [TPV Virtual] y [pago tokenizado]

2.6 Recursos dedicados

Como ya se ha señalado, la construcción de [MiPago Wallet] ha sido un esfuerzo compartido entre [Gobierno Vasco] (*como impulsor de [MiPago]*), [Kutxabank] (*intermediador con [RedSys]*) y el propio [RedSys] (*como prestador de servicios [TPV virtual]*)

2.6.1. Recursos Técnicos

MiPago (Gobierno Vasco)	Sistemas informáticos del [Gobierno Vasco] albergados en [EJIE]
Kutxabank	Sistemas informáticos y de interoperabilidad con [RedSys]
RedSys	Sistemas informáticos y de interoperabilidad con otras [Entidades Financieras] y medios de pago (<i>VISA, MasterCard, etc</i>)

2.6.2. Recursos Humanos

	Actor	Funciones
MiPago (Gobierno Vasco)	[Dirección de Atención a la Ciudadanía y Servicios Digitales]	Sponsor Dirección funcional de proyecto
	Equipo de proyecto de [MiPago] en [EJIE]	Dirección técnica del proyecto Construcción de la solución
	Ingeniería y Operación en [EJIE]	Gestión de Cambios Despliegue de infraestructuras
Kutxabank	Equipo de Medios de Pago	Coordinación con RedSys Construcción de la solución de intermediación [MiPago]<>[RedSys]
RedSys	Equipo de Medios de Pago	Construcción de la solución de intermediación [Kutxabank] <> [RedSys]

2.6.3. Recursos Económicos

Se desconocen los recursos económicos incurridos por [Kutxabank] o [RedSys]; únicamente se pueden proporcionar datos acerca del [Gobierno Vasco] (MiPago):

Coste económico	60.000 €	en un proyecto que ha tardado en construirse	8 meses
-----------------	-----------------	--	----------------

3 ANEXO: Detalle técnico del proyecto

[MiPago] en muy grandes líneas ofrece dos formas de [pago electrónico] de liquidaciones con [tarjeta]:

Pago con una [tarjeta] de una [Entidad Financiera Colaboradora]

El pago se hace en la propia [Entidad Financiera] (*no se utilizan sistemas de intercambio entre [Entidades Financieras]*), lo que hace que **NO existan comisiones** por operación

Pago con una [tarjeta] de OTRAS [Entidades Financieras] (*no colaboradoras*) (VISA / MASTERCARD, etc)

Para hacer el pago, se utiliza un [TPV virtual] proporcionado por un intermediario (RedSys) y que se encarga del intercambio entre [Entidades Financieras]

Este modo de pago conlleva el **pago comisiones** por operación

Las [Administraciones] en lo que se refiere al [pago electrónico] tienen ciertas *particularidades* respecto a un comercio *normal* puesto que el enorme volumen de transacciones y la necesidad de automatizar el circuito de principio a fin, requiere de la implementación por parte de las [Entidades Financieras] de **sistemas ad-hoc, específicos para las [Administraciones]**.

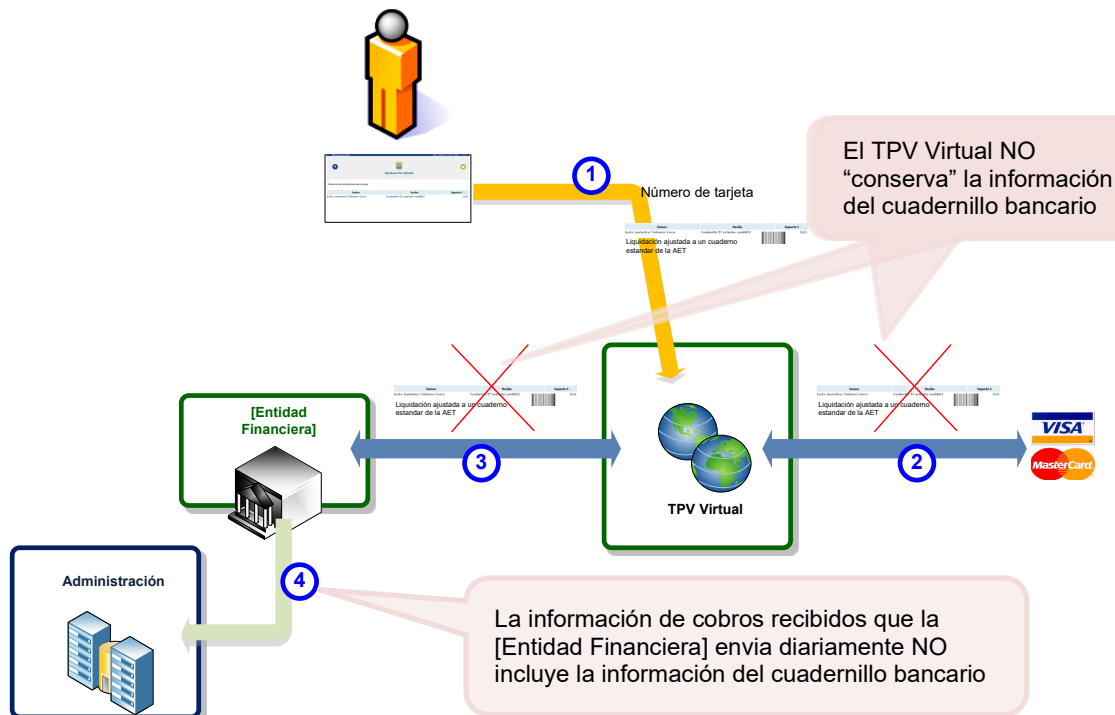
... sin embargo, los [TPV virtual] de propósito general (*los utilizados en comercios*) NO están pensados para el caso de uso de las [Administraciones], así que [Kutxabank] junto con [MiPago] (*las administraciones vascas*) ha construido un **recubrimiento de un [TPV virtual] estándar ofrecido por [RedSys]** y que tiene como objetivo fundamental **mantener la información del cuadernillo bancario en todo el circuito**.

Este recubrimiento surgió ante los problemas que plantea el [TPV Virtual] (*RedSys*):

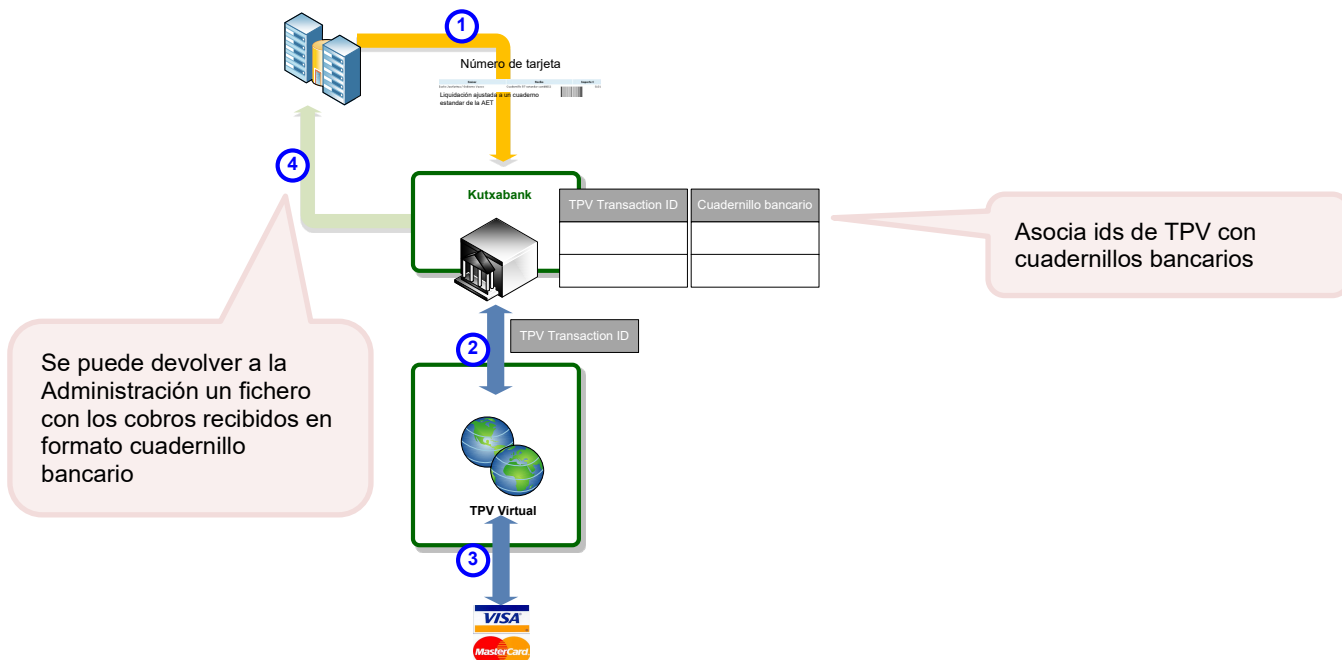
1. El [TPV virtual] NO es capaz de “mantener” la información del [cuadernillo bancario] con lo que la [Entidad Financiera] NO puede devolver al final del día los cobros recibidos en base a dicha información del cuadernillo bancario
2. El [TPV virtual] NO genera NRC (*Números de referencia completos*) como “firma” / comprobante de las transacciones

El NRC permite certificar que el pago es correcto SIN necesidad de hacer una llamada remota a sistemas de la [Entidad Financiera] y se obtiene a partir de los datos de la liquidación mediante la firma de los datos [liquidación] con una clave simétrica (*compartida entre las [Entidades Financieras] y la MiPago*).

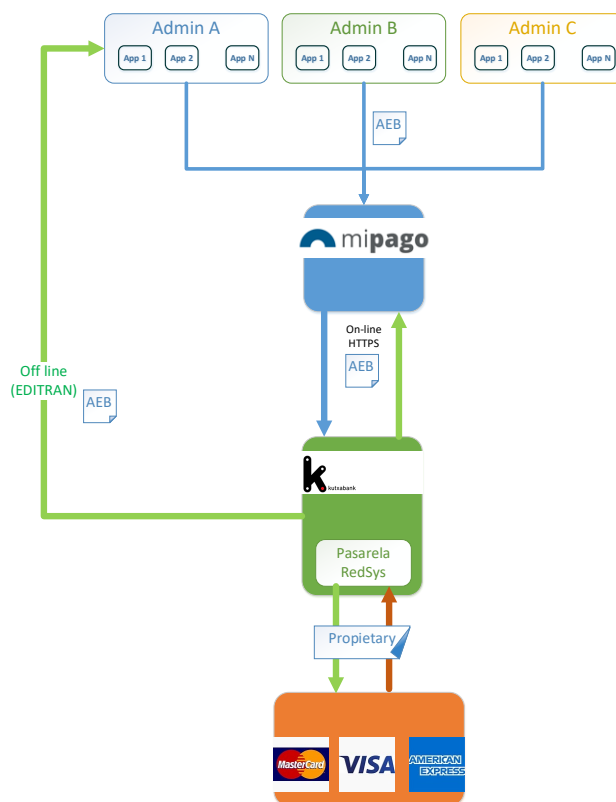
Un NRC emitido por una [Entidad Financiera] puede ser validado autónomamente por [MiPago con las Entidades Financieras] simplemente volviendo a generar la misma firma; si la firma generada por la [Pasarela con las Entidades Financieras] y la emitida por la [Entidad Financiera] coinciden, se puede asegurar que la liquidación ha sido efectivamente pagada.



Como solución [KutxaBank] y [MiPago] desarrollaron un servicio que hace de **intermediario** entre la [MiPago] y el [TPV Virtual] de [RedSys] y que **asocia los ID de transacción del [TPV virtual] con los cuadernillos bancarios utilizados por las [administraciones]**, generando además un NRC para cada operación



El esquema general es:



Es importante recordar dos aspectos de la solución:

Manejo de números de tarjeta	Una de las premisas de [MiPago] es que <i>-por razones de seguridad-</i> , en ningún caso la Administración (MiPago) debe conocer los números de tarjeta con los que se hacen las operaciones
Comisiones	En el [pago web en Entidades Financieras colaboradoras] "normal", NO hay comisiones para las [Administraciones] puesto que el pago se hace directamente en la [Entidad Emisora] con uno de sus clientes (<i>es de alguna manera asimilable a una transferencia</i>) ... sin embargo, el uso de un [TPV Virtual] implica una comisión para la [Administración] si la tarjeta NO pertenece a la [Entidad Financiera] que proporciona el servicio de TPV. Esta comisión se repercute a la Administración

Esta solución de **recubrimiento de [TPV Virtual] proporcionada por [KutxaBank]** ha venido dando servicio a la perfección durante los últimos 10 años, sin embargo, plantea **problemas de usabilidad**, sobre todo en el caso de **pagos recurrentes utilizando el móvil** (*aunque también la web*).

Para realizar el pago utilizando la funcionalidad de [pago con tarjeta de otras entidades], el usuario/a debe introducir [dígitos de la tarjeta] + [fecha de caducidad] + [CVV] + OTP (*ej SMS*)

... en especial en el caso de pagos recurrentes (*ej: recargas de tarjetas de transporte, pago de tasas de aparcamiento, tickets del comedor, etc*), la necesidad de **teclear** los dígitos de la [tarjeta de pago] + CVV en el móvil hacen el sistema **poco usable**

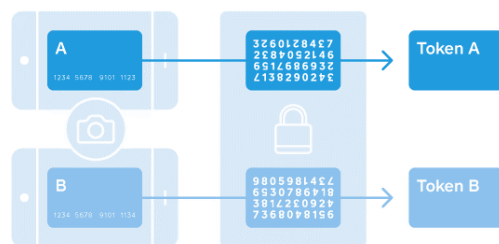
Además, las nuevas normativas de **[pago seguro]** que se están poniendo en práctica exigen que:

- Si el pago se hace en **internet**, se han de utilizar mecanismos adicionales de identificación del usuario/a: **dobles factores de identificación** basado en el [número de tarjeta] + [envío de un código de un solo uso al móvil del usuario/a] (OTP=*One Time Password*)
- Si el pago se hace utilizando **lectura de tarjeta**, este se ha de hacer en base a la **lectura del chip EMV / NFC** (*y no de la banda magnética*) cumpliendo una estricta normativa de seguridad en cuanto a protocolos de comunicación como a arquitectura de la solución técnica.

La **solución** al problema de usabilidad expuesto es **evitar la necesidad de que el ciudadano/a deba teclear** [número de tarjeta] + [fecha de caducidad] + [CVV] tanto en la web como en el móvil, para ello se utiliza la solución de **[pago tokenizado]** de [RedSys] adaptada a las necesidades de las [Administraciones]

La [tokenización] permite proteger datos sensibles reemplazándolos por un número generado mediante un algoritmo (*el [token]*)

En el caso de las [tarjetas de pago], el [número de tarjeta] es sustituido por un [token] que puede ser enviado SIN que se expongan datos sensibles (*el número de tarjeta*)



El objetivo final de la [tokenización] es **evitar que se pueda duplicar la información de la [tarjeta de pago] en otra [tarjeta]**

(*si alguien consigue el token NO puede obtener datos de la tarjeta a partir del mismo*)

Ejemplos de [tokenización]

Apple pay /
Google pay

1. El usuario/a saca una foto de su [tarjeta de pago] desde su móvil o teclea sus datos (*número + fecha de caducidad + cvv*)
2. Los datos de la [tarjeta de pago] se envían al emisor de la misma que devuelve un [token] en su lugar (*los datos de la tarjeta ya NO son necesarios en el móvil y se pueden descartar*)
3. El [token] se almacena en el móvil y a partir de ese momento puede ser utilizado para pagar en lugar de la tarjeta

En grandes líneas, el sistema funciona de la siguiente manera:

- Un proveedor de servicios TPV (RedSys) emite un **[token]** asociado a la [tarjeta de pago] que puede ser **utilizado en múltiples transacciones** para identificar la [tarjeta] a la que *cargar* la transacción
- El [token] **se almacena encriptado en un [wallet]** habitualmente en el móvil y **NO se puede acceder al mismo a no ser que se el usuario/a introduzca un password o se haga una lectura biométrica** (ej: *huella o reconocimiento facial*)
Si se pierde la clave que da acceso al [wallet], el [token] NO puede ser recuperado y ha de emitirse otro
- Cuando el usuario/a paga una [liquidación], **presenta el [token] en lugar de** [número de tarjeta] + [caducidad] + [CVV]

Este sistema tiene evidentes **ventajas** frente al uso de la [tarjeta]

- Se pueden asociar tantos [token] como se quiera a la misma [tarjeta de pago]
- Si el [token] se compromete basta con **revocarlo** y emitir otro (*en el caso de una [tarjeta de pago] habría que emitir otra tarjeta con las complicaciones que eso conlleva*)
- En caso de que alguien tenga acceso al [token] a pesar de que podría utilizarlo para pagar, NO podría obtener los datos de la [tarjeta de pago] a la que está asociado así que **NO podría duplicar** esta [tarjeta de pago]

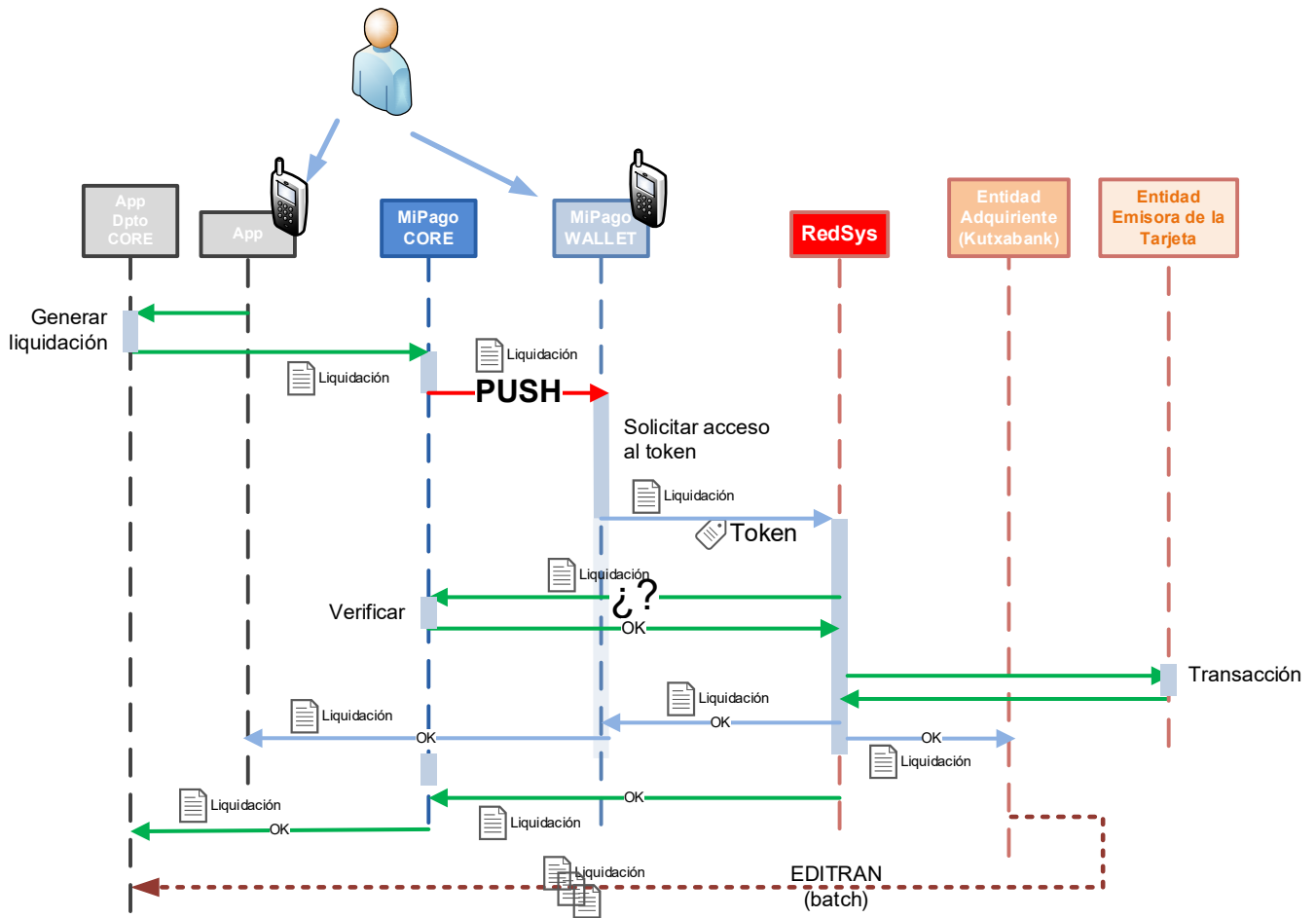
En el caso concreto del problema de [usabilidad] del [pago con tarjeta de otras entidades] se ha creado una [app móvil] (**MiPago Wallet**) que:

- Actúa de **[wallet]** de [tokens] emitidos para ser utilizados exclusivamente en pagos recurrentes de las [Administraciones Públicas Vascas] (*el [token] emitido NO podría ser utilizado para otro tipo de pagos*)
- **Interopera** con los servicios de:
 - [MiPago]
 - La [Entidad Financiera] que proporciona el intermediario con el [TPV Virtual] (Kutxabank) utilizando los mensajes que se basen en los estándares que utilizan las [Administraciones] (AEB57 / 60) de forma que se reutiliza el esquema de funcionamiento del [pago con tarjeta de otras entidades]:
 - Se conservan los datos de las [liquidaciones] (AEB57 / 60) extremo a extremo
 - Se puede incorporar en cualquier aplicación de negocio sin cambios respecto del uso de cualquier otro medio de pago (*[pago web en entidades financieras colaboradoras] o [pago con tarjeta de otras entidades]*)

A continuación, se describen DOS casos de uso del sistema:

- Un pago en la [web]
- Un pago desde una aplicación móvil (*ej: recarga de una [tarjeta de transporte]*)

Escenario 1: Pago web



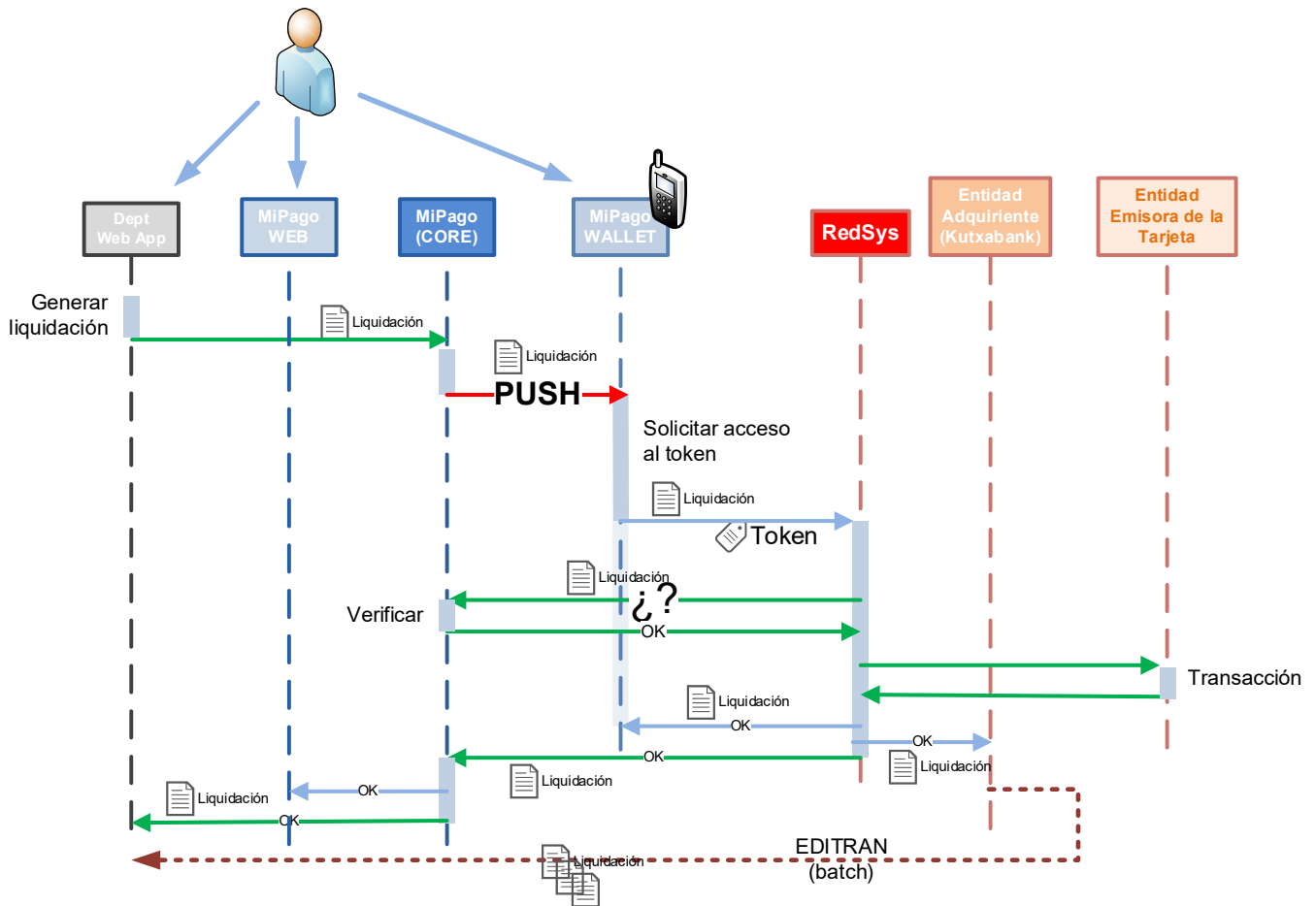
1. El usuario/a utiliza una aplicación web de una [Administración] y genera una [liquidación]
2. La [liquidación] se inicializa en [MiPago]
3. El usuario accede a la interfaz web de [MiPago] y selección [MiPago Wallet]
4. El servidor de [MiPago] hace un **PUSH** a la [app MiPago Wallet] en el móvil del usuario/a **enviándole los datos de la [liquidación]**
5. La app móvil [MiPago Wallet] se activa solicitando **autorización** para el pago (*y mostrando todos los detalles del mismo*)
6. La app [MiPago Wallet] envía la [petición de pago] al proveedor del servicio de [pago por token] (*RedSys*)
7. El servidor del servicio de [pago por token] (*RedSys*)
 - a. **Consulta** al servidor de [MiPago] para asegurarse de que se trata de una [petición de pago] legítima
 - b. **Ejecuta la transacción** contactando con el [emisor de la tarjeta]
 - c. La *respuesta* de la transacción se devuelve
 - A la [Entidad Financiera Adquiriente] del servicio [TPV] (*Kutxabank en el caso de [MiPago]*)
 - Al servidor de [MiPago] (*como cualquier pago*) -*quien a su vez informa on-line a los servidores de la [administración]*-
 - A la app [MiPago Wallet] (*que es quien inició la transacción*)
8. [MiPago Wallet] indica al usuario/a el resultado de la transacción

La página web del PC durante todo este proceso ha estado *esperando* haciendo *pooling* a [MiPago] (*preguntando de cuando en cuando*) por la finalización de la transacción.

Cuando esta finaliza, a su vez, también muestra al usuario/a el resultado de la misma

Escenario 1: Pago móvil

(el escenario es **idéntico** al anterior con la única diferencia de que todo se desarrolla en el móvil)



1. El usuario/a utiliza una app móvil de una [Administración] y genera una [liquidación]
2. La [liquidación] se inicializa en [MiPago]
3. El servidor de [MiPago] hace un **PUSH** a la [app MiPago Wallet] en el móvil del usuario/a **enviándole los datos de la [liquidación]**
4. La app móvil [MiPago Wallet] se activa solicitando **autorización** para el pago (*y mostrando todos los detalles del mismo*)
9. El servidor del servicio de [pago por token] (*RedSys*)
 - a. **Consulta** al servidor de [MiPago] para asegurarse de que se trata de una [petición de pago] legítima
 - b. **Ejecuta la transacción** contactando con el emisor de la tarjeta o haciendo las operativas internas que sean necesarias
 - c. La *respuesta* de la transacción se devuelve
 - Al servidor de [MiPago] (*como cualquier pago*) -quien a su vez informa on-line a los servidores de la [administración]-
 - A la app [MiPago Wallet] (*que es quien inició la transacción*)

[MiPago Wallet] indica al usuario/a el resultado de la transacción (*devuelve el resultado a al app que inició el proceso*)